



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

Americas Headquarters

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

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 NON-INFRINGEMENT 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.

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.

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: <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)

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Configuring OSPF 1

- Finding Feature Information 1
- Information About OSPF 2
 - Cisco OSPF Implementation 2
 - Router Coordination for OSPF 2
 - Route Distribution for OSPF 2
 - OSPF Network Type 3
 - Area Parameters 4
 - Original LSA Behavior 7
 - LSA Group Pacing with Multiple Timers 7
- How to Configure OSPF 9
 - Enabling OSPF 9
 - Configuring OSPF Interface Parameters 10
 - Configuring OSPF over Different Physical Networks 12
 - Configuring OSPF for Point-to-Multipoint Broadcast Networks 12
 - Configuring OSPF for Nonbroadcast Networks 14
 - Configuring OSPF Area Parameters 15
 - Configuring OSPFv2 NSSA 16
 - Configuring an OSPFv2 NSSA Area and Its Parameters 16
 - Configuring an NSSA ABR as a Forced NSSA LSA Translator 18
 - Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility 19
 - Configuring OSPF NSSA Parameters 20
 - Prerequisites 20
 - Configuring Route Summarization Between OSPF Areas 21
 - Configuring Route Summarization When Redistributing Routes into OSPF 21
 - Establishing Virtual Links 21
 - Generating a Default Route 22
 - Configuring Lookup of DNS Names 23

Forcing the Router ID Choice with a Loopback Interface	23
Controlling Default Metrics	24
Changing the OSPF Administrative Distances	25
Configuring OSPF on Simplex Ethernet Interfaces	26
Configuring Route Calculation Timers	26
Configuring OSPF over On-Demand Circuits	27
Prerequisites	28
Logging Neighbors Going Up or Down	29
Changing the LSA Group Pacing Interval	30
Blocking OSPF LSA Flooding	31
Reducing LSA Flooding	31
Ignoring MOSPF LSA Packets	31
Monitoring and Maintaining OSPF	32
Displaying OSPF Update Packet Pacing	34
Restrictions for OSPF	35
Configuration Examples for OSPF	35
Example: OSPF Point-to-Multipoint	35
Example: OSPF Point-to-Multipoint with Broadcast	36
Example: OSPF Point-to-Multipoint with Nonbroadcast	37
Example: Variable-Length Subnet Masks	38
Example: Configuring OSPF NSSA	38
Example: OSPF NSSA Area with RFC 3101 Disabled and RFC 1587 Active	40
Example: OSPF Routing and Route Redistribution	42
Example: Basic OSPF Configuration	42
Example: Basic OSPF Configuration for Internal Router ABR and ASBRs	42
Example: Complex Internal Router with ABR and ASBR	44
Example: Complex OSPF Configuration for ABR	46
Examples: Route Map	47
Example: Changing the OSPF Administrative Distances	50
Example: OSPF over On-Demand Routing	51
Example: LSA Group Pacing	52
Example: Blocking OSPF LSA Flooding	52
Example: Ignoring MOSPF LSA Packets	52
Additional References for OSPF Not-So-Stubby Areas (NSSA)	52
Feature Information for Configuring OSPF	53

CHAPTER 2**Configuring OSPF TTL Security Check and OSPF Graceful Shutdown 55**

- Finding Feature Information 55
- Information About OSPF TTL Security Check and OSPF Graceful Shutdown 56
 - TTL Security Check for OSPF 56
 - Transitioning Existing Networks to Use TTL Security Check 56
 - TTL Security Check for OSPF Virtual and Sham Links 56
 - Benefits of the OSPF Support for TTL Security Check 56
 - OSPF Graceful Shutdown 57
- How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown 57
 - Configuring TTL Security Check on All OSPF Interfaces 57
 - Configuring TTL Security Check on a Per-Interface Basis 58
 - Configuring OSPF Graceful Shutdown on a Per-Interface Basis 60
- Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown 61
 - Example: Transitioning an Existing Network to Use TTL Security Check 61
- Additional References 62
- Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown 63

CHAPTER 3**Enabling OSPFv2 on an Interface Basis 67**

- Finding Feature Information 67
- Prerequisites for Enabling OSPFv2 on an Interface Basis 67
- Restrictions on Enabling OSPFv2 on an Interface Basis 68
- Information About Enabling OSPFv2 on an Interface Basis 68
 - Benefits of Enabling OSPFv2 on an Interface Basis 68
 - Implications of Configuring OSPFv2 On a Router Basis or an Interface Basis 68
- How to Enable OSPFv2 on an Interface Basis 69
 - Enabling OSPFv2 on an Interface 69
- Configuration Example for Enabling OSPFv2 on an Interface 70
 - Example Enabling OSPFv2 on an Interface 70
- Additional References 71
- Feature Information for Enabling OSPFv2 on an Interface Basis 72

CHAPTER 4**OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3 75**

- Finding Feature Information 75

Prerequisites for OSPF Enhanced Traffic Statistics	76
Information About OSPF Enhanced Traffic Statistics	76
How to Display and Clear OSPF Enhanced Traffic Statistics	76
Displaying and Clearing OSPF Traffic Statistics for OSPFv2	76
Displaying and Clearing OSPF Traffic Statistics for OSPFv3	77
Configuration Examples for OSPF Enhanced Traffic Commands	78
Displaying and Clearing Enhanced Traffic Statistics for OSPFv2 Example	78
Displaying and Clearing Enhanced Traffic Statistics for OSPFv3 Example	80
Additional References	81
Feature Information for OSPF Enhanced Traffic Statistics	83

CHAPTER 5

OSPF SNMP ifIndex Value for Interface ID in Data Fields	85
Finding Feature Information	85
Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields	86
Information About SNMP ifIndex Value for Interface ID in Data Fields	86
Benefits of Choosing to Identify Interfaces by the SNMP MIB-II ifIndex Value	86
How OSPFv2 and OSPFv3 Use the SNMP MIB-II ifIndex Value	86
How to Configure SNMP ifIndex Value for Interface ID in Data Fields	87
Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers	87
Configuration Examples for SNMP ifIndex Value for Interface ID in Data Fields	88
Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2	88
Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3	89
Additional References	92
Feature Information for OSPF SNMP ifIndex Value for Interface ID	93

CHAPTER 6

OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements	95
Finding Feature Information	95
Prerequisites for Excluding Connected IP Prefixes from LSAs	96
Information About Excluding Connected IP Prefixes from LSAs	96
Previous Methods to Limit the Number of IP Prefixes Carried in LSAs	96
Feature Overview	96
How to Exclude Connected IP Prefixes from OSPF LSAs	97
Excluding IP Prefixes per OSPF Process	97
Excluding IP Prefixes on a Per-Interface Basis	99
Troubleshooting IP Prefix Suppression	100

Configuration Examples for Excluding Connected IP Prefixes from LSAs	102
Excluding IP Prefixes from LSAs for an OSPF Process Example	102
Excluding IP Prefixes from LSAs for a Specified Interface Example	102
Additional References	103
Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements	104
Glossary	105

CHAPTER 7**OSPFv2 Local RIB 107**

Finding Feature Information	107
Prerequisites for OSPFv2 Local RIB	108
Restrictions for OSPFv2 Local RIB	108
Information About OSPFv2 Local RIB	108
How to Configure OSPFv2 Local RIB	108
Changing the Default Local RIB Criteria	109
Changing the Administrative Distance for Discard Routes	110
Troubleshooting Tips	112
Configuration Examples for OSPFv2 Local RIB	112
Example: Changing the Default Local RIB Criteria	112
Example: Changing the Administrative Distance for Discard Routes	112
Additional References	113
Feature Information for OSPFv2 Local RIB	114

CHAPTER 8**IPv6 Routing: OSPFv3 117**

Finding Feature Information	117
Prerequisites for IPv6 Routing: OSPFv3	117
Restrictions for IPv6 Routing: OSPFv3	118
Information About IPv6 Routing: OSPFv3	118
How OSPFv3 Works	118
Comparison of OSPFv3 and OSPF Version 2	118
LSA Types for OSPFv3	119
NBMA in OSPFv3	120
Load Balancing in OSPFv3	120
Addresses Imported into OSPFv3	120
OSPFv3 Customization	121

OSPFv3 Cost Calculation	121
Force SPF in OSPFv3	123
How to Configure Load Balancing in OSPFv3	123
Configuring the OSPFv3 Device Process	123
Configuring NBMA Interfaces in OSPFv3	126
Forcing an SPF Calculation	128
Verifying OSPFv3 Configuration and Operation	129
Configuration Examples for Load Balancing in OSPFv3	132
Example: Configuring the OSPFv3 Device Process	132
Example: Configuring NBMA Interfaces	132
Example: Forcing SPF Configuration	133
Additional References	133
Feature Information for IPv6 Routing: OSPFv3	134

CHAPTER 9**OSPFv3 Authentication Trailer 135**

Finding Feature Information	135
Information About OSPFv3 Authentication Trailer	135
Overview of OSPFv3 Authentication Trailer	135
How to Configure OSPFv3 Authentication Trailer	137
Configuring OSPFv3 Authentication Trailer	137
Configuration Examples for OSPFv3 Authentication Trailer	139
Example: Configuring OSPFv3 Authentication Trailer	139
Example: Verifying OSPFv3 Authentication Trailer	139
Additional References for OSPFv3 Authentication Trailer	140
Feature Information for OSPFv3 Authentication Trailer	141

CHAPTER 10**TTL Security Support for OSPFv3 on IPv6 143**

Finding Feature Information	143
Restrictions for TTL Security Support for OSPFv3 on IPv6	143
Prerequisites for TTL Security Support for OSPFv3 on IPv6	144
Information About TTL Security Support for OSPFv3 on IPv6	144
OSPFv3 TTL Security Support for Virtual and Sham Links	144
How to Configure TTL Security Support for OSPFv3 on IPv6	145
Configuring TTL Security Support on Virtual Links for OSPFv3 on IPv6	145
Configuring TTL Security Support on Sham Links for OSPFv3 on IPv6	146

Configuration Examples for TTL Security Support for OSPFv3 on IPv6	147
Example: TTL Security Support on Virtual Links for OSPFv3 on IPv6	147
Example: TTL Security Support on Sham Links for OSPFv3 on IPv6	148
Additional References	148
Feature Information for TTL Security Support for OSPFv3 on IPv6	149

CHAPTER 11**OSPFv3 Fast Convergence: LSA and SPF Throttling 151**

Finding Feature Information	151
Information About OSPFv3 Fast Convergence: LSA and SPF Throttling	152
Fast Convergence: LSA and SPF Throttling	152
How to Configure OSPFv3 Fast Convergence: LSA and SPF Throttling	152
Tuning LSA and SPF Timers for OSPFv3 Fast Convergence	152
Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence	153
Configuration Examples for OSPFv3 Fast Convergence: LSA and SPF Throttling	155
Example: Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence	155
Additional References	155
Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling	156

CHAPTER 12**OSPF Forwarding Address Suppression in Translated Type-5 LSAs 159**

Finding Feature Information	159
Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs	160
Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs	160
Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs	160
When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs	160
How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs	162
Suppressing OSPF Forwarding Address in Translated Type-5 LSAs	162
Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs	163
Example Suppressing OSPF Forwarding Address in Translated Type-5 LSAs	163
Additional References	163
Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs	164



CHAPTER

1

Configuring OSPF

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

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

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

- [Finding Feature Information, page 1](#)
- [Information About OSPF, page 2](#)
- [How to Configure OSPF, page 9](#)
- [Configuration Examples for OSPF, page 35](#)
- [Additional References for OSPF Not-So-Stubby Areas \(NSSA\), page 52](#)
- [Feature Information for Configuring OSPF, page 53](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About OSPF

Cisco OSPF Implementation

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

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

Router Coordination for OSPF

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

Route Distribution for OSPF

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

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

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

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

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

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

OSPF Network Type

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

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

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

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

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

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

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

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

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

You can specify the following neighbor parameters, as required:

- Priority for a neighboring router
- Nonbroadcast poll interval

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

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

Area Parameters

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

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

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

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



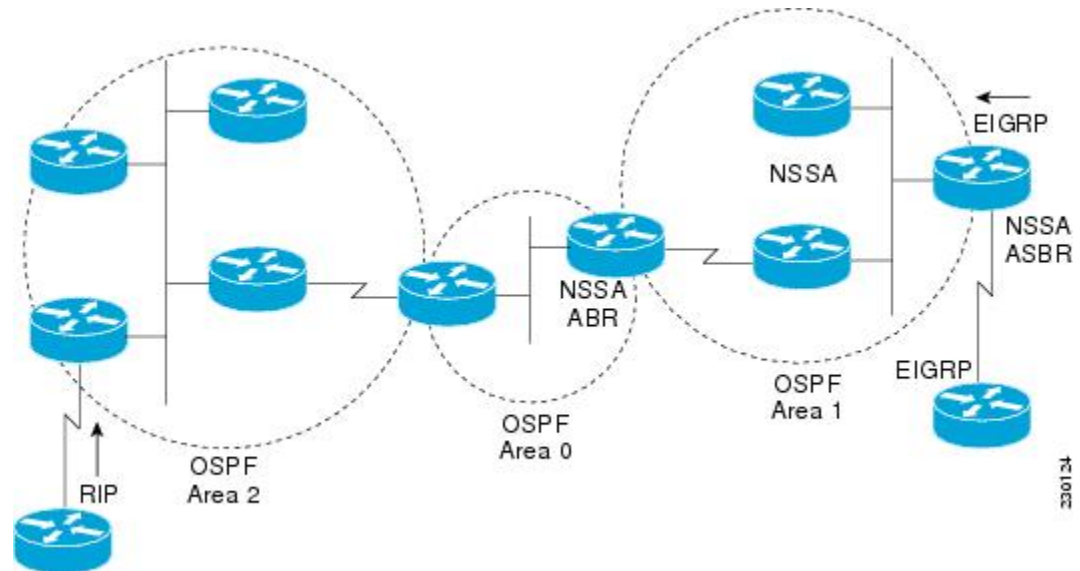
Note

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

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

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

Figure 1: OSPF NSSA



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

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

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

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

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

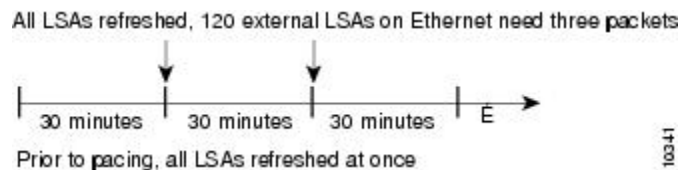
OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

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

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

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



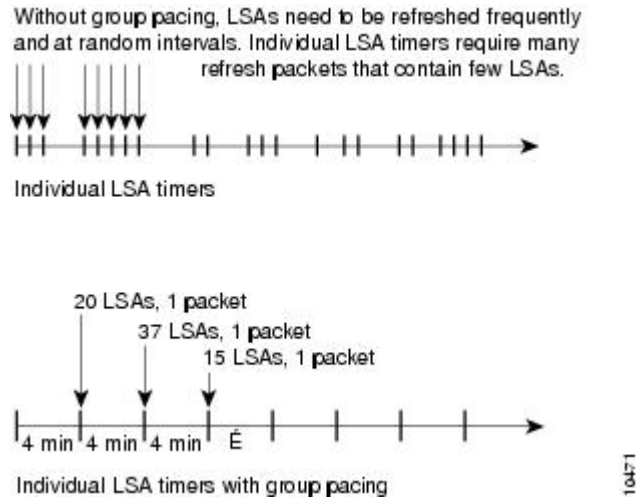
LSA Group Pacing with Multiple Timers

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

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

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

Figure 3: OSPF LSAs on Individual Timers with Group Pacing



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

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

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

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

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

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

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

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

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

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

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

How to Configure OSPF

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

Enabling OSPF

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

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

Configuring OSPF Interface Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ip ospf cost *cost***
5. **ip ospf retransmit-interval *seconds***
6. **ip ospf transmit-delay *seconds***
7. **ip ospf priority *number-value***
8. **ip ospf hello-interval *seconds***
9. **ip ospf dead-interval *seconds***
10. **ip ospf authentication-key *key***
11. **ip ospf message-digest-key *key-id md5 key***
12. **ip ospf authentication [*message-digest* | null]**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip ospf cost <i>cost</i> Example: Device(config-if)# ip ospf cost 65	Explicitly specifies the cost of sending a packet on an OSPF interface.
Step 5	ip ospf retransmit-interval <i>seconds</i> Example: Device(config-if)# ip ospf retransmit-interval 1	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
Step 6	ip ospf transmit-delay <i>seconds</i> Example: Device(config-if)# ip ospf transmit-delay	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
Step 7	ip ospf priority <i>number-value</i> Example: Device(config-if)# ip ospf priority 1	Sets priority to help determine the OSPF designated router for a network.
Step 8	ip ospf hello-interval <i>seconds</i> Example: Device(config-if)# ip ospf hello-interval 1	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.

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

Configuring OSPF over Different Physical Networks

Configuring OSPF for Point-to-Multipoint Broadcast Networks

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring OSPF for Nonbroadcast Networks

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring OSPF Area Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf *process-id***
4. **area *area-id* authentication**
5. **area *area-id* stub [no summary]**
6. **area *area-id* default-cost *cost***
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: <pre>Device(config)# router ospf 10</pre>	Enables OSPF routing and enters router configuration mode.

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

Configuring OSPFv2 NSSA

Configuring an OSPFv2 NSSA Area and Its Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {**metric-value** | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]
5. **network** *ip-address wildcard-mask area area-id*
6. **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]
7. **summary-address** *prefix mask* [**not-advertise**] [**tag** *tag*] [**nssa-only**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 10	Enables OSPF routing and enters router configuration mode. <ul style="list-style-type: none"> • The <i>process-id</i> argument identifies the OSPF process. The range is from 1 to 65535.
Step 4	redistribute <i>protocol</i> [<i>process-id</i>] { level-1 level-1-2 level-2 } [<i>autonomous-system-number</i>] [metric { metric-value transparent }] [metric-type <i>type-value</i>] [match { internal external 1 external 2 }] [tag <i>tag-value</i>] [route-map <i>map-tag</i>] [subnets] [nssa-only] Example: Device(config-router)# redistribute rip subnets	Redistributes routes from one routing domain to another routing domain. <ul style="list-style-type: none"> • In the example, Routing Information Protocol (RIP) subnets are redistributed into the OSPF domain.
Step 5	network <i>ip-address wildcard-mask area area-id</i> Example: Device(config-router)# network 192.168.129.11 0.0.0.255 area 1	Defines the interfaces on which OSPF runs and the area ID for those interfaces.
Step 6	area <i>area-id nssa</i> [no-redistribution] [default-information-originate [metric] [metric-type]] [no-summary] [nssa-only] Example: Device(config-router)# area 1 nssa	Configures a Not-So-Stubby Area (NSSA) area.
Step 7	summary-address <i>prefix mask</i> [not-advertise] [tag <i>tag</i>] [nssa-only] Example: Device(config-router)# summary-address 10.1.0.0	Controls the route summarization and filtering during the translation and limits the summary to NSSA areas.

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

Configuring an NSSA ABR as a Forced NSSA LSA Translator

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 1	Enables OSPF routing and enters router configuration mode. <ul style="list-style-type: none"> • The <i>process-id</i> argument identifies the OSPF process. The range is from 1 to 65535.

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

Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf process-id Example: Device(config)# router ospf 1	Enables OSPF routing and enters router configuration mode. <ul style="list-style-type: none"> • The <i>process-id</i> argument identifies the OSPF process. • Use router ospf process-id command to enable OSPFv2 routing.
Step 4	compatible rfc1587 Example: Device(config-router)# compatible rfc1587	Enables the device to be RFC 1587 compliant.
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF NSSA Parameters

Prerequisites

Evaluate the following considerations before you implement this feature:

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

Configuring Route Summarization Between OSPF Areas

Configuring Route Summarization When Redistributing Routes into OSPF

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>summary-address {ip-address mask prefix mask}</code> <code>[not-advertise][tag tag [nssa-only]</code> Example: Device#(config-router) summary-address 10.1.0.0 255.255.0.0	Specifies an address and mask that covers redistributed routes, so that only one summary route is advertised. <ul style="list-style-type: none"> • You can use the optional not-advertise keyword to filter out a set of routes.

Establishing Virtual Links

SUMMARY STEPS

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

DETAILED STEPS

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

Generating a Default Route

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 109	Enables OSPF routing and enters router configuration mode.
Step 4	default-information originate [always] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-name</i>] Example: Device(config-router)# default-information originate always	Forces the ASBR to generate a default route into the OSPF routing domain. Note The always keyword includes the following exception when a route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Configuring Lookup of DNS Names

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip ospf name-lookup`
4. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip ospf name-lookup Example: Device# ip ospf name-lookup	Enables OSPF routing and enters router configuration mode.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Forcing the Router ID Choice with a Loopback Interface

SUMMARY STEPS

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

DETAILED STEPS

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

Controlling Default Metrics

SUMMARY STEPS

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

DETAILED STEPS

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

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

Changing the OSPF Administrative Distances

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring OSPF on Simplex Ethernet Interfaces

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

Configuring Route Calculation Timers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf process-id**
4. **timers throttle spf spf-start spf-hold spf-max-wait**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 109	Enables OSPF routing and enters router configuration mode.
Step 4	timers throttle spf <i>spf-start spf-hold spf-max-wait</i> Example: Device(config-router)# timers throttle spf 5 1000 9000	Configures route calculation timers.
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF over On-Demand Circuits

SUMMARY STEPS

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

DETAILED STEPS

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

What to Do Next



Note

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

Prerequisites

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

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

Logging Neighbors Going Up or Down

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router ospf process-id`
4. `log-adjacency-changes [detail]`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf process-id Example: Device(config)# router ospf 109	Enables OSPF routing and enters router configuration mode.
Step 4	log-adjacency-changes [detail] Example: Device(config-router)# log-adjacency-changes detail	Changes the group pacing of LSAs. Note Configure the log-adjacency-changes command if you want to know about OSPF neighbors going up or down without turning on the debug ip ospf adjacency EXEC command because the log-adjacency-changes command provides a higher-level view of the peer relationship with less output. Configure the log-adjacency-changes detail command if you want to see messages for each state change.
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Changing the LSA Group Pacing Interval

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf *process-id***
4. **timers pacing lsa-group *seconds***
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 109	Enables OSPF routing and enters router configuration mode.
Step 4	timers pacing lsa-group <i>seconds</i> Example: Device(config-router)# timers pacing lsa-group 60	Changes the group pacing of LSAs.
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Blocking OSPF LSA Flooding

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

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

Command	Purpose
<code>neighbor <i>ip-address</i> database-filter all out</code>	Blocks the flooding of OSPF LSA packets to the specified neighbor.

Reducing LSA Flooding

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

Ignoring MOSPF LSA Packets

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

Monitoring and Maintaining OSPF

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

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

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

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

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

Displaying OSPF Update Packet Pacing

SUMMARY STEPS

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

DETAILED STEPS

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

Restrictions for OSPF

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

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

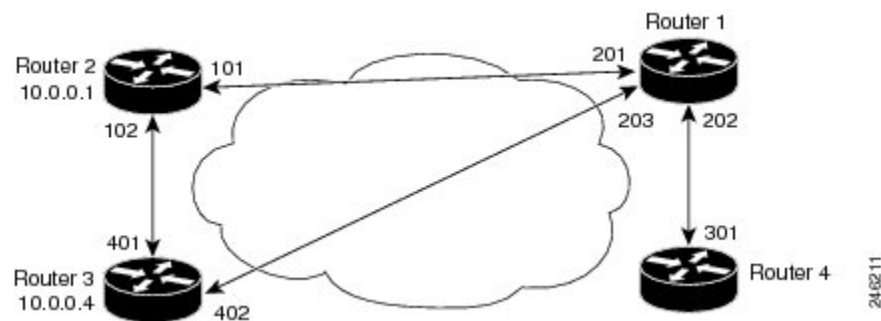
Because the maximum size of an IP packet is 65,535 bytes, there is still an upper bound on the number of links possible on a router.

Configuration Examples for OSPF

Example: OSPF Point-to-Multipoint

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

Figure 4: OSPF Point-to-Multipoint Example



Router 1 Configuration

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

Router 2 Configuration

```

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

```

Router 3 Configuration

```

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

```

Router 4 Configuration

```

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

```

Example: OSPF Point-to-Multipoint with Broadcast

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

```

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

```

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

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

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

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

The route information in the first configuration is as follows:

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

Example: OSPF Point-to-Multipoint with Nonbroadcast

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

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

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

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

```

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

```

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

```
Device# show ip ospf neighbor
```

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

Example: Variable-Length Subnet Masks

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

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

```

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

```

Example: Configuring OSPF NSSA

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

Device 1

```

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

```



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

Device 2

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

Device 3

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

Device 4

```

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

```

Device 5

```

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

```

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

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

```
Device# show ip ospf
```

```

Routing Process "ospf 1" with ID 10.0.2.1
Start time: 00:00:25.512, Time elapsed: 00:01:02.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec

```

```

LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 0 normal 0 stub 1 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area 1
Number of interfaces in this area is 1
It is a NSSA area
Configured to translate Type-7 LSAs, inactive (RFC3101 support
disabled)
Area has no authentication
SPF algorithm last executed 00:00:07.160 ago
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x0245F0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
    
```

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

Table 1: show ip ospf Field Descriptions

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

Device2# **show ip ospf database nssa**

```

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

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

Table 2: show ip ospf database nssa Field Descriptions

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

Example: OSPF Routing and Route Redistribution

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

Three types of examples follow:

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

Example: Basic OSPF Configuration

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

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 9000
 network 10.93.0.0 0.0.0.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 10.94.0.0
 redistribute ospf 9000
 default-metric 1
```

Example: Basic OSPF Configuration for Internal Router ABR and ASBRs

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

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

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

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

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

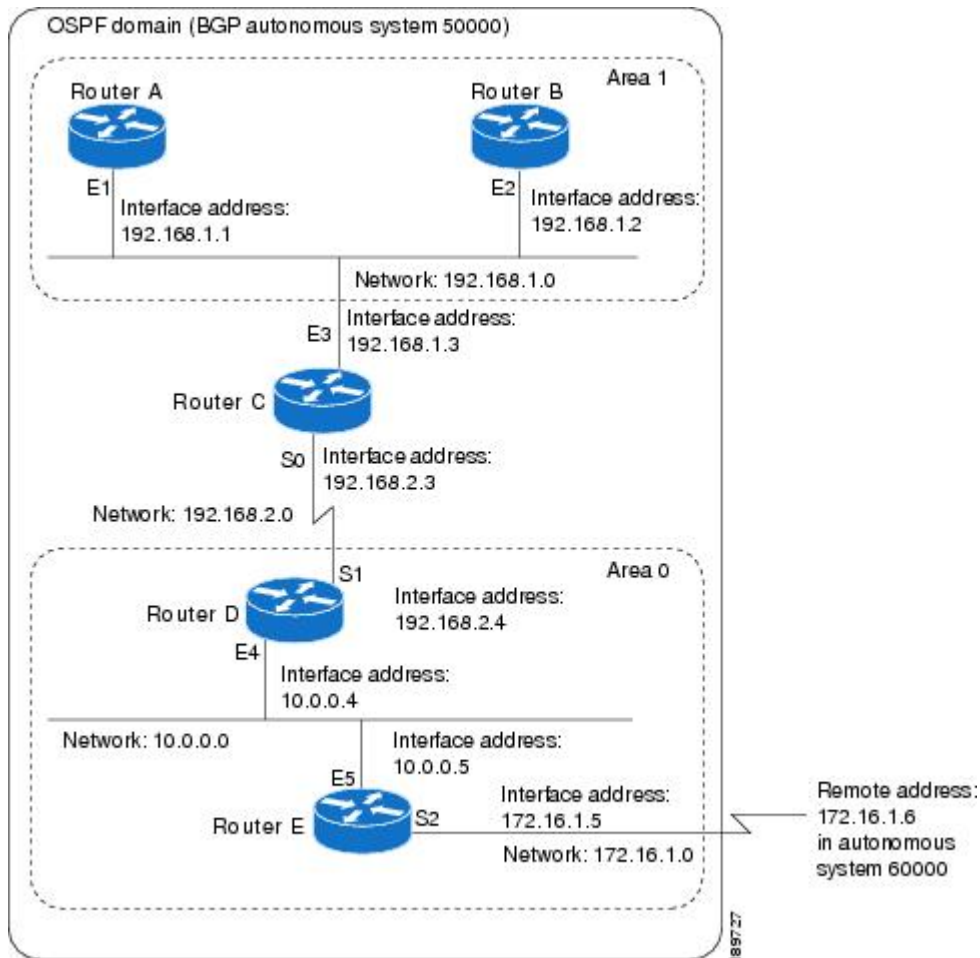
The second **network area** command is evaluated next. For area 2, the same process is then applied to all interfaces (except Ethernet interface 0). Assume that a match is determined for Ethernet interface 1. OSPF is then enabled for that interface, and Ethernet interface 1 is attached to area 2.

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

Example: Complex Internal Router with ABR and ASBR

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

Figure 5: Sample OSPF Autonomous System Network Map



In this configuration, five routers are configured with OSPF:

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

**Note**

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

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

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

Router A Configuration—Internal Router

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

Router B Configuration—Internal Router

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

Router C Configuration—ABR

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

Router D Configuration—Internal Router

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

Router E Configuration—ASBR

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

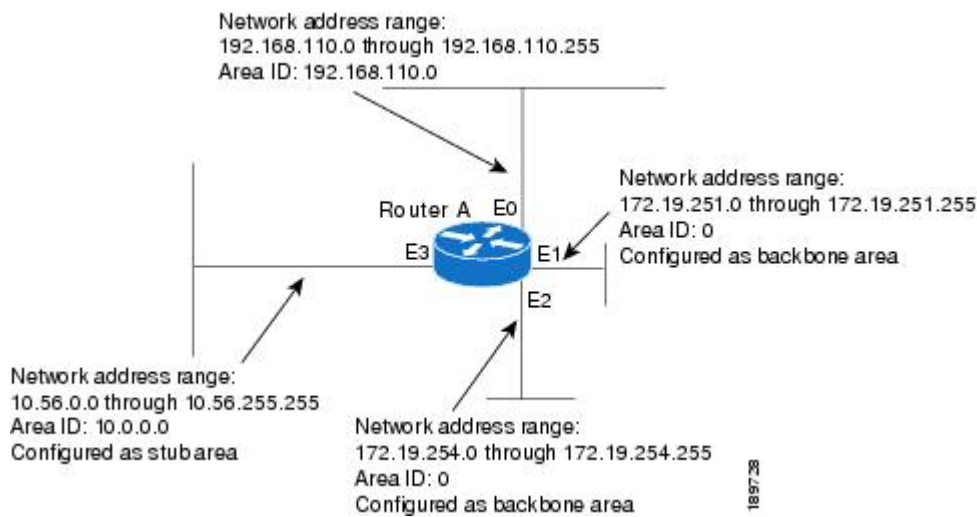
Example: Complex OSPF Configuration for ABR

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

- Basic OSPF configuration
- Route redistribution

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

Figure 6: Interface and Area Specifications for OSPF Sample Configuration



The basic configuration tasks in this example are as follows:

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

Configuration tasks associated with redistribution are as follows:

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

The following is a sample OSPF configuration:

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

In the following configuration, OSPF is on network 172.16.0.0:

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

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

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

Examples: Route Map

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

The following example redistributes all OSPF routes into IGRP:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Note**

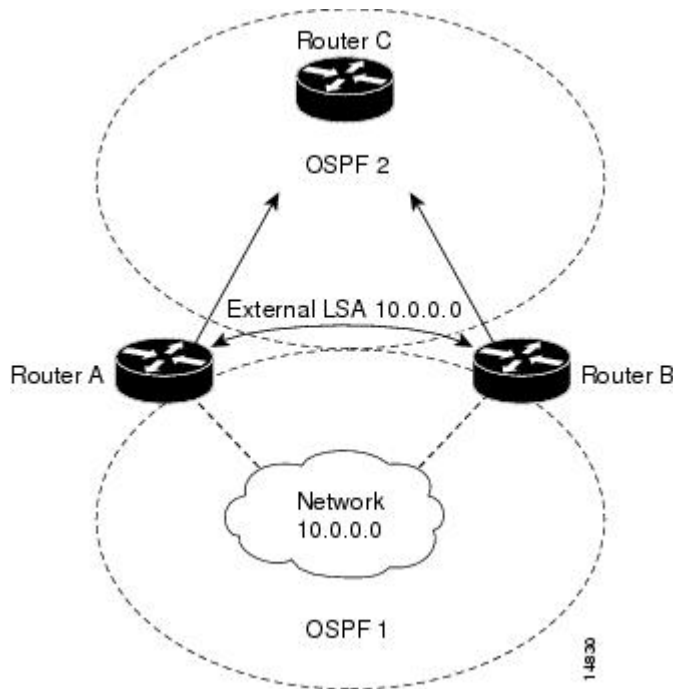
Only routes external to the OSPF process can be used for tracking, such as non-OSPF routes or OSPF routes from a separate OSPF process.

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

Example: Changing the OSPF Administrative Distances

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

Figure 7: OSPF Administrative Distance



Router A Configuration

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

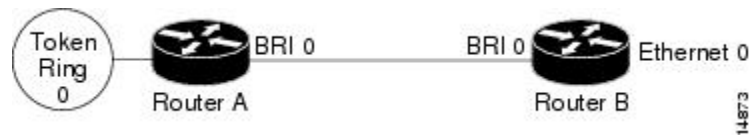
Router B Configuration

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

Example: OSPF over On-Demand Routing

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

Figure 8: OSPF over On-Demand Circuit



Router A Configuration

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

Router B Configuration

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

```

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

```

Example: LSA Group Pacing

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

```

router ospf
 timers pacing lsa-group 60

```

Example: Blocking OSPF LSA Flooding

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

```

interface ethernet 0
 ip ospf database-filter all out

```

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

```

router ospf 109
 neighbor 10.10.10.45 database-filter all out

```

Example: Ignoring MOSPF LSA Packets

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

```

router ospf 109
 ignore lsa mospf

```

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

Related Documents

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

RFCs

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

Technical Assistance

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

Feature Information for Configuring OSPF

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

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

Table 3: Feature Information for OSPF

Feature Name	Releases	Feature Information
OSPF	Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.6E	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. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.



Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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

- [Finding Feature Information, page 55](#)
- [Information About OSPF TTL Security Check and OSPF Graceful Shutdown, page 56](#)
- [How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown, page 57](#)
- [Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown, page 61](#)
- [Additional References, page 62](#)
- [Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown, page 63](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About OSPF TTL Security Check and OSPF Graceful Shutdown

TTL Security Check for OSPF

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

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

Transitioning Existing Networks to Use TTL Security Check

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

TTL Security Check for OSPF Virtual and Sham Links

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

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

Benefits of the OSPF Support for TTL Security Check

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

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

OSPF Graceful Shutdown

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

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

How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown

Configuring TTL Security Check on All OSPF Interfaces

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring TTL Security Check on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface <i>type number</i></p> <p>Example:</p> <pre>Device(config)# interface GigabitEthernet 0/0/0</pre>	Configures an interface type and enters interface configuration mode.
Step 4	<p>ip ospf ttl-security [hops <i>hop-count</i> disable]</p> <p>Example:</p> <pre>Device(config-if)# ip ospf ttl-security</pre>	<p>Configures TTL security check feature on a specific interface.</p> <ul style="list-style-type: none"> The <i>hop-count</i> argument range is from 1 to 254. The disable keyword can be used to disable TTL security on an interface. It is useful only if the ttl-security all-interfaces command initially enabled TTL security on all OSPF interfaces, in which case disable can be used as an override or to turn off TTL security on a specific interface. In the example, TTL security is being disabled on GigabitEthernet interface 0/0/0.
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>show ip ospf [<i>process-id</i>] interface [<i>interface type interface-number</i>] [brief] [multicast] [topology <i>topology-name</i> base]</p> <p>Example:</p> <pre>Device# show ip ospf interface gigabitethernet 0/0/0</pre>	(Optional) Displays OSPF-related interface information.
Step 7	<p>show ip ospf neighbor <i>interface-type interface-number</i> [<i>neighbor-id</i>][detail]</p> <p>Example:</p> <pre>Device# show ip ospf neighbor 10.199.199.137</pre>	<p>(Optional) Displays OSPF neighbor information on a per-interface basis.</p> <ul style="list-style-type: none"> If one side of the connection has TTL security enabled, the other side shows the neighbor in the INIT state.

	Command or Action	Purpose
Step 8	show ip ospf [<i>process-id</i>] traffic [<i>interface-type interface-number</i>] Example: Device# show ip ospf traffic	(Optional) Displays OSPF traffic statistics. <ul style="list-style-type: none"> The number of times a TTL security check failed is included in the output.
Step 9	debug ip ospf adj Example: Device# debug ip ospf adj	(Optional) Initiates debugging of OSPF adjacency events. <ul style="list-style-type: none"> Information about dropped packets, including interface type and number, neighbor IP address, and TTL value, is included in the command output.

Configuring OSPF Graceful Shutdown on a Per-Interface Basis

SUMMARY STEPS

- enable
- configure terminal
- interface *type number*
- ip ospf shutdown
- end
- show ip ospf [*process-id*] interface [*interface type interface-number*] [**brief**] [**multicast**] [*topology topology-name* | **base**]
- show ip ospf [*process-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/1/0	Configures an interface type and number and enters interface configuration mode.
Step 4	ip ospf shutdown Example: Device(config-if)# ip ospf shutdown	Initiates an OSPF protocol graceful shutdown at the interface level. <ul style="list-style-type: none"> • When the ip ospf shutdown interface command is entered, the interface on which it is configured sends a link-state update advising its neighbors that is going down, which allows those neighbors to begin routing OSPF traffic around this router.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	show ip ospf [<i>process-id</i>] interface [<i>interface type interface-number</i>] [brief] [multicast] [topology topology-name base }] Example: Device# show ip ospf interface GigabitEthernet 0/1/0	(Optional) Displays OSPF-related interface information.
Step 7	show ip ospf [<i>process-id</i>] Example: Device# show ip ospf	(Optional) Displays general information about OSPF routing processes.

Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

Example: Transitioning an Existing Network to Use TTL Security Check

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

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

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

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

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

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

Table 4: Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

Feature Name	Releases	Feature Information
OSPF Graceful Shutdown	Cisco IOS XE Release 3.3SG Cisco IOS XE Release 3.6E	<p>This feature provides the ability to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away.</p> <p>A graceful shutdown of a protocol can be initiated on all OSPF interfaces or on a specific interface.</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • ip ospf shutdown • show ip ospf • show ip ospf interface • shutdown (router OSPF) <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>

Feature Name	Releases	Feature Information
OSPF TTL Security Check	Cisco IOS XE Release 3.3SG Cisco IOS XE Release 3.6E	<p>This feature increases protection against OSPF denial of service attacks, enables checking of TTL values on OSPF packets from neighbors, and allows users to set TTL values sent to neighbors.</p> <p>The following commands were introduced or modified:</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <ul style="list-style-type: none"> • area sham-link cost • area virtual-link • debug ip ospf adj • ip ospf ttl-security • show ip ospf interface • show ip ospf neighbor • show ip ospf traffic • ttl-security all-interfaces <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



Enabling OSPFv2 on an Interface Basis

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

- [Finding Feature Information, page 67](#)
- [Prerequisites for Enabling OSPFv2 on an Interface Basis, page 67](#)
- [Restrictions on Enabling OSPFv2 on an Interface Basis, page 68](#)
- [Information About Enabling OSPFv2 on an Interface Basis, page 68](#)
- [How to Enable OSPFv2 on an Interface Basis, page 69](#)
- [Configuration Example for Enabling OSPFv2 on an Interface, page 70](#)
- [Additional References, page 71](#)
- [Feature Information for Enabling OSPFv2 on an Interface Basis, page 72](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Enabling OSPFv2 on an Interface Basis

OSPFv2 must be running on your network.

Restrictions on Enabling OSPFv2 on an Interface Basis

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

Information About Enabling OSPFv2 on an Interface Basis

Benefits of Enabling OSPFv2 on an Interface Basis

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

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

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

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

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

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

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

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

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

Interface Is Not Configured by `network area` Command

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

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

Removing an ip ospf area Command

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

New Processes

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

Link-State Advertisements and Shortest Path First

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

How to Enable OSPFv2 on an Interface Basis

Enabling OSPFv2 on an Interface

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Example for Enabling OSPFv2 on an Interface

Example Enabling OSPFv2 on an Interface

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

```
Device(config)# interface GigabitEthernet 0/2/1
Device(config-if)# bandwidth 10000
```



```
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ip ospf hello-interval 1
Device(config-if)# ip ospf 1 area 0
```

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2328	<i>OSPF Version 2</i>

Technical Assistance

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

Feature Information for Enabling OSPFv2 on an Interface Basis

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

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

Table 5: Feature Information for Enabling OSPFv2 on an Interface Basis

Feature Name	Releases	Feature Information
<p>Enabling OSPFv2 on an Interface Basis</p> <p>Note This feature was originally named "Area Command in Interface Mode for OSPFv2."</p>	<p>Cisco IOS XE Release 3.3SG</p> <p>Cisco IOS XE Release 3.6E</p>	<p>This document describes how to enable OSPFv2 on a per-interface basis to simplify the configuration of unnumbered interfaces. The ip ospf area command allows you to enable OSPFv2 explicitly on an interface. The ip ospf area command is an alternative to enabling OSPFv2 through the address of the interface that matches the address range specified by the network area command.</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands are introduced or modified in the feature documented in this module:</p> <ul style="list-style-type: none"> • ip ospf area. <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



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 75](#)
- [Prerequisites for OSPF Enhanced Traffic Statistics, page 76](#)
- [Information About OSPF Enhanced Traffic Statistics, page 76](#)
- [How to Display and Clear OSPF Enhanced Traffic Statistics, page 76](#)
- [Configuration Examples for OSPF Enhanced Traffic Commands, page 78](#)
- [Additional References, page 81](#)
- [Feature Information for OSPF Enhanced Traffic Statistics, page 83](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for OSPF Enhanced Traffic Statistics

OSPFv2 or OSPFv3 must be configured on the router.

Information About OSPF Enhanced Traffic Statistics

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

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

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

How to Display and Clear OSPF Enhanced Traffic Statistics

Displaying and Clearing OSPF Traffic Statistics for OSPFv2

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	show ip ospf [<i>process-id</i>] traffic [<i>interface-type interface-number</i>] Example: Device# show ip ospf traffic	Displays OSPFv2 traffic statistics.
Step 3	clear ip ospf traffic Example: Device# clear ip ospf traffic	Clears OSPFv2 traffic statistics.

Displaying and Clearing OSPF Traffic Statistics for OSPFv3

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ipv6 ospf [<i>process-id</i>] traffic [<i>interface-type interface-number</i>] Example: Device# show ipv6 ospf traffic	Displays OSPFv3 traffic statistics.

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

Configuration Examples for OSPF Enhanced Traffic Commands

Displaying and Clearing Enhanced Traffic Statistics for OSPFv2 Example

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

```

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

```



```

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

```

```

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

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

```

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

```
Device# 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:

```

Device# show ipv6 ospf traffic

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

```

```

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

```

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

```
Device# clear ipv6 ospf traffic
```

Additional References

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

Related Documents

Related Topic	Document Title
OSPF commands	<i>Cisco IOS IP Routing: OSPF Command Reference</i>
OSPF configuration	Configuring OSPF

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
	--

Technical Assistance

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

Feature Information for OSPF Enhanced Traffic Statistics

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

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

Table 6: Feature Information for OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

Feature Name	Releases	Feature Information
OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3	Cisco IOS XE Release 3.3SG Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands were introduced or modified: clear ipv6 ospf traffic, show ip ospf traffic, show ipv6 ospf traffic.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



CHAPTER 5

OSPF SNMP ifIndex Value for Interface ID in Data Fields

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

- [Finding Feature Information, page 85](#)
- [Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields, page 86](#)
- [Information About SNMP ifIndex Value for Interface ID in Data Fields, page 86](#)
- [How to Configure SNMP ifIndex Value for Interface ID in Data Fields, page 87](#)
- [Configuration Examples for SNMP ifIndex Value for Interface ID in Data Fields, page 88](#)
- [Additional References, page 92](#)
- [Feature Information for OSPF SNMP ifIndex Value for Interface ID, page 93](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields

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

Information About SNMP ifIndex Value for Interface ID in Data Fields

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

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

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

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

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

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

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

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

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

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

Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Do one of the following: <ul style="list-style-type: none"> • router ospf <i>process-id</i> [vrf <i>vpn-name</i>] • • ipv6 router ospf <i>process-id</i> 	Configures an OSPFv2 routing process and enters router configuration mode. Configures an OSPFv3 routing process and enters router configuration mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config)# router ospf 4</pre> <p>Example:</p> <p>Example:</p> <pre>Device(config)# ipv6 router ospf 4</pre>	<p>Note If you configure an OSPFv3 routing process, that uses IPv6, you must have already enabled IPv6.</p>
Step 4	<p>interface-id snmp-if-index</p> <p>Example:</p> <pre>Device(config-router)# interface-id snmp-if-index</pre>	Configures OSPF interfaces with the SNMP interface index identification numbers (ifIndex values).
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config-router)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Repeat this task for each OSPF process for which you want the interfaces to use the SNMP MIB-II ifIndex numbers.</p>
Step 6	<p>show snmp mib ifmib ifindex [<i>type number</i>] [detail][free-list]</p> <p>Example:</p> <pre>Device# show snmp mib ifmib ifindex GigabitEthernet 0/0</pre>	Displays SNMP interface index identification numbers (ifIndex values) for all the system interfaces or the specified system interface.

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

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2

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

```
Device# configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# router ospf 1
Device(config-router)# interface-id snmp-if-index
Device(config-router)# ^Z
Device# show ip ospf 1 1 data router self
OSPF Router with ID (172.16.0.1) (Process ID 1)
Router Link States (Area 1)
LS age: 6
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 172.16.0.1
Advertising Router: 172.16.0.1
LS Seq Number: 8000007
Checksum: 0x63AF
Length: 48
Area Border Router
Number of Links: 2
Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 172.17.0.1
(Link Data) Router Interface address: 0.0.0.53
Number of TOS metrics: 0
TOS 0 Metrics: 64
Link connected to: a Stub Network
(Link ID) Network/subnet number: 192.168.0.11
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metrics: 1
Device# show snmp mib ifmib ifindex serial 13/0

Serial13/0: Ifindex = 53

```

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3

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

```

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

```

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

```

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

```

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3

```

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

```

```

LS age: 151
LS Type: Intra-Area-Prefix-LSA
Link State ID: 1006
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x6E24
Length: 44
Referenced LSA Type: 2002
Referenced Link State ID: 6
Referenced Advertising Router: 172.16.0.1
Number of Prefixes: 1
Prefix Address: 2002:0:1::
Prefix Length: 64, Options: None, Metric: 0
Device# show ipv6 ospf database router
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
Router Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 5 (DoNotAge)
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000004
  Checksum: 0xEE5C
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 70
      Neighbor Interface ID: 71
      Neighbor Router ID: 172.16.0.1
  LS age: 162
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000004
  Checksum: 0xCE7C
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 71
      Neighbor Interface ID: 70
      Neighbor Router ID: 10.0.0.1
  Router Link States (Area 1)
  Routing Bit Set on this LSA
  LS age: 176
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000003
  Checksum: 0xC807
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Transit Network
      Link Metric: 10
      Local Interface ID: 6
      Neighbor (DR) Interface ID: 6
      Neighbor (DR) Router ID: 172.16.0.1
  LS age: 175
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000004
  Checksum: 0xBD10
  Length: 40
  Area Border Router

```

```

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

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Protecting TE tunnel interfaces	MPLS Traffic Engineering--Fast Reroute Link and Node Protection section in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>

Standards

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

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • None 	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for OSPF SNMP ifIndex Value for Interface ID

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

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

Table 7: Feature Information for OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields

Feature Name	Releases	Feature Information
OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields	Cisco IOS XE Release 3.3SG Cisco IOS XE Release 3.6E	<p>This allows you to choose either the current interface number or the SNMP ifIndex value for the interface ID in OSPFv2 and OSPFv3 data fields. The advantage to using the SNMP MIB-II ifIndex value is that this number corresponds to the number that the user will see reported by SNMP.</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following command is introduced or modified by the feature documented in this module: interface-id snmp-if-index</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

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

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

- [Finding Feature Information, page 95](#)
- [Prerequisites for Excluding Connected IP Prefixes from LSAs, page 96](#)
- [Information About Excluding Connected IP Prefixes from LSAs, page 96](#)
- [How to Exclude Connected IP Prefixes from OSPF LSAs, page 97](#)
- [Configuration Examples for Excluding Connected IP Prefixes from LSAs, page 102](#)
- [Additional References, page 103](#)
- [Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements, page 104](#)
- [Glossary, page 105](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Excluding Connected IP Prefixes from LSAs

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

Information About Excluding Connected IP Prefixes from LSAs

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

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

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

Feature Overview

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

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

**Note**

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

Globally Suppressing IP Prefix Advertisements per OSPF Process

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

**Note**

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

Suppressing IP Prefix Advertisements on a Per-Interface Basis

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

**Note**

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

How to Exclude Connected IP Prefixes from OSPF LSAs

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

Excluding IP Prefixes per OSPF Process

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> [vrf <i>vpn-name</i>] Example: Device(config)# router ospf 23	Configures an OSPFv2 routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	prefix-suppression Example: Device(config-router)# prefix-suppression	Prevents OSPF from advertising all IP prefixes except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces.
Step 5	end Example: Device(config-router)# end	Returns to privileged EXEC mode.
Step 6	show ip ospf Example: Device# show ip ospf	Displays general information about OSPF routing processes. Note Use this command to verify that IP prefix suppression has been enabled.

Examples

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

```

Device# show ip ospf

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

```

Excluding IP Prefixes on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Device(config)# interface GigabitEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip ospf prefix-suppression [disable] Example: Device(config-if)# ip ospf prefix-suppression	Prevents OSPF from advertising IP prefixes that belong to a specific interface, except those that are associated with secondary IP addresses. Note When you enter the ip ospf prefix suppression command in interface configuration mode, it takes precedence over the prefix-suppression command that is entered in router configuration mode.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	show ip ospf interface	Displays OSPF-related interface information.

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

Examples

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

```
Device# show ip ospf interface

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

Troubleshooting IP Prefix Suppression

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug ip ospf lsa-generation Example: Device# debug ip ospf lsa-generation	Displays informations about each OSPF LSA generated.

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

Examples

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

```

Device# debug ip ospf lsa-generation

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

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

```

Configuration Examples for Excluding Connected IP Prefixes from LSAs

Excluding IP Prefixes from LSAs for an OSPF Process Example

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

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

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

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

Excluding IP Prefixes from LSAs for a Specified Interface Example

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

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


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

```
Device# show ip ospf interface

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

Additional References

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

Related Documents

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

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

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

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

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

Table 8: Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

Feature Name	Releases	Feature Information
OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements	Cisco IOS XE 3.2SE Cisco IOS XE Release 3.6E	<p>The OSPF mechanism to exclude connected IP prefixes from LSA advertisements is deployed in large networks, limiting the number of IP prefixes that are carried in the OSPF LSAs can speed up OSPF convergence.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.</p> <p>No new commands were introduced or modified.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>

Glossary

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

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



OSPFv2 Local RIB

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

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

- [Finding Feature Information, page 107](#)
- [Prerequisites for OSPFv2 Local RIB, page 108](#)
- [Restrictions for OSPFv2 Local RIB, page 108](#)
- [Information About OSPFv2 Local RIB, page 108](#)
- [How to Configure OSPFv2 Local RIB, page 108](#)
- [Configuration Examples for OSPFv2 Local RIB, page 112](#)
- [Additional References, page 113](#)
- [Feature Information for OSPFv2 Local RIB, page 114](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for OSPFv2 Local RIB

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

Restrictions for OSPFv2 Local RIB

This feature is available only for IP Version 4 networks.

Information About OSPFv2 Local RIB

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

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

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

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

How to Configure OSPFv2 Local RIB

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

Changing the Default Local RIB Criteria

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> [vrf <i>vpn-name</i>] Example: Device(config)# router ospf 23	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	local-rib-criteria [forwarding-address] [inter-area-summary] [nssa-translation] Example: Device(config-router)# local-rib-criteria forwarding-address	Specifies that the OSPF local RIB will be used for route validation.
Step 5	end Example: Device(config-router)# end	Returns to privileged EXEC mode.

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

Changing the Administrative Distance for Discard Routes



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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

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

Example

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

```
Device# show ip route 192.168.0.0 255.255.255.0
```

```
Routing entry for 192.168.0.0/24
```

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

```
Routing Descriptor Blocks:
```

```
* directly connected, via Null0
```

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

Troubleshooting Tips

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

Configuration Examples for OSPFv2 Local RIB

Example: Changing the Default Local RIB Criteria

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

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

Example: Changing the Administrative Distance for Discard Routes

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

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

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

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

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

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

Additional References

The following sections provide references related to OSPFv2 Local RIB.

Related Documents

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

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPFv2 Local RIB

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

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

Table 9: Feature Information for the OSPFv2 Local RIB

Feature Name	Releases	Feature Information
OSPFv2 Local RIB	Cisco IOS XE Release 3.3SG Cisco IOS XE Release 3.6E	<p>With the OSPFv2 Local RIB feature, each OSPF protocol instance has its own local Routing Information Base (RIB). The OSPF local RIB serves as the primary state for OSPF SPF route computation. The global RIB is not updated with intermediate results during the SPF. Instead, the global RIB is updated only when routes are added, deleted, or changed, thereby reducing global RIB computation. This reduced update activity may result in fewer dropped packets.</p> <p>This feature is enabled by default and does not need to be configured. This document describes some optional configuration tasks to modify how the global and local RIBs function, although it is recommended to keep the default settings.</p> <p>In Cisco IOS XE Release 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands were introduced or modified: debug ip ospf rib, discard-route, local-rib-criteria, show ip ospf rib.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



IPv6 Routing: OSPFv3

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

- [Finding Feature Information, page 117](#)
- [Prerequisites for IPv6 Routing: OSPFv3, page 117](#)
- [Restrictions for IPv6 Routing: OSPFv3, page 118](#)
- [Information About IPv6 Routing: OSPFv3, page 118](#)
- [How to Configure Load Balancing in OSPFv3, page 123](#)
- [Configuration Examples for Load Balancing in OSPFv3, page 132](#)
- [Additional References, page 133](#)
- [Feature Information for IPv6 Routing: OSPFv3, page 134](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for IPv6 Routing: OSPFv3

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

Restrictions for IPv6 Routing: OSPFv3

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

Information About IPv6 Routing: OSPFv3

How OSPFv3 Works

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

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

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

Comparison of OSPFv3 and OSPF Version 2

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

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

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

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

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

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

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

LSA Types for OSPFv3

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

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

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

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

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

NBMA in OSPFv3

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

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

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

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

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

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

Load Balancing in OSPFv3

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

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

Addresses Imported into OSPFv3

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

OSPFv3 Customization

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



Caution

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

OSPFv3 Cost Calculation

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

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

Figure 9: Overall Link Cost Formula

$$\text{LinkCost} = \text{OC} + \text{BW} \left(\frac{\text{Throughput_weight}}{100} \right) + \text{Resources} \left(\frac{\text{Resources_weight}}{100} \right) + \text{Latency} \left(\frac{\text{Latency_weight}}{100} \right) + \text{L2_factor} \left(\frac{\text{L2_weight}}{100} \right)$$

$$\text{OC} = \left[\frac{\text{ospf_reference_bw}}{(\text{MDR})(1000)} \right] \quad \text{ospf_reference_bw} = 10^8$$

$$\text{BW} = \frac{(65535) \left(100 - \frac{\text{CDR}}{\text{MDR}} (100) \right)}{100}$$

$$\text{Resources} = \frac{(100 - \text{resources})^3 (65535)}{1000000}$$

$$\text{Latency} = \text{latency}$$

$$\text{L2_factor} = \frac{(100 - \text{RLQ})(65535)}{100}$$

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

Table 10: OSPFv3 Cost Calculation Definitions

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

231048

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

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

Table 11: Recommended Value Settings for OSPFv3 Cost Metrics

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

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

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

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

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

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

Force SPF in OSPFv3

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

How to Configure Load Balancing in OSPFv3

Configuring the OSPFv3 Device Process

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospfv3 [<i>process-id</i>] Example: Device(config)# router ospfv3 1	Enters router configuration mode for the IPv4 or IPv6 address family.
Step 4	area <i>area-ID</i> [default-cost nssa stub] Example: Device(config-router)# area 1	Configures the OSPFv3 area.

	Command or Action	Purpose
Step 5	auto-cost reference-bandwidth <i>Mbps</i> Example: <pre>Device(config-router)# auto-cost reference-bandwidth 1000</pre>	Controls the reference value OSPFv3 uses when calculating metrics for interfaces in an IPv4 OSPFv3 process.
Step 6	default { <i>area area-ID</i> [<i>range ipv6-prefix</i> virtual-link router-id]} [default-information originate [<i>always</i> metric metric-type route-map] distance distribute-list prefix-list prefix-list-name { <i>in</i> <i>out</i> } [<i>interface</i>] maximum-paths paths redistribute protocol summary-prefix ipv6-prefix] Example: <pre>Device(config-router)# default area 1</pre>	Returns an OSPFv3 parameter to its default value.
Step 7	ignore lsa mospf Example: <pre>Device(config-router)# ignore lsa mospf</pre>	Suppresses the sending of syslog messages when the device receives LSA Type 6 multicast OSPFv3 packets, which are unsupported.
Step 8	interface-id snmp-if-index Example: <pre>Device(config-router)# interface-id snmp-if-index</pre>	Configures OSPFv3 interfaces with Simple Network Management Protocol (SNMP) MIB-II interface Index (ifIndex) identification numbers in IPv4 and IPv6.
Step 9	log-adjacency-changes [detail] Example: <pre>Device(config-router)# log-adjacency-changes</pre>	Configures the device to send a syslog message when an OSPFv3 neighbor goes up or down.
Step 10	passive-interface [default <i>interface-type interface-number</i>] Example: <pre>Device(config-router)# passive-interface default</pre>	Suppresses sending routing updates on an interface when an IPv4 OSPFv3 process is used.
Step 11	queue-depth { <i>hello</i> update } { <i>queue-size</i> unlimited } Example: <pre>Device(config-router)# queue-depth update 1500</pre>	Configures the number of incoming packets that the IPv4 OSPFv3 process can keep in its queue.

	Command or Action	Purpose
Step 12	router-id <i>router-id</i> Example: Device(config-router)# router-id 10.1.1.1	Enter this command to use a fixed router ID.

Configuring NBMA Interfaces in OSPFv3

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

Before You Begin

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

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



Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no switchport**
5. **ipv6 enable**
6. **ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

DETAILED STEPS

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

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface type number</p> <p>Example:</p> <pre>Device(config)# interface GigabitEthernet 0/0</pre>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	<p>no switchport</p> <p>Example:</p> <pre>Device (config-if)# no switchport</pre>	Moves an interface into Layer 3 mode.
Step 5	<p>ipv6 enable</p> <p>Example:</p> <pre>Device (config-if)#ipv6 enable</pre>	Enables ipv6 on an interface.
Step 6	<p>ipv6 ospf neighbor ipv6-address [priority number] [poll-interval seconds] [cost number] [database-filter all out]</p> <p>Example:</p> <pre>Device(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01</pre>	Configures an OSPFv3 neighboring device.

Forcing an SPF Calculation

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear ospfv3 [<i>process-id</i>] force-spf Example: Device# clear ospfv3 1 force-spf	Runs SPF calculations for an OSPFv3 process. <ul style="list-style-type: none"> • If the clear ospfv3 force-spf command is configured, it overwrites the clear ipv6 ospf configuration. • Once the clear ospfv3 force-spf command has been used, the clear ipv6 ospf command cannot be used.
Step 3	clear ospfv3 [<i>process-id</i>] process Example: Device# clear ospfv3 2 process	Resets an OSPFv3 process. <ul style="list-style-type: none"> • If the clear ospfv3 force-spf command is configured, it overwrites the clear ipv6 ospf configuration. • Once the clear ospfv3 force-spf command has been used, the clear ipv6 ospf command cannot be used.
Step 4	clear ospfv3 [<i>process-id</i>] redistribution Example: Device# clear ospfv3 redistribution	Clears OSPFv3 route redistribution. <ul style="list-style-type: none"> • If the clear ospfv3 force-spf command is configured, it overwrites the clear ipv6 ospf configuration. • Once the clear ospfv3 force-spf command has been used, the clear ipv6 ospf command cannot be used.
Step 5	clear ipv6 ospf [<i>process-id</i>] { process force-spf redistribution } Example: Device# clear ipv6 ospf force-spf	Clears the OSPFv3 state based on the OSPFv3 routing process ID, and forces the start of the SPF algorithm. <ul style="list-style-type: none"> • If the clear ospfv3 force-spf command is configured, it overwrites the clear ipv6 ospf configuration.

	Command or Action	Purpose
		<ul style="list-style-type: none"> Once the clear ospfv3 force-spf command has been used, the clear ipv6 ospf command cannot be used.

Verifying OSPFv3 Configuration and Operation

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show ospfv3 [<i>process-id</i>] [<i>address-family</i>] border-routers</p> <p>Example:</p> <pre>Device# show ospfv3 border-routers</pre>	Displays the internal OSPFv3 routing table entries to an ABR and ASBR.
Step 3	<p>show ospfv3 [<i>process-id</i>] [<i>area-id</i>] [<i>address-family</i>] database [database-summary internal external [<i>ipv6-prefix</i>] [<i>link-state-id</i>] grace inter-area prefix [<i>ipv6-prefix</i> <i>link-state-id</i>] inter-area router [<i>destination-router-id</i> <i>link-state-id</i>] link [interface <i>interface-name</i> <i>link-state-id</i>] network [<i>link-state-id</i>] nssa-external [<i>ipv6-prefix</i>] [<i>link-state-id</i>] prefix [ref-lsa {router network} <i>link-state-id</i>] promiscuous router [<i>link-state-id</i>] unknown [{area as link} [<i>link-state-id</i>]] [adv-router <i>router-id</i>] [self-originate]</p> <p>Example:</p> <pre>Device# show ospfv3 database</pre>	Displays lists of information related to the OSPFv3 database for a specific device.
Step 4	<p>show ospfv3 [<i>process-id</i>] [<i>address-family</i>] events [generic interface lsa neighbor reverse rib spf]</p> <p>Example:</p> <pre>Device# show ospfv3 events</pre>	Displays detailed information about OSPFv3 events.
Step 5	<p>show ospfv3 [<i>process-id</i>] [<i>area-id</i>] [<i>address-family</i>] flood-list [<i>interface-type</i> <i>interface-number</i>]</p> <p>Example:</p> <pre>Device# show ospfv3 flood-list</pre>	Displays a list of OSPFv3 LSAs waiting to be flooded over an interface.
Step 6	<p>show ospfv3 [<i>process-id</i>] [<i>address-family</i>] graceful-restart</p> <p>Example:</p> <pre>Device# show ospfv3 graceful-restart</pre>	Displays OSPFv3 graceful restart information.
Step 7	<p>show ospfv3 [<i>process-id</i>] [<i>area-id</i>] [<i>address-family</i>] interface [<i>type number</i>] [brief]</p> <p>Example:</p> <pre>Device# show ospfv3 interface</pre>	Displays OSPFv3-related interface information.

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

Configuration Examples for Load Balancing in OSPFv3

Example: Configuring the OSPFv3 Device Process

```

Device# show ospfv3 database
      OSPFv3 Device with ID (172.16.4.4) (Process ID 1)
      Device Link States (Area 0)
      ADV Device      Age      Seq#      Fragment ID  Link count  Bits
172.16.4.4          239      0x80000003  0             1            B
172.16.6.6          239      0x80000003  0             1            B
      Inter Area Prefix Link States (Area 0)
      ADV Device      Age      Seq#      Prefix
172.16.4.4          249      0x80000001  FEC0:3344::/32
172.16.4.4          219      0x80000001  FEC0:3366::/32
172.16.6.6          247      0x80000001  FEC0:3366::/32
172.16.6.6          193      0x80000001  FEC0:3344::/32
172.16.6.6          82       0x80000001  FEC0::/32
      Inter Area Device Link States (Area 0)
      ADV Device      Age      Seq#      Link ID      Dest DevID
172.16.4.4          219      0x80000001  50529027     172.16.3.3
172.16.6.6          193      0x80000001  50529027     172.16.3.3
      Link (Type-8) Link States (Area 0)
      ADV Device      Age      Seq#      Link ID      Interface
172.16.4.4          242      0x80000002  14           PO4/0
172.16.6.6          252      0x80000002  14           PO4/0
      Intra Area Prefix Link States (Area 0)
      ADV Device      Age      Seq#      Link ID      Ref-lstype  Ref-LSID
172.16.4.4          242      0x80000002  0            0x2001      0
172.16.6.6          252      0x80000002  0            0x2001      0

```

```

Device# show ospfv3 neighbor

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

```

Example: Configuring NBMA Interfaces

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

```

interface GigabitEthernet 0/0
no switchport
ipv6 enable

ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C0

```

Example: Forcing SPF Configuration

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

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

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

Feature Information for IPv6 Routing: OSPFv3

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

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

Table 12: Feature Information for IPv6 Routing: OSPFv3

Feature Name	Releases	Feature Information
IPv6 Routing: OSPFv3	Cisco IOS XE Release 3.2.0SG Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.6E	OSPF version 3 for IPv6 expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.



OSPFv3 Authentication Trailer

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

- [Finding Feature Information, page 135](#)
- [Information About OSPFv3 Authentication Trailer, page 135](#)
- [How to Configure OSPFv3 Authentication Trailer, page 137](#)
- [Configuration Examples for OSPFv3 Authentication Trailer, page 139](#)
- [Additional References for OSPFv3 Authentication Trailer, page 140](#)
- [Feature Information for OSPFv3 Authentication Trailer, page 141](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About OSPFv3 Authentication Trailer

Overview of OSPFv3 Authentication Trailer

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

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

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

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

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

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

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

See RFC 6506 for more details on the authentication procedure.

How to Configure OSPFv3 Authentication Trailer

Configuring OSPFv3 Authentication Trailer

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 2/0	Specifies the interface type and number.
Step 4	ospfv3 [<i>pid</i>] [<i>ipv4</i> <i>ipv6</i>] authentication { key-chain <i>chain-name</i> null }	Specifies the authentication type for an OSPFv3 instance.
	Example: Device(config-if)# ospfv3 1 ipv4 authentication key-chain ospf-1	

	Command or Action	Purpose
Step 5	router ospfv3 [<i>process-id</i>] Example: Device(config-if)# router ospfv3 1	Enters OSPFv3 router configuration mode.
Step 6	address-family ipv6 unicast vrf <i>vrf-name</i> Example: Device(config-router)# address-family ipv6 unicast vrf vrf1	Configures the IPv6 address family in the OSPFv3 process and enters IPv6 address family configuration mode.
Step 7	area <i>area-id</i> authentication { key-chain <i>chain-name</i> null } Example: Device(config-router-af)# area 1 authentication key-chain ospf-chain-1	Configures the authentication trailer on all interfaces in the OSPFv3 area.
Step 8	area <i>area-id</i> virtual-link <i>router-id</i> authentication key-chain <i>chain-name</i> Example: Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1	Configures the authentication for virtual links.
Step 9	area <i>area-id</i> sham-link <i>source-address destination-address</i> authentication key-chain <i>chain-name</i> Example: Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1	Configures the authentication for sham links.
Step 10	authentication mode { deployment normal } Example: Device(config-router-af)# authentication mode deployment	Specifies the type of authentication used for the OSPFv3 instance. <ul style="list-style-type: none"> The deployment keyword provides adjacency between configured and unconfigured authentication devices.
Step 11	end Example: Device(config-router-af)# end	Exits IPv6 address family configuration mode and returns to privileged EXEC mode.
Step 12	show ospfv3 interface Example: Device# show ospfv3	(Optional) Displays OSPFv3-related interface information.
Step 13	show ospfv3 neighbor [<i>detail</i>] Example: Device# show ospfv3 neighbor detail	(Optional) Displays OSPFv3 neighbor information on a per-interface basis.

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

Configuration Examples for OSPFv3 Authentication Trailer

Example: Configuring OSPFv3 Authentication Trailer

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

Example: Verifying OSPFv3 Authentication Trailer

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

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

```
Device# show ospfv3 neighbor detail

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

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

```

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

```

```
Device# show ospfv3 interface
```

```
GigabitEthernet0/0 is up, line protocol is up
```

```
...
```

```

Cryptographic authentication enabled
Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-keys
Last retransmission scan time is 0 msec, maximum is 0 msec

```

Additional References for OSPFv3 Authentication Trailer

Related Documents

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

Standards and RFCs

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

Technical Assistance

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

Feature Information for OSPFv3 Authentication Trailer

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

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

Table 13: Feature Information for OSPFv3 Authentication Trailer

Feature Name	Releases	Feature Information
OSPFv3 Authentication Trailer	Cisco IOS XE 3.6E	<p>The OSPFv3 Authentication Trailer feature as specified in RFC 6506 provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication.</p> <p>In Cisco IOS XE 3.6E, this feature was supported on the following platforms:</p> <ul style="list-style-type: none"> • Catalyst 3850 Series Switches • Catalyst 3650 Series Switches • Catalyst 4000 series Switches • Cisco 5700 Series Wireless LAN Controllers <p>The following commands were introduced or modified: ospfv3 authentication key-chain, authentication mode, debug ospfv3 vrf authentication.</p>



TTL Security Support for OSPFv3 on IPv6

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

- [Finding Feature Information, page 143](#)
- [Restrictions for TTL Security Support for OSPFv3 on IPv6, page 143](#)
- [Prerequisites for TTL Security Support for OSPFv3 on IPv6, page 144](#)
- [Information About TTL Security Support for OSPFv3 on IPv6, page 144](#)
- [How to Configure TTL Security Support for OSPFv3 on IPv6, page 145](#)
- [Configuration Examples for TTL Security Support for OSPFv3 on IPv6, page 147](#)
- [Additional References, page 148](#)
- [Feature Information for TTL Security Support for OSPFv3 on IPv6, page 149](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Restrictions for TTL Security Support for OSPFv3 on IPv6

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

Prerequisites for TTL Security Support for OSPFv3 on IPv6

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

Information About TTL Security Support for OSPFv3 on IPv6

OSPFv3 TTL Security Support for Virtual and Sham Links

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

**Note**

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

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

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

**Note**

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

How to Configure TTL Security Support for OSPFv3 on IPv6

Configuring TTL Security Support on Virtual Links for OSPFv3 on IPv6

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring TTL Security Support on Sham Links for OSPFv3 on IPv6

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

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

Configuration Examples for TTL Security Support for OSPFv3 on IPv6

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

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

```

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

```

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

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

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

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
IPv6 routing: OSPFv3	"IPv6 Routing: OSPFv3" module

MIBs

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

Technical Assistance

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

Feature Information for TTL Security Support for OSPFv3 on IPv6

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

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

Table 14: TTL Security Support for OSPFv3 on IPv6

Feature Name	Software Releases	Feature Information
TTL Security Support for OSPFv3 on IPv6	Cisco IOS XE Release 3.4SG Cisco IOS XE Release 3.6E	<p>The TTL Security Support for OSPFv3 on IPv6 feature increases protection against OSPFv3 denial of service attacks.</p> <p>In Cisco IOS XE Release 3.4 SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands were introduced or modified by this feature: area sham-link, area virtual-link.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



CHAPTER 11

OSPFv3 Fast Convergence: LSA and SPF Throttling

The Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSAs) and shortest-path first (SPF) throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability. It also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds.

- [Finding Feature Information, page 151](#)
- [Information About OSPFv3 Fast Convergence: LSA and SPF Throttling, page 152](#)
- [How to Configure OSPFv3 Fast Convergence: LSA and SPF Throttling, page 152](#)
- [Configuration Examples for OSPFv3 Fast Convergence: LSA and SPF Throttling, page 155](#)
- [Additional References, page 155](#)
- [Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling, page 156](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About OSPFv3 Fast Convergence: LSA and SPF Throttling

Fast Convergence: LSA and SPF Throttling

The OSPFv3 LSA and SPF throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability. It also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds.

OSPFv3 can use static timers for rate-limiting SPF calculation and LSA generation. Although these timers are configurable, the values used are specified in seconds, which poses a limitation on OSPFv3 convergence. LSA and SPF throttling achieves subsecond convergence by providing a more sophisticated SPF and LSA rate-limiting mechanism that is able to react quickly to changes and also provide stability and protection during prolonged periods of instability.

How to Configure OSPFv3 Fast Convergence: LSA and SPF Throttling

Tuning LSA and SPF Timers for OSPFv3 Fast Convergence

This task can be performed in Cisco IOS Release 15.1(3)S and 15.2(1)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *[process-id]*
4. **timers lsa arrival** *milliseconds*
5. **timers pacing flood** *milliseconds*
6. **timers pacing lsa-group** *seconds*
7. **timers pacing retransmission** *milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospfv3 [<i>process-id</i>] Example: Device(config)# router ospfv3 1	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	timers lsa arrival <i>milliseconds</i> Example: Device(config-rtr)# timers lsa arrival 300	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.
Step 5	timers pacing flood <i>milliseconds</i> Example: Device(config-rtr)# timers pacing flood 30	Configures LSA flood packet pacing.
Step 6	timers pacing lsa-group <i>seconds</i> Example: Device(config-router)# timers pacing lsa-group 300	Changes the interval at which OSPFv3 LSAs are collected into a group and refreshed, checksummed, or aged.
Step 7	timers pacing retransmission <i>milliseconds</i> Example: Device(config-router)# timers pacing retransmission 100	Configures LSA retransmission packet pacing in IPv4 OSPFv3.

Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence

This task can be performed in releases prior to Cisco IOS Release 15.1(3)S and 15.2(1)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa** *start-interval hold-interval max-interval*
6. **timers lsa arrival** *milliseconds*
7. **timers pacing flood** *milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 router ospf <i>process-id</i> Example: Device(config)# ipv6 router ospf 1	Enables OSPFv3 router configuration mode.
Step 4	timers throttle spf <i>spf-start spf-hold spf-max-wait</i> Example: Device(config-rtr)# timers throttle spf 200 200 200	Turns on SPF throttling.
Step 5	timers throttle lsa <i>start-interval hold-interval max-interval</i> Example: Device(config-rtr)# timers throttle lsa 300 300 300	Sets rate-limiting values for OSPFv3 LSA generation.
Step 6	timers lsa arrival <i>milliseconds</i> Example: Device(config-rtr)# timers lsa arrival 300	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.

	Command or Action	Purpose
Step 7	timers pacing flood <i>milliseconds</i> Example: Device(config-rtr)# timers pacing flood 30	Configures LSA flood packet pacing.

Configuration Examples for OSPFv3 Fast Convergence: LSA and SPF Throttling

Example: Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence

The following example show how to display the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
  ospf 2
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	IPv6 Configuration Guide
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Related Topic	Document Title
OSPFv3 Fast Convergence: LSA and SPF Throttling	" <i>OSPF Link-State Advertisement Throttling</i> " module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

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

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

Table 15: Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

Feature Name	Releases	Feature Information
OSPFv3 Fast Convergence: LSA and SPF Throttling	Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.6E	<p>The OSPFv3 LSA and SPF throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



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 159](#)
- [Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 160](#)
- [Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 160](#)
- [How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs, page 162](#)
- [Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 163](#)
- [Additional References, page 163](#)
- [Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 164](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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

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

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

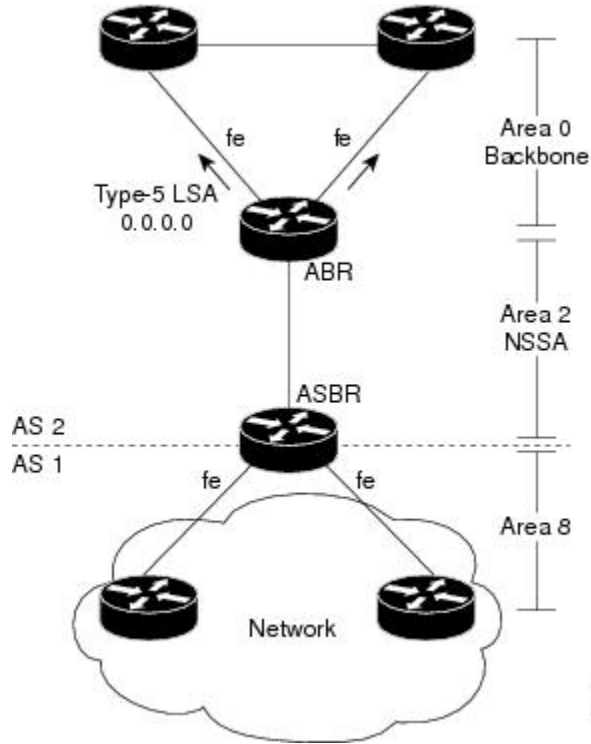
The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes an NSSA ABR to translate Type-7 LSAs to Type-5 LSAs, but use the 0.0.0.0 as the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding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

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

In the figure below, it would be advantageous to filter Area 2 addresses from Area 0 to minimize the number of routes introduced into the backbone (Area 0). However, using the **area range** command to consolidate and summarize routes at the area boundary--filtering the Area 2 addresses--will not work because the Area 2 addresses include forwarding addresses for Type-7 LSAs that are generated by the ASBR. If these Type-7

LSA forwarding addresses have been filtered out of Area 0, the backbone routers cannot reach the prefixes advertised in the translated Type-5 LSAs (autonomous system external LSAs).

Figure 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



Caution

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 1	Enables OSPF routing and enters device configuration mode. <ul style="list-style-type: none"> • The <i>process-id</i> argument identifies the OSPF process.
Step 4	area <i>area-id</i> nssa translate type7 suppress-fa Example: Device(config-router)# area 10 nssa translate type7 suppress-fa	Configures an area as a not-so-stubby-area (NSSA) and suppresses the forwarding address in translated Type-7 LSAs.

	Command or Action	Purpose
Step 5	end Example: Device(config-router)# end	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

Example Suppressing OSPF Forwarding Address in Translated Type-5 LSAs

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

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

Additional References

Related Documents

Related Topic	Document Title
OSPF commands	<i>Cisco IOS IP Routing: OSPF Command Reference</i>
OSPFv3 Address Families	“OSPFv3 Address Families” module

Standards

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

MIBs

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

RFCs

RFCs	Title
Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587.	<i>The OSPF NSSA Option</i>

Technical Assistance

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

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

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

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

Table 16: Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

Feature Name	Releases	Feature Information
OSPF Forwarding Address Suppression in Translated Type-5 LSAs	Cisco IOS XE Release 3.1.0 SG Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.1.0SG, support was added for the Cisco Catalyst 4000 Series Switches.</p> <p>The following commands are introduced or modified:</p> <ul style="list-style-type: none"> • area nssa translate • show ip ospf <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>

