IP Routing: OSPF Configuration Guide, Cisco IOS Release 15E

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

CONTENTS

CHAPTER 1 **Configuring OSPF TTL Security Check and OSPF Graceful Shutdown** 1

- Finding Feature Information 1
- Information About OSPF TTL Security Check and OSPF Graceful Shutdown 2
  - TTL Security Check for OSPF 2
  - Transitioning Existing Networks to Use TTL Security Check 2
  - TTL Security Check for OSPF Virtual and Sham Links 2
  - Benefits of the OSPF Support for TTL Security Check 2
  - OSPF Graceful Shutdown 3
- How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown 3
  - Configuring TTL Security Check on All OSPF Interfaces 3
  - Configuring TTL Security Check on a Per-Interface Basis 4
  - Configuring OSPF Graceful Shutdown on a Per-Interface Basis 6
- Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown 7
  - Example: Transitioning an Existing Network to Use TTL Security Check 7
- Additional References 8
- Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown 9

CHAPTER 2 **Enabling OSPFv2 on an Interface Basis** 13

- Finding Feature Information 13
- Prerequisites for Enabling OSPFv2 on an Interface Basis 13
- Restrictions on Enabling OSPFv2 on an Interface Basis 14
- Information About Enabling OSPFv2 on an Interface Basis 14
  - Benefits of Enabling OSPFv2 on an Interface Basis 14
  - Implications of Configuring OSPFv2 On a Router Basis or an Interface Basis 14
- How to Enable OSPFv2 on an Interface Basis 15
  - Enabling OSPFv2 on an Interface 15
- Configuration Example for Enabling OSPFv2 on an Interface 16

Example Enabling OSPFv2 on an Interface 16
Additional References 17
Feature Information for Enabling OSPFv2 on an Interface Basis 18

CHAPTER 3 Configuring NSSA for OSPFv2 21
Finding Feature Information 21
Information About Configuring NSSA for OSPF 21
Characteristics of RFC 3101 21
RFC 1587 Compliance 22
ABR as NSSA Link State Advertisement Translator 22
How to Configure NSSA for OSPF 24
Configuring an OSPFv2 NSSA Area and Its Parameters 24
Configuring an NSSA ABR as a Forced NSSA LSA Translator 26
Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility 27
Configuration Examples for OSPF 28
Example: Configuring OSPF NSSA 28
Example: OSPF NSSA Area with RFC 3101 Disabled and RFC 1587 Active 30
Example: Verifying OSPF NSSA 32
Additional References for OSPF Not-So-Stubby Areas (NSSA) 37
Feature Information for Configuring NSSA 38

CHAPTER 4 Configuring NSSA for OSPFv3 39
Finding Feature Information 39
Information About Configuring NSSA for OSPFv3 39
RFC 1587 Compliance 39
ABR as OSPFv3 NSSA LSA Translator 40
How to Configure NSSA for OSPFv3 42
Configuring an OSPFv3 NSSA Area and Its Parameters 42
Configuring an NSSA ABR as a Forced NSSA LSA Translator for OSPFv3 44
Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility 45
Configuration Examples for Configuring NSSA for OSPFv3 46
Example: NSSA for OSPFv3 46
Additional References for Configuring NSSA for OSPFv3 48
Feature Information for Configuring NSSA for OSPFv3 48

CHAPTER 5 **IPv6 Routing: OSPFv3 Authentication Support with IPsec** 51

Finding Feature Information 51

Prerequisites for IPv6 Routing: OSPFv3 Authentication Support with IPsec 51

Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec 52

OSPFv3 Authentication Support with IPsec 52

How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec 53

Configuring IPsec on OSPFv3 53

Defining Authentication on an Interface 53

Defining Authentication in an OSPFv3 Area 54

Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec 55

Example: Defining Authentication on an Interface 55

Example: Defining Authentication in an OSPFv3 Area 56

Additional References 56

Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec 57

CHAPTER 6 **OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3** 59

Finding Feature Information 59

Prerequisites for OSPF Enhanced Traffic Statistics 60

Information About OSPF Enhanced Traffic Statistics 60

How to Display and Clear OSPF Enhanced Traffic Statistics 60

Displaying and Clearing OSPF Traffic Statistics for OSPFv2 60

Displaying and Clearing OSPF Traffic Statistics for OSPFv3 61

Configuration Examples for OSPF Enhanced Traffic Commands 62

Displaying and Clearing Enhanced Traffic Statistics for OSPFv2 Example 62

Displaying and Clearing Enhanced Traffic Statistics for OSPFv3 Example 64

Additional References 65

Feature Information for OSPF Enhanced Traffic Statistics 67

CHAPTER 7 **OSPF SNMP ifIndex Value for Interface ID in Data Fields** 69

Finding Feature Information 69

Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields 70

Information About SNMP ifIndex Value for Interface ID in Data Fields 70

Benefits of Choosing to Identify Interfaces by the SNMP MIB-II ifIndex Value 70

How OSPFv2 and OSPFv3 Use the SNMP MIB-II ifIndex Value 70

How to Configure SNMP ifIndex Value for Interface ID in Data Fields 71
Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers 71
Configuration Examples for SNMP ifIndex Value for Interface ID in Data Fields 72
Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2 72
Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3 73
Additional References 76
Feature Information for OSPF SNMP ifIndex Value for Interface ID 77

CHAPTER 8 **OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements 79**
Finding Feature Information 79
Prerequisites for Excluding Connected IP Prefixes from LSAs 80
Information About Excluding Connected IP Prefixes from LSAs 80
Previous Methods to Limit the Number of IP Prefixes Carried in LSAs 80
Feature Overview 80
How to Exclude Connected IP Prefixes from OSPF LSAs 81
Excluding IP Prefixes per OSPF Process 81
Excluding IP Prefixes on a Per-Interface Basis 83
Troubleshooting IP Prefix Suppression 84
Configuration Examples for Excluding Connected IP Prefixes from LSAs 86
Excluding IP Prefixes from LSAs for an OSPF Process Example 86
Excluding IP Prefixes from LSAs for a Specified Interface Example 86
Additional References 87
Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements 88
Glossary 88

CHAPTER 9 **OSPF Nonstop Routing 91**
Finding Feature Information 91
Restrictions for OSPF Nonstop Routing 91
Information About OSPF Nonstop Routing 92
OSPF NSR Functionality 92
How to Configure OSPF Nonstop Routing 92
Configuring OSPF NSR 92
Troubleshooting Tips 93
Configuration Examples for OSPF Nonstop Routing 94

Example: Configuring OSPF NSR 94
Example: Verifying OSPF NSR 94
Additional References for OSPF Nonstop Routing 95
Feature Information for OSPF Nonstop Routing 96

CHAPTER 10 OSPFv2 Local RIB 97
Finding Feature Information 97
Prerequisites for OSPFv2 Local RIB 98
Restrictions for OSPFv2 Local RIB 98
Information About OSPFv2 Local RIB 98
Function of the OSPF Local RIB 98
How to Configure the OSPFv2 Local RIB Feature 98
Changing the Default Local RIB Criteria 99
Changing the Administrative Distance for Discard Routes 100
Troubleshooting Tips 102
Configuration Examples for the OSPFv2 Local RIB Feature 102
Example: Changing the Default Local RIB Criteria 102
Example: Changing the Administrative Distance for Discard Routes 102
Additional References 103
Feature Information for the OSPFv2 Local RIB Feature 104

CHAPTER 11 IPv6 Routing: OSPFv3 107
Finding Feature Information 107
Prerequisites for IPv6 Routing: OSPFv3 107
Restrictions for IPv6 Routing: OSPFv3 108
Information About IPv6 Routing: OSPFv3 108
How OSPFv3 Works 108
Comparison of OSPFv3 and OSPF Version 2 108
LSA Types for OSPFv3 109
NBMA in OSPFv3 110
Load Balancing in OSPFv3 110
Addresses Imported into OSPFv3 110
OSPFv3 Customization 111
OSPFv3 Cost Calculation 111
Force SPF in OSPFv3 113

How to Configure Load Balancing in OSPFv3 113
Configuring the OSPFv3 Device Process 113
Configuring NBMA Interfaces in OSPFv3 116
Forcing an SPF Calculation 118
Verifying OSPFv3 Configuration and Operation 119
Configuration Examples for Load Balancing in OSPFv3 122
Example: Configuring the OSPFv3 Device Process 122
Example: Configuring NBMA Interfaces 122
Example: Forcing SPF Configuration 123
Additional References 123
Feature Information for IPv6 Routing: OSPFv3 124

CHAPTER 12 OSPFv3 Demand Circuit Ignore 125
Finding Feature Information 125
Information About OSPFv3 Demand Circuit Ignore 125
Demand Circuit Ignore Support 125
How to Configure OSPFv3 Demand Circuit Ignore 126
Configuring Demand Circuit Ignore Support for OSPFv3 126
Configuration Examples for OSPFv3 Demand Circuit Ignore 127
Example: Demand Circuit Ignore Support for OSPFv3 127
Additional References for OSPFv3 Demand Circuit Ignore 127
Feature Information for OSPFv3 Demand Circuit Ignore 128

CHAPTER 13 OSPFv3 Max-Metric Router LSA 131
Finding Feature Information 131
Information About OSPFv3 Max-Metric Router LSA 131
OSPFv3 Max-Metric Router LSA 131
How to Configure OSPFv3 Max-Metric Router LSA 132
Configuring the OSPFv3 Max-Metric Router LSA 132
Configuration Examples for OSPFv3 Max-Metric Router LSA 133
Example: Verifying the OSPFv3 Max-Metric Router LSA 133
Additional References 134
Feature Information for OSPFv3 Max-Metric Router LSA 135

CHAPTER 14 OSPFv3 MIB 137

Finding Feature Information 137
Prerequisites for OSPFv3 MIB 137
Restrictions for OSPFv3 MIB Support 138
Information About OSPFv3 MIB 138
OSPFv3 MIB 138
OSPFv3 TRAP MIB 138
How to Configure OSPFv3 MIB 138
Enabling Specific OSPFv3 Traps 138
Verifying OSPFv3 MIB Traps on the Device 140
Configuration Examples for OSPFv3 MIB 141
Example: Enabling and Verifying OSPFv3 MIB Traps 141
Additional References for OSPFv3 MIB 141
Feature Information for OSPFv3 MIB 142

CHAPTER 15 OSPFv3 VRF-Lite/PE-CE 143
Finding Feature Information 143
Restrictions for OSPFv3 VRF-Lite/PE-CE 143
Information About OSPFv3 VRF-Lite/PE-CE 144
Support for OSPFv3 VRF-Lite and PE-CE 144
How to Configure VRF-Lite/PE-CE 145
Configuring a VRF in an IPv6 Address Family for OSPFv3 145
Enabling an OSPFv3 IPv6 Address Family on a VRF Interface 146
Configuring a Sham-Link for OSPFv3 PE-CE 147
Configuring a Domain ID for an OSPFv3 PE-CE 150
Configuring VRF-Lite Capability for OSPFv3 151
Configuration Examples for OSPFv3 VRF-Lite/PE-CE 153
Example: Configuring a Provider Edge Device to Provide IPv6 and IPv4 Routing 153
Example: Configuring a Provider Edge Device for VRF-Lite 154
Additional References for OSPFv3 VRF-Lite/PE-CE 155
Feature Information for OSPFv3 VRF-Lite/PE-CE 156

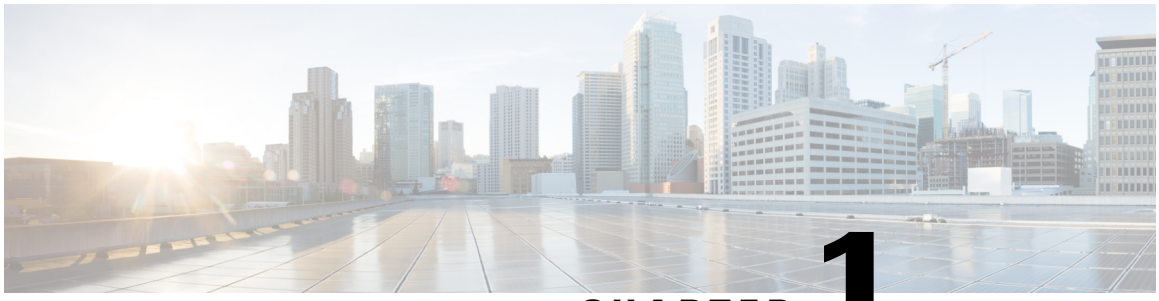
CHAPTER 16 OSPFv3 Authentication Trailer 157
Finding Feature Information 157
Information About OSPFv3 Authentication Trailer 157
Overview of OSPFv3 Authentication Trailer 157

How to Configure OSPFv3 Authentication Trailer 159
Configuring OSPFv3 Authentication Trailer 159
Configuration Examples for OSPFv3 Authentication Trailer 161
Example: Configuring OSPFv3 Authentication Trailer 161
Example: Verifying OSPFv3 Authentication Trailer 161
Additional References for OSPFv3 Authentication Trailer 162
Feature Information for OSPFv3 Authentication Trailer 163

CHAPTER 17 OSPF ABR Type 3 LSA Filtering 165
Finding Feature Information 165
Benefits 165
Restrictions 166
Related Features and Technologies 166
Configuration Tasks 166
Configuring OSPF ABR Type 3 LSA Filtering 166
Configuring OSPF ABR Type 3 LSA Filtering 167
Verifying OSPF ABR Type 3 LSA Filtering 167
Monitoring and Maintaining OSPF ABR Type 3 LSA Filtering 168
Configuration Examples 168
Additional References 168
Feature Information for the OSPF ABR Type 3 LSA Filtering 170

CHAPTER 18 Graceful Shutdown Support for OSPFv3 171
Finding Feature Information 171
Information About Graceful Shutdown Support for OSPFv3 171
OSPFv3 Graceful Shutdown 171
How to Configure Graceful Shutdown Support for OSPFv3 172
Configuring Graceful Shutdown of the OSPFv3 Process 172
Configuring Graceful Shutdown of the OSPFv3 Process in Address-Family Configuration Mode 173
Configuring OSPFv3 Graceful Shutdown of the OSPFv3 Interface 175
Configuration Examples for Graceful Shutdown Support for OSPFv3 176
Example: Configuring Graceful Shutdown of the OSPFv3 Process 176
Example: Configuring Graceful Shutdown of the OSPFv3 Interface 177
Additional References for Graceful Shutdown Support for OSPFv3 177

Feature Information for Graceful Shutdown Support for OSPFv3 178



CHAPTER 1

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 1
- Information About OSPF TTL Security Check and OSPF Graceful Shutdown, page 2
- How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown, page 3
- Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown, page 7
- Additional References, page 8
- Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown, page 9

Finding Feature Information

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

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

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

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

Configuring TTL Security Check on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Configuring OSPF Graceful Shutdown on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

Example: Transitioning an Existing Network to Use TTL Security Check

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

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

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

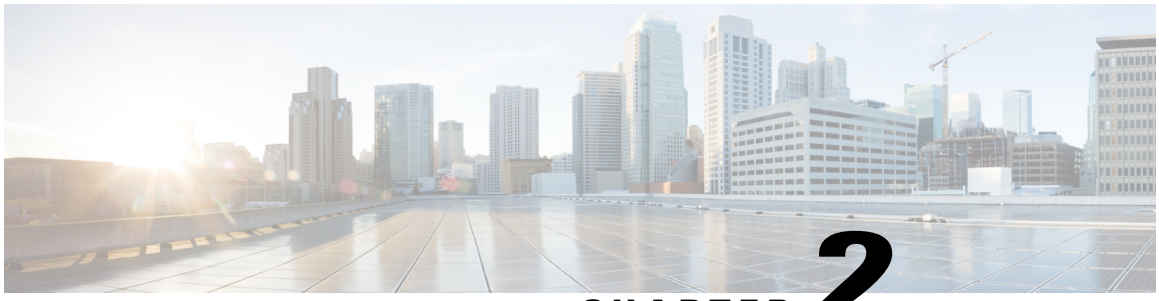
Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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

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

Table 1: Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

Feature Name	Releases	Feature Information
OSPF Graceful Shutdown	Cisco IOS Release 15.1(1)SG	This feature provides the ability to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. A graceful shutdown of a protocol can be initiated on all OSPF interfaces or on a specific interface. In Cisco IOS 15.1(1)SG, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: • **ip ospf shutdown** • **show ip ospf** • **show ip ospf interface** • **shutdown (router OSPF)**
OSPF TTL Security Check	Cisco IOS Release 15.1(1)SG	This feature increases protection against OSPF denial of service attacks, enables checking of TTL values on OSPF packets from neighbors, and allows users to set TTL values sent to neighbors. The following commands were introduced or modified: In Cisco IOS 15.1(1)SG, support was added for the Cisco Catalyst 4000 Series Switches. • **area sham-link cost** • **area virtual-link** • **debug ip ospf adj** • **ip ospf ttl-security** • **show ip ospf interface** • **show ip ospf neighbor** • **show ip ospf traffic** • **ttl-security all-interfaces**



CHAPTER 2

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 13
- Prerequisites for Enabling OSPFv2 on an Interface Basis, page 13
- Restrictions on Enabling OSPFv2 on an Interface Basis, page 14
- Information About Enabling OSPFv2 on an Interface Basis, page 14
- How to Enable OSPFv2 on an Interface Basis, page 15
- Configuration Example for Enabling OSPFv2 on an Interface, page 16
- Additional References, page 17
- Feature Information for Enabling OSPFv2 on an Interface Basis, page 18

Finding Feature Information

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

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

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

Configuration Example for Enabling OSPFv2 on an Interface

Example Enabling OSPFv2 on an Interface

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

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# bandwidth 10000
Router(config-if)# ip address 172.16.1.1 255.255.255.0
```

```
Router(config-if)# ip ospf hello-interval 1
Router(config-if)# ip ospf 1 area 0
```

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2328	*OSPF Version 2*

Technical Assistance

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

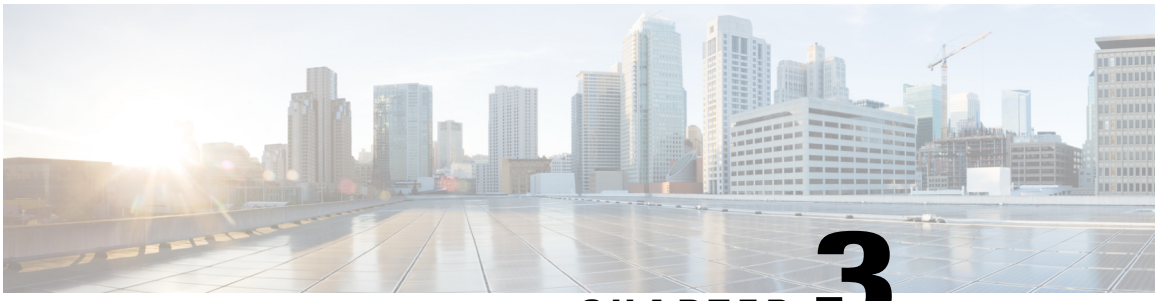
Feature Information for Enabling OSPFv2 on an Interface Basis

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

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

Table 2: Feature Information for Enabling OSPFv2 on an Interface Basis

Feature Name	Releases	Feature Information
Enabling OSPFv2 on an Interface Basis **Note** This feature was originally named "Area Command in Interface Mode for OSPFv2."	Cisco IOS Release 15.1(1)SG	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. In Cisco IOS 15.1(1) SG, support was added for the Cisco Catalyst 4000 Series Switches. The following commands are introduced or modified in the feature documented in this module: • **ip ospf area.**



CHAPTER 3

Configuring NSSA for OSPFv2

The Not-So-Stubby Area (NSSA) feature for OSPFv2 enhances the Type 7 autonomous-system external routing calculation and translates the Type 7 Link State Advertisement (LSA) into Type 5 LSA. This feature adds support for the OSPF NSSA specification that is defined by RFC 3101, OSPF Not-So-Stubby Area (NSSA) Option . RFC 3101 replaces RFC 1587, OSPF Not-So-Stubby Area (NSSA) Option, and is backward compatible with RFC 1587. For additional information refer to RFC 3101.

- Finding Feature Information, page 21
- Information About Configuring NSSA for OSPF, page 21
- How to Configure NSSA for OSPF, page 24
- Configuration Examples for OSPF, page 28
- Additional References for OSPF Not-So-Stubby Areas (NSSA), page 37
- Feature Information for Configuring NSSA, page 38

Finding Feature Information

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

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

Information About Configuring NSSA for OSPF

Characteristics of RFC 3101

RFC 3101 describes the following features:

- Provides an option of importing OSPF summary routes into a Not-So-Stubby Area (NSSA) as Type-3 summary-Link State Advertisement (LSA).
- Refines the setting of the forwarding address in Type-7 LSAs .
- Revises the Type-7 external route calculation .
- Strengthens the process of translating Type-7 LSAs into Type-5 LSAs.
- Modifies the process of flushing translated Type-7 LSAs.
- Defines the P-bit (propagate bit) default as clear.

RFC 1587 Compliance

RFC 3101 compliance is automatically enabled on the devices. Use the **compatible rfc1587** command in router configuration mode to revert to route selection that is based on RFC 1587. When you configure the device to be compatible with RFC 1587, the device performs the following actions:

- Reverts the route selection process to RFC 1587.
- Configures Autonomous System Border Router (ASBR) to configure the P (propagate bit) and zero-forwarding address.
- Disables always translating Area Border Router (ABR).

ABR as NSSA Link State Advertisement Translator

Use the Not-So-Stubby Area (NSSA) for Open Shortest Path First version 2 (OSPFv2) feature to simplify administration in a network that connects a central site that uses OSPF to a remote site that is using a different routing protocol.

When the NSSA feature was not implemented, the connection between the border device at the corporate site and the remote device was not established as an OSPF stub area due to following reasons:

- Routes for the remote site were not redistributed into the stub area.
- Two routing protocols had to be maintained.

A protocol such as Routing Information Protocol (RIP) is run to handle the redistribution.

By implementing NSSA, you can extend OSPF to include the remote connection by defining the area between the border device at the corporate site and the remote device as an NSSA.

As with OSPF stub areas, NSSA areas cannot be injected with distributed routes via Type 5 Link State Advertisement (LSA). Route redistribution into an NSSA area is possible only with Type 7 LSA. An NSSA Autonomous System Border Router (ASBR) generates the Type 7 LSA , and an NSSA Area Border Router (ABR) translates the Type 7 LSA into a Type 5 LSA. These LSAs can be flooded throughout the OSPF routing domain. Route summarization and filtering are supported during the translation.

Route summarization is the consolidation of advertised addresses. This feature enables an ABR to advertise a single summary route to other areas. 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.

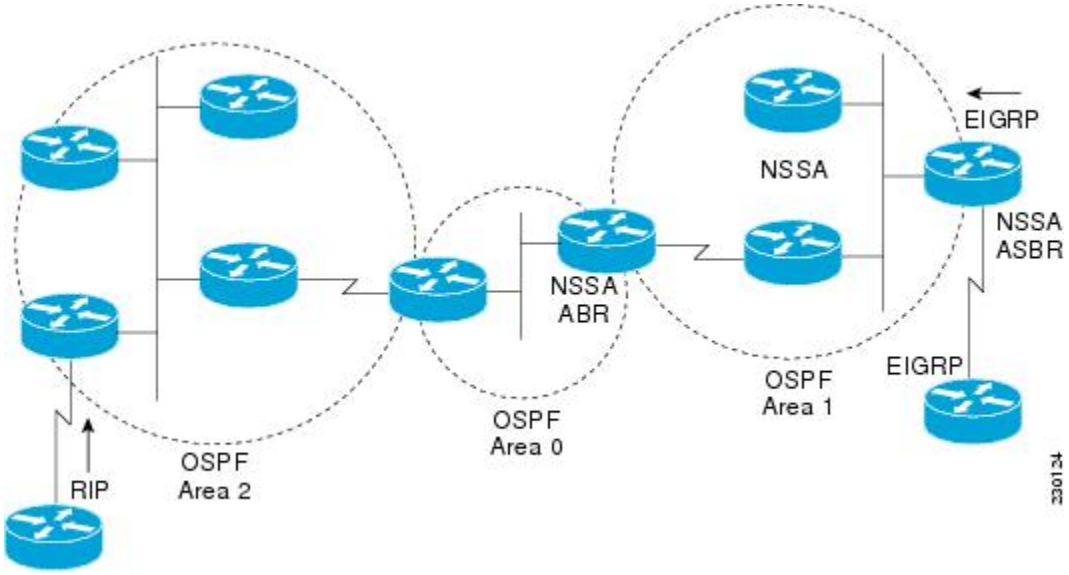
When routes from other protocols are redistributed to OSPF area, each route is advertised individually in an external LSA. However, you can configure the Cisco IOS software to advertise a single route with a specified network address and mask for all the redistributed routes that are covered by a specified network address and mask. Thus, the size of the OSPF link-state database decreases.

RFC 3101 allows you to configure an NSSA ABR device as a forced NSSA LSA translator.

Note Even a forced translator might not translate all LSAs; translation depends on the content 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 are not 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 include the EIGRP routes to the OSPF NSSA by generating Type 7 LSAs.

Figure 1: OSPF NSSA

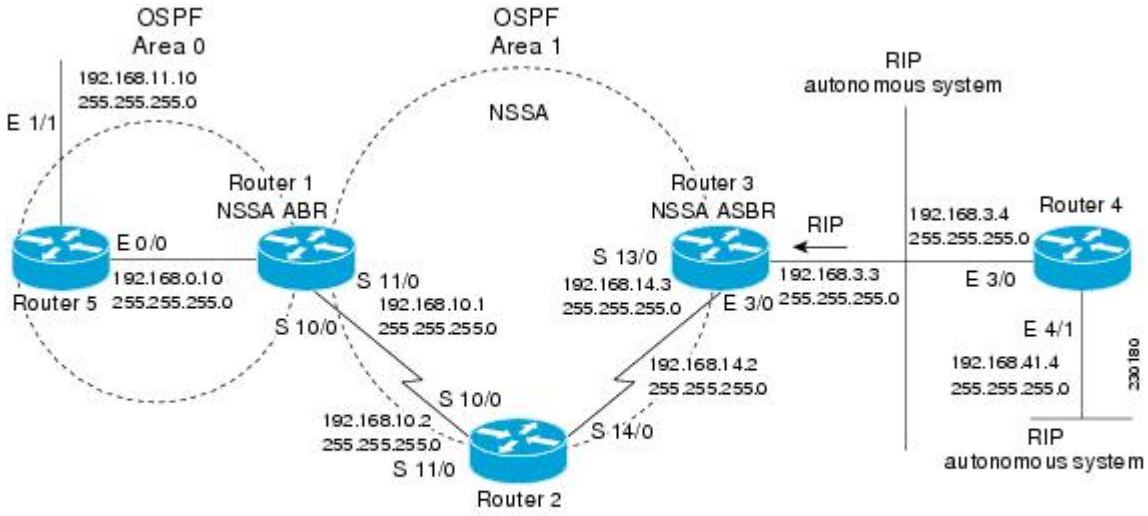


The redistributed routes from the RIP device are not allowed into OSPF Area 1 because NSSA is an extension to the stub area. The stub area characteristics still exist, including the exclusion of Type 5 LSAs.

The figure below shows the OSPF stub network with NSSA Area 1. The redistributed routes that Device 4 is propagating from the two RIP networks is translated into Type 7 LSAs by NSSA ASBR Device 3. Device 2,

which is configured to be the NSSA ABR, translates the Type 7 LSAs back to Type 5 so that they can be flooded through the rest of the OSPF stub network within OSPF Area 0.

Figure 2: OSPF NSSA Network with NSSA ABR and ASBR Devices



How to Configure NSSA for OSPF

Configuring an OSPFv2 NSSA Area and Its Parameters

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring an NSSA ABR as a Forced NSSA LSA Translator

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. The range is from 1 to 65535.

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

Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Examples for OSPF

Example: Configuring OSPF NSSA

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

Device 1

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

```
 ip address 192.168.10.1 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 area 1 nssa
!
end
```

Device 2

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

Device 3

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

```
 redistribute ospf 1 metric 15
 network 192.168.3.0
end
```

Device 4

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

Device 5

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

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

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

```
Device# show ip ospf

Routing Process "ospf 1" with ID 10.0.2.1
Start time: 00:00:25.512, Time elapsed: 00:01:02.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
```

```
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 0 normal 0 stub 1 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area 1
Number of interfaces in this area is 1
It is a NSSA area
Configured to translate Type-7 LSAs, inactive (RFC3101 support
disabled)
Area has no authentication
SPF algorithm last executed 00:00:07.160 ago
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x0245F0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

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

Table 3: 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 4: show ip ospf database nssa Field Descriptions

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

Example: Verifying OSPF NSSA

The following is sample output from the **show ip ospf** command. The output displays that OSPF Area 1 is an NSSA area.

```
Device2# show ip ospf

 Routing Process "ospf 1" with ID 10.1.0.2
 Start time: 00:00:01.392, Time elapsed: 12:03:09.480
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 0 normal 0 stub 1 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area 1
  Number of interfaces in this area is 2
! It is a NSSA area
  Area has no authentication
  SPF algorithm last executed 11:37:58.836 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 7. Checksum Sum 0x045598
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0


Device2# show ip ospf data

            OSPF Router with ID (10.1.0.2) (Process ID 1)
  Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.0.1        10.1.0.1        1990        0x80000016 0x00CBCB 2
```

```
10.1.0.2        10.1.0.2        1753        0x80000016 0x009371 4
10.1.0.3        10.1.0.3        1903        0x80000016 0x004149 2

  Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.0.0     10.1.0.1        1990        0x80000017 0x00A605
192.168.11.0    10.1.0.1        1990        0x80000015 0x009503

  Type-7 AS External Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Tag
192.168.3.0     10.1.0.3        1903        0x80000015 0x00484F 0
192.168.41.0    10.1.0.3        1903        0x80000015 0x00A4CC 0
```

The following is sample output from the **show ip ospf database data** command. The output displays additional information about redistribution between Type 5 and Type 7 LSAs for routes that are injected into the NSSA area and then flooded through the OSPF network.

```
Device2# show ip ospf database data

            OSPF Router with ID (10.1.0.2) (Process ID 1)
Area 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    2        0        0

Prefixes redistributed in Type-7  0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Subtotal      7        0        0

Process 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    2        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Type-5 Ext    0        0        0

Prefixes redistributed in Type-5  0
  Opaque AS     0        0        0
  Total         7        0        0
```

The following is sample output from the **show ip ospf database nssa** command. The output displays detailed information for Type 7 to Type 5 translations:

```
Device2# show ip ospf database nssa

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

```
  Routing Bit Set on this LSA
  LS age: 1903
! Options: (No TOS-capability, Type 7/5 translation, DC)
  LS Type: AS External Link
  Link State ID: 192.168.41.0 (External Network Number )
  Advertising Router: 10.1.0.3
  LS Seq Number: 80000015
  Checksum: 0xA4CC
  Length: 36
  Network Mask: /24
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 20
  Forward Address: 192.168.14.3
  External Route Tag: 0
```

The following sample output from the **show ip ospf** command displays that the device is acting as an ASBR and OSPF Area 1 is configured as an NSSA area:

```
Device3# show ip ospf

 Routing Process "ospf 1" with ID 10.1.0.3
 Start time: 00:00:01.392, Time elapsed: 12:02:34.572
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
!It is an autonomous system boundary router
 Redistributing External Routes from,
    rip, includes subnets in redistribution
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 0 normal 0 stub 1 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area 1
  Number of interfaces in this area is 1
! It is a NSSA area
  Area has no authentication
  SPF algorithm last executed 11:38:13.368 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 7. Checksum Sum 0x050CF7
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

The table below describes the significant fields shown in the **show ip ospf** command output.

Table 5: show ip ospf Field Descriptions

Field	Description
Routing process "ospf 1" with ID 10.1.0.3	Process ID and OSPF router ID.

Field	Description
Supports ...	Number of types of service supported (Type 0 only).
Summary Link update interval	Specifies summary update interval in hours:minutes:seconds, and time until next update.
External Link update interval	Specifies external update interval in hours:minutes:seconds, and time until next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
SPF calculations	Lists start, hold, and maximum wait interval values in milliseconds.
Number of areas	Number of areas in router, area addresses, and so on.
SPF algorithm last executed	Shows the last time an SPF calculation was performed in response to topology change event records.
Link State Update Interval	Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update.
Link State Age Interval	Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.

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

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

```
Device# show ip ospf

Routing Process "ospf 1" with ID 10.0.2.1
Start time: 00:00:25.512, Time elapsed: 00:01:02.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
```

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

The table below describes the significant fields shown in the **show ip ospf** command output.

Table 6: 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 significant fields shown in the **show ip ospf database nssa** command output.

Table 7: show ip ospf database nssa Field Description

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

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

Related Documents

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

RFCs

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

Technical Assistance

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

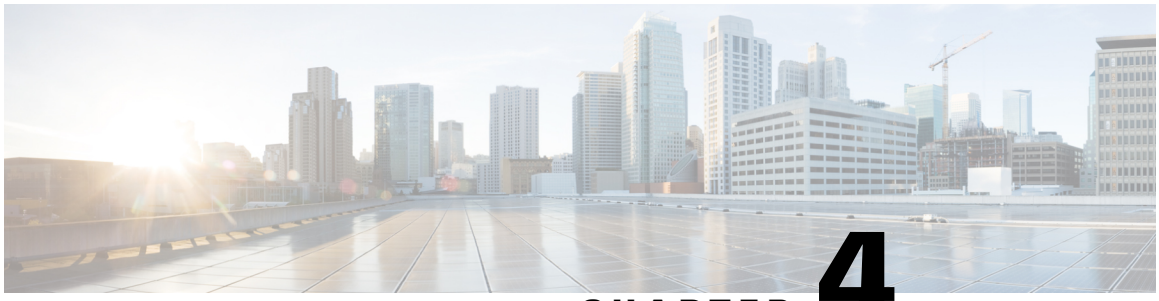
Feature Information for Configuring NSSA

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

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

Table 8: Feature Information for NSSA

Feature Name	Releases	Feature Information
OSPF Support for NSSA RFC 3101	15.2(1)E	The OSPF Not-So-Stubby Areas (NSSA) feature enhances the Type 7 autonomous-system external routing calculation and translates the Type 7 Link State Advertisement (LSA) into Type 5 LSA. This feature adds support for the OSPF NSSA specification defined by RFC 3101 (OSPF Not-So-Stubby Area (NSSA) Option). In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **area nssa translate**, **compatible rfc1587**.



CHAPTER 4

Configuring NSSA for OSPFv3

Cisco Open Short Shortest Path First version 3 (OSPFv3) allows you to configure a Not-So-Stubby Area (NSSA). An NSSA is similar to a stub area, except that an NSSA allows you to import autonomous system (AS) external routes within an NSSA using redistribution. This feature adds support for the OSPFv3 NSSA specification described by RFC 3101. RFC 3101 replaced and is backward compatible with RFC 1587.

- Finding Feature Information, page 39
- Information About Configuring NSSA for OSPFv3, page 39
- How to Configure NSSA for OSPFv3, page 42
- Configuration Examples for Configuring NSSA for OSPFv3, page 46
- Additional References for Configuring NSSA for OSPFv3, page 48
- Feature Information for Configuring NSSA for OSPFv3, page 48

Finding Feature Information

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

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

Information About Configuring NSSA for OSPFv3

RFC 1587 Compliance

RFC 3101 compliance is automatically enabled on the devices. Use the **compatible rfc1587** command in router configuration mode to revert to route selection that is based on RFC 1587. When you configure the device to be compatible with RFC 1587, the device performs the following actions:

- Reverts the route selection process to RFC 1587.
- Configures Autonomous System Border Router (ASBR) to configure the P (propagate bit) and zero-forwarding address.
- Disables always translating Area Border Router (ABR).

ABR as OSPFv3 NSSA LSA Translator

Use the Not-So-Stubby Area (NSSA) for Open Shortest Path First version 3 (OSPFv3) feature to simplify administration in a network that connects a central site that uses OSPFv3 to a remote site that uses a different routing protocol.

When the NSSA feature is not implemented, the connection between the border device at the corporate site and the remote device is not established as an OSPFv3 stub area due to following reasons:

- Routes for the remote site are not redistributed into the stub area.
- Two routing protocols must be maintained.

A protocol such as Routing Information Protocol (RIP) for IPv6 is run to handle the redistribution. By implementing NSSA, you can extend OSPFv3 to include the remote connection by defining the area between the border device at the corporate site and the remote device as an NSSA.

As with OSPFv3 stub areas, NSSA areas cannot be injected with distributed routes via a Type 5 Link State Advertisement (LSA). Route redistribution into an NSSA area is possible only with a Type 7 LSA. An NSSA Autonomous System Border Router (ASBR) generates the Type 7 LSA , and an NSSA Area Border Router (ABR) translates the Type 7 LSA into a Type 5 LSA. These LSAs can be flooded throughout the OSPFv3 routing domain. Route summarization and filtering are supported during the translation.

Route summarization is the consolidation of advertised addresses. This feature enables an ABR to advertise a single summary route to other areas. 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 an OSPFv3 area, each route is advertised individually in an external LSA. However, you can configure the Cisco IOS software to advertise a single route with a specified network address and mask for all the redistributed routes that are covered by a specified network address and mask. Thus, the size of the OSPFv3 link-state database decreases.

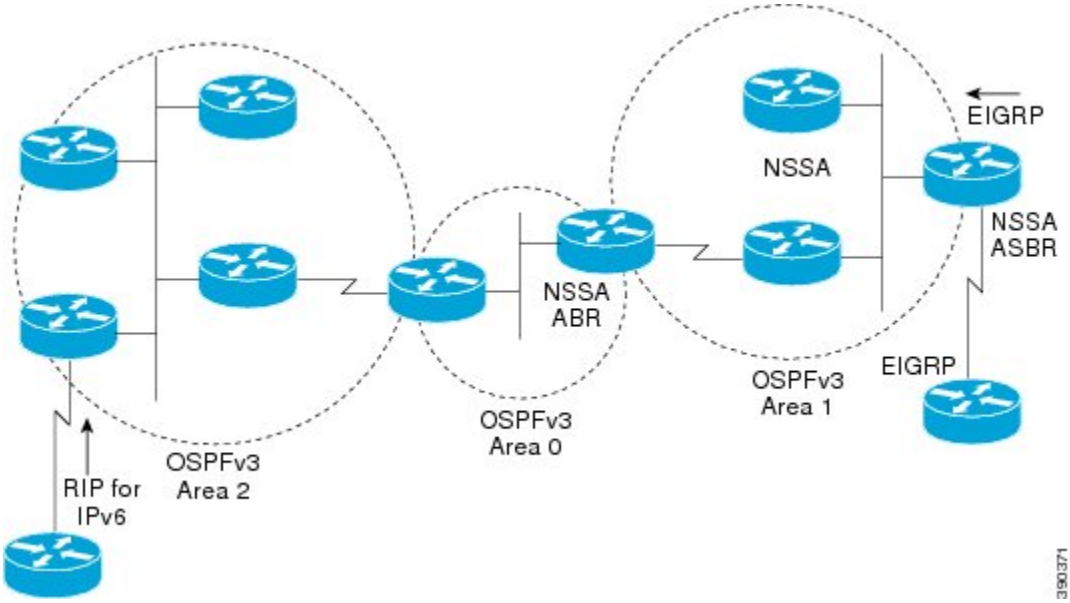
RFC 3101 allows you to configure an NSSA ABR device as a forced NSSA LSA translator.

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

The figure below shows a network diagram in which OSPFv3 Area 1 is defined as the stub area. The Enhanced Interior Gateway Routing Protocol (EIGRP) routes are not propagated into the OSPFv3 domain because

routing redistribution is not allowed in the stub area. However, once OSPFv3 Area 1 is defined as an NSSA, an NSSA ASBR can include the EIGRP routes to the OSPFv3 NSSA by generating Type 7 LSAs.

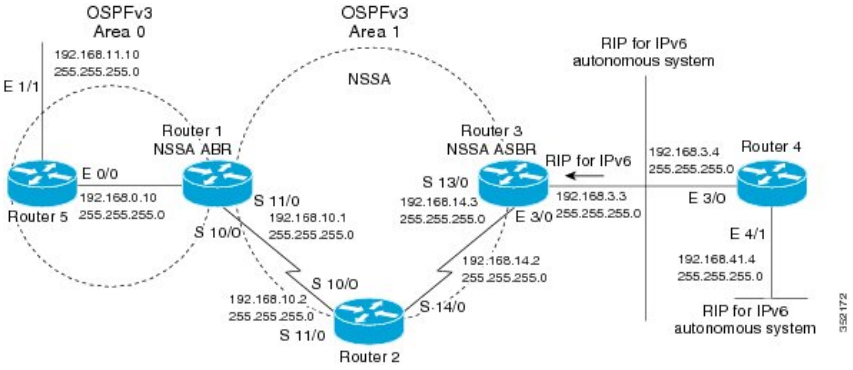
Figure 3: OSPFv3 NSSA



The redistributed routes from the RIP device are not allowed into OSPFv3 Area 1 because NSSA is an extension to the stub area. The stub area characteristics still exist, including the exclusion of Type 5 LSAs.

The figure below shows the OSPFv3 stub network with NSSA Area 1. The redistributed routes that Device 4 is propagating from the two RIP networks are translated into Type 7 LSAs by NSSA ASBR Device 3. Device 2, which is configured to be the NSSA ABR, translates the Type 7 LSAs back to Type 5 so that they can be flooded through the rest of the OSPFv3 stub network within OSPFv3 Area 0.

Figure 4: OSPFv3 NSSA Network with NSSA ABR and ASBR Devices



How to Configure NSSA for OSPFv3

Configuring an OSPFv3 NSSA Area and Its Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **area** *area-id* **nssa default-information-originate nssa-only**
5. **address-family** {**ipv4** | **ipv6**} [**unicast**]
6. Enter either of the following commands:
   - (For IPv4) **summary-prefix** {*ip-prefix* | *ip-address-mask*} [**not-advertise** | [**tag** *tag-value*] [**nssa-only**]]
   - (For IPv6) **summary-prefix** *ipv6-prefix* [**not-advertise** | [**tag** *tag-value*] [**nssa-only**]]
7. **exit**
8. **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*] [**nssa-only**]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 10`	Enables OSPFv3 routing and enters router configuration mode. • The *process-id* argument identifies the OSPFv3 process. The range is from 1 to 65535.
Step 4	**area** *area-id* **nssa default-information-originate nssa-only**	Configures an NSSA area and sets the default advertisement to this NSSA area.

	Command or Action	Purpose
	Example: `Device(config-router)# area 1 nssa default-information-originate nssa-only`	• In the example, area 1 is configured as an NSSA area. • The **nssa-only** keyword instructs the device to instigate Type-7 LSA with cleared P-bit, thereby, preventing LSA translation to Type 5 on NSSA ABR device.

Step 5	**address-family** {**ipv4** | **ipv6**} [**unicast**]
	Example:
	`Device(config-router)# address-family ipv4 unicast`
	`OR`
	`Device(config-router)# address-family ipv6 unicast`
		Enables address family configuration mode for Open Shortest Path First version 3 (OSPFv3).
		• The **address-family ipv4 unicast** command configures an IPv4 address family.
		• The **address-family ipv6 unicast** command configures an IPv6 address family.

Step 6	Enter either of the following commands:
	• (For IPv4) **summary-prefix** {*ip-prefix* | *ip-address-mask*} [**not-advertise** | [**tag** *tag-value*] [**nssa-only**]]
	• (For IPv6) **summary-prefix** *ipv6-prefix* [**not-advertise** | [**tag** *tag-value*] [**nssa-only**]]
	Example:
	(For IPv4)
	`Device(config-router-af)# summary-prefix 10.1.0.0/16 nssa-only`
	(For IPv6)
	`Device(config-router-af)# summary-prefix 2001:DB8::/32 nssa-only`
		• (For IPv4 address family only) Defines an IPv4 summary prefix and address mask in Open Shortest Path First version 3 (OSPFv3) and summarizes all routes redistributed from other routing protocols.
		• (For IPv6 address family only) Defines an IPv6 summary prefix in Open Shortest Path First version 3 (OSPFv3) and summarizes all routes redistributed from other routing protocols.
		• The **nssa-only** keyword instructs the device to instigate Type-7 LSA with cleared P-bit, thereby, preventing LSA translation to Type 5 on NSSA ABR router.

Step 7	**exit** **Example:** `Device(config-router-af)# exit`	Exits address-family router configuration mode and returns to the router configuration mode.
Step 8	**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*] [**nssa-only**] **Example:** `Device(config-router)# redistribute rip nssa-only`	Redistributes routes from one routing domain into another routing domain. • In the example, Routing Information Protocol (RIP) subnets are redistributed into the OSPFv3 domain.

	Command or Action	Purpose
Step 9	**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 for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **area** *area-id* **nssa translate type7 always**
5. **area** *area-id* **nssa translate type7 suppress-fa**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Enables OSPFv3 routing and enters router configuration mode. • The *process-id* argument identifies the OSPFv3 process. The range is from 1 to 65535.

	Command or Action	Purpose
Step 4	**area** *area-id* **nssa translate type7 always** **Example:** `Device(config-router)# area 10 nssa translate type7 always`	Configures a Not-So-Stubby Area Area Border Router (NSSA ABR) device as a forced NSSA Link State Advertisement (LSA) translator. **Note** You can use the **always** keyword to configure an NSSA ABR device as a forced NSSA LSA translator. This command can be used if RFC 3101 is disabled and RFC 1587 is used.

Step 5	**area** *area-id* **nssa translate type7 suppress-fa**
	
	Example:
	
	`Device(config-router)# area 10 nssa translate type7 suppress-fa`
	
	`OR`
	
	`Device (config-router)# address-family [ipv4|ipv6] unicast`
	`Device (config-router-af)# area 10 nssa translate type7 suppress-fa`
	`Device (config-router-af)# exit`
		Allows the ABR to suppress the forwarding address in translated Type 5 LSA.
		Note You can configure this command in both router configuration mode and address-family configuration mode.

Step 6	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **compatible rfc1587**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Enables OSPFv3 routing and enters router configuration mode. • The *process-id* argument identifies the OSPFv3 process.
Step 4	**compatible rfc1587** **Example:** `Device(config-router)# compatible rfc1587`	Changes the method used to perform route selection to RFC 1587 compatibility and disables RFC 3101.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configuring NSSA for OSPFv3

Example: NSSA for OSPFv3

Use the **show ospfv3** command to confirm that the device is acting as an Autonomous System Border Router (ASBR) and that the Open Shortest Path First version 3 (OSPFv3) Area 1 has been configured as a Not-So-Stubby Area (NSSA) area.

```
Device# show ospfv3

 OSPFv3 1 address-family ipv4
 Router ID 3.3.3.3
 Supports NSSA (compatible with RFC 1587)
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static
```

```
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 0 normal 0 stub 1 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
   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)
       Perform type-7/type-5 LSA translation, suppress forwarding address
       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 significant **show ip ospf** display fields and their descriptions.

Table 9: show ospfv3 Field Descriptions

Field	Description
Supports NSSA (compatible with RFC 1587)	Specifies that RFC 1587 is active or that the OSPFv3 NSSA area is RFC 1587 compatible.
Configured to translate Type-7 LSAs, inactive (RFC3101 support disabled)	Specifies that the OSPFv3 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.

The output of the router LSA in LSDB shows Nt-Bit if it is set in the header of LSA.

```
Router Link States (Area 1)

  LS age: 94
  Options: (N-Bit, R-bit, DC-Bit, AF-Bit, Nt-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 2.2.2.2
  LS Seq Number: 80000002
  Checksum: 0x8AD5
  Length: 56
  Area Border Router
  AS Boundary Router
  Unconditional NSSA translator
  Number of Links: 2
```

The “Unconditional NSSA translator” line indicates that the status of the NSSA ASBR router is as a forced NSSA LSA translator.

Additional References for Configuring NSSA for OSPFv3

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
OSPFv3 in IPv6 routing	"IPv6 Routing: OSPFv3" module

RFCs

RFC	Title
RFC 1587	The OSPF NSSA Option
RFC 3101	The OSPF NSSA Option

Technical Assistance

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

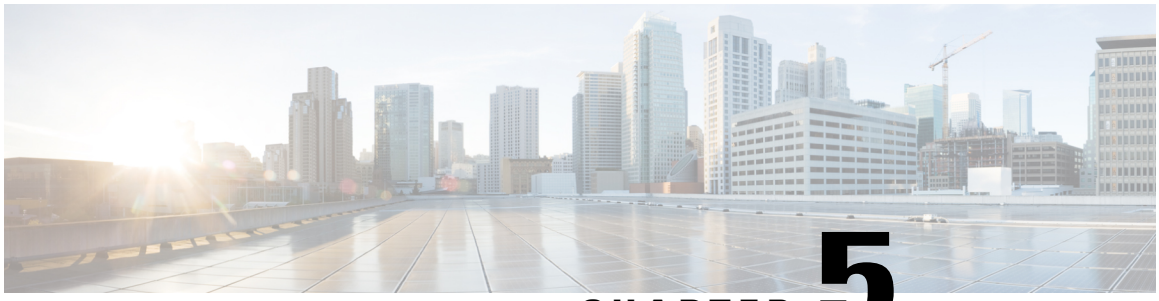
Feature Information for Configuring NSSA for OSPFv3

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

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

Table 10: Feature Information for Configuring NSSA for OSPFv3

Feature Name	Releases	Feature Information
OSPFv3 Support for NSSA	15.2(1)E	Cisco Open Short Shortest Path First version 3 (OSPFv3) allows you to configure a Not-So-Stubby Area (NSSA). An NSSA is similar to a stub area, except that an NSSA allows you to import autonomous system (AS) external routes within an NSSA using redistribution. This feature adds support for the OSPFv3 NSSA specification described by RFC 3101. RFC 3101 replaced and is backward compatible with RFC 1587. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **area nssa translate**, **compatible rfc1587**, **show ospfv3**.



CHAPTER 5

IPv6 Routing: OSPFv3 Authentication Support with IPsec

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

- Finding Feature Information, page 51
- Prerequisites for IPv6 Routing: OSPFv3 Authentication Support with IPsec, page 51
- Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec, page 52
- How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec, page 53
- Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec, page 55
- Additional References, page 56
- Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec, page 57

Finding Feature Information

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

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

Prerequisites for IPv6 Routing: OSPFv3 Authentication Support with IPsec

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

Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec

OSPFv3 Authentication Support with IPsec

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

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

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

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

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

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

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

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

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

How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec

Configuring IPsec on OSPFv3

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

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

You can configure authentication and encryption on virtual links.

Defining Authentication on an Interface

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.

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

Defining Authentication in an OSPFv3 Area

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router ospf** *process-id* **Example:** `Device(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**area** *area-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* **Example:** `Device(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	Enables authentication in an OSPFv3 area.

Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Example: Defining Authentication on an Interface

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

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

Example: Defining Authentication in an OSPFv3 Area

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

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

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec	"*Configuring OSPF*" module

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

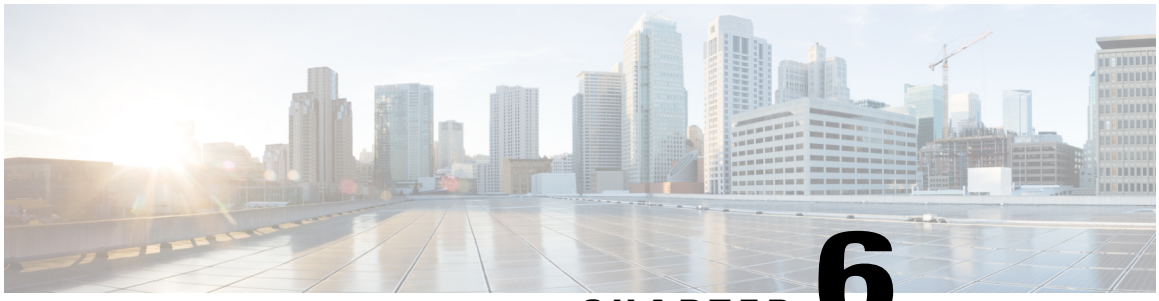
Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec

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

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

Table 11: Feature Information for IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec

Feature Name	Releases	Feature Information
IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec	15.0(2)SE	OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. In Cisco IOS 15.0(2)SE, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **area authentication (IPv6)**, **ipv6 ospf authentication**, **ipv6 router ospf**, **ospfv3 authentication**.



CHAPTER 6

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 59
- Prerequisites for OSPF Enhanced Traffic Statistics, page 60
- Information About OSPF Enhanced Traffic Statistics, page 60
- How to Display and Clear OSPF Enhanced Traffic Statistics, page 60
- Configuration Examples for OSPF Enhanced Traffic Commands, page 62
- Additional References, page 65
- Feature Information for OSPF Enhanced Traffic Statistics, page 67

Finding Feature Information

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

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

Prerequisites for 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ip ospf traffic statistics`	Displays OSPFv2 traffic statistics.
Step 3	**clear ip ospf traffic** **Example:** `Router# clear ip ospf traffic`	Clears OSPFv2 traffic statistics.

Displaying and Clearing OSPF Traffic Statistics for OSPFv3

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

	Command or Action	Purpose
Step 3	**clear ipv6 ospf traffic** **Example:** `Router# 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:

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

```
  RX LS req     0                   0
  RX LS upd     0                   0
  RX LS ack     0                   0
  RX Total      0                   0
  TX Failed     0                   0
  TX Hello      16                  1216
  TX DB des     0                   0
  TX LS req     0                   0
  TX LS upd     0                   0
  TX LS ack     0                   0
  TX Total      16                  1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  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:

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

Displaying and Clearing Enhanced Traffic Statistics for OSPFv3 Example

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

```
Router# show ipv6 ospf traffic

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

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

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

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

Additional References

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

Related Documents

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

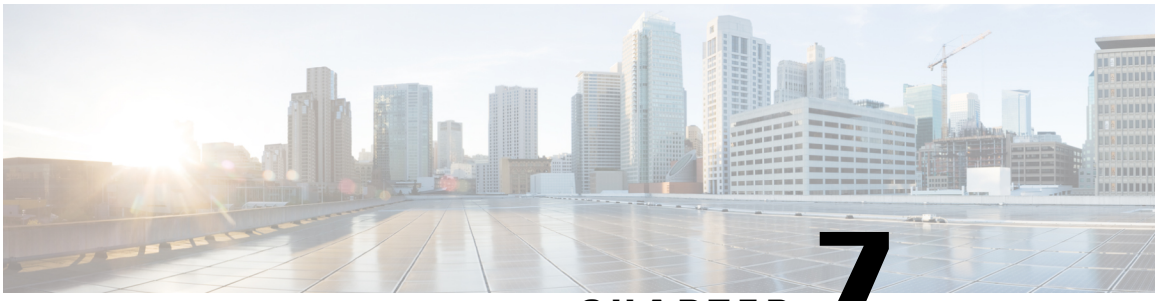
Feature Information for OSPF Enhanced Traffic Statistics

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: 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 Release 15.1(1)SG	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. In Cisco IOS 15.1(1) SG, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **clear ipv6 ospf traffic**, **show ip ospf traffic**, **show ipv6 ospf traffic**.



CHAPTER 7

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 69
- Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields, page 70
- Information About SNMP ifIndex Value for Interface ID in Data Fields, page 70
- How to Configure SNMP ifIndex Value for Interface ID in Data Fields, page 71
- Configuration Examples for SNMP ifIndex Value for Interface ID in Data Fields, page 72
- Additional References, page 76
- Feature Information for OSPF SNMP ifIndex Value for Interface ID, page 77

Finding Feature Information

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

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

Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields

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

Information About SNMP ifIndex Value for Interface ID in Data Fields

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

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

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

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

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

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

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

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

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

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

Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **router ospf** *process-id* [**vrf** *vpn-name*] • • **ipv6 router ospf** *process-id*	Configures an OSPFv2 routing process and enters router configuration mode. Configures an OSPFv3 routing process and enters router configuration mode.

	Command or Action	Purpose

	Example:
	`Router(config)# router ospf 4`
	Example:
	Example:
	`Router(config)# ipv6 router ospf 4`
		Note If you configure an OSPFv3 routing process, that uses IPv6, you must have already enabled IPv6.

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

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

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2

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

```
Router# configure terminal
```

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

Serial13/0: Ifindex = 53
```

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3

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

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

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

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

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

```
  LS age: 151
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 1006
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x6E24
  Length: 44
  Referenced LSA Type: 2002
  Referenced Link State ID: 6
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:1::
  Prefix Length: 64, Options: None, Metric: 0
Router# show ipv6 ospf database router

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
Router Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 5 (DoNotAge)
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000004
  Checksum: 0xEE5C
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 70
      Neighbor Interface ID: 71
      Neighbor Router ID: 172.16.0.1
LS age: 162
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xCE7C
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 71
      Neighbor Interface ID: 70
      Neighbor Router ID: 10.0.0.1
Router Link States (Area 1)
Routing Bit Set on this LSA
LS age: 176
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 10.0.0.1
LS Seq Number: 80000003
Checksum: 0xC807
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
LS age: 175
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xBD10
Length: 40
```

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

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

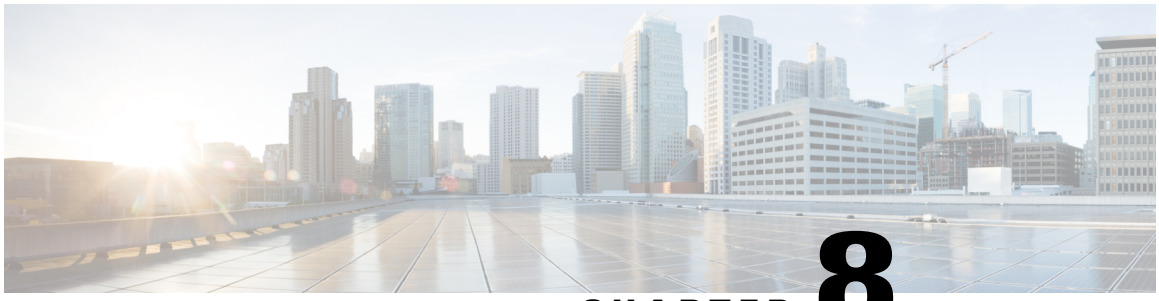
Feature Information for OSPF SNMP ifIndex Value for Interface ID

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

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

Table 13: 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 Release 15.1(1)SG	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. In Cisco IOS 15.1(1) SG, support was added for the Cisco Catalyst 4000 Series Switches. The following command is introduced or modified by the feature documented in this module: **interface-id snmp-if-index**



CHAPTER 8

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 79
- Prerequisites for Excluding Connected IP Prefixes from LSAs, page 80
- Information About Excluding Connected IP Prefixes from LSAs, page 80
- How to Exclude Connected IP Prefixes from OSPF LSAs, page 81
- Configuration Examples for Excluding Connected IP Prefixes from LSAs, page 86
- Additional References, page 87
- Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements, page 88
- Glossary, page 88

Finding Feature Information

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

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

Prerequisites for 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**prefix-suppression** **Example:** `Router(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:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf** **Example:** `Router# 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.

```
Router# show ip ospf

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

Excluding IP Prefixes on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf prefix-suppression** [**disable**] **Example:** `Router(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:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf interface**	Displays OSPF-related interface information.

	Command or Action	Purpose
	Example: `Router# 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 Ethernet interface 0/0.

```
Router# 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
.
.
.
```

Troubleshooting IP Prefix Suppression

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip ospf lsa-generation** **Example:** `Router# debug ip ospf lsa-generation`	Displays informations about each OSPF LSA generated.

	Command or Action	Purpose
Step 3	**debug condition interface** *interface-type interface-number* [**dlci** *dlci*] [**vc** {*vci* | *vpi* | *vci*}] **Example:** `Router# 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:** `Router# show debugging`	Displays information about the types of debugging that are enabled for your router.
Step 5	**show logging** [**slot** *slot-number* | **summary**] **Example:** `Router# 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.

```
Router# debug ip ospf lsa-generation

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

IP routing:
   OSPF summary lsa generation debugging is on
Condition 1: interface Et0/0 (1 flags triggered)
        Flags: Et0/0
Router# 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.

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

Excluding IP Prefixes from LSAs for a Specified Interface Example

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

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

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

```
Router# show ip ospf interface

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

Additional References

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

Related Documents

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

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

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

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

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

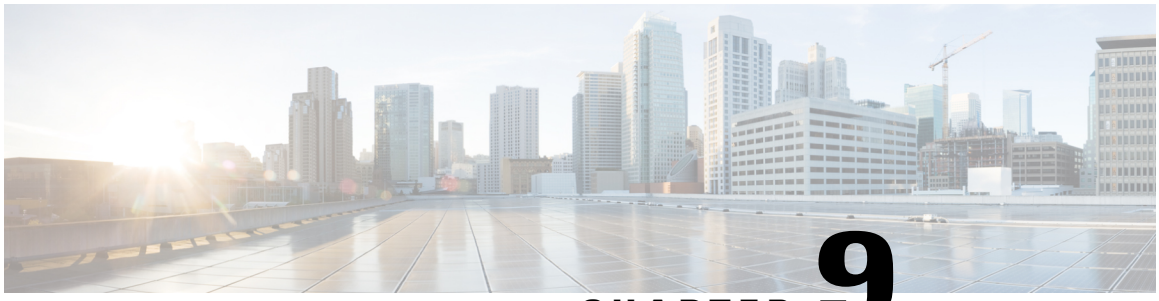
Table 14: Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

Feature Name	Releases	Feature Information
OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements	15.2(1)E	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. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. No new commands were introduced or modified.

Glossary

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

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



CHAPTER 9

OSPF Nonstop Routing

The OSPF Nonstop Routing feature allows a device with redundant Route Processors (RPs) to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned RP switchovers. The OSPF state is maintained by checkpointing the state information from OSPF on the active RP to the standby RP. After a switchover to the standby RP, OSPF uses the checkpointed information to continue operations without interruption.

- Finding Feature Information, page 91
- Restrictions for OSPF Nonstop Routing, page 91
- Information About OSPF Nonstop Routing, page 92
- How to Configure OSPF Nonstop Routing, page 92
- Configuration Examples for OSPF Nonstop Routing, page 94
- Additional References for OSPF Nonstop Routing, page 95
- Feature Information for OSPF Nonstop Routing, page 96

Finding Feature Information

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

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

Restrictions for OSPF Nonstop Routing

- OSPF Nonstop Routing (NSR) is available only for platforms with redundant RPs running Cisco IOS Release 15.1(2)S, 15.2(1)E, or later releases.
- OSPF NSR can significantly increase the memory used by OSPF during certain phases of its operation. CPU usage also can be increased. Before configuring OSPF NSR, you must be aware of the device

memory capacity and estimate the likely memory requirements of OSPF NSR. For more information, see the section Configuring OSPF NSR, on page 92. For devices in which memory and CPU are limited, consider using OSPF Nonstop Forwarding (NSF) instead. For more information, see RFC 3623, *OSPF Graceful Restart*.

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

Information About OSPF Nonstop Routing

OSPF NSR Functionality

Although OSPF Nonstop Routing (NSR) serves a similar function to OSPF Nonstop Forwarding (NSF), it works differently. With NSF, OSPF on the newly active standby RP initially has no state information. OSPF uses extensions to the OSPF protocol to recover its state from neighboring OSPF devices. For the recovery to work, the neighbors must support the NSF protocol extensions and be willing to act as “helpers” to the device that is restarting. The neighbors must also continue forwarding data traffic to the device that is restarting while protocol state recovery takes place.

With NSR, by contrast, the device that performs the switchover preserves its state internally, and in most cases the neighbors are unaware of the switchover. Because assistance is not needed from neighboring devices, NSR can be used in situations where NSF cannot be used; for example, in networks where not all neighbors implement the NSF protocol extensions, or where network topology changes during the recovery making NSF unreliable, use NSR instead of NSF.

How to Configure OSPF Nonstop Routing

Configuring OSPF NSR

Before You Begin

Ensure that Nonstop Routing (NSR) is supported on the device. The **nsr** command in router configuration mode is supported only on devices that support NSR.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Configures an OSPF routing process and enters router configuration mode.
Step 4	**nsr** **Example:** `Device(config-router)# nsr`	Configures NSR.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show ip ospf** [*process-id*] **nsr** [**objects** | **statistics**] **Example:** `Device# show ip ospf 109 nsr`	Displays OSPF NSR status information.

Troubleshooting Tips

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

```
Device# show processes|include OSPF

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

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

```
Device# show processes memory 276

Process ID: 276
Process Name: OSPF-1 Router
Total Memory Held: 4454800 bytes
```

In the above example, OSPF is using 4,454,800 bytes, or approximately 4.5 megabytes (MB). Because OSPF NSR can consume double this memory for brief periods, ensure that the device has at least 5 MB of free memory before enabling OSPF NSR.

Configuration Examples for OSPF Nonstop Routing

Example: Configuring OSPF NSR

The following example shows how to configure OSPF NSR:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 1
Device(config-router)# nsr
Device(config-router)# end
```

Example: Verifying OSPF NSR

The following is sample output from the **show ip ospf nsr** command. The output displays that OSPF NSR is configured and OSPF on the standby RP is fully synchronized and ready to continue operation if the active RP fails or if a manual switchover is performed.

```
Device# show ip ospf 1 nsr

Standby RP
 Operating in duplex mode
 Redundancy state: STANDBY HOT
 Peer redundancy state: ACTIVE
 ISSU negotiation complete
 ISSU versions compatible
Routing Process "ospf 1" with ID 10.1.1.100
 NSR configured
 Checkpoint message sequence number: 3290
 Standby synchronization state: synchronized
 Bulk sync operations:  1
 Last sync start time:  15:22:48.971 UTC Fri Jan 14 2011
 Last sync finish time: 15:22:48.971 UTC Fri Jan 14 2011
 Last sync lost time:   -
 Last sync reset time:  -
 LSA Count: 2, Checksum Sum 0x00008AB4
```

The following is sample output from the **show ip ospf nsr statistics** command. The output displays the current global and per OSPF instance state of NSR processing along with other statistics.

```
Device# show ip ospf nsr statistics

 Pending checkpoint requests (current/max): 0/109
```

```
Pending checkpoint messages (current/max): 0/109
Routing Process "ospf 1" with ID 10.1.1.100
Pending checkpoint requests (current/max): 0/109
Pending checkpoint messages (current/max): 0/109
Time spent scheduling bulk syncs (max): 0 ms
Time spent in checkpoint loop (average/max): 1/9 ms
Checkpoint loop interruptions: 0
```

Additional References for OSPF Nonstop Routing

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Configuring IETF NSF or Cisco NSF	"Configuring NSF-OSPF" module in the *Cisco IOS High Availability Configuration Guide*

Standard and RFCs

Standard/RFC	Title
RFC 2328	*OSPF Version 2*
RFC 3623	*Graceful OSPF Restart*

Technical Assistance

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

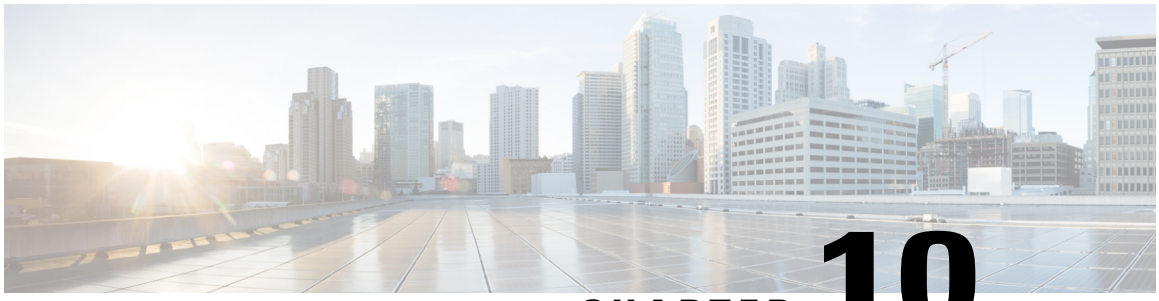
Feature Information for OSPF Nonstop Routing

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

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

Table 15: Feature Information for OSPF Nonstop Routing

Feature Name	Releases	Feature Information
OSPF NSR	15.2(1)E	The OSPF Nonstop Routing feature allows a device with redundant Route Processors to maintain its OSPF state and adjacencies across planned and unplanned RP switchovers. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. In Cisco IOS Release 15.2(1)E, the following commands were introduced: **clear ip ospf nsr**, **debug ip ospf ha**, **debug ip ospf nsr**.



CHAPTER 10

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 97
- Prerequisites for OSPFv2 Local RIB, page 98
- Restrictions for OSPFv2 Local RIB, page 98
- Information About OSPFv2 Local RIB, page 98
- How to Configure the OSPFv2 Local RIB Feature, page 98
- Configuration Examples for the OSPFv2 Local RIB Feature, page 102
- Additional References, page 103
- Feature Information for the OSPFv2 Local RIB Feature, page 104

Finding Feature Information

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

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

Prerequisites for 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

Function of the OSPF Local RIB

A device 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, OSPF installs discard routes to null0 for any area range (internal) or summary-address (external) prefixes that it advertises to other devices. 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.

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.

How to Configure the OSPFv2 Local RIB Feature

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. This section describes the following optional tasks:

Changing the Default Local RIB Criteria

Note It is recommended that you not change the default values because they are conservative and preserve the current global RIB behavior.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf** *process-id* **rib** [**redistribution**] [*network-prefix*] [*network-mask*] [**detail**] **Example:** `Router# show ip ospf 23 rib`	Displays information for the OSPF local RIB or locally redistributed routes.

Changing the Administrative Distance for Discard Routes

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**discard-route** [**external** [*distance*]] [**internal** [*distance*]] **Example:** `Router(config-router)# discard-route external 150`	Reinstalls either an external or internal discard route that was previously removed. **Note** You can now specify the administrative distance for internal and external discard routes.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**] **Example:** `Router# show ip route ospf 23`	Displays the current state of the routing table. **Note** Entering the **show ip route** command will verify the changed administrative distance values for external and internal discard routes.

Examples

The sample output displayed for the **show ip route** command confirms that the administrative distance for the IP route 192.168.0.0 255.255.255.0 is 110.

```
Router# show ip route 192.168.0.0 255.255.255.0

Routing entry for 192.168.0.0/24
Known via "ospf 1", distance 110, metric 0, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
```

Troubleshooting Tips

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 the OSPFv2 Local RIB Feature

Example: Changing the Default Local RIB Criteria

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

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

Example: Changing the Administrative Distance for Discard Routes

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

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

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

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

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

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

Additional References

The following sections provide references related to the OSPFv2 Local RIB feature.

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
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

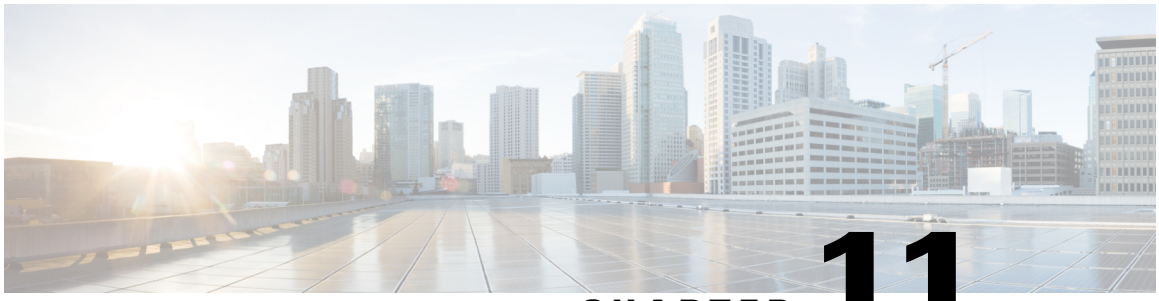
Feature Information for the OSPFv2 Local RIB Feature

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

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

Table 16: Feature Information for the OSPFv2 Local RIB Feature

Feature Name	Releases	Feature Information
OSPFv2 Local RIB	15.1(1)SG	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. In Cisco IOS 15.2(1)SG, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **debug ip ospf rib**, **discard-route**, **local-rib-criteria**, **show ip ospf rib**.



CHAPTER 11

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 107
- Prerequisites for IPv6 Routing: OSPFv3, page 107
- Restrictions for IPv6 Routing: OSPFv3, page 108
- Information About IPv6 Routing: OSPFv3, page 108
- How to Configure Load Balancing in OSPFv3, page 113
- Configuration Examples for Load Balancing in OSPFv3, page 122
- Additional References, page 123
- Feature Information for IPv6 Routing: OSPFv3, page 124

Finding Feature Information

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

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

Prerequisites for 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.

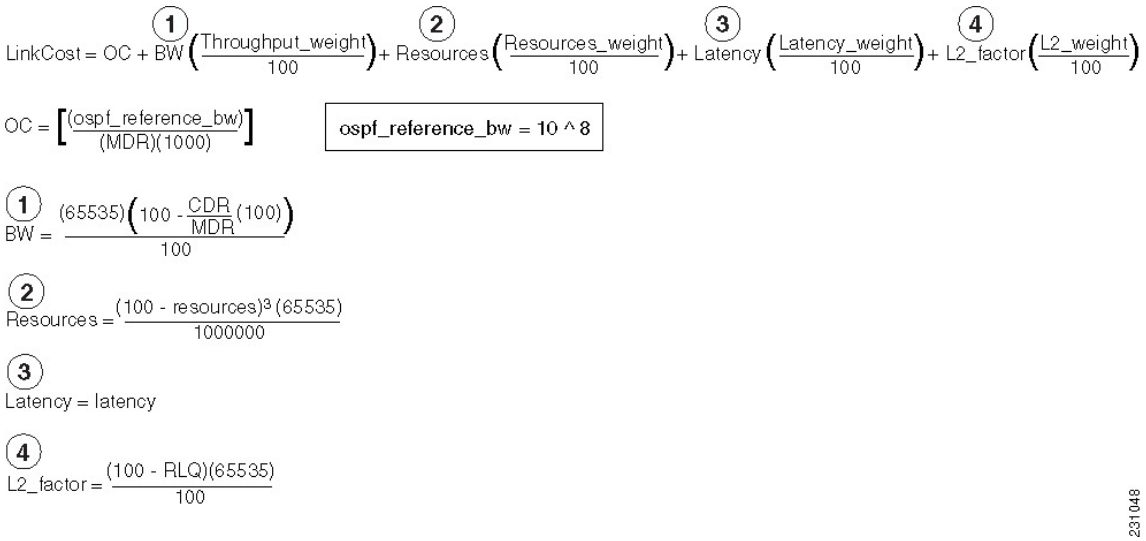
Caution Be careful when changing the defaults. Changing defaults will affect your OSPFv3 network, possibly adversely.

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 5: Overall Link Cost Formula



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

Table 17: 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.

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

DETAILED STEPS

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

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

	Command or Action	Purpose
Step 12	**queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**} **Example:** `Device(config-router)# queue-depth update 1500`	Configures the number of incoming packets that the IPv4 OSPFv3 process can keep in its queue.
Step 13	**router-id** *router-id* **Example:** `Device(config-router)# router-id 10.1.1.1`	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. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. **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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **Example:** `Device(config-if)# frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120`	Defines the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address. • In this example, the NBMA link is Frame Relay. For other kinds of NBMA links, different mapping commands are used.
Step 5	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **Example:** `Device(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	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. • Enter your password if prompted.
Step 2	**clear ospfv3** [*process-id*] **force-spf** **Example:** `Device# clear ospfv3 1 force-spf`	Runs SPF calculations for an OSPFv3 process. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 3	**clear ospfv3** [*process-id*] **process** **Example:** `Device# clear ospfv3 2 process`	Resets an OSPFv3 process. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 4	**clear ospfv3** [*process-id*] **redistribution** **Example:** `Device# clear ospfv3 redistribution`	Clears OSPFv3 route redistribution. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 5	**clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} **Example:** `Device# clear ipv6 ospf force-spf`	Clears the OSPFv3 state based on the OSPFv3 routing process ID, and forces the start of the SPF algorithm. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration.

	Command or Action	Purpose
		• 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
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**show ospfv3** [*process-id*] [*address-family*] **border-routers** **Example:** `Device# show ospfv3 border-routers`	Displays the internal OSPFv3 routing table entries to an ABR and ASBR.
Step 3	**show ospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**] **Example:** `Device# show ospfv3 database`	Displays lists of information related to the OSPFv3 database for a specific device.
Step 4	**show ospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **Example:** `Device# show ospfv3 events`	Displays detailed information about OSPFv3 events.
Step 5	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number* **Example:** `Device# show ospfv3 flood-list`	Displays a list of OSPFv3 LSAs waiting to be flooded over an interface.
Step 6	**show ospfv3** [*process-id*] [*address-family*] **graceful-restart** **Example:** `Device# show ospfv3 graceful-restart`	Displays OSPFv3 graceful restart information.
Step 7	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**] **Example:** `Device# show ospfv3 interface`	Displays OSPFv3-related interface information.

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

Configuration Examples for Load Balancing in OSPFv3

Example: Configuring the OSPFv3 Device Process

```
Device# show ospfv3 database
            OSPFv3 Device with ID (172.16.4.4) (Process ID 1)
                Device Link States (Area 0)
ADV Device         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Device Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Dest DevID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0


Device# show ospfv3 neighbor

OSPFv3 Device with ID (10.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.4.4.4        1    FULL/  -        00:00:39    12              vm1
OSPFv3 Device with ID (10.2.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.5.4.4          1    FULL/  -        00:00:35    12              vm1
```

Example: 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 serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
 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	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
IPv6 Routing: OSPFv3	"*Configuring OSPF*" module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

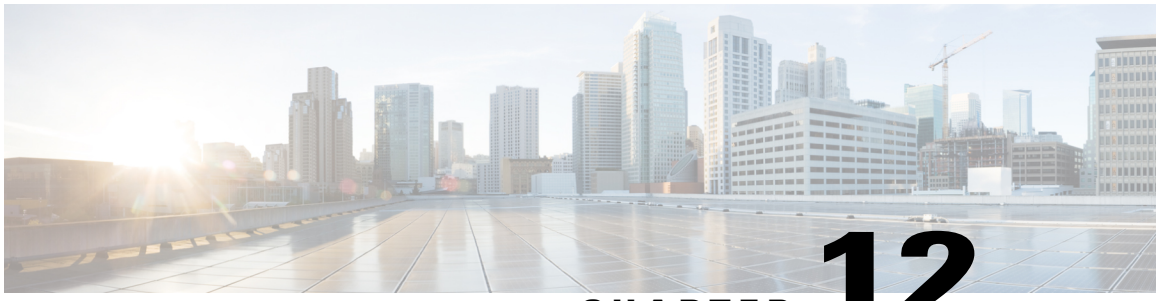
Feature Information for IPv6 Routing: OSPFv3

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

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

Table 19: Feature Information for IPv6 Routing: OSPFv3

Feature Name	Releases	Feature Information
IPv6 Routing: OSPFv3	12.2(25)SG 15.0(2)SG	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 15.0(2)SG, support was added for the Cisco Catalyst 4000 Series Switches.



CHAPTER 12

OSPFv3 Demand Circuit Ignore

This feature enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** command.

- Finding Feature Information, page 125
- Information About OSPFv3 Demand Circuit Ignore, page 125
- How to Configure OSPFv3 Demand Circuit Ignore, page 126
- Configuration Examples for OSPFv3 Demand Circuit Ignore, page 127
- Additional References for OSPFv3 Demand Circuit Ignore, page 127
- Feature Information for OSPFv3 Demand Circuit Ignore, page 128

Finding Feature Information

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

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

Information About OSPFv3 Demand Circuit Ignore

Demand Circuit Ignore Support

Demand Circuit Ignore Support enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** command. Demand circuit ignore instructs the router not to accept Demand Circuit (DC) negotiation and is a useful configuration option on the point-to-multipoint interface of the Hub router.

How to Configure OSPFv3 Demand Circuit Ignore

Configuring Demand Circuit Ignore Support for OSPFv3

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/1/0`	Configures an interface type and number and enters interface configuration mode.
Step 4	Enter one of the following commands: • **ipv6 ospf demand-circuit ignore** • **ospfv3 demand-circuit ignore**	Prevents an interface from accepting demand-circuit requests from other devices.

	Command or Action	Purpose

	Example:
	`Device(config-if)# ipv6 ospf demand-circuit ignore`
	Example:
	`Device(config-if)# ospfv3 demand-circuit ignore`	

Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ospfv3** *process-id* [*area-id*] [*address-family*] **[vrf** {*vrf-name* **|*** }] **interface** [*type number*] [**brief**] **Example:** `Device# show ospfv3 interface GigabitEthernet 0/1/0`	(Optional) Displays OSPFv3-related interface information.

Configuration Examples for OSPFv3 Demand Circuit Ignore

Example: Demand Circuit Ignore Support for OSPFv3

The following example shows how to configure demand circuit ignore support for OSPFv3:

```
interface Serial0/0
 ip address 6.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 network point-to-multipoint
 ospfv3 demand-circuit ignore
 ospfv3 1 ipv6 area 0
```

Additional References for OSPFv3 Demand Circuit Ignore

The following sections provide references related to the OSPFv3 Demand Circuit Ignore feature.

Related Documents

Related Topic	Document Title
OSPF configuration tasks	“Configuring OSPF”

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

Technical Assistance

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

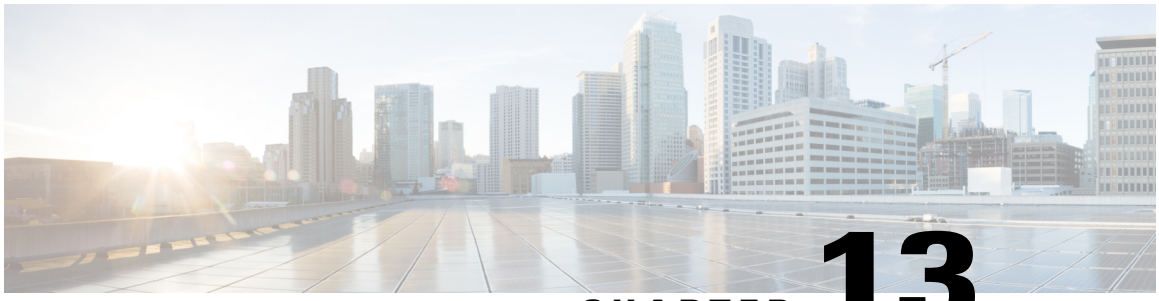
Feature Information for OSPFv3 Demand Circuit Ignore

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

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

Table 20: Feature Information for OSPFv3 Demand Circuit Ignore

Feature Name	Releases	Feature Information
OSPFv3 Demand Circuit Ignore	Cisco IOS Release 15.2(1)E	The OSPFv3 Demand Circuit Ignore feature enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** command. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: • **ipv6 ospf demand-circuit** • **ospfv3 demand-circuit**



CHAPTER 13

OSPFv3 Max-Metric Router LSA

The Open Shortest Path First version 3 (OSPFv3) max-metric router link-state advertisement (LSA) feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through the device if there are better alternate paths.

- Finding Feature Information, page 131
- Information About OSPFv3 Max-Metric Router LSA, page 131
- How to Configure OSPFv3 Max-Metric Router LSA, page 132
- Configuration Examples for OSPFv3 Max-Metric Router LSA, page 133
- Additional References, page 134
- Feature Information for OSPFv3 Max-Metric Router LSA, page 135

Finding Feature Information

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

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

Information About OSPFv3 Max-Metric Router LSA

OSPFv3 Max-Metric Router LSA

The OSPFv3 max-metric router LSA feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through

the device if there are better alternate paths. After a specified timeout or a notification from Border Gateway Protocol (BGP), OSPFv3 advertises the LSAs with normal metrics.

The max-metric LSA control places the OSPFv3 router into the stub router role using its LSA advertisement. A stub router only forwards packets destined to go to its directly connected links. In OSPFv3 networks, a device could become a stub router by advertising large metrics for its connected links, so that the cost of a path through this device becomes larger than that of an alternative path. OSPFv3 stub router advertisement allows a device to advertise the infinity metric (0xFFFF) for its connected links in router LSAs and advertise the normal interface cost if the link is a stub network.

How to Configure OSPFv3 Max-Metric Router LSA

Configuring the OSPFv3 Max-Metric Router LSA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **address-family ipv6 unicast**
5. **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]]
6. **end**
7. **show ospfv3** [*process-id*] **max-metric**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode.

	Command or Action	Purpose
Step 4	**address-family ipv6 unicast** **Example:** `Device(config)# address-family ipv6 unicast`	Configures an instance of the OSPFv3 process in the IPv6 address family.
Step 5	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]] **Example:** `Device(config-router-af)# max-metric router-lsa on-startup wait-for-bgp`	Configures a device that is running the OSPFv3 protocol to advertise a maximum metric so that other devices do not prefer the device as an intermediate hop in their SPF calculations.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.
Step 7	**show ospfv3** [*process-id*] **max-metric** **Example:** `Device# show ospfv3 1 max-metric`	Displays OSPFv3 maximum metric origination information.

Configuration Examples for OSPFv3 Max-Metric Router LSA

Example: Verifying the OSPFv3 Max-Metric Router LSA

```
Router# show ipv6 ospf max-metric

           OSPFv3 Router with ID (192.1.1.1) (Process ID 1)

 Start time: 00:00:05.886, Time elapsed: 3d02h
 Originating router-LSAs with maximum metric
    Condition: always, State: active
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
OSPFv3 Max-Metric Router LSA	"*OSPF Link-State Advertisement Throttling* " module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

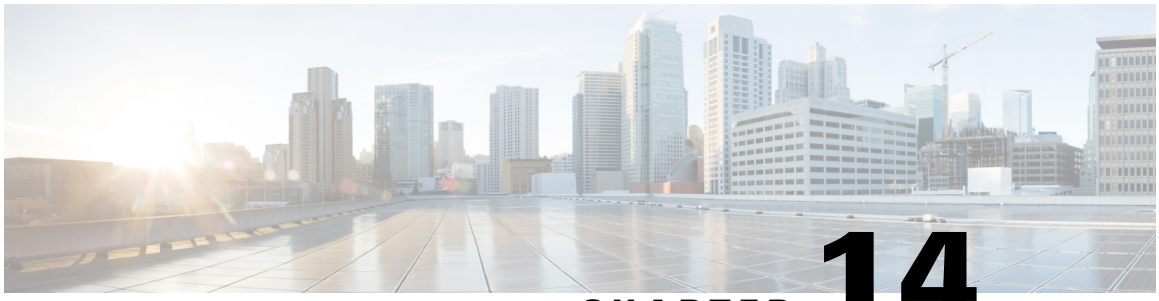
Feature Information for OSPFv3 Max-Metric Router LSA

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

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

Table 21: Feature Information for OSPFv3 Max-Metric Router LSA

Feature Name	Releases	Feature Information
OSPFv3 Max-Metric Router LSA	15.2(1)E	The OSPFv3 max-metric router LSA feature enables OSPF to advertise its locally generated router LSAs with a maximum metric. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **max-metric router-lsa**, **show ipv6 ospf max-metric**, **show ospfv3 max-metric**.



CHAPTER 14

OSPFv3 MIB

The OSPFv3 MIB feature enables remote monitoring and troubleshooting of Open Shortest Path First version 3 (OSPFv3) processes using standard Simple Network Management Protocol (SNMP) management workstations. The protocol information collected by the OSPFv3 MIB objects and trap objects can be used to derive statistics that helps monitor and improve overall network performance.

- Finding Feature Information, page 137
- Prerequisites for OSPFv3 MIB , page 137
- Restrictions for OSPFv3 MIB Support, page 138
- Information About OSPFv3 MIB, page 138
- How to Configure OSPFv3 MIB, page 138
- Configuration Examples for OSPFv3 MIB, page 141
- Additional References for OSPFv3 MIB, page 141
- Feature Information for OSPFv3 MIB , page 142

Finding Feature Information

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

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

Prerequisites for OSPFv3 MIB

- Ensure that Open Shortest Path First version 3 (OSPFv3) is configured on the device.
- Ensure that Simple Network Management Protocol (SNMP) is enabled on the device before notifications (traps) can be configured or before SNMP GET operations can be performed.

Restrictions for OSPFv3 MIB Support

- To monitor multiple Open Shortest Path First version 3 (OSPFv3) processes, each process must be associated with a Simple Network Management Protocol (SNMP) context.
- To monitor multiple VRFs, each VRF must be associated with an SNMP context.

Information About OSPFv3 MIB

OSPFv3 MIB

Open Shortest Path First version 3 (OSPFv3) is the IPv6 implementation of OSPF. The OSPFv3 MIB is documented in RFC 5643 and defines a MIB for managing OSPFv3 processes through Simple Network Management Protocol (SNMP).

Users can constantly monitor the changing state of an OSPF network by using MIB objects. The MIB objects gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes.

OSPFv3 TRAP MIB

The ospfv3Notifications MIB object contains the OSPFv3 trap MIB objects that enable and disable OSPF traps in the Cisco IOS CLI. These OSPFv3 trap MIB objects are provided by the RFC 5643 standard OSPFv3 MIB.

How to Configure OSPFv3 MIB

Enabling Specific OSPFv3 Traps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. **snmp-server enable traps ospfv3 errors** [**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**]
5. **snmp-server enable traps ospfv3 rate-limit** *seconds trap-number*
6. **snmp-server enable traps ospfv3 state-change** [**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Device(config)# snmp-server host 172.20.2.162 version 2c public ospfv3`	Specifies a recipient (target host) for Simple Network Management Protocol (SNMP) notification operations. • If the *notification-type* is not specified, all enabled notifications (traps or informs) are sent to the specified host. • If you want to send only the Open Shortest Path First version 3 (OSPFv3) notifications to the specified host, you can use the optional **ospfv3** keyword as the *notification-types* . Entering the **ospfv3** keyword enables the ospfv3Notifications MIB object.
Step 4	**snmp-server enable traps ospfv3 errors** [**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**] **Example:** `Device(config)# snmp-server enable traps ospfv3 errors`	Enables SNMP notifications for OSPFv3 errors.
Step 5	**snmp-server enable traps ospfv3 rate-limit** *seconds trap-number* **Example:** `Device(config)# snmp-server enable traps ospfv3 rate-limit 20 20`	Sets the rate limit for the number of SNMP OSPFv3 notifications that are sent in each OSPFv3 SNMP notification rate-limit window.
Step 6	**snmp-server enable traps ospfv3 state-change** [**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**]	Enables SNMP OSPFv3 notifications for OSPFv3 transition state changes.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server enable traps ospfv3 state-change`	
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Verifying OSPFv3 MIB Traps on the Device

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show running-config** [*options*]

Example:

```
Device# show running-config | include traps
```

Displays the contents of the currently running configuration file and includes information about enabled traps.

- Verifies which traps are enabled.

Configuration Examples for OSPFv3 MIB

Example: Enabling and Verifying OSPFv3 MIB Traps

The following example shows how to enable all OSPFv3 error traps:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps ospfv3 errors
Device(config)# end
```

The following example shows how to verify that the traps are enabled:

```
Device> enable
Device# show running-config | include traps

snmp-server enable traps ospfv3 errors
```

Additional References for OSPFv3 MIB

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
OSPF configuration tasks	"Configuring OSPF" module in *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard	Title
RFC 5643	*Management Information Base for OSPFv3*

MIBs

MIB	MIBs Link
OSPFv3-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

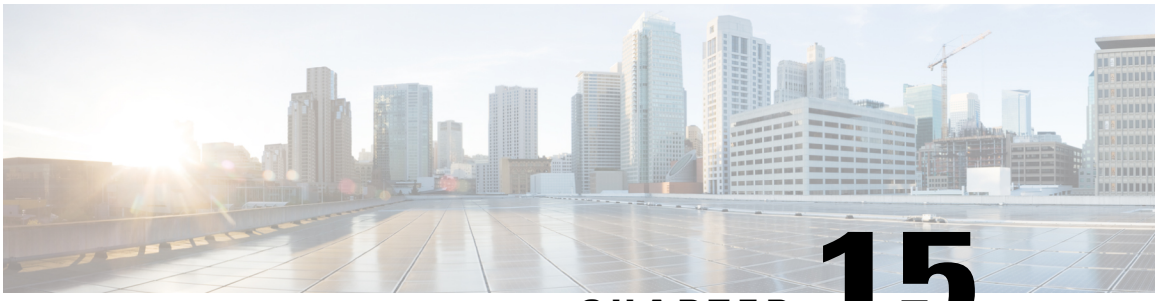
Feature Information for OSPFv3 MIB

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

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

Table 22: Feature Information for OSPFv3 MIB

Feature Name	Releases	Feature Information
OSPFv3 MIB	15.2(1)E	The OSPFv3 MIB feature enables remote monitoring and troubleshooting of OSPFv3 processes using standard SNMP management workstations. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **snmp-server host**, **snmp-server enable traps ospfv3 errors**, **snmp-server enable traps ospfv3 rate-limit**, **snmp-server enable traps ospfv3 state-change**.



CHAPTER 15

OSPFv3 VRF-Lite/PE-CE

The OSPFv3 VRF-Lite/PE-CE feature adds Open Shortest Path First version 3 (OSPFv3) support for nondefault VPN routing and forwarding (VRF) instances. OSPFv3 can be used as a provider-edge-customer-edge (PE-CE) routing protocol as specified in RFC 6565, *OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*. OSPFv3 in a nondefault VRF instance supports routing of IPv4 and IPv6 address families.

- Finding Feature Information, page 143
- Restrictions for OSPFv3 VRF-Lite/PE-CE, page 143
- Information About OSPFv3 VRF-Lite/PE-CE, page 144
- How to Configure VRF-Lite/PE-CE, page 145
- Configuration Examples for OSPFv3 VRF-Lite/PE-CE, page 153
- Additional References for OSPFv3 VRF-Lite/PE-CE, page 155
- Feature Information for OSPFv3 VRF-Lite/PE-CE, 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 at the end of this module.

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

Restrictions for OSPFv3 VRF-Lite/PE-CE

In Cisco IOS Release 15.2(2)S and later releases, OSPFv3 interface commands in the **ipv6 ospf** format are no longer supported in VRF interface configuration mode. You must configure them in the new format, **ospfv3**.

The **ospfv3** commands can have one of following formats:

- **ospfv3 —**Applies to all OSPFv3 processes and address families on a given interface.

- **ospfv3** *process-id* —Applies to an OSPFv3 process with the configured process ID and to both IPv4 and IPv6 address families.
- **ospfv3** *process-id address-family-ID* —Applies to an OSPFv3 process with the configured process ID and the configured address family.

More specific commands take precedence over less specific commands, as shown in the following descending order:

1. Commands that specify a process ID and an address family.
2. Commands that specify only a process ID.
3. Commands that specify neither a process ID nor an address family.

In Cisco IOS Release 15.2(2)S and later releases, you cannot use the **ipv6 ospf router** *process-id* command to configure OSPFv3 VRF instances. You must configure the **router ospfv3** *process-id* command in global configuration mode and specify the address family for the configured VRF in router configuration mode.

Information About OSPFv3 VRF-Lite/PE-CE

Support for OSPFv3 VRF-Lite and PE-CE

Open Shortest Path First version 3 (OSPFv3) operates in nondefault VPN routing and forwarding (VRF) instances for both IPv6 and IPv4 address families and, transports the routes across a Border Gateway Protocol (BGP) or a Multiprotocol Label Switching (MPLS) backbone. On the provider edge (PE) device, customer routes are installed together by OSPFv3 and BGP in a common VRF or address family and each protocol is configured to redistribute the routes of the other. BGP combines the prefixes redistributed into it with a route-distinguisher value defined for the VRF and advertises them to other MPLS-BGP speakers in the same autonomous system using the VPNv4 or VPNv6 address family as appropriate.

The OSPFv3 route selection algorithm prefers intra-area routes across the back-door link over inter-area routes through the MPLS backbone. Sham-links are a type of virtual link across the MPLS backbone that connect OSPFv3 instances on different PEs. OSPFv3 instances tunnel protocol packets through the backbone and form adjacencies. Because OSPFv3 considers the sham-link as an intra-area connection, sham-link serves as a valid alternative to an intra-area back-door link.

Domain IDs are used to determine whether the routes are internal or external. They describe the administrative domain of the OSPFv3 instance from which the route originates. Every PE has a 48-bit primary domain ID (which may be NULL) and zero or more secondary domain IDs.

How to Configure VRF-Lite/PE-CE

Configuring a VRF in an IPv6 Address Family for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Configures an OSPF routing process and enters router configuration mode.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters router address family configuration mode.
Step 8	**end** **Example:** `Device(config-router-af)# end`	Exists router address family configuration mode and returns to privileged EXEC mode.

Enabling an OSPFv3 IPv6 Address Family on a VRF Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
5. **ipv6 enable**
6. **ospfv3** *process-id* {**ipv4** | **ipv6**} **area** *area-id* [**instance** *instance-id*]
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Serial6/0`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] **Example:** `Device(config-if)# vrf forwarding v1`	Associates an interface with a VRF.
Step 5	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the interface that is associated with the VRF.
Step 6	**ospfv3** *process-id* {**ipv4** | **ipv6**} **area** *area-id* [**instance** *instance-id*] **Example:** `Device(config-if)# ospfv3 1 ipv6 area 0`	Enables the OSPFv3 IPv6 address family on the VRF interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a Sham-Link for OSPFv3 PE-CE

Before You Begin

The OSPFv3 PE-CE feature supports direct forwarding on Border Gateway Protocol (BGP) routes.

Before you configure a sham-link, you must create a Multiprotocol Label Switching (MPLS) backbone, configure a device as an MPLS VPN PE device, and configure OSPFv3 as the provider-edge-customer-edge (PE-CE) protocol in a virtual routing and forwarding (VRF) instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **description** *string*
5. **vrf forwarding** *vrf-name*
6. **ipv6 address** *ipv6-address/prefix-length*
7. **ipv6 enable**
8. **end**
9. **router ospfv3** *process-id*
10. **address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf** *vrf-name*]
11. **redistribute** *process-id* [*options*]
12. **area** *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**ttl-security hops** *hop-count*]
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface loopback** *interface-number* **Example:** `Device(config)# interface loopback 0`	Creates a loopback interface to be used as an endpoint of the sham-link on a provider edge device and enters interface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-if)# description Sham-link endpoint`	Provides a description of the interface to help you track its status.
Step 5	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding vrf1`	Associates the loopback interface with a VRF.

	Command or Action	Purpose
Step 6	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/48`	Configures an IPv6 address of the loopback interface on a provider edge device.
Step 7	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the loopback interface.
Step 8	**end** **Example:** `Device# end`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Enters router configuration mode.
Step 10	**address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Enters IPv6 address family configuration mode for OSPFv3.
Step 11	**redistribute** *process-id* [*options*] **Example:** `Device(config-router-af)# redistribute bgp 2`	Redistributes IPv6 routes from the specified source BGP routing domain into the specified destination routing domain. **Note** PE-CE redistribution is always from BGP.
Step 12	**area** *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**ttl-security hops** *hop-count*] **Example:** `Device(config-router-af)# area 0 sham-link 2001:DB8:0:ABCD::1 2001:DB8:0:ABCD::2 cost 100`	Enables the sham-link and specifies its source and destination addresses.
Step 13	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Configuring a Domain ID for an OSPFv3 PE-CE

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **domain-id type** *type* **value** *hex-value*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Enters router configuration mode.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters address family configuration mode..
Step 8	**domain-id type** *type* **value** *hex-value* **Example:** `Device(config-router-af)# domain-id type 0205 value 800EFFFF12AB`	Configures the BGP domain ID. • The value for **type** can be 0005, 0105, 0205, or 8005. • The value for **value** is an arbitrary 48-bit number encoded as 12 hexadecimal digits.
Step 9	**end** **Example:** `Device(config-router-af)# end`	Exists router address family mode and returns to privileged EXEC mode.

Configuring VRF-Lite Capability for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **capability vrf-lite**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Enables router configuration mode for the IPv4 or IPv6 address family.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters address family configuration mode.
Step 8	**capability vrf-lite** **Example:** `Device(config-router-af)# capability vrf-lite`	Applies the multi-VRF capability to the OSPF process.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-router-af)# end`	Exists router address family mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv3 VRF-Lite/PE-CE

Example: Configuring a Provider Edge Device to Provide IPv6 and IPv4 Routing

The following example shows how to configure a provider edge (PE) device to provide IPv6 and IPv4 routing for a user on VRF “v1” and IPv6 routing for a user on VRF “v2”:

```
vrf definition v1
 rd 1:1
 route-target export 100:1
 route-target import 100:1
!
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 route-target export 200:2
 route-target import 200:2
!
address-family ipv6
 exit-address-family
!
interface Loopback1
 vrf forwarding v1
 ipv6 address 2001:DB8:0:ABCD::1/48
!
interface Serial5/0
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:0:ABCD::3/48
 ospfv3 1 ipv6 area 1
!
interface Serial6/0
 vrf forwarding v1
 ip address 10.0.0.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 10.1.1.1
!
router ospfv3
!
log-adjacency-changes detail
!
address-family ipv4 unicast vrf v1
 router-id 10.2.2.2
 redistribute bgp 1
```

```
 exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 2001:DB8:1::1
 domain-id type 0205 value 111111222222
 area 0 sham-link 2001:DB8:0:ABCD::5 2001:DB8:0:ABCD::7
 redistribute bgp 1
 exit-address-family
address-family ipv6 unicast vrf v2
 router-id 2001:DB8:1::3
 redistribute bgp 1
 exit
!
router bgp 1
 bgp router-id 10.3.3.3
 no bgp default ipv4-unicast
 neighbor 10.0.0.4 remote-as 1
 neighbor 10.0.0.4 update-source-Loopback0
!
address-family ipv4
 exit-address-family
!
address-family vpnv4
 neighbor 10.0.0.4
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family vpnv6
 neighbor 10.0.0.4 activate
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family ipv4 vrf v1
 redistribute ospfv3 1
 exit-address-family
!
address-family ipv6 vrf v1
 redistribute ospf 1
 exit-address-family
!
address-family ipv6 vrf v2
 redistribute ospf 1
 exit-address-family
!
```

Example: Configuring a Provider Edge Device for VRF-Lite

```
vrf definition v1
 rd 1:1
 !
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 !
address-family ipv6
 exit-address-family
!
interface FastEthernet0/0
 no ip address
 !
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 vrf forwarding v1
 ip address 192.168.1.1 255.255.255.0
```

```
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 0
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 vrf forwarding v2
 ipv6 enable
 ospfv3 1 ipv6 area 0
!
interface FastEthernet0/1
 rf forwarding v1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 1
 ospfv3 1 ipv4 area 0
 no keepalive
!
interface FastEthernet0/2
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:1::1
 ipv6 enable
 ospfv3 1 ipv6 area 1
!
router ospfv3 1
!
address-family ipv6 unicast vrf v2
 router-id 192.168.2.1
 capability vrf-lite
 exit-address-family
!
address-family ipv4 unicast vrf v1
  router-id 192.168.1.4
  capability vrf-lite
exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 192.168.1.1
 capability vrf-lite
 exit-address-family
!
```

Additional References for OSPFv3 VRF-Lite/PE-CE

Related Documents

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

RFCs

RFC	Title
RFC 5838	Support of Address Families in OSPFv3

RFC	Title
RFC 6565	OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol

Technical Assistance

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

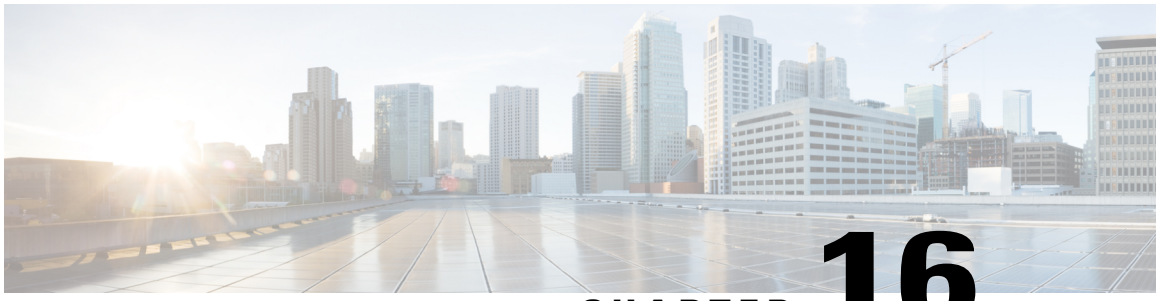
Feature Information for OSPFv3 VRF-Lite/PE-CE

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

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

Table 23: Feature Information for OSPFv3 VRF-Lite/PE-CE

Feature Name	Releases	Feature Information
OSPFv3 VRF-Lite/PE-CE	15.2(1)E	The OSPFv3 VRF-Lite/PE-CE feature adds OSPFv3 support for nondefault VRF instances. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: **area sham-link** (OSPFv3), **capability vrf-lite** (OSPFv3).



CHAPTER 16

OSPFv3 Authentication Trailer

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

- Finding Feature Information, page 157
- Information About OSPFv3 Authentication Trailer, page 157
- How to Configure OSPFv3 Authentication Trailer, page 159
- Configuration Examples for OSPFv3 Authentication Trailer, page 161
- Additional References for OSPFv3 Authentication Trailer, page 162
- Feature Information for OSPFv3 Authentication Trailer, page 163

Finding Feature Information

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

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

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** {**strict** | **deployment** | **normal**}
11. **exit**
12. **show ospfv3 interface**
13. **show ospfv3 neighbor** [*detail*]
14. **debug ospfv3 vrf authentication**

DETAILED STEPS

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

	Command or Action	Purpose
Step 5	**router ospfv3** [*process-id*] **Example:** `Device(config-if)# router ospfv3 1`	Enters OSPFv3 router configuration mode.
Step 6	**address-family ipv6 unicast vrf** *vrf-name* **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Configures the IPv6 address family in the OSPFv3 process and enters IPv6 address family configuration mode.
Step 7	**area** *area-id* **authentication** {**key-chain** *chain-name* | **null**} **Example:** `Device(config-router-af)# area 1 authentication key-chain ospf-chain-1`	Configures the authentication trailer on all interfaces in the OSPFv3 area.
Step 8	**area** *area-id* **virtual-link** *router-id* **authentication key-chain** *chain-name* **Example:** `Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1`	Configures the authentication for virtual links.
Step 9	**area** *area-id* **sham-link** *source-address destination-address* **authentication key-chain** *chain-name* **Example:** `Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1`	Configures the authentication for sham links.
Step 10	**authentication mode** {**strict** | **deployment** | **normal**} **Example:** `Device(config-router-af)# authentication mode deployment`	Specifies the type of authentication used for the OSPFv3 instance. • When the **strict** keyword is used, the expired keys cannot be used for sending or receiving packets. • The **deployment** keyword provides adjacency between configured and unconfigured authentication devices.
Step 11	**exit** **Example:** `Device(config-router-af)# exit`	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.

	Command or Action	Purpose
Step 13	**show ospfv3 neighbor** [*detail*] **Example:** `Device# show ospfv3 neighbor detail`	(Optional) Displays OSPFv3 neighbor information on a per-interface basis.
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 Ethernet 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 strict 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 Ethernet0/0
```

```
    Neighbor: interface-id 2, link-local address FE80::A8BB:CCFF:FE01:2D00
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.2.2.2 BDR is 1.1.1.1
    Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Options is 0x000413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Dead timer due in 00:00:33
    Neighbor is up for 00:05:07
    Last packet authentication succeed
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec


Device# show ospfv3 interface

Ethernet0/0 is up, line protocol is up
...
  Cryptographic authentication enabled
    Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-keys
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Additional References for OSPFv3 Authentication Trailer

Related Documents

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

Standards and RFCs

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

Technical Assistance

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

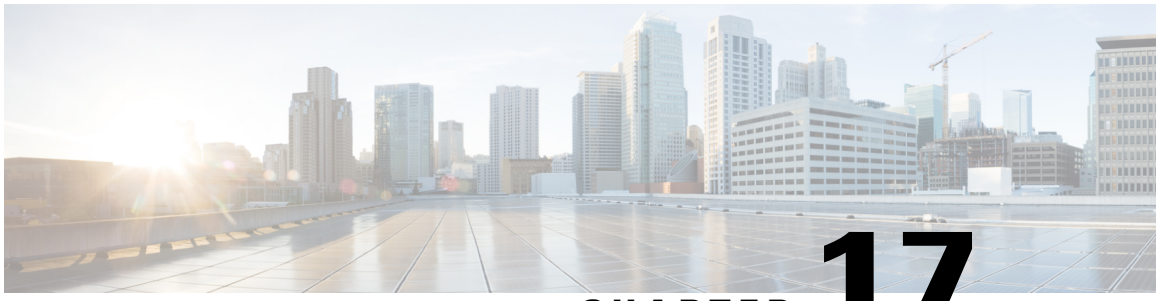
Feature Information for OSPFv3 Authentication Trailer

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

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

Table 24: Feature Information for OSPFv3 Authentication Trailer

Feature Name	Releases	Feature Information
OSPFv3 Authentication Trailer	Cisco IOS 15.2(2)E	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. In Cisco IOS 15.2(2)E, this feature was supported on the following platforms: • Catalyst 2960 Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches The following commands were introduced or modified: **ospfv3 authentication key-chain**, **authentication mode**, **debug ospfv3 vrf authentication**.



CHAPTER 17

OSPF ABR Type 3 LSA Filtering

The OSPF ABR Type 3 LSA Filtering feature extends the ability of an ABR that is running the OSPF protocol to filter type 3 link-state advertisements (LSAs) that are sent between different OSPF areas. This feature allows only packets with specified prefixes to be sent from one area to another area and restricts all packets with other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time.

- Finding Feature Information, page 165
- Benefits, page 165
- Restrictions, page 166
- Configuration Tasks, page 166
- Configuration Examples, page 168
- Additional References, page 168
- Feature Information for the OSPF ABR Type 3 LSA Filtering, page 170

Finding Feature Information

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

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

Benefits

The OSPF ABR Type 3 LSA Filtering feature gives the administrator improved control of route distribution between OSPF areas.

Restrictions

Only type 3 LSAs that originate from an ABR are filtered.

Related Features and Technologies

This feature is an extension of the OSPF routing protocol. For more information about configuring OSPF and configuring route summarization and filtering, refer to the "OSPF" module of the Cisco IOS IP Configuration Guide, Release 12.4 and the Cisco IOS IP Routing Protocols Command Reference, Release 12.4T.

Configuration Tasks

See the following sections for configuration tasks for the OSPF ABR Type 3 LSA Filtering feature. Each task in the list is identified as either required or optional:

Configuring OSPF ABR Type 3 LSA Filtering

SUMMARY STEPS

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **area** *area-id* **filter-list prefix** *prefix-list-name* **in**
3. Router(config-router)# **exit**
4. Router(config)# **ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit network/len** [**ge** *ge-value*] [**le** *le-value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** *process-id*	Configures the router to run an OSPF process.
Step 2	Router(config-router)# **area** *area-id* **filter-list prefix** *prefix-list-name* **in**	Configures the router to filter interarea routes into the specified area.
Step 3	Router(config-router)# **exit**	Exits router configuration mode and returns to global configuration mode.
Step 4	Router(config)# **ip prefix-list** *list-name* [**seq** *seq-value*] **deny**	**permit network/len** [**ge** *ge-value*] [**le** *le-value*]	Creates a prefix list with the name specified for the *list-name* argument.

Configuring OSPF ABR Type 3 LSA Filtering

To filter interarea routes out of a specified area, use the following commands beginning in router configuration mode:

SUMMARY STEPS

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **area** *area-id* **filter-list prefix** *prefix-list-name* **out**
3. Router(config-router)# **exit**
4. Router(config)# **ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit network/len** [**ge** *ge-value*] [**le** *le-value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** *process-id*	Configures the router to run an OSPF process.
Step 2	Router(config-router)# **area** *area-id* **filter-list prefix** *prefix-list-name* **out**	Configures the router to filter interarea routes out of the specified area.
Step 3	Router(config-router)# **exit**	Exits router configuration mode and returns to global configuration mode.
Step 4	Router(config)# **ip prefix-list** *list-name* [**seq** *seq-value*] **deny**	**permit network/len** [**ge** *ge-value*] [**le** *le-value*]	Creates a prefix list with the name specified for the *list-name* argument.

Verifying OSPF ABR Type 3 LSA Filtering

To verify that the OSPF ABR Type 3 LSA Filtering feature has been configured, use the **show ip ospf** command in the EXEC mode. The **show ip ospf** command will show that this feature has been enabled by listing the area filter as "in" or "out." The following is sample output from the **show ip ospf** command:

```
router# show ip ospf 1
  Routing Process "ospf 1" with ID 172.16.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an area border router
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  External flood list length 0
     Area BACKBONE(0)
         Number of interfaces in this area is 2
         Area has no authentication
         SPF algorithm executed 6 times
```

```
        Area ranges are
           10.0.0.0/8 Passive Advertise
        Area-filter AREA_0_IN in
        Area-filter AREA_0_OUT out
        Number of LSA 5. Checksum Sum 0x29450
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 4 times
        Area ranges are
        Area-filter AREA_1_IN in
        Area-filter AREA_1_OUT out
        Number of LSA 6. Checksum Sum 0x30100
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Monitoring and Maintaining OSPF ABR Type 3 LSA Filtering

Command	Purpose
`Router#` **show ip prefix-list**	Displays information about a prefix list or prefix list entries.

Configuration Examples

The following configuration example output shows interarea filtering that is applied to both incoming and outgoing routes:

```
Router(config)# router ospf 1
 log-adjacency-changes
 area 1 filter-list prefix AREA_1_OUT out
 area 3 filter-list prefix AREA_3_IN in
 network 10.0.0.0 0.255.255.255 area 3
 network 172.16.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.255.255.255 area 1
!
ip prefix-list AREA_1_OUT seq 10 permit 10.25.0.0/8 ge 16
ip prefix-list AREA_1_OUT seq 20 permit 172.20.20.0/24
!
ip prefix-list AREA_3_IN seq 10 permit 172.31.0.0/16
!
```

Additional References

The following sections provide references related to OSPF ABR Type 3 LSA Filtering.

Related Documents

Related Topic	Document Title
Configuring OSPF ABR Type 3 LSA Filtering	Configuring OSPF ABR Type 3 LSA Filtering
OSPF commands: complete command syntax, command mode, command history, command defaults, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
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
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

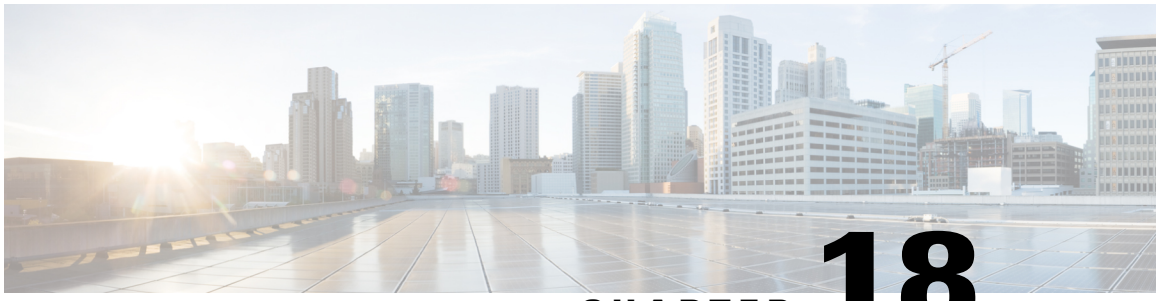
Feature Information for the OSPF ABR Type 3 LSA Filtering

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

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

Table 25: Feature Information for OSPF ABR Type 3 LSA Filtering

Feature Name	Releases	Feature Informatoin
OSPF ABR Type 3 LSA Filtering	15.2(1)E	This feature was integrated into Cisco IOS Release 15.2(1)E.



CHAPTER 18

Graceful Shutdown Support for OSPFv3

This feature provides the ability to temporarily shut down an Open Shortest Path First version 3 (OSPFv3) process or interface in the least disruptive manner, and to notify its neighbors that it is going away. A graceful shutdown of a protocol can be initiated on all OSPFv3 interfaces or on a specific interface.

- Finding Feature Information, page 171
- Information About Graceful Shutdown Support for OSPFv3, page 171
- How to Configure Graceful Shutdown Support for OSPFv3, page 172
- Configuration Examples for Graceful Shutdown Support for OSPFv3, page 176
- Additional References for Graceful Shutdown Support for OSPFv3, page 177
- Feature Information for Graceful Shutdown Support for OSPFv3, page 178

Finding Feature Information

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

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

Information About Graceful Shutdown Support for OSPFv3

OSPFv3 Graceful Shutdown

The Graceful Shutdown for OSPFv3 feature provides the ability to temporarily shut down the OSPFv3 protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path. A graceful shutdown of the OSPFv3 protocol can be initiated using the **shutdown** command in router configuration mode or in address family configuration mode.

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

How to Configure Graceful Shutdown Support for OSPFv3

Configuring Graceful Shutdown of the OSPFv3 Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ipv6 router ospf** *process-id*
   - **router ospfv3** *process-id*
4. **shutdown**
5. **end**
6. Do one of the following:
   - **show ipv6 ospf** [*process-id*]
   - **show ospfv3** [*process-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **ipv6 router ospf** *process-id* • **router ospfv3** *process-id*	Enables OSPFv3 routing and enters router configuration mode.

	Command or Action	Purpose

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

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast** [**vrf** *vrf-name*]
5. **shutdown**
6. **end**
7. **show ospfv3** [*process-id*]

DETAILED STEPS

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

Configuring OSPFv3 Graceful Shutdown of the OSPFv3 Interface

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet`	Configures an interface type and number and enters interface configuration mode.
Step 4	Do one of the following: • **ipv6 ospf shutdown** • **ospfv3 shutdown** **Example:** `Device(config-if)# ipv6 ospf shutdown`	Initiates an OSPFv3 protocol graceful shutdown at the interface level. • When the **ipv6 ospf shutdown** interface command is entered, the interface on which it is configured sends a link-state update advising its neighbors that is going down, which allows those neighbors to begin routing OSPFv3 traffic around this device.

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

Configuration Examples for Graceful Shutdown Support for OSPFv3

Example: Configuring Graceful Shutdown of the OSPFv3 Process

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

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

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

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

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

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

Example: Configuring Graceful Shutdown of the OSPFv3 Interface

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

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

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

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

Additional References for Graceful Shutdown Support for OSPFv3

Related Documents

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

Technical Assistance

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

Feature Information for Graceful Shutdown Support for OSPFv3

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

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

Table 26: Feature Information for Graceful Shutdown Support for OSPFv3

Feature Name	Releases	Feature Information
Graceful Shutdown Support for OSPFv3	15.2(1)E	This feature provides the ability to temporarily shut down an Open Shortest Path First version 3 (OSPFv3) process or interface in the least disruptive manner, and to notify its neighbors that it is going away. A graceful shutdown of a protocol can be initiated on all OSPFv3 interfaces or on a specific interface. In Cisco IOS 15.2(1)E, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced: • **ipv6 ospf shutdown** • **ospfv3 shutdown** • **shutdown (router ospfv3)**