Junos® OS

OSPF Feature Guide for Routing Devices

Release
13.2

Published: 2013-07-22

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS OSPF Feature Guide for Routing Devices
13.2

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

Part 5 Index

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- ACX Series
- J Series
- SRX Series
- T Series
- MX Series
- M Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xix defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xx defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the**[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Introduction to OSPF

OSPF Overview

OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). OSPF uses link-state information to make routing decisions, making route calculations using the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm). Each router running OSPF floods link-state advertisements throughout the AS or area that contain information about that router's attached interfaces and routing metrics. Each router uses the information in these link-state advertisements to calculate the least cost path to each network and create a routing table for the protocol.

Junos OS supports OSPF version 2 (OSPFv2) and OSPF version 3 (OSPFv3), including virtual links, stub areas, and for OSPFv2, authentication. Junos OS does not support type-of-service (ToS) routing.

OSPF was designed for the Transmission Control Protocol/Internet Protocol (TCP/IP) environment and as a result explicitly supports IP subnetting and the tagging of externally derived routing information. OSPF also provides for the authentication of routing updates.

OSPF routes IP packets based solely on the destination IP address contained in the IP packet header. OSPF quickly detects topological changes, such as when router interfaces become unavailable, and calculates new loop-free routes quickly and with a minimum of routing overhead traffic.

NOTE: On SRX Series devices, when only one link-protection is configured under the OSPF interface, the device does not install an alternative route in the forwarding table. When the per-packet load-balancing is enabled as a workaround, the device does not observe both the OSPF metric and sending the traffic through both the interfaces.

An OSPF AS can consist of a single area, or it can be subdivided into multiple areas. In a single-area OSPF network topology, each router maintains a database that describes the topology of the AS. Link-state information for each router is flooded throughout the AS. In a multiarea OSPF topology, each router maintains a database that describes the topology of its area, and link-state information for each router is flooded throughout that area. All routers maintain summarized topologies of other areas within an AS. Within each area, OSPF routers have identical topological databases. When the AS or area topology changes, OSPF ensures that the contents of all routers' topological databases converge quickly.

All OSPFv2 protocol exchanges can be authenticated. OSPFv3 relies on IPsec to provide this functionality. This means that only trusted routers can participate in the AS's routing. A variety of authentication schemes can be used. A single authentication scheme is configured for each area, which enables some areas to use stricter authentication than others.

Externally derived routing data (for example, routes learned from BGP) is passed transparently throughout the AS. This externally derived data is kept separate from the OSPF link-state data. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundaries of the AS.

NOTE: By default, Junos OS is compatible with RFC 1583, *OSPF Version 2*. In Junos OS Release 8.5 and later, you can disable compatibility with RFC 1583 by including the **no-rfc-1583** statement. For more information, see "Example: Disabling OSPFv2 Compatibility with RFC 1583" on page 118.

This topic describes the following information:

OSPF Default Route Preference Values

The Junos OS routing protocol process assigns a default preference value to each route that the routing table receives. The default value depends on the source of the route. The preference value is from 0 through 4,294,967,295 (232 – 1), with a lower value indicating a more preferred route. Table 3 on page 6 lists the default preference values for OSPF.

Table 3: Default Route Preference Values for OSPF

How Route Is Learned	Default Preference	Statement to Modify Default Preference
OSPF internal route	10	OSPF **preference**
OSPF AS external routes	150	OSPF **external-preference**

OSPF Routing Algorithm

OSPF uses the shortest-path-first (SPF) algorithm, also referred to as the Dijkstra algorithm, to determine the route to each destination. All routing devices in an area run this algorithm in parallel, storing the results in their individual topological databases. Routing devices with interfaces to multiple areas run multiple copies of the algorithm. This section provides a brief summary of how the SPF algorithm works.

When a routing device starts, it initializes OSPF and waits for indications from lower-level protocols that the router interfaces are functional. The routing device then uses the OSPF hello protocol to acquire neighbors, by sending hello packets to its neighbors and receiving their hello packets.

On broadcast or nonbroadcast multiaccess networks (physical networks that support the attachment of more than two routing devices), the OSPF hello protocol elects a designated router for the network. This routing device is responsible for sending *link-state advertisements* (LSAs) that describe the network, which reduces the amount of network traffic and the size of the routing devices' topological databases.

The routing device then attempts to form *adjacencies* with some of its newly acquired neighbors. (On multiaccess networks, only the designated router and backup designated router form adjacencies with other routing devices.) Adjacencies determine the distribution of routing protocol packets. Routing protocol packets are sent and received only on adjacencies, and topological database updates are sent only along adjacencies. When adjacencies have been established, pairs of adjacent routers synchronize their topological databases.

A routing device sends LSA packets to advertise its state periodically and when its state changes. These packets include information about the routing device's adjacencies, which allows detection of nonoperational routing devices.

Using a reliable algorithm, the routing device floods LSAs throughout the area, which ensures that all routing devices in an area have exactly the same topological database. Each routing device uses the information in its topological database to calculate a shortest-path tree, with itself as the root. The routing device then uses this tree to route network traffic.

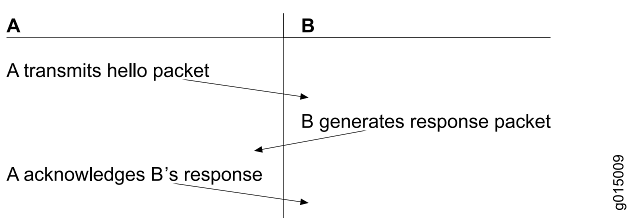
The description of the SPF algorithm up to this point has explained how the algorithm works within a single area (*intra-area routing*). For internal routers to be able to route to destinations outside the area (*interarea routing*), the area border routers must inject additional routing information into the area. Because the area border routers are connected to the backbone, they have access to complete topological data about the backbone. The area border routers use this information to calculate paths to all destinations outside its area and then advertise these paths to the area's internal routers.

Autonomous system (AS) boundary routers flood information about external autonomous systems throughout the AS, except to stub areas. Area border routers are responsible for advertising the paths to all AS boundary routers.

OSPF Three-Way Handshake

OSPF creates a topology map by flooding LSAs across OSPF-enabled links. LSAs announce the presence of OSPF-enabled interfaces to adjacent OSPF interfaces. The exchange of LSAs establishes bidirectional connectivity between all adjacent OSPF interfaces (neighbors) using a three-way handshake, as shown in Figure 1 on page 7.

Figure 1: OSPF Three-Way Handshake



In Figure 1 on page 7, Router A sends hello packets out all its OSPF-enabled interfaces when it comes online. Router B receives the packet, which establishes that Router B can receive traffic from Router A. Router B generates a response to Router A to acknowledge receipt of the hello packet. When Router A receives the response, it establishes that Router B can receive traffic from Router A. Router A then generates a final response packet to inform Router B that Router A can receive traffic from Router B. This three-way handshake ensures bidirectional connectivity.

As new neighbors are added to the network or existing neighbors lose connectivity, the adjacencies in the topology map are modified accordingly through the exchange (or absence) of LSAs. These LSAs advertise only the incremental changes in the network, which helps minimize the amount of OSPF traffic on the network. The adjacencies are shared and used to create the network topology in the topological database.

OSPF Version 3

OSPFv3 is a modified version of OSPF that supports IP version 6 (IPv6) addressing. OSPFv3 differs from OSPFv2 in the following ways:

- All neighbor ID information is based on a 32-bit router ID.
- The protocol runs per link rather than per subnet.
- Router and network link-state advertisements (LSAs) do not carry prefix information.
- Two new LSA types are included: link-LSA and intra-area-prefix-LSA.
- Flooding scopes are as follows:
  - Link-local
  - Area
  - AS
- Link-local addresses are used for all neighbor exchanges except virtual links.
- Authentication is removed. The IPv6 authentication header relies on the IP layer.
- The packet format has changed as follows:
  - Version number 2 is now version number 3.
  - The **db** option field has been expanded to 24 bits.
  - Authentication information has been removed.
  - Hello messages do not have address information.
  - Two new option bits are included: **R** and **V6**.
- Type 3 summary LSAs have been renamed *inter-area-prefix-LSAs*.
- Type 4 summary LSAs have been renamed *inter-area-router-LSAs*.

Related Documentation

- Understanding OSPF Areas and Backbone Areas on page 27
- OSPF Configuration Overview on page 14
- *OSPF Version 3 for IPv6*
- Example: Disabling OSPFv2 Compatibility with RFC 1583 on page 118

OSPF Areas and Router Functionality Overview

In OSPF, a single autonomous system (AS) can be divided into smaller groups called *areas*. This reduces the number of link-state advertisements (LSAs) and other OSPF overhead traffic sent on the network, and it reduces the size of the topology database that each router must maintain. The routing devices that participate in OSPF routing perform one or more functions based on their location in the network.

This topic describes the following OSPF area types and routing device functions:

Areas

An *area* is a set of networks and hosts within an AS that have been administratively grouped together. We recommend that you configure an area as a collection of contiguous IP subnetted networks. Routing devices that are wholly within an area are called *internal routers*. All interfaces on internal routers are directly connected to networks within the area.

The topology of an area is hidden from the rest of the AS, thus significantly reducing routing traffic in the AS. Also, routing within the area is determined only by the area's topology, providing the area with some protection from bad routing data.

All routing devices within an area have identical topology databases.

Area Border Routers

Routing devices that belong to more than one area and connect one or more OSPF areas to the backbone area are called *area border routers* (ABRs). At least one interface is within the backbone while another interface is in another area. ABRs also maintain a separate topological database for each area to which they are connected.

Backbone Areas

An OSPF *backbone area* consists of all networks in area ID 0.0.0.0, their attached routing devices, and all ABRs. The backbone itself does not have any ABRs. The backbone distributes routing information between areas. The backbone is simply another area, so the terminology and rules of areas apply: a routing device that is directly connected to the backbone is an internal router on the backbone, and the backbone's topology is hidden from the other areas in the AS.

The routing devices that make up the backbone must be physically contiguous. If they are not, you must configure *virtual links* to create the appearance of backbone connectivity. You can create virtual links between any two ABRs that have an interface to a common nonbackbone area. OSPF treats two routing devices joined by a virtual link as if they were connected to an unnumbered point-to-point network.

AS Boundary Routers

Routing devices that exchange routing information with routing devices in non-OSPF networks are called *AS boundary routers*. They advertise externally learned routes throughout the OSPF AS. Depending on the location of the AS boundary router in the network, it can be an ABR, a backbone router, or an internal router (with the exception of stub areas). Internal routers within a stub area cannot be an AS boundary router because stub areas cannot contain any Type 5 LSAs.

Routing devices within the area where the AS boundary router resides know the path to that AS boundary router. Any routing device outside the area only knows the path to the nearest ABR that is in the same area where the AS boundary router resides.

Backbone Router

Backbone routers are routing devices that have one or more interfaces connected to the OSPF backbone area (area ID 0.0.0.0).

Internal Router

Routing devices that connect to only one OSPF area are called *internal routers*. All interfaces on internal routers are directly connected to networks within a single area.

Stub Areas

Stub areas are areas through which or into which AS external advertisements are not flooded. You might want to create stub areas when much of the topological database consists of AS external advertisements. Doing so reduces the size of the topological databases and therefore the amount of memory required on the internal routers in the stub area.

Routing devices within a stub area rely on the default routes originated by the area's ABR to reach external AS destinations. You must configure the **default-metric** option on the ABR before it advertises a default route. Once configured, the ABR advertises a default route in place of the external routes that are not being advertised within the stub area, so that routing devices in the stub area can reach destinations outside the area.

The following restrictions apply to stub areas: you cannot create a virtual link through a stub area, a stub area cannot contain an AS boundary router, the backbone cannot be a stub area, and you cannot configure an area as both a stub area and a not-so-stubby area.

Not-So-Stubby Areas

An OSPF stub area has no external routes in it, so you cannot redistribute from another protocol into a stub area. A *not-so-stubby area* (NSSA) allows external routes to be flooded within the area. These routes are then leaked into other areas. However, external routes from other areas still do not enter the NSSA.

The following restriction applies to NSSAs: you cannot configure an area as both a stub area and an NSSA.

Transit Areas

Transit areas are used to pass traffic from one adjacent area to the backbone (or to another area if the backbone is more than two hops away from an area). The traffic does not originate in, nor is it destined for, the transit area.

Related Documentation

- OSPF Overview on page 4
- Packets Overview on page 11
- OSPF Configuration Overview on page 14
- Understanding OSPF Areas and Backbone Areas on page 27
- Understanding OSPF Stub Areas, Totally Stubby Areas, and Not-So-Stubby Areas on page 35

Packets Overview

There are several types of link-state advertisement (LSA) packets.

This topic describes the following information:

OSPF Packet Header

All OSPFv2 packets have a common 24-byte header, and OSPFv3 packets have a common 16-byte header, that contains all information necessary to determine whether OSPF should accept the packet. The header consists of the following fields:

- Version number—The current OSPF version number. This can be either **2** or **3**.
- Type—Type of OSPF packet.

- Packet length—Length of the packet, in bytes, including the header.
- Router ID—IP address of the router from which the packet originated.
- Area ID—Identifier of the area in which the packet is traveling. Each OSPF packet is associated with a single area. Packets traveling over a virtual link are labeled with the backbone area ID, 0.0.0.0. .
- Checksum—Fletcher checksum.
- Authentication—(OSPFv2 only) Authentication scheme and authentication information.
- Instance ID—(OSPFv3 only) Identifier used when there are multiple OSPFv3 realms configured on a link.

Hello Packets

Routers periodically send hello packets on all interfaces, including virtual links, to establish and maintain neighbor relationships. Hello packets are multicast on physical networks that have a multicast or broadcast capability, which enables dynamic discovery of neighboring routers. (On nonbroadcast networks, dynamic neighbor discovery is not possible, so you must configure all neighbors statically as described in "Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network" on page 125.)

Hello packets consist of the OSPF header plus the following fields:

- Network mask—(OSPFv2 only) Network mask associated with the interface.
- Hello interval—How often the router sends hello packets. All routers on a shared network must use the same hello interval.
- Options—Optional capabilities of the router.
- Router priority—The router's priority to become the designated router.
- Router dead interval—How long the router waits without receiving any OSPF packets from a router before declaring that router to be down. All routers on a shared network must use the same router dead interval.
- Designated router—IP address of the designated router.
- Backup designated router—IP address of the backup designated router.
- Neighbor—IP addresses of the routers from which valid hello packets have been received within the time specified by the router dead interval.

Database Description Packets

When initializing an adjacency, OSPF exchanges database description packets, which describe the contents of the topological database. These packets consist of the OSPF header, packet sequence number, and the link-state advertisement's header.

Link-State Request Packets

When a router detects that portions of its topological database are out of date, it sends a link-state request packet to a neighbor requesting a precise instance of the database.

These packets consist of the OSPF header plus fields that uniquely identify the database information that the router is seeking.

Link-State Update Packets

Link-state update packets carry one or more link-state advertisements one hop farther from their origin. The router multicasts (floods) these packets on physical networks that support multicast or broadcast mode. The router acknowledges all link-state update packets and, if retransmission is necessary, sends the retransmitted advertisements unicast.

Link-state update packets consist of the OSPF header plus the following fields:

- Number of advertisements—Number of link-state advertisements included in this packet.
- Link-state advertisements—The link-state advertisements themselves.

Link-State Acknowledgment Packets

The router sends link-state acknowledgment packets in response to link-state update packets to verify that the update packets have been received successfully. A single acknowledgment packet can include responses to multiple update packets.

Link-state acknowledgment packets consist of the OSPF header plus the link-state advertisement header.

Link-State Advertisement Packet Types

Link-state request, link-state update, and link-state acknowledgment packets are used to reliably flood link-state advertisement packets. OSPF sends the following types of link-state advertisements:

- Router link advertisements—Are sent by all routers to describe the state and cost of the router's links to the area. These link-state advertisements are flooded throughout a single area only.
- Network link advertisements—Are sent by designated routers to describe all the routers attached to the network. These link-state advertisements are flooded throughout a single area only.
- Summary link advertisements—Are sent by area border routers to describe the routes that they know about in other areas. There are two types of summary link advertisements: those used when the destination is an IP network, and those used when the destination is an AS boundary router. Summary link advertisements describe interarea routes, that is, routes to destinations outside the area but within the AS. These link-state advertisements are flooded throughout the advertisement's associated areas.
- AS external link advertisement—Are sent by AS boundary routers to describe external routes that they know about. These link-state advertisements are flooded throughout the AS (except for stub areas).

Each link-state advertisement type describes a portion of the OSPF routing domain. All link-state advertisements are flooded throughout the AS.

Each link-state advertisement packet begins with a common 20-byte header.

Related Documentation

- OSPF Overview on page 4
- OSPF Areas and Router Functionality Overview on page 9
- OSPF Configuration Overview on page 14
- OSPF Designated Router Overview on page 23
- Understanding OSPFv2 Authentication on page 173
- OSPF Timers Overview on page 201

OSPF External Metrics Overview

When OSPF exports route information from external autonomous systems (ASs), it includes a cost, or *external metric*, in the route. OSPF supports two types of external metrics: Type 1 and Type 2. The difference between the two metrics is how OSPF calculates the cost of the route. Type 1 external metrics are equivalent to the link-state metric, where the cost is equal to the sum of the internal costs plus the external cost. This means that Type 1 external metrics include the external cost to the destination as well as the cost (metric) to reach the AS boundary router. Type 2 external metrics are greater than the cost of any path internal to the AS. Type 2 external metrics use only the external cost to the destination and ignore the cost (metric) to reach the AS boundary router. By default, OSPF uses the Type 2 external metric.

OSPF Configuration Overview

To activate OSPF on a network, you must enable the protocol on all interfaces within the network on which OSPF traffic is to travel. To enable OSPF, you must configure one or more interfaces on the device within an OSPF area. Once the interfaces are configured, OSPF link-state advertisements (LSAs) are transmitted on all OSPF-enabled interfaces, and the network topology is shared throughout the network.

To complete the minimum device configuration for a node in an OSPF network involves:

1. Configuring the device interfaces.
   See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
2. Configuring the router identifiers for the devices in your OSPF network
3. Creating the backbone area (area 0) for your OSPF network and adding the appropriate interfaces to the area

   NOTE: Once you complete this step, OSPF begins sending LSAs. No additional configuration is required to enable OSPF traffic on the network.

You can further define your OSPF network depending on your network requirements. Some optional configurations involve:

- Adding additional areas to your network and configure area border routers (ABRs)
- Enabling dial-on-demand routing backup on the OSPF-enabled interface to configure OSPF across a demand circuit such as an ISDN link. (You must have already configured an ISDN interface.) Because demand circuits do not pass all traffic required to maintain an OSPF adjacency (hello packets, for example), you configure dial-on-demand routing so individual nodes in an OSPF network can maintain adjacencies despite the lack of LSA exchanges.
- Reducing the amount of memory that the nodes use to maintain the topology database by configuring stub and not-so-stubby areas
- Ensuring that only trusted routing devices participate in the autonomous systems' routing by enabling authentication
- Controlling the flow of traffic across the network by configuring path metrics and route selection

When describing how to configure OSPF, the following terms are used as follows:

- OSPF refers to both OSPF version 2 (OSPFv2) and OSPF version 3 (OSPFv3)
- OSPFv2 refers to OSPF version 2
- OSPFv3 refers to OSPF version 3

CHAPTER 2

Introduction to OSPF Routing Policy

OSPF Routing Policy Overview

All routing protocols store their routing information in the routing table. The routing table uses this collected route information to determine the active routes to destinations. The routing table then installs the active routes into its forwarding table and also exports them back into the routing protocols. It is these exported routes that the protocols advertise.

OSPF has a set of default rules that determine which routes it places in the routing table and advertises from the routing table. The default rules for all routing protocols are known as the *default routing policy*. The default routing policy is always present. You can further control which routes the protocol stores in the routing table and which routes the routing table exports into the protocol by defining a *routing policy* for that protocol. A routing policy has a major impact on the flow of routing information or packets within or through the device. The match conditions and actions allow you to configure a customized policy to fit your needs. A user-defined routing policy preempts the default routing policy.

To create a routing policy, you must define the policy and apply it. You define the policy by specifying the criteria that a route must match and the actions to perform if a match occurs. You then apply the policy to OSPF.

Default OSPF Routing Policy

OSPF is a link-state protocol that exchanges routes between systems within an autonomous system (AS). All devices within an AS must share the same link-state database, which includes routes to reachable prefixes and the metrics associated with the prefixes. The default import policy for OSPF is to accept all learned routes and import them into the routing table. The default export policy for OSPF is to reject everything. OSPF does not actually export its internally learned routes (the directly connected routes on interfaces that are running the protocol). OSPF uses link-state advertisement (LSA) flooding to advertise both local routes and learned routes, and LSA flooding is not affected by the export policy.

Related Documentation

- Understanding OSPF Routing Policy on page 281

CHAPTER 3

OSPF Reference

Supported OSPF and OSPFv3 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for OSPF and OSPF version 3 (OSPFv3).

- RFC 1583, *OSPF Version 2*
- RFC 1765, *OSPF Database Overflow*
- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 2154, *OSPF with Digital Signatures*
- RFC 2328, *OSPF Version 2*
- RFC 2370, *The OSPF Opaque LSA Option*

  Support is provided by the **update-threshold** configuration statement at the **[edit protocols rsvp interface *interface-name*]** hierarchy level.
- RFC 2740, *OSPF for IPv6* (partial support for RFC 5340)

  Junos OS does not support the following components of RFC 5340:

  - Multiple interfaces on the same link
  - Deprecation of Multicast Extensions to OSPF (MOSPF) for IPv6
  - Not-so-stubby area (NSSA) specification
  - Link LSA suppression
  - LSA options and prefix options updates
  - IPv6 site-local addresses
- RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3623, *Graceful OSPF Restart*
- RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
- RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*

- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

  Only interface switching is supported.

- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*
- RFC 4812, *OSPF Restart Signaling*
- RFC 4813, *OSPF Link-Local Signaling*
- RFC 4915, *Multi-Topology (MT) Routing in OSPF*
- RFC 5185, *OSPF Multi-Area Adjacency*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5838, *Support of Address Families in OSPFv3*
- Internet draft draft-ietf-ospf-af-alt-10.txt, *Support of address families in OSPFv3*
- Internet draft draft-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection*

  Transmission of echo packets is not supported.

The following RFCs do not define standards, but provide information about OSPF and related technologies. The IETF classifies them as “Informational.”

- RFC 3137, *OSPF Stub Router Advertisement*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

Related Documentation

- *Supported IPv6 Standards*
- OSPF Overview on page 4
- *Accessing Standards Documents on the Internet*

PART 2

Configuration

CHAPTER 4

Basic OSPF Area Configuration

Examples: Configuring OSPF Designated Routers

OSPF Designated Router Overview

Large LANs that have many routing devices and therefore many OSPF adjacencies can produce heavy control-packet traffic as link-state advertisements (LSAs) are flooded across the network. To alleviate the potential traffic problem, OSPF uses designated routers on all multiaccess networks (broadcast and nonbroadcast multiaccess [NBMA] networks types). Rather than broadcasting LSAs to all their OSPF neighbors, the routing devices send their LSAs to the designated router. Each multiaccess network has a designated router, which performs two main functions:

- Originate network link advertisements on behalf of the network.
- Establish adjacencies with all routing devices on the network, thus participating in the synchronizing of the link-state databases.

In LANs, the election of the designated router takes place when the OSPF network is initially established. When the first OSPF links are active, the routing device with the highest router identifier (defined by the **router-id** configuration value, which is typically the IP address of the routing device, or the loopback address) is elected the designated router. The routing device with the second highest router identifier is elected the backup designated router. If the designated router fails or loses connectivity, the backup designated router assumes its role and a new backup designated router election takes place between all the routers in the OSPF network.

OSPF uses the router identifier for two main purposes: to elect a designated router, unless you manually specify a priority value, and to identify the routing device from which a packet is originated. At designated router election, the router priorities are evaluated first, and the routing device with the highest priority is elected designated router. If router priorities tie, the routing device with the highest router identifier, which is typically the routing device's IP address, is chosen as the designated router. If you do not configure a router identifier, the IP address of the first interface to come online is used. This is usually the loopback interface. Otherwise, the first hardware interface with an IP address is used.

At least one routing device on each logical IP network or subnet must be eligible to be the designated router for OSPFv2. At least one routing device on each logical link must be eligible to be the designated router for OSPFv3.

By default, routing devices have a priority of 128. A priority of 0 marks the routing device as ineligible to become the designated router. A priority of 1 means the routing device has the least chance of becoming a designated router. A priority of 255 means the routing device is always the designated router.

Example: Configuring an OSPF Router Identifier

This example shows how to configure an OSPF router identifier.

Requirements

Before you begin:

- Identify the interfaces on the routing device that will participate in OSPF. You must enable OSPF on all interfaces within the network on which OSPF traffic is to travel.
- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.

Overview

The router identifier is used by OSPF to identify the routing device from which a packet originated. Junos OS selects a router identifier according to the following set of rules:

1. By default, Junos OS selects the lowest configured physical IP address of an interface as the router identifier.
2. If a loopback interface is configured, the IP address of the loopback interface becomes the router identifier.
3. If multiple loopback interfaces are configured, the lowest loopback address becomes the router identifier.
4. If a router identifier is explicitly configured using the **router-id** ***address*** statement under the **[edit routing-options]** hierarchy level, the above three rules are ignored.

NOTE: If the router identifier is modified in a network, the link-state advertisements (LSAs) advertised by the previous router identifier are retained in the OSPF database until the LSA retransmit interval has timed out.

If the router identifier is not configured explicitly and an interface IP address is used as the router identifier, the established OSPF adjacency flaps when the interface goes down, or when it is brought back into the network. When the interface is brought back into the network, or a new interface is introduced into the network, the router identifier is selected again based on the rules stated above. Hence, it is strongly recommended that you explicitly configure the router identifier under the **[edit routing-options]** hierarchy level to avoid unpredictable behavior if the interface address on a loopback interface changes.

NOTE: The router identifier behavior described here holds good even when configured under **[edit routing-instances *routing-instance-name* routing-options]** and **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options]** hierarchy levels.

In this example, you configure the OSPF router identifier by setting its router ID value to the IP address of the device, which is 177.162.4.24.

Configuration

CLI Quick Configuration

To quickly configure an OSPF router identifier, copy the following command and paste it into the CLI.

```
[edit]
set routing-options router-id 177.162.4.24
```

Step-by-Step Procedure

To configure an OSPF router identifier:

1. Configure the OSPF router identifier by entering the **[router-id]** configuration value.

   ```
   [edit]
   user@host# set routing-options router-id 177.162.4.24
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show routing-options router-id** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show routing-options router-id
router-id 177.162.4.24;
```

Verification

After you configure the router ID and activate OSPF on the routing device, the router ID is referenced by multiple OSPF operational mode commands that you can use to monitor and troubleshoot the OSPF protocol. The router ID fields are clearly marked in the output.

Example: Controlling OSPF Designated Router Election

This example shows how to control OSPF designated router election.

- Requirements on page 26
- Overview on page 26
- Configuration on page 26
- Verification on page 27

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.

Overview

This example shows how to control OSPF designated router election. Within the example, you set the OSPF interface to **ge-/0/0/1** and the device priority to 200. The higher the priority value, the greater likelihood the routing device will become the designated router.

By default, routing devices have a priority of 128. A priority of 0 marks the routing device as ineligible to become the designated router. A priority of 1 means the routing device has the least chance of becoming a designated router.

Configuration

CLI Quick Configuration

To quickly configure an OSPF designated router election, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.3 interface ge-0/0/1 priority 200
```

Step-by-Step Procedure

To control OSPF designated router election:

1. Configure an OSPF interface and specify the device priority.

   NOTE: To specify an OSPFv3 interface, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.3 interface ge-0/0/1 priority 200
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```


Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.3 {
  interface ge-0/0/1.0 {
    priority 200;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Designated Router Election

Purpose Based on the priority you configured for a specific OSPF interface, you can confirm the address of the area's designated router. The DR ID, DR, or DR-ID field displays the address of the area's designated router. The BDR ID, BDR, or BDR-ID field displays the address of the backup designated router.

Action From operational mode, enter the **show ospf interface** and the **show ospf neighbor** commands for OSPFv2, and enter the **show ospf3 interface** and the **show ospf3 neighbor** commands for OSPFv3.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- OSPF Configuration Overview on page 14

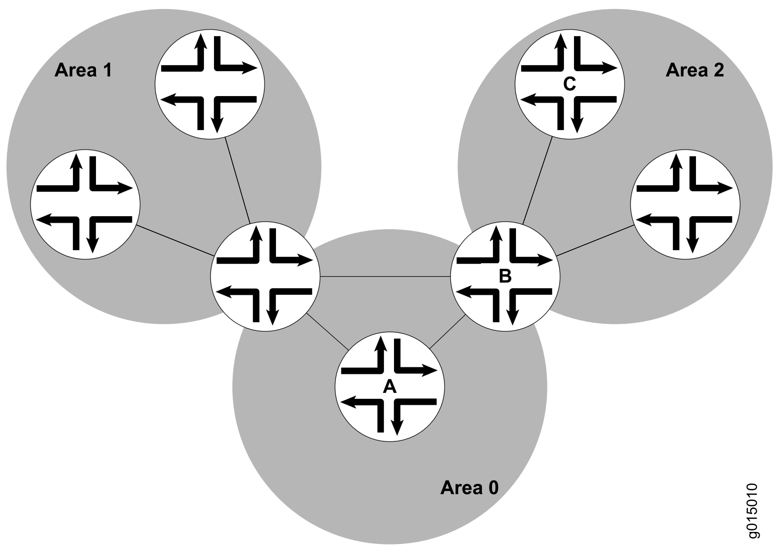
Examples: Configuring OSPF Areas

Understanding OSPF Areas and Backbone Areas

OSPF networks in an autonomous system (AS) are administratively grouped into *areas*. Each area within an AS operates like an independent network and has a unique 32-bit area ID, which functions similar to a network address. Within an area, the topology database contains only information about the area, link-state advertisements (LSAs) are flooded only to nodes within the area, and routes are computed only within the area. The topology of an area is hidden from the rest of the AS, thus significantly reducing routing traffic in the AS. Subnetworks are divided into other areas, which are connected to form the whole of the main network. Routing devices that are wholly within an area are called *internal routers*. All interfaces on internal routers are directly connected to networks within the area.

The central area of an AS, called the *backbone area*, has a special function and is always assigned the area ID 0.0.0.0. (Within a simple, single-area network, this is also the ID of the area.) Area IDs are unique numeric identifiers, in dotted decimal notation, but they are not IP addresses. Area IDs need only be unique within an AS. All other networks or areas in the AS must be directly connected to the backbone area by a routing device that has interfaces in more than one area. These connecting routing devices are called *area border routers* (ABRs). Figure 2 on page 28 shows an OSPF topology of three areas connected by two ABRs.

Figure 2: Multiarea OSPF Topology



Because all areas are adjacent to the backbone area, OSPF routers send all traffic not destined for their own area through the backbone area. The ABRs in the backbone area are then responsible for transmitting the traffic through the appropriate ABR to the destination area. The ABRs summarize the link-state records of each area and advertise destination address summaries to neighboring areas. The advertisements contain the ID of the area in which each destination lies, so that packets are routed to the appropriate ABR. For example, in the OSPF areas shown in Figure 2 on page 28, packets sent from Router A to Router C are automatically routed through ABR B.

Junos OS supports active backbone detection. Active backbone detection is implemented to verify that ABRs are connected to the backbone. If the connection to the backbone area is lost, then the routing device's default metric is not advertised, effectively rerouting traffic through another ABR with a valid connection to the backbone. Active backbone detection enables transit through an ABR with no active backbone connection. An ABR advertises to other routing devices that it is an ABR even if the connection to the backbone is down, so that the neighbors can consider it for interarea routes.

An OSPF restriction requires all areas to be directly connected to the backbone area so that packets can be properly routed. All packets are routed first to the backbone area by default. Packets that are destined for an area other than the backbone area are then routed to the appropriate ABR and on to the remote host within the destination area.

Example: Configuring a Single-Area OSPF Network

This example shows how to configure a single-area OSPF network.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.

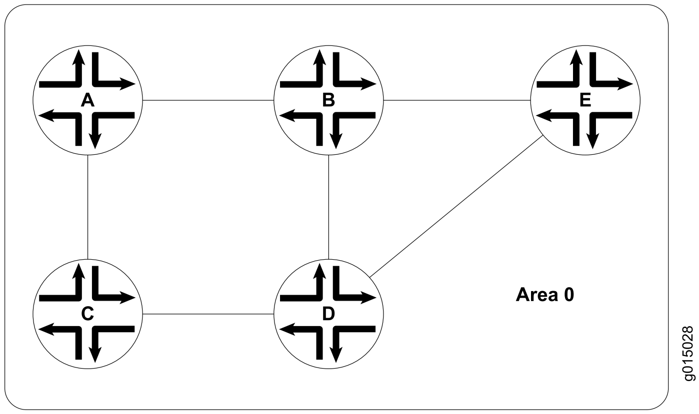
Overview

To activate OSPF on a network, you must enable the OSPF protocol on all interfaces within the network on which OSPF traffic is to travel. To enable OSPF, you must configure one or more interfaces on the device within an OSPF area. Once the interfaces are configured, OSPF LSAs are transmitted on all OSPF-enabled interfaces, and the network topology is shared throughout the network.

In an autonomous system (AS), the backbone area is always assigned area ID 0.0.0.0 (within a simple, single-area network, this is also the ID of the area). Area IDs are unique numeric identifiers, in dotted decimal notation. Area IDs need only be unique within an AS. All other networks or areas in the AS must be directly connected to the backbone area by area border routers that have interfaces in more than one area. You must also create a backbone area if your network consists of multiple areas. In this example, you create the backbone area and add interfaces, such as **ge-0/0/0**, as needed to the OSPF area.

To use OSPF on the device, you must configure at least one OSPF area, such as the one shown in Figure 3 on page 30.

Figure 3: Typical Single-Area OSPF Network Topology



Configuration

CLI Quick Configuration

To quickly configure a single-area OSPF network, copy the following command and paste it into the CLI. You repeat this configuration for all interfaces that are part of the OSPF area.

```
[edit]
set protocols ospf area 0.0.0.0 interface ge-0/0/0
```

Step-by-Step Procedure

To configure a single-area OSPF network:

1. Configure the single-area OSPF network by specifying the area ID and associated interface.

   NOTE: For a single-area OSPFv3 network, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.0 interface ge-0/0/0
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface ge-0/0/0.0;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Interfaces in the Area

Purpose Verify that the interface for OSPF or OSPFv3 has been configured for the appropriate area. Confirm that the Area field displays the value that you configured.

Action From operational mode, enter the **show ospf interface** command for OSPFv2, and enter the **show ospf3 interface** command for OSPFv3.

Example: Configuring a Multiarea OSPF Network

This example shows how to configure a multiarea OSPF network. To reduce traffic and topology maintenance for the devices in an OSPF autonomous system (AS), you can group the OSPF-enabled routing devices into multiple areas.

- Requirements on page 31
- Overview on page 31
- Configuration on page 32
- Verification on page 34

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.

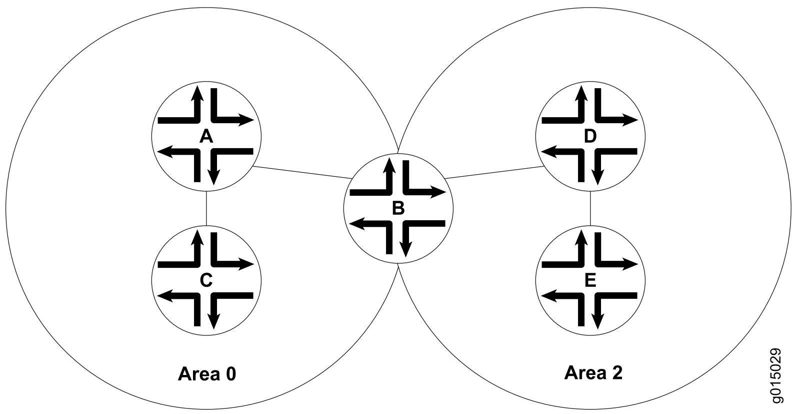
Overview

To activate OSPF on a network, you must enable the OSPF protocol on all interfaces within the network on which OSPF traffic is to travel. To enable OSPF, you must configure one or more interfaces on the device within an OSPF area. Once the interfaces are configured, OSPF LSAs are transmitted on all OSPF-enabled interfaces, and the network topology is shared throughout the network.

Each OSPF area consists of routing devices configured with the same area number. The backbone area is always assigned area ID 0.0.0.0. (All area identifiers (IDs) must be unique within an AS.) All other networks or areas in the AS must be directly connected to the backbone area by a router that has interfaces in more than one area. In Figure 4 on page 32, Devices A and C are in the backbone area (area 0), and Devices D and E are in area 2. Device B has a special role. This is the area border router that connects area 0 and area 2. The area border router maintains a separate topological database for each area to which it is connected.

To reduce traffic and topology maintenance for the devices in an OSPF AS, you can group them into multiple areas as shown in Figure 4 on page 32. In this example, you create the backbone area, create an additional area (area 2) and assign it unique area ID 0.0.0.2, and you configure Device B as the area border router, where interface **ge-0/0/0** participates in OSPF area 0 and interface **ge-0/0/2** participates in OSPF area 2.

Figure 4: Typical Multiarea OSPF Network Topology



Configuration

CLI Quick Configuration

To quickly configure a multiarea OSPF network, copy the following commands and paste them into the CLI. You repeat this configuration for all interfaces that are part of the OSPF area.

Device A

```
[edit]
set protocols ospf area 0.0.0.0 interface ge-0/0/0
set protocols ospf area 0.0.0.0 interface ge-0/0/1
```

Device C

```
[edit]
set protocols ospf area 0.0.0.0 interface ge-0/0/0
```

Device B

```
[edit]
set protocols ospf area 0.0.0.0 interface ge-0/0/0
set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

Device D

```
[edit]
set protocols ospf area 0.0.0.2 interface ge-0/0/0
set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

Device E

```
[edit]
set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

Step-by-Step Procedure

To configure a multiarea OSPF network:

1. Configure the backbone area.

NOTE: For an OSPFv3 network, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@A# set protocols ospf area 0.0.0.0 interface ge-0/0/0
user@A# set protocols ospf area 0.0.0.0 interface ge-0/0/1
```

```
[edit]
user@C# set protocols ospf area 0.0.0.0 interface ge-0/0/0
```

```
[edit]
user@B# set protocols ospf area 0.0.0.0 interface ge-0/0/0
```

2. Configure an additional area for your OSPF network.

```
[edit]
user@B# set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

```
[edit]
user@D# set protocols ospf area 0.0.0.2 interface ge-0/0/0
user@D# set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

```
[edit]
user@E# set protocols ospf area 0.0.0.2 interface ge-0/0/2
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@A# show protocols ospf
area 0.0.0.0 {
  interface ge-0/0/0.0;
  interface ge-0/0/1.0;
}
```

```
user@C# show protocols ospf
area 0.0.0.0 {
  interface ge-0/0/0.0;
}
```

```
user@B# show protocols ospf
area 0.0.0.0 {
  interface ge-0/0/0.0;
}
area 0.0.0.2 {
  interface ge-0/0/2.0;
}
```

```
user@D# show protocols ospf
area 0.0.0.2 {
```

```
    interface ge-0/0/0.0;
    interface ge-0/0/2.0;
}
user@E# show protocols ospf
area 0.0.0.2 {
    interface ge-0/0/2.0;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the Interfaces in the Area on page 34

Verifying the Interfaces in the Area

Purpose Verify that the interface for OSPF or OSPFv3 has been configured for the appropriate area. Confirm that the Area field displays the value that you configured.

Action From operational mode, enter the **show ospf interface** command for OSPFv2, and enter the **show ospf3 interface** command for OSPFv3.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- OSPF Configuration Overview on page 14

CHAPTER 5

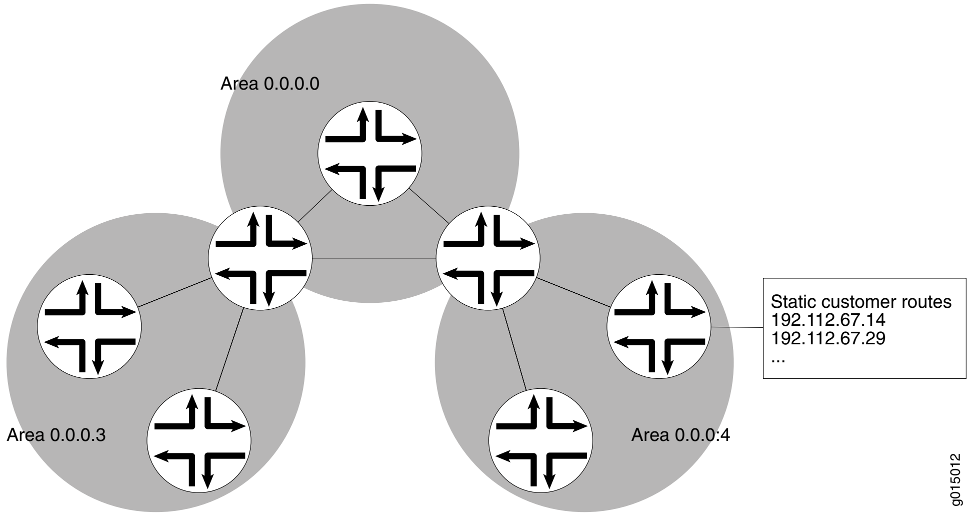
Advanced OSPF Area Configuration

Examples: Configuring OSPF Stub and Not-So-Stubby Areas

Understanding OSPF Stub Areas, Totally Stubby Areas, and Not-So-Stubby Areas

Figure 5 on page 36 shows an autonomous system (AS) across which many external routes are advertised. If external routes make up a significant portion of a topology database, you can suppress the advertisements in areas that do not have links outside the network. By doing so, you can reduce the amount of memory the nodes use to maintain the topology database and free it for other uses.

Figure 5: OSPF AS Network with Stub Areas and NSSAs



To control the advertisement of external routes into an area, OSPF uses stub areas. By designating an area border router (ABR) interface to the area as a stub interface, you suppress external route advertisements through the ABR. Instead, the ABR advertises a default route (through itself) in place of the external routes and generates network summary (Type 3) link-state advertisements (LSAs). Packets destined for external routes are automatically sent to the ABR, which acts as a gateway for outbound traffic and routes the traffic appropriately.

NOTE: You must explicitly configure the ABR to generate a default route when attached to a stub or not-so-stubby-area (NSSA). To inject a default route with a specified metric value into the area, you must configure the default-metric option and specify a metric value.

For example, area 0.0.0.3 in Figure 5 on page 36 is not directly connected to the outside network. All outbound traffic is routed through the ABR to the backbone and then to the destination addresses. By designating area 0.0.0.3 as a stub area, you reduce the size of the topology database for that area by limiting the route entries to only those routes internal to the area.

A stub area that only allows routes internal to the area and restricts Type 3 LSAs from entering the stub area is often called a *totally stubby area*. You can convert area 0.0.0.3 to a totally stubby area by configuring the ABR to only advertise and allow the default route to enter into the area. External routes and destinations to other areas are no longer summarized or allowed into a totally stubby area.

NOTE: If you incorrectly configure a totally stubby area, you might encounter network connectivity issues. You should have advanced knowledge of OSPF and understand your network environment before configuring totally stubby areas.

Similar to area 0.0.0.3 in Figure 5 on page 36, area 0.0.0.4 has no external connections. However, area 0.0.0.4 has static customer routes that are not internal OSPF routes. You can limit the external route advertisements to the area and advertise the static customer routes by designating the area an NSSA. In an NSSA, the AS boundary router generates NSSA external (Type 7) LSAs and floods them into the NSSA, where they are contained. Type 7 LSAs allow an NSSA to support the presence of AS boundary routers and their corresponding external routing information. The ABR converts Type 7 LSAs into AS external (Type 5) LSAs and leaks them to the other areas, but external routes from other areas are not advertised within the NSSA.

Example: Configuring OSPF Stub and Totally Stubby Areas

This example shows how to configure an OSPF stub area and a totally stubby area to control the advertisement of external routes into an area.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

The backbone area, which is 0 in Figure 6 on page 39, has a special function and is always assigned the area ID 0.0.0.0. Area IDs are unique numeric identifiers, in dotted decimal notation. Area IDs need only be unique within an autonomous system (AS). All other networks or areas (such as 3, 7, and 9) in the AS must be directly connected to the backbone area by area border routers (ABRs) that have interfaces in more than one area.

Stub areas are areas through which or into which OSPF does not flood AS external link-state advertisements (Type 5 LSAs). You might create stub areas when much of the topology database consists of AS external advertisements and you want to minimize the size of the topology databases on the internal routers in the stub area.

The following restrictions apply to stub areas:

- You cannot create a virtual link through a stub area.
- A stub area cannot contain an AS boundary router.
- You cannot configure the backbone as a stub area.
- You cannot configure an area as both a stub area and an not-so-stubby area (NSSA).

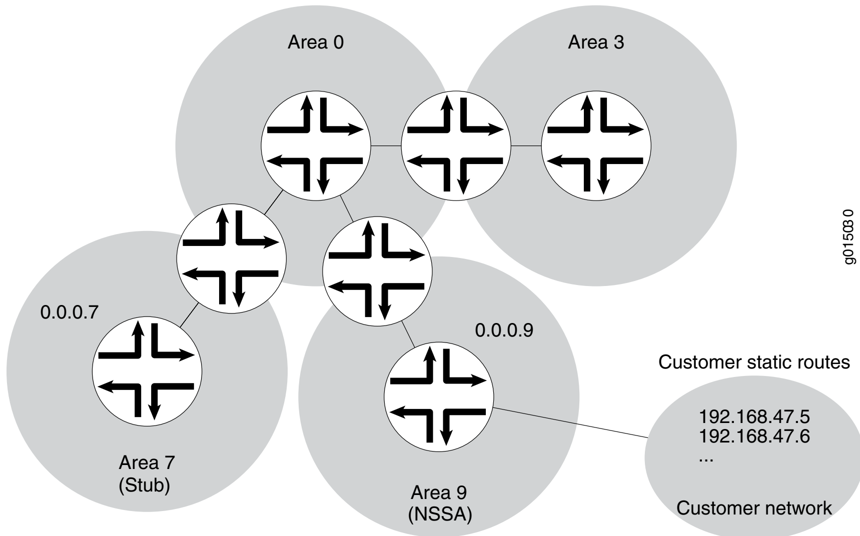
In this example, you configure each routing device in area 7 (area ID 0.0.0.7) as a stub router and some additional settings on the ABR:

- **stub**—Specifies that this area become a stub area and not be flooded with Type 5 LSAs. You must include the **stub** statement on all routing devices that are in area 7 because this area has no external connections.
- **default-metric**—Configures the ABR to generate a default route with a specified metric into the stub area. This default route enables packet forwarding from the stub area to external destinations. You configure this option only on the ABR. The ABR does not automatically generate a default route when attached to a stub. You must explicitly configure this option to generate a default route.
- **no-summaries**—(Optional) Prevents the ABR from advertising summary routes into the stub area by converting the stub area into a totally stubby area. If configured in combination with the **default-metric** statement, a totally stubby area only allows routes internal to the area and advertises the default route into the area. External routes and destinations to other areas are no longer summarized or allowed into a totally stubby area. Only the ABR requires this additional configuration because it is the only routing device within the totally stubby area that creates Type 3 LSAs used to receive and send traffic from outside of the area.

NOTE:
In Junos OS Release 8.5 and later, the following applies:

- A router-identifier interface that is not configured to run OSPF is no longer advertised as a stub network in OSPF LSAs.
- OSPF advertises a local route with a prefix length of 32 as a stub link if the loopback interface is configured with a prefix length other than 32. OSPF also advertises the direct route with the configured mask length, as in earlier releases.

Figure 6: OSPF Network Topology with Stub Areas and NSSAs



Configuration

CLI Quick Configuration

- To quickly configure an OSPF stub area, copy the following command and paste it into the CLI. You must configure all routing devices that are part of the stub area.

```
[edit]
set protocols ospf area 0.0.0.7 stub
```

- To quickly configure the ABR to inject a default route into the area, copy the following command and paste it into the CLI. You apply this configuration only on the ABR.

```
[edit]
set protocols ospf area 0.0.0.7 stub default-metric 10
```

- (Optional) To quickly configure the ABR to restrict all summary advertisements and allow only internal routes and default route advertisements into the area, copy the following command and paste it into the CLI. You apply this configuration only on the ABR.

```
[edit]
set protocols ospf area 0.0.0.7 stub no-summaries
```

Step-by-Step Procedure

To configure OSPF stub areas:

1. On all routing devices in the area, configure an OSPF stub area.

   NOTE: To specify an OSPFv3 stub area, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.7 stub
   ```

2. On the ABR, inject a default route into the area.

```
[edit]
user@host# set protocols ospf area 0.0.0.7 stub default-metric 10
```

3. (Optional) On the ABR, restrict summary LSAs from entering the area. This step converts the stub area into a totally stubby area.

```
[edit]
user@host# set protocols ospf area 0.0.0.7 stub no-summaries
```

4. If you are done configuring the devices, commit the configuration.

```
[edit]
user@host# commit
```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on all routing devices:

```
user@host# show protocols ospf
area 0.0.0.7 {
  stub;
}
```

Configuration on the ABR (the output also includes the optional setting):

```
user@host# show protocols ospf
area 0.0.0.7 {
  stub default-metric 10 no-summaries;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the Interfaces in the Area on page 40
- Verifying the Type of OSPF Area on page 40

Verifying the Interfaces in the Area

Purpose Verify that the interface for OSPF has been configured for the appropriate area. Confirm that the output includes Stub as the type of OSPF area.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Verifying the Type of OSPF Area

Purpose Verify that the OSPF area is a stub area. Confirm that the output displays Normal Stub as the Stub type.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** command for OSPFv3.

Example: Configuring OSPF Not-So-Stubby Areas

This example shows how to configure an OSPF not-so-stubby area (NSSA) to control the advertisement of external routes into an area.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

The backbone area, which is 0 in Figure 7 on page 43, has a special function and is always assigned the area ID 0.0.0.0. Area IDs are unique numeric identifiers, in dotted decimal notation. Area IDs need only be unique within an AS. All other networks or areas (such as 3, 7, and 9) in the AS must be directly connected to the backbone area by ABRs that have interfaces in more than one area.

An OSPF stub area has no external routes, so you cannot redistribute routes from another protocol into a stub area. OSPF NSSAs allow external routes to be flooded within the area.

In addition, you might have a situation when exporting Type 7 LSAs into the NSSA is unnecessary. When an AS boundary router is also an ABR with an NSSA attached, Type 7 LSAs are exported into the NSSA by default. If the ABR is attached to multiple NSSAs, a separate Type 7 LSA is exported into each NSSA by default. During route redistribution, this routing device generates both Type 5 LSAs and Type 7 LSAs. You can disable exporting Type 7 LSAs into the NSSA.

NOTE: The following restriction applies to NSSAs: You cannot configure an area as both a stub area and an NSSA.

You configure each routing device in area 9 (area ID 0.0.0.9) with the following setting:

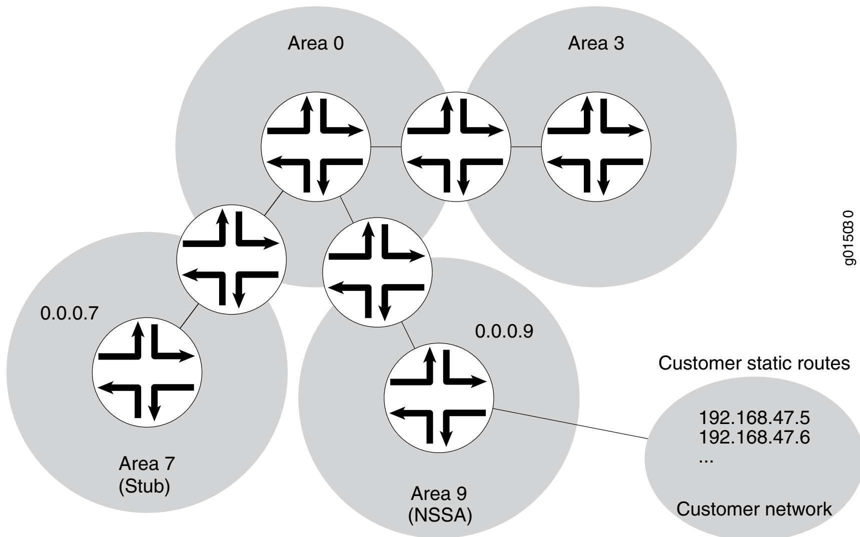
- **nssa**—Specifies an OSPF NSSA. You must include the **nssa** statement on all routing devices in area 9 because this area only has external connections to static routes.

You also configure the ABR in area 9 with the following additional settings:

- **no-summaries**—Prevents the ABR from advertising summary routes into the NSSA. If configured in combination with the **default-metric** statement, the NSSA only allows routes internal to the area and advertises the default route into the area. External routes and destinations to other areas are no longer summarized or allowed into the NSSA. Only the ABR requires this additional configuration because it is the only routing device within the NSSA that creates Type 3 LSAs used to receive and send traffic from outside the area.
- **default-lsa**—Configures the ABR to generate a default route into the NSSA. In this example, you configure the following:
  - **default-metric**—Specifies that the ABR generate a default route with a specified metric into the NSSA. This default route enables packet forwarding from the NSSA to external destinations. You configure this option only on the ABR. The ABR does not automatically generate a default route when attached to an NSSA. You must explicitly configure this option for the ABR to generate a default route.
  - **metric-type**—(Optional) Specifies the external metric type for the default LSA, which can be either Type 1 or Type 2. When OSPF exports route information from external ASs, it includes a cost, or external metric, in the route. The difference between the two metrics is how OSPF calculates the cost of the route. Type 1 external metrics are equivalent to the link-state metric, where the cost is equal to the sum of the internal costs plus the external cost. Type 2 external metrics use only the external cost assigned by the AS boundary router. By default, OSPF uses the Type 2 external metric.
  - **type-7**—(Optional) Floods Type 7 default LSAs into the NSSA if the **no-summaries** statement is configured. By default, when the **no-summaries** statement is configured, a Type 3 LSA is injected into NSSAs for Junos OS release 5.0 and later. To support backward compatibility with earlier Junos OS releases, include the **type-7** statement.

The second example also shows the optional configuration required to disable exporting Type 7 LSAs into the NSSA by including the **no-nssa-abr** statement on the routing device that performs the functions of both an ABR and an AS boundary router.

Figure 7: OSPF Network Topology with Stub Areas and NSSAs



Configuration

- Configuring Routing Devices to Participate in a Not-So-Stubby-Area on page 43
- Disabling the Export of Type 7 Link State Advertisements into Not-So-Stubby Areas on page 45

Configuring Routing Devices to Participate in a Not-So-Stubby-Area

CLI Quick Configuration

To quickly configure an OSPF NSSA, copy the following command and paste it into the CLI. You must configure all routing devices that are part of the NSSA.

```
[edit]
set protocols ospf area 0.0.0.9 nssa
```

To quickly configure an ABR that participates in an OSPF NSSA, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf area 0.0.0.9 nssa default-lsa default-metric 10
set protocols ospf area 0.0.0.9 nssa default-lsa metric-type 1
set protocols ospf area 0.0.0.9 nssa default-lsa type-7
set protocols ospf area 0.0.0.9 nssa no-summaries
```

Step-by-Step Procedure

To configure OSPF NSSAs:

1. On all routing devices in the area, configure an OSPF NSSA.

   NOTE: To specify an OSPFv3 NSSA area, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.9 nssa
   ```


2. On the ABR, enter OSPF configuration mode and specify the NSSA area 0.0.0.9 that you already created.

   ```
   [edit ]
   user@host# edit protocols ospf area 0.0.0.9 nssa
   ```

3. On the ABR, inject a default route into the area.

   ```
   [edit protocols ospf area 0.0.0.9 nssa]
   user@host# set default-lsa default-metric 10
   ```

4. (Optional) On the ABR, specify the external metric type for the default route.

   ```
   [edit protocols ospf area 0.0.0.9 nssa]
   user@host# set default-lsa metric-type 1
   ```

5. (Optional) On the ABR, specify the flooding of Type 7 LSAs.

   ```
   [edit protocols ospf area 0.0.0.9 nssa]
   user@host# set default-lsa type-7
   ```

6. On the ABR, restrict summary LSAs from entering the area.

   ```
   [edit protocols ospf area 0.0.0.9 nssa]
   user@host# set no-summaries
   ```

7. If you are done configuring the devices, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.9 nssa]
   user@host# commit
   ```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on all routing devices in the area:

```
user@host# show protocols ospf
area 0.0.0.9 {
  nssa;
}
```

Configuration on the ABR. The output also includes the optional **metric-type** and **type-7** statements.

```
user@host# show protocols ospf
  area 0.0.0.9 {
  nssa {
    default-lsa {
      default-metric 10;
      metric-type 1;
      type-7;
    }
    no-summaries;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Disabling the Export of Type 7 Link State Advertisements into Not-So-Stubby Areas

CLI Quick Configuration

To quickly disable exporting Type 7 LSAs into the NSSA, copy the following command and paste it into the CLI. You configure this setting on an AS boundary router that is also an ABR with an NSSA area attached.

```
[edit]
set protocols ospf no-nssa-abr
```

Step-by-Step Procedure

You can configure this setting if you have an AS boundary router that is also an ABR with an NSSA area attached.

1. Disable exporting Type 7 LSAs into the NSSA.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf no-nssa-abr
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
no-nssa-abr;
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the Interfaces in the Area on page 45
- Verifying the Type of OSPF Area on page 46
- Verifying the Type of LSAs on page 46

Verifying the Interfaces in the Area

Purpose

Verify that the interface for OSPF has been configured for the appropriate area. Confirm that the output includes Stub NSSA as the type of OSPF area.

Action

From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Verifying the Type of OSPF Area

Purpose Verify that the OSPF area is a stub area. Confirm that the output displays Not so Stubby Stub as the Stub type.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** command for OSPFv3.

Verifying the Type of LSAs

Purpose Verify the type of LSAs that are in the area. If you disabled exporting Type 7 LSAs into an NSSA, confirm that the Type field does not include NSSA as a type of LSA.

Action From operational mode, enter the **show ospf database** command for OSPFv2, and enter the **show ospf3 database** command for OSPFv3.

Related Documentation

- Example: Configuring OSPFv3 Stub and Totally Stubby Areas on page 46
- OSPF Areas and Router Functionality Overview on page 9
- OSPF Configuration Overview on page 14

Example: Configuring OSPFv3 Stub and Totally Stubby Areas

Understanding OSPFv3 Stub and Totally Stubby Areas

Junos OS OSPFv3 configuration for IPv6 networks is identical to OSPFv2 configuration. You configure the protocol with **set ospf3** commands instead of **set ospf** commands and use **show ospf3** commands instead of **show ospf** commands to check the OSPF status. Also, make sure to set IPv6 addresses on the interfaces running OSPFv3.

Stub areas are areas through which or into which OSPF does not flood AS external link-state advertisements (Type 5 LSAs). You might create stub areas when much of the topology database consists of AS external advertisements and you want to minimize the size of the topology databases on the internal routers in the stub area.

The following restrictions apply to stub areas:

- You cannot create a virtual link through a stub area.
- A stub area cannot contain an AS boundary router.
- You cannot configure the backbone as a stub area.
- You cannot configure an area as both a stub area and an not-so-stubby area (NSSA).

Example: Configuring OSPFv3 Stub and Totally Stubby Areas

This example shows how to configure an OSPFv3 stub area and a totally stubby area to control the advertisement of external routes into an area.

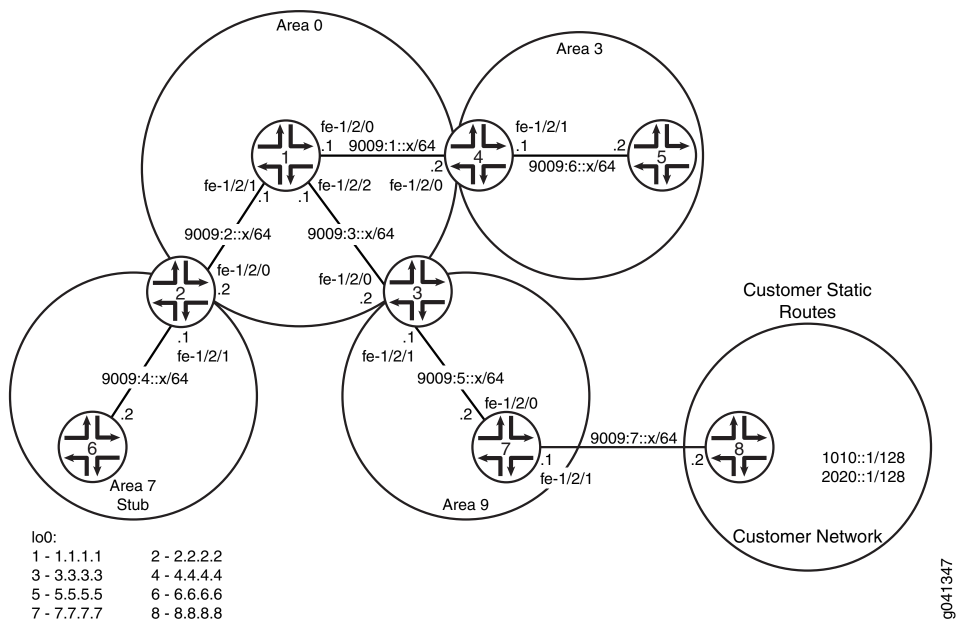
Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

Figure 8 on page 47 shows the topology used in this example.

Figure 8: OSPFv3 Network Topology with Stub Areas



In this example, you configure each routing device in area 7 (area ID 0.0.0.7) as a stub router and some additional settings on the ABR:

- **stub**—Specifies that this area become a stub area and not be flooded with Type 5 LSAs. You must include the **stub** statement on all routing devices that are in area 7 because this area has no external connections.
- **default-metric**—Configures the ABR to generate a default route with a specified metric into the stub area. This default route enables packet forwarding from the stub area to external destinations. You configure this option only on the ABR. The ABR does not

automatically generate a default route when attached to a stub. You must explicitly configure this option to generate a default route.

- **no-summaries**—(Optional) Prevents the ABR from advertising summary routes into the stub area by converting the stub area into a totally stubby area. If configured in combination with the **default-metric** statement, a totally stubby area only allows routes internal to the area and advertises the default route into the area. External routes and destinations to other areas are no longer summarized or allowed into a totally stubby area. Only the ABR requires this additional configuration because it is the only routing device within the totally stubby area that creates Type 3 LSAs used to receive and send traffic from outside of the area.

NOTE:
In Junos OS Release 8.5 and later, the following applies:

- A router-identifier interface that is not configured to run OSPF is no longer advertised as a stub network in OSPF LSAs.
- OSPF advertises a local route with a prefix length of 32 as a stub link if the loopback interface is configured with a prefix length other than 32. OSPF also advertises the direct route with the configured mask length, as in earlier releases.

"CLI Quick Configuration" on page 48 shows the configuration for all of the devices in Figure 8 on page 47. The section "Step-by-Step Procedure" on page 49 describes the steps on Device 2, Device 6, Device 7, and Device 8.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device 1

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::1/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:2::1/64
set interfaces fe-1/2/2 unit 0 family inet6 address 9009:3::1/64
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.0 interface fe-1/2/2.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
```

Device 2

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:2::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
set interfaces lo0 unit 0 family inet address 2.2.2.2/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.7 stub default-metric 10
set protocols ospf3 area 0.0.0.7 stub no-summaries
set protocols ospf3 area 0.0.0.7 interface fe-1/2/1.0
```

Device 3

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:3::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:5::1/64
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.9 interface fe-1/2/1.0
```

Device 4

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:6::1/64
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.3 interface fe-1/2/1.0
```

Device 5

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:6::2/64
set interfaces lo0 unit 0 family inet address 5.5.5.5/32
set protocols ospf3 area 0.0.0.3 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.3 interface lo0.0 passive
```

Device 6

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:4::2/64
set interfaces lo0 unit 0 family inet address 6.6.6.6/32
set protocols ospf3 area 0.0.0.7 stub
set protocols ospf3 area 0.0.0.7 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.7 interface lo0.0 passive
```

Device 7

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:5::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:7::1/64
set interfaces lo0 unit 0 family inet address 7.7.7.7/32
set protocols ospf3 export static-to-ospf
set protocols ospf3 area 0.0.0.9 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.9 interface lo0.0 passive
set policy-options policy-statement static-to-ospf term 1 from protocol static
set policy-options policy-statement static-to-ospf term 1 then accept
set routing-options rib inet6.0 static route 1010::1/128 next-hop 9009:7::2
set routing-options rib inet6.0 static route 2020::1/128 next-hop 9009:7::2
```

Device 8

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:7::2/64
set interfaces lo0 unit 0 family inet address 8.8.8.8/32
set interfaces lo0 unit 0 family inet6 address 1010::1/128
set interfaces lo0 unit 0 family inet6 address 2020::1/128
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 2:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@2# set fe-1/2/0 unit 0 family inet6 address 9009:2::2/64
   user@2# set fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
   user@2# set lo0 unit 0 family inet address 2.2.2.2/32
   ```

2. Enable OSPFv3 on the interfaces that are in area 0.

```
[edit protocols ospf3 area 0.0.0.0]
user@2# set interface fe-1/2/0.0
user@2# set interface lo0.0 passive
```

3. Enable OSPFv3 on the interface that is in area 7.

```
[edit protocols ospf3 area 0.0.0.7]
user@2# set interface fe-1/2/1.0
```

4. Specify area 7 as an OSPFv3 stub area.

   The **stub** statement is required on all routing devices in the area.

```
[edit protocols ospf3 area 0.0.0.7]
user@2# set stub
```

5. On the ABR, inject a default route into the area.

```
[edit protocols ospf3 area 0.0.0.7]
user@2# set stub default-metric 10
```

6. (Optional) On the ABR, restrict summary LSAs from entering the area.

   This step converts the stub area into a totally stubby area.

```
[edit protocols ospf3 area 0.0.0.7]
user@2# set stub no-summaries
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 6:

1. Configure the interfaces.

```
[edit interfaces]
user@6# set fe-1/2/0 unit 0 family inet6 address 9009:4::2/64
user@6# set lo0 unit 0 family inet address 6.6.6.6/32
```

2. Enable OSPFv3 on the interface that is in area 7.

```
[edit protocols ospf3 area 0.0.0.7]
user@6# set interface fe-1/2/0.0
user@6# set interface lo0.0 passive
```

3. Specify area 7 as an OSPFv3 stub area.

   The **stub** statement is required on all routing devices in the area.

```
[edit protocols ospf3 area 0.0.0.7]
user@6# set stub
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 7:

1. Configure the interfaces.


```
[edit interfaces]
user@7# set fe-1/2/0 unit 0 family inet6 address 9009:5::2/64
user@7# set fe-1/2/1 unit 0 family inet6 address 9009:7::1/64
user@7# set lo0 unit 0 family inet address 7.7.7.7/32
```

2. Enable OSPFv3 on the interface that is in area 9.

```
[edit protocols ospf3 area 0.0.0.9]
user@7# set interface fe-1/2/0.0
user@7# set interface lo0.0 passive
```

3. Configure static routes that enable connectivity to the customer routes.

```
[edit routing-options rib inet6.0 static]
user@7# set route 1010::1/128 next-hop 9009:7::2
user@7# set route 2020::1/128 next-hop 9009:7::2
```

4. Configure a routing policy to redistribute the static routes.

```
[edit policy-options policy-statement static-to-ospf term 1]
user@7# set from protocol static
user@7# set then accept
```

5. Apply the routing policy to the OSPFv3 instance.

```
[edit protocols ospf3]
user@7# set export static-to-ospf
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 8:

1. Configure the interfaces.

```
[edit interfaces]
user@8# set fe-1/2/0 unit 0 family inet6 address 9009:7::2/64
user@8# set lo0 unit 0 family inet address 8.8.8.8/32
```

2. Configure two loopback interface addresses to simulate customer routes.

```
[edit interfaces lo0 unit 0 family inet6]
user@8# set address 1010::1/128
user@8# set address 2020::1/128
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device 2

```
user@2# show interfaces
fe-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:2::2/64;
    }
  }
}
```

```
fe-1/2/1 {
   unit 0 {
      family inet6 {
         address 9009:4::1/64;
      }
   }
}
lo0 {
   unit 0 {
      family inet {
         address 2.2.2.2/32;
      }
   }
}

user@2# show protocols
ospf3 {
   area 0.0.0.0 {
      interface fe-1/2/0.0;
      interface lo0.0 {
         passive;
      }
   }
   area 0.0.0.7 {
      stub default-metric 10 no-summaries;
      interface fe-1/2/1.0;
   }
}
```

Device 6

```
user@6# show interfaces
fe-1/2/0 {
   unit 0 {
      family inet6 {
         address 9009:4::2/64;
      }
   }
}
lo0 {
   unit 0 {
      family inet {
         address 6.6.6.6/32;
      }
   }
}

user@6# show protocols
ospf3 {
   area 0.0.0.7 {
      stub;
      interface fe-1/2/0.0;
      interface lo0.0 {
         passive;
      }
   }
}
```

Device 7

```
user@7# show interfaces
fe-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:5::2/64;
    }
  }
}
fe-1/2/1 {
  unit 0 {
    family inet6 {
      address 9009:7::1/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 7.7.7.7/32;
    }
  }
}

user@7# show protocols
ospf3 {
  export static-to-ospf;
  area 0.0.0.9 {
    interface fe-1/2/0.0;
    interface lo0.0 {
      passive;
    }
  }
}

user@7# show policy-options
policy-statement static-to-ospf {
  term 1 {
    from protocol static;
    then accept;
  }
}

user@7# show routing-options
rib inet6.0 {
  static {
    route 1010::1/128 next-hop 9009:7::2;
    route 2020::1/128 next-hop 9009:7::2;
  }
}
```

Device 8

```
user@8# show interfaces
fe-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:7::2/64;
    }
  }
```

```
}
lo0 {
  unit 0 {
    family inet {
      address 8.8.8.8/32;
    }
    family inet6 {
      address 1010::1/128;
      address 2020::1/128;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Type of OSPFv3 Area

Purpose Verify that the OSPFv3 area is a stub area. Confirm that the output displays Stub as the Stub type.

Action From operational mode on Device 2 and on Device 6, enter the **show ospf3 overview** command.

```
user@2> show ospf3 overview
Instance: master
  Router ID: 2.2.2.2
  Route table index: 51
  Area border router
  LSA refresh time: 50 minutes
  Area: 0.0.0.0
    Stub type: Not Stub
    Area border routers: 2, AS boundary routers: 0
    Neighbors
      Up (in full state): 1
  Area: 0.0.0.7
    Stub type: Stub, Stub cost: 10
    Area border routers: 0, AS boundary routers: 0
    Neighbors
      Up (in full state): 1
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 24
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed

user@6> show ospf3 overview
Instance: master
  Router ID: 6.6.6.6
  Route table index: 46
  LSA refresh time: 50 minutes
  Area: 0.0.0.7
    Stub type: Stub
    Area border routers: 1, AS boundary routers: 0
    Neighbors
```



```
    Up (in full state): 1
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 17
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed
```

Meaning On Device 2, the stub type of area 0 is **Not Stub**. The stub type of area 7 is **Stub**. The stub default metric is 10.

On Device 6, the stub type of area 7 is **Stub**.

Verifying the Routes in the OSPFv3 Stub Area

Purpose Make sure that the expected routes are present in the routing tables.

Action From operational mode on Device 6 and Device 2, enter the **show route** command.

```
user@6> show route
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

6.6.6.6/32         *[Direct/0] 1d 01:57:12
                    > via lo0.0

inet6.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[OSPF3/10] 00:10:52, metric 11
                    > via fe-1/2/0.0
9009:4::/64        *[Direct/0] 1d 01:56:31
                    > via fe-1/2/0.0
                    [OSPF3/10] 1d 01:56:31, metric 1
                    > via fe-1/2/0.0
9009:4::2/128      *[Local/0] 1d 01:56:53
                      Local via fe-1/2/0.0
fe80::/64          *[Direct/0] 1d 01:56:31
                    > via fe-1/2/0.0
fe80::2a0:a514:0:a4c/128
                   *[Local/0] 1d 01:56:53
                      Local via fe-1/2/0.0
ff02::5/128        *[OSPF3/10] 1d 01:58:22, metric 1
                      MultiRecv

user@2> show route
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2.2.2.2/32         *[Direct/0] 1d 02:16:13
                    > via lo0.0

inet6.0: 14 destinations, 17 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1010::1/128        *[OSPF3/150] 00:30:15, metric 0, tag 0
                    > via fe-1/2/0.0
2020::1/128        *[OSPF3/150] 00:30:15, metric 0, tag 0
                    > via fe-1/2/0.0
9009:1::/64        *[OSPF3/10] 1d 02:15:54, metric 2
```



```
                          > via fe-1/2/0.0
9009:2::/64              *[Direct/0] 1d 02:15:54
                          > via fe-1/2/0.0
                          [OSPF3/10] 1d 02:15:54, metric 1
                          > via fe-1/2/0.0
9009:2::2/128            *[Local/0] 1d 02:15:54
                            Local via fe-1/2/0.0
9009:3::/64              *[OSPF3/10] 1d 02:15:54, metric 2
                          > via fe-1/2/0.0
9009:4::/64              *[Direct/0] 1d 02:15:54
                          > via fe-1/2/1.0
                          [OSPF3/10] 05:38:05, metric 1
                          > via fe-1/2/1.0
9009:4::1/128            *[Local/0] 1d 02:15:54
                            Local via fe-1/2/1.0
9009:5::/64              *[OSPF3/10] 1d 02:15:54, metric 3
                          > via fe-1/2/0.0
9009:6::/64              *[OSPF3/10] 1d 01:33:10, metric 3
                          > via fe-1/2/0.0
fe80::/64                *[Direct/0] 1d 02:15:54
                          > via fe-1/2/0.0
                          [Direct/0] 1d 02:15:54
                          > via fe-1/2/1.0
fe80::2a0:a514:0:64c/128
                         *[Local/0] 1d 02:15:54
                            Local via fe-1/2/0.0
fe80::2a0:a514:0:94c/128
                         *[Local/0] 1d 02:15:54
                            Local via fe-1/2/1.0
ff02::5/128              *[OSPF3/10] 1d 02:17:45, metric 1
                            MultiRecv
```

Meaning On Device 6, the default route has been learned because of the **default-metric** statement on the ABR, Device 2. Otherwise, the only OSPFv3 routes in Device 6's routing table are the network address 9009:4::/64 and the OSPFv3 multicast address ff02::5/128 for all SPF link-state routers, also known as AllSPFRouters.

On Device 2, all of the OSPFv3 routes have been learned, including the external customer routes, 1010::1/128 and 2020::1/128.

Related Documentation

- Examples: Configuring OSPF Stub and Not-So-Stubby Areas on page 35
- Example: Configuring OSPFv3 Not-So-Stubby Areas with Filtering on page 69

Example: Configuring OSPFv3 Not-So-Stubby Areas

- Understanding OSPFv3 Not-So-Stubby Areas on page 56
- Example: Configuring OSPFv3 Not-So-Stubby Areas on page 57

Understanding OSPFv3 Not-So-Stubby Areas

Like an OSPF stub area, an OSPFv3 stub area has no external routes, so you cannot redistribute routes from another protocol into a stub area. Not-so-stubby-areas (NSSAs) allow external routes to be flooded within the area. Routers in an NSSA do not receive external link-state advertisements (LSAs) from area border routers (ABRs), but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the ABR then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network.

Example: Configuring OSPFv3 Not-So-Stubby Areas

This example shows how to configure an OSPFv3 not-so-stubby area (NSSA) to control the advertisement of external routes into the area.

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

In this example, Device 7 redistributes static Customer 1 routes into OSPFv3. Device 7 is in area 9, which is configured as an NSSA. Device 3 is the ABR attached to the NSSA. An NSSA is a type of stub area that can import autonomous system external routes and send them to other areas, but still cannot receive AS-external routes from other areas. Because area 9 is defined as an NSSA, Device 7 uses type 7 LSAs to tell the ABR (Device 3) about these external routes. Device 3 then translates the type 7 routes to type 5 external LSAs and floods them as normal to the rest of the OSPF network.

In area 3, Device 5 redistributes static Customer 2 routes into OSPFv3. These routes are learned on Device 3, but not on Device 7 or 10. Device 3 injects a default static route into area 9 so that Device 7 and 10 can still reach the Customer 2 routes.

You configure each routing device in area 9 (area ID 0.0.0.9) with the following setting:

- **nssa**—Specifies an OSPFv3 NSSA. You must include the **nssa** statement on all routing devices in area 9.

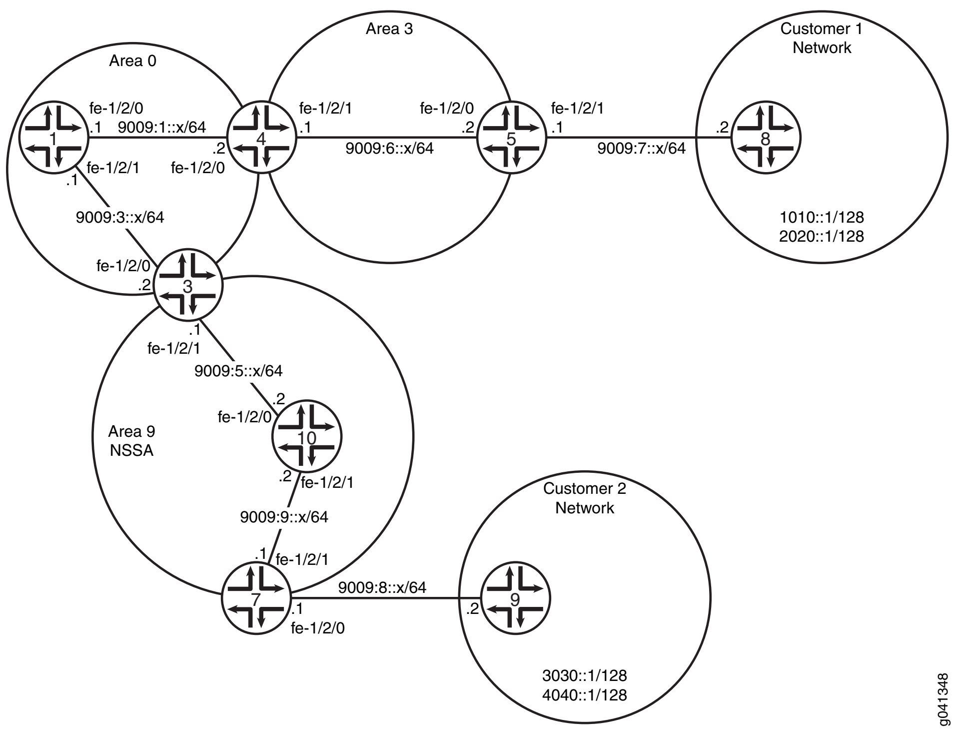
You also configure the ABR in area 9 with the following additional settings:

- **no-summaries**—Prevents the ABR from advertising summary routes into the NSSA. If configured in combination with the **default-metric** statement, the NSSA only allows routes internal to the area and advertises the default route into the area. External routes and destinations to other areas are no longer summarized or allowed into the NSSA. Only the ABR requires this additional configuration because it is the only routing device within the NSSA that creates Type 3 summary LSAs used to receive and send traffic from outside the area.
- **default-lsa**—Configures the ABR to generate a default route into the NSSA. In this example, you configure the following:
  - **default-metric**—Specifies that the ABR generate a default route with a specified metric into the NSSA. This default route enables packet forwarding from the NSSA

to external destinations. You configure this option only on the ABR. The ABR does not automatically generate a default route when attached to an NSSA. You must explicitly configure this option for the ABR to generate a default route.

- **metric-type**—(Optional) Specifies the external metric type for the default LSA, which can be either Type 1 or Type 2. When OSPFv3 exports route information from external ASs, it includes a cost, or external metric, in the route. The difference between the two metrics is how OSPFv3 calculates the cost of the route. Type 1 external metrics are equivalent to the link-state metric, where the cost is equal to the sum of the internal costs plus the external cost. Type 2 external metrics use only the external cost assigned by the AS boundary router. By default, OSPFv3 uses the Type 2 external metric.
- **type-7**—(Optional) Floods Type 7 default LSAs into the NSSA if the **no-summaries** statement is configured. By default, when the **no-summaries** statement is configured, a Type 3 LSA is injected into NSSAs for Junos OS release 5.0 and later. To support backward compatibility with earlier Junos OS releases, include the **type-7** statement.

Figure 9: OSPFv3 Network Topology with an NSSA



"CLI Quick Configuration" on page 58 shows the configuration for all of the devices in Figure 9 on page 58. The section "Step-by-Step Procedure" on page 60 describes the steps on Device 3, Device 7, and Device 9.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device 1

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::1/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:3::1/64
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.5
set protocols ospf3 area 0.0.0.0 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
```

Device 3

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:3::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:5::1/64
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.9 nssa default-lsa default-metric 10
set protocols ospf3 area 0.0.0.9 nssa default-lsa metric-type 1
set protocols ospf3 area 0.0.0.9 nssa default-lsa type-7
set protocols ospf3 area 0.0.0.9 nssa no-summaries
set protocols ospf3 area 0.0.0.9 interface fe-1/2/1.0
```

Device 4

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:6::1/64
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.3 interface fe-1/2/1.0
```

Device 5

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:6::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:7::1/64
set interfaces lo0 unit 0 family inet address 5.5.5.5/32
set protocols ospf3 export static-to-ospf
set protocols ospf3 area 0.0.0.3 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.3 interface lo0.0 passive
set policy-options policy-statement static-to-ospf term 1 from protocol static
set policy-options policy-statement static-to-ospf term 1 then accept
set routing-options rib inet6.0 static route 1010::1/128 next-hop 9009:7::2
set routing-options rib inet6.0 static route 2020::1/128 next-hop 9009:7::2
```

Device 7

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:8::1/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:9::1/64
set interfaces lo0 unit 0 family inet address 7.7.7.7/32
set protocols ospf3 export static2-to-ospf
set protocols ospf3 area 0.0.0.9 nssa
set protocols ospf3 area 0.0.0.9 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.9 interface lo0.0 passive
set policy-options policy-statement static2-to-ospf term 1 from protocol static
set policy-options policy-statement static2-to-ospf term 1 then accept
set routing-options rib inet6.0 static route 3030::1/128 next-hop 9009:8::2
set routing-options rib inet6.0 static route 4040::1/128 next-hop 9009:8::2
```

Device 8

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:7::2/64
set interfaces lo0 unit 0 family inet address 8.8.8.8/32
set interfaces lo0 unit 0 family inet6 address 1010::1/128
```

set interfaces lo0 unit 0 family inet6 address 2020::1/128

Device 9

set interfaces fe-1/2/0 unit 0 family inet6 address 9009:8::2/64
set interfaces lo0 unit 0 family inet address 9.9.9.9/32
set interfaces lo0 unit 0 family inet6 address 3030::1/128
set interfaces lo0 unit 0 family inet6 address 4040::1/128

Device 10

set interfaces fe-1/2/0 unit 0 family inet6 address 9009:5::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:9::2/64
set interfaces lo0 unit 0 family inet address 10.10.10.10/32
set protocols ospf3 area 0.0.0.9 nssa
set protocols ospf3 area 0.0.0.9 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.9 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.9 interface lo0.0 passive

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 3:

1. Configure the interfaces.

   [edit interfaces]
   user@3# **set fe-1/2/0 unit 0 family inet6 address 9009:3::2/64**
   user@3# **set fe-1/2/1 unit 0 family inet6 address 9009:5::1/64**
   user@3# **set lo0 unit 0 family inet address 3.3.3.3/32**

2. Enable OSPFv3 on the interfaces that are in area 0.

   [edit protocols ospf3 area 0.0.0.0]
   user@3# **set interface fe-1/2/0.0**
   user@3# **set interface lo0.0 passive**

3. Enable OSPFv3 on the interface that is in area 9.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set interface fe-1/2/1.0**

4. Configure an OSPFv3 NSSA.

   The **nssa** statement is required on all routing devices in the area.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set nssa**

5. On the ABR, inject a default route into the area.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set default-lsa default-metric 10**

6. (Optional) On the ABR, specify the external metric type for the default route.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set nssa default-lsa metric-type 1**

7. (Optional) On the ABR, specify the flooding of Type 7 LSAs.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set nssa default-lsa type-7**

8. On the ABR, restrict summary LSAs from entering the area.

   [edit protocols ospf3 area 0.0.0.9]
   user@3# **set nssa no-summaries**

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 5:

1. Configure the interfaces.

   [edit interfaces]
   user@5# **set fe-1/2/0 unit 0 family inet6 address 9009:6::2/64**
   user@5# **set fe-1/2/1 unit 0 family inet6 address 9009:7::1/64**
   user@5# **set lo0 unit 0 family inet address 5.5.5.5/32**

2. Enable OSPFv3 on the interface that is in area 3.

   [edit protocols ospf3 area 0.0.0.3]
   user@5# **set interface fe-1/2/0.0**
   user@5# **set interface lo0.0 passive**

3. Configure static routes that enable connectivity to the customer routes.

   [edit routing-options rib inet6.0 static]
   user@5# **set route 1010::1/128 next-hop 9009:7::2**
   user@5# **set route 2020::1/128 next-hop 9009:7::2**

4. Configure a routing policy to redistribute the static routes.

   [edit policy-options policy-statement static-to-ospf term 1]
   user@5# **set from protocol static**
   user@5# **set then accept**

5. Apply the routing policy to the OSPFv3 instance.

   [edit protocols ospf3]
   user@5# **set export static-to-ospf**

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 7:

1. Configure the interfaces.

   [edit interfaces]
   user@7# **set fe-1/2/0 unit 0 family inet6 address 9009:5::2/64**
   user@7# **set fe-1/2/1 unit 0 family inet6 address 9009:7::1/64**
   user@7# **set lo0 unit 0 family inet address 7.7.7.7/32**

2. Enable OSPFv3 on the interface that is in area 9.

   [edit protocols ospf3 area 0.0.0.9]
   user@7# **set interface fe-1/2/0.0**
   user@7# **set interface lo0.0 passive**

3. Configure an OSPFv3 NSSA.

   The **nssa** statement is required on all routing devices in the area.

   ```
   [edit protocols ospf3 area 0.0.0.9]
   user@7# set nssa
   ```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 8:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@8# set fe-1/2/0 unit 0 family inet6 address 9009:7::2/64
   user@8# set lo0 unit 0 family inet address 8.8.8.8/32
   ```

2. Configure two loopback interface addresses to simulate customer routes.

   ```
   [edit interfaces lo0 unit 0 family inet6]
   user@8# set address 1010::1/128
   user@8# set address 2020::1/128
   ```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device 3

```
user@3# show interfaces
fe-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:3::2/64;
    }
  }
}
fe-1/2/1 {
  unit 0 {
    family inet6 {
      address 9009:5::1/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 3.3.3.3/32;
    }
  }
}
}

user@3# show protocols
ospf3 {
```

```
    area 0.0.0.0 {
        interface fe-1/2/0.0;
        interface lo0.0 {
            passive;
        }
    }
    area 0.0.0.9 {
        nssa {
            default-lsa {
                default-metric 10;
                metric-type 1;
                type-7;
            }
            no-summaries;
        }
        interface fe-1/2/1.0;
    }
}
```

Device 5

```
user@5# show interfaces
fe-1/2/0 {
    unit 0 {
        family inet6 {
            address 9009:6::2/64;
        }
    }
}
fe-1/2/1 {
    unit 0 {
        family inet6 {
            address 9009:7::1/64;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 5.5.5.5/32;
        }
    }
}

user@5# show protocols
ospf3 {
    export static-to-ospf;
    area 0.0.0.3 {
        interface fe-1/2/0.0;
        interface lo0.0 {
            passive;
        }
    }
}

user@5# show policy-options
policy-statement static-to-ospf {
    term 1 {
```

```
      from protocol static;
      then accept;
    }
}
```

user@5# **show routing-options**

```
rib inet6.0 {
    static {
      route 1010::1/128 next-hop 9009:7::2;
      route 2020::1/128 next-hop 9009:7::2;
    }
}
```

Device 7

user@7# **show interfaces**

```
fe-1/2/0 {
    unit 0{
      family inet6 {
        address 9009:5::2/64;
      }
    }
}
lo0 {
    unit 0 {
      family inet {
        address 7.7.7.7/32;
      }
    }
}
```

user@7# **show protocols**

```
ospf3 {
    area 0.0.0.9 {
      nssa;
      interface fe-1/2/0.0;
      interface lo0.0 {
        passive;
      }
    }
}
```

Device 8

user@8# **show interfaces**

```
fe-1/2/0 {
    unit 0 {
      family inet6 {
        address 9009:7::2/64;
      }
    }
}
lo0 {
    unit 0 {
      family inet {
        address 8.8.8.8/32;
      }
      family inet6 {
        address 1010::1/128;
        address 2020::1/128;
      }
```

```
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Type of OSPFv3 Area

Purpose Verify that the OSPFv3 area is an NSSA area. Confirm that the output displays **Stub NSSA** as the Stub type.

Action From operational mode on Device 3, Device 7, and Device 10 enter the **show ospf3 overview** command.

```
user@3> show ospf3 overview
Instance: master
  Router ID: 3.3.3.3
  Route table index: 36
  Area border router, AS boundary router, NSSA router
  LSA refresh time: 50 minutes
  Area: 0.0.0.0
    Stub type: Not Stub
    Area border routers: 2, AS boundary routers: 0
    Neighbors
      Up (in full state): 1
  Area: 0.0.0.9
    Stub type: Stub NSSA, Stub cost: 10
    Area border routers: 0, AS boundary routers: 1
    Neighbors
      Up (in full state): 1
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 22
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed

user@7> show ospf3 overview
Instance: master
  Router ID: 7.7.7.7
  Route table index: 44
  AS boundary router, NSSA router
  LSA refresh time: 50 minutes
  Area: 0.0.0.9
    Stub type: Stub NSSA
    Area border routers: 1, AS boundary routers: 1
    Neighbors
      Up (in full state): 1
  Topology: default (ID 0)
    Prefix export count: 2
    Full SPF runs: 11
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed

user@10> show ospf3 overview
Instance: master
  Router ID: 10.10.10.10
```



```
  Route table index: 55
  NSSA router
  LSA refresh time: 50 minutes
  Area: 0.0.0.9
    Stub type: Stub NSSA
    Area border routers: 1, AS boundary routers: 2
    Neighbors
      Up (in full state): 2
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 6
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed
```

Meaning On Device 3, the stub type of area 0 is **Not Stub**. The stub type of area 9 is **Stub NSSA**. The stub default metric is 10.

On Device 7 and Device 10, the stub type of area 9 is **Stub NSSA**.

Verifying the Routes in the OSPFv3 Stub Area

Purpose Make sure that the expected routes are present in the routing tables.

Action From operational mode on Device 7 and Device 3, enter the **show route** command.

```
user@7> show route
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

7.7.7.7/32         *[Direct/0] 3d 03:00:23
                    > via lo0.0

inet6.0: 12 destinations, 14 routes (12 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[OSPF3/150] 01:01:31, metric 12, tag 0
                    > via fe-1/2/1.0
3030::1/128        *[Static/5] 01:01:43
                    > to 9009:8::2 via fe-1/2/0.0
4040::1/128        *[Static/5] 01:01:43
                    > to 9009:8::2 via fe-1/2/0.0
9009:5::/64        *[OSPF3/10] 01:01:33, metric 2
                    > via fe-1/2/1.0
9009:8::/64        *[Direct/0] 01:01:43
                    > via fe-1/2/0.0
9009:8::1/128      *[Local/0] 01:02:01
                      Local via fe-1/2/0.0
9009:9::/64        *[Direct/0] 01:01:45
                    > via fe-1/2/1.0
                    [OSPF3/10] 01:01:44, metric 1
                    > via fe-1/2/1.0
9009:9::1/128      *[Local/0] 01:02:01
                      Local via fe-1/2/1.0
fe80::/64          *[Direct/0] 01:01:45
                    > via fe-1/2/1.0
                    [Direct/0] 01:01:43
                    > via fe-1/2/0.0
fe80::2a0:a514:0:f4c/128
                   *[Local/0] 01:02:01
```



```
                      Local via fe-1/2/0.0
fe80::2a0:a514:0:114c/128
                   *[Local/0] 01:02:01
                      Local via fe-1/2/1.0
ff02::5/128        *[OSPF3/10] 3d 03:01:25, metric 1
                      MultiRecv
```

user@10> **show route**

```
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.10/32     *[Direct/0] 01:01:59
                    > via lo0.0

inet6.0: 11 destinations, 14 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[OSPF3/150] 01:01:35, metric 11, tag 0
                    > via fe-1/2/0.0
3030::1/128        *[OSPF3/150] 01:01:35, metric 0, tag 0
                    > via fe-1/2/1.0
4040::1/128        *[OSPF3/150] 01:01:35, metric 0, tag 0
                    > via fe-1/2/1.0
9009:5::/64        *[Direct/0] 01:01:50
                    > via fe-1/2/0.0
                    [OSPF3/10] 01:01:50, metric 1
                    > via fe-1/2/0.0
9009:5::2/128      *[Local/0] 01:01:50
                      Local via fe-1/2/0.0
9009:9::/64        *[Direct/0] 01:01:50
                    > via fe-1/2/1.0
                    [OSPF3/10] 01:01:40, metric 1
                    > via fe-1/2/1.0
9009:9::2/128      *[Local/0] 01:01:50
                      Local via fe-1/2/1.0
fe80::/64          *[Direct/0] 01:01:50
                    > via fe-1/2/0.0
                    [Direct/0] 01:01:50
                    > via fe-1/2/1.0
fe80::2a0:a514:0:c4c/128
                   *[Local/0] 01:01:50
                      Local via fe-1/2/0.0
fe80::2a0:a514:0:124c/128
                   *[Local/0] 01:01:50
                      Local via fe-1/2/1.0
ff02::5/128        *[OSPF3/10] 01:02:16, metric 1
                      MultiRecv
```

user@3> **show route**

```
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3.3.3.3/32         *[Direct/0] 3d 03:03:10
                    > via lo0.0

inet6.0: 15 destinations, 18 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1010::1/128        *[OSPF3/150] 01:04:21, metric 0, tag 0
                    > via fe-1/2/0.0
2020::1/128        *[OSPF3/150] 01:04:21, metric 0, tag 0
```

```
                         > via fe-1/2/0.0
3030::1/128             *[OSPF3/150] 01:03:57, metric 0, tag 0
                         > via fe-1/2/1.0
4040::1/128             *[OSPF3/150] 01:03:57, metric 0, tag 0
                         > via fe-1/2/1.0
9009:1::/64             *[OSPF3/10] 3d 03:02:06, metric 2
                         > via fe-1/2/0.0
9009:3::/64             *[Direct/0] 3d 03:02:55
                         > via fe-1/2/0.0
                         [OSPF3/10] 3d 03:02:54, metric 1
                         > via fe-1/2/0.0
9009:3::2/128           *[Local/0] 3d 03:02:55
                           Local via fe-1/2/0.0
9009:5::/64             *[Direct/0] 01:04:09
                         > via fe-1/2/1.0
                         [OSPF3/10] 01:04:09, metric 1
                         > via fe-1/2/1.0
9009:5::1/128           *[Local/0] 3d 03:02:54
                           Local via fe-1/2/1.0
9009:6::/64             *[OSPF3/10] 3d 02:19:14, metric 3
                         > via fe-1/2/0.0
9009:9::/64             *[OSPF3/10] 01:04:02, metric 2
                         > via fe-1/2/1.0
fe80::/64               *[Direct/0] 3d 03:02:55
                         > via fe-1/2/0.0
                         [Direct/0] 01:04:09
                         > via fe-1/2/1.0
fe80::2a0:a514:0:84c/128
                        *[Local/0] 3d 03:02:55
                           Local via fe-1/2/0.0
fe80::2a0:a514:0:b4c/128
                        *[Local/0] 3d 03:02:54
                           Local via fe-1/2/1.0
ff02::5/128             *[OSPF3/10] 3d 03:03:50, metric 1
                           MultiRecv
```

Meaning On Device 7, the default route has been learned because of the **default-metric** statement on the ABR, Device 3. Otherwise, the only OSPFv3 routes in Device 7's routing table are those local to area 9 and the OSPFv3 multicast address ff02::5/128 for all SPF link-state routers, also known as AllSPFRouters.

Device 10 has the default route injected by Device 3 and also the OSPF external routes injected by Device 7.

Neither Device 7 nor Device 10 has the external customer routes that were injected into OSPFv3 by Device 5.

On Device 3, all of the OSPFv3 routes have been learned, including the external customer routes, 1010::1/128 and 2020::1/128.

Verifying the Type of LSAs

Purpose Verify the type of LSAs that are in the area.

Action From operational mode on Device 7, enter the **show ospf3 database nssa detail** command.

`user@7>` show ospf3 database **nssa detail**


```
Area 0.0.0.9
 Type       ID               Adv Rtr          Seq          Age  Cksum  Len
NSSA       0.0.0.1          3.3.3.3          0x8000002a  1462  0xf406  28
  Prefix ::/0
  Prefix-options 0x0, Metric 10, Type 1,
NSSA      *0.0.0.1          7.7.7.7          0x80000003  1625  0x88df  60
  Prefix 3030::1/128
  Prefix-options 0x8, Metric 0, Type 2,
   Fwd addr 9009:9::1,
NSSA      *0.0.0.2          7.7.7.7          0x80000003  1025  0xef57  60
  Prefix 4040::1/128
  Prefix-options 0x8, Metric 0, Type 2,
   Fwd addr 9009:9::1,
```

Meaning On Device 7, the NSSA LSAs are the type 1 external default route, learned from Device 3, and the type 2 external static routes to the Customer 1 network.

Related Documentation

- Example: Configuring OSPFv3 Stub and Totally Stubby Areas on page 46
- Example: Configuring OSPFv3 Not-So-Stubby Areas with Filtering on page 69

Example: Configuring OSPFv3 Not-So-Stubby Areas with Filtering

Understanding NSSA Filtering

You might have a situation when exporting Type 7 LSAs into a not-so-stubby area (NSSA) is unnecessary. When an autonomous system (AS) boundary router is also an area border router (ABR) with an NSSA attached, Type 7 LSAs are exported into the NSSA by default.

Also, when the ABR is attached to multiple NSSAs, a separate Type 7 LSA is exported into each NSSA by default. During route redistribution, this routing device generates both Type 5 LSAs and Type 7 LSAs.

You can disable exporting Type 7 LSAs into the NSSA by including the **no-nssa-abr** statement on the routing device.

Example: Configuring OSPFv3 Not-So-Stubby Areas with Filtering

This example shows how to configure an OSPFv3 no-so-stubby area (NSSA) when there is no need to inject external routes into the NSSA as type 7.

Requirements

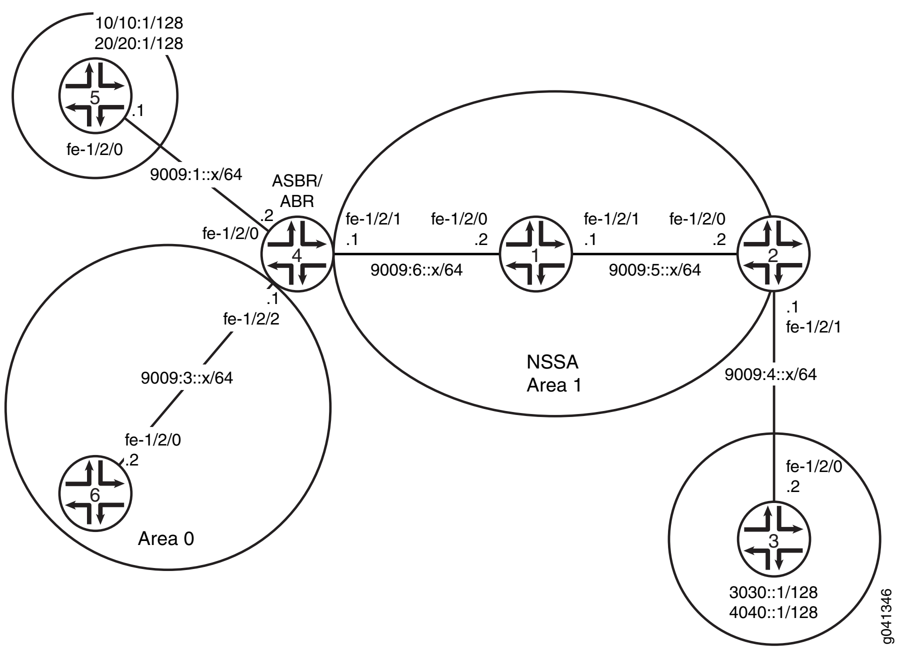
No special configuration beyond device initialization is required before configuring this example.

Overview

When an autonomous system border router (ASBR) is also an NSSA area border router (ABR), the routing device generates type 5 as well as type 7 LSAs. You can prevent the router from creating type 7 LSAs for the NSSA with the **no-nssa-abr** statement.

In this example, Device 5 and Device 3 are in customer networks. Device 4 and Device 2 are both injecting the customer routes into OSPFv3. Area 1 is an NSSA. Because Device 4 is both an NSSA ABR and an ASBR, it is injecting both type 5 and type 7 LSAs into area 1. To stop type 7 LSAs from being injected into area 1, the **no-nssa-abr** statement in included in the Device 4 configuration.

Figure 10: OSPFv3 Network Topology with an NSSA ABR That Is Also an ASBR



"CLI Quick Configuration" on page 70 shows the configuration for all of the devices in Figure 10 on page 70. The section "Step-by-Step Procedure" on page 72 describes the steps on Device 4.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device 1

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:6::2/64
```

```
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:5::1/64
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
set protocols ospf3 area 0.0.0.1 nssa
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
```

Device 2

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:5::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
set interfaces lo0 unit 0 family inet address 2.2.2.2/32
set protocols ospf3 export static2-to-ospf
set protocols ospf3 area 0.0.0.1 nssa
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set policy-options policy-statement static2-to-ospf term 1 from protocol static
set policy-options policy-statement static2-to-ospf term 1 then accept
set routing-options rib inet6.0 static route 3030::1/128 next-hop 9009:4::2
set routing-options rib inet6.0 static route 4040::1/128 next-hop 9009:4::2
```

Device 3

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:4::2/64
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces lo0 unit 0 family inet6 address 3030::1/128
set interfaces lo0 unit 0 family inet6 address 4040::1/128
set routing-options rib inet6.0 static route ::/0 next-hop 9009:4::1
```

Device 4

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:6::1/64
set interfaces fe-1/2/2 unit 0 family inet6 address 9009:3::1/64
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set protocols ospf3 export static-to-ospf
set protocols ospf3 no-nssa-abr
set protocols ospf3 area 0.0.0.0 interface fe-1/2/2.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 nssa default-lsa default-metric 10
set protocols ospf3 area 0.0.0.1 nssa default-lsa metric-type 1
set protocols ospf3 area 0.0.0.1 nssa default-lsa type-7
set protocols ospf3 area 0.0.0.1 nssa no-summaries
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
set policy-options policy-statement static-to-ospf term 1 from protocol static
set policy-options policy-statement static-to-ospf term 1 then accept
set routing-options rib inet6.0 static route 1010::1/128 next-hop 9009:1::1
set routing-options rib inet6.0 static route 2020::1/128 next-hop 9009:1::1
```

Device 5

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:1::1/64
set interfaces lo0 unit 0 family inet address 5.5.5.5/32
set interfaces lo0 unit 0 family inet6 address 1010::1/128
set interfaces lo0 unit 0 family inet6 address 2020::1/128
set routing-options rib inet6.0 static route ::/0 next-hop 9009:1::2
```

Device 6

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:3::2/64
set interfaces lo0 unit 0 family inet address 6.6.6.6/32
set protocols ospf3 area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 4:

1. Configure the interfaces.

   [edit interfaces]
   user@4# **set fe-1/2/0 unit 0 family inet6 address 9009:1::2/64**
   user@4# **set fe-1/2/1 unit 0 family inet6 address 9009:6::1/64**
   user@4# **set fe-1/2/2 unit 0 family inet6 address 9009:3::1/64**
   user@4# **set lo0 unit 0 family inet address 4.4.4.4/32**

2. Enable OSPFv3 on the interfaces that are in area 0.

   [edit protocols ospf3 area 0.0.0.0]
   user@4# **set interface fe-1/2/2.0**
   user@4# **set interface lo0.0 passive**

3. Enable OSPFv3 on the interface that is in area 1.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set interface fe-1/2/1.0**

4. Configure an OSPFv3 NSSA.

   The **nssa** statement is required on all routing devices in the area.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set nssa**

5. On the ABR, inject a default route into the area.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set nssa default-lsa default-metric 10**

6. (Optional) On the ABR, specify the external metric type for the default route.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set nssa default-lsa metric-type 1**

7. (Optional) On the ABR, specify the flooding of Type 7 LSAs.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set nssa default-lsa type-7**

8. On the ABR, restrict summary LSAs from entering the area.

   [edit protocols ospf3 area 0.0.0.1]
   user@4# **set nssa no-summaries**

9. Disable exporting Type 7 LSAs into the NSSA.

   This setting is useful if you have an AS boundary router that is also an ABR with an NSSA area attached.

   [edit protocols ospf3]
   user@4# **set no-nssa-abr**

10. Configure static routes to the customer network.

    [edit routing-options rib inet6.0 static]


```
user@4# set route 1010::1/128 next-hop 9009:1::1
user@4# set route 2020::1/128 next-hop 9009:1::1
```

11. Configure a policy to inject the static routes into OSPFv3.

```
[edit policy-options policy-statement static-to-ospf term 1]
user@4# set from protocol static
user@4# set then accept
```

12. Apply the policy to OSPFv3.

```
[edit protocols ospf3]
user@4# set export static-to-ospf
```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device 4

```
user@4# show interfaces
fe-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:1::2/64;
    }
  }
  unit 0 {
    family inet6 {
      address 9009:6::1/64;
    }
  }
  unit 0 {
    family inet6 {
      address 9009:3::1/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 4.4.4.4/32;
    }
  }
}

user@4# show protocols
ospf3 {
  export static-to-ospf;
  no-nssa-abr;
  area 0.0.0.0 {
    interface fe-1/2/2.0;
    interface lo0.0 {
      passive;
    }
  }
  area 0.0.0.1 {
```

```
        nssa {
          default-lsa {
            default-metric 10;
            metric-type 1;
            type-7;
          }
          no-summaries;
        }
        interface fe-1/2/1.0;
      }
    }
```

```
    user@4# show policy-options
    policy-statement static-to-ospf {
      term 1 {
        from protocol static;
        then accept;
      }
    }
```

```
    user@4# show routing-options
    rib inet6.0 {
      static {
        route 1010::1/128 next-hop 9009:1::1;
        route 2020::1/128 next-hop 9009:1::1;
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Routes in the OSPFv3 Stub Area

Purpose Make sure that the expected routes are present in the routing tables.

Action From operational mode on Device 1 and Device 6, enter the **show route** command.

```
user@1> show route
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32         *[Direct/0] 03:25:44
                    > via lo0.0

inet6.0: 11 destinations, 14 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[OSPF3/150] 01:52:58, metric 11, tag 0
                    > via fe-1/2/0.0
3030::1/128        *[OSPF3/150] 02:44:02, metric 0, tag 0
                    > via fe-1/2/1.0
4040::1/128        *[OSPF3/150] 02:44:02, metric 0, tag 0
                    > via fe-1/2/1.0
9009:5::/64        *[Direct/0] 03:25:34
                    > via fe-1/2/1.0
```

```
                    [OSPF3/10] 03:25:24, metric 1
                    > via fe-1/2/1.0
9009:5::1/128      *[Local/0] 03:25:34
                      Local via fe-1/2/1.0
9009:6::/64        *[Direct/0] 03:25:34
                    > via fe-1/2/0.0
                    [OSPF3/10] 03:25:34, metric 1
                    > via fe-1/2/0.0
9009:6::2/128      *[Local/0] 03:25:34
                      Local via fe-1/2/0.0
fe80::/64          *[Direct/0] 03:25:34
                    > via fe-1/2/0.0
                    [Direct/0] 03:25:34
                    > via fe-1/2/1.0
fe80::2a0:a514:0:44c/128
                   *[Local/0] 03:25:34
                      Local via fe-1/2/0.0
fe80::2a0:a514:0:74c/128
                   *[Local/0] 03:25:34
                      Local via fe-1/2/1.0
ff02::5/128        *[OSPF3/10] 03:27:00, metric 1
                      MultiRecv

user@6> show route
inet.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

6.6.6.6/32         *[Direct/0] 03:26:57
                    > via lo0.0

inet6.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1010::1/128        *[OSPF3/150] 03:16:59, metric 0, tag 0
                    > via fe-1/2/0.0
2020::1/128        *[OSPF3/150] 03:16:59, metric 0, tag 0
                    > via fe-1/2/0.0
3030::1/128        *[OSPF3/150] 02:44:34, metric 0, tag 0
                    > via fe-1/2/0.0
4040::1/128        *[OSPF3/150] 02:44:34, metric 0, tag 0
                    > via fe-1/2/0.0
9009:3::/64        *[Direct/0] 03:26:29
                    > via fe-1/2/0.0
                    [OSPF3/10] 03:26:29, metric 1
                    > via fe-1/2/0.0
9009:3::2/128      *[Local/0] 03:26:29
                      Local via fe-1/2/0.0
9009:5::/64        *[OSPF3/10] 02:44:34, metric 3
                    > via fe-1/2/0.0
9009:6::/64        *[OSPF3/10] 03:16:59, metric 2
                    > via fe-1/2/0.0
fe80::/64          *[Direct/0] 03:26:29
                    > via fe-1/2/0.0
fe80::2a0:a514:0:64c/128
                   *[Local/0] 03:26:29
                      Local via fe-1/2/0.0
ff02::5/128        *[OSPF3/10] 03:27:37, metric 1
                      MultiRecv
```

Meaning On Device 1, the default route (::/0) has been learned because of the **default-metric** statement on the ABR, Device 4. The customer routes 3030::1 and 4040::1 have been learned from Device 2. The 1010::1 and 2020::1 have been suppressed. They are not needed because the default route can be used instead.

On Device 6 which in area 0, all of the customer routes have been learned.

Verifying the Type of LSAs

Purpose Verify the type of LSAs that are in the area.

Action From operational mode on Device 1, enter the **show ospf3 database nssa detail** command.

```
user@4> show ospf3 database nssa detail
Area 0.0.0.1
 Type       ID               Adv Rtr          Seq         Age  Cksum  Len
NSSA       0.0.0.1          2.2.2.2          0x80000004  2063  0xceaf  60
  Prefix 3030::1/128
  Prefix-options 0x8, Metric 0, Type 2,
   Fwd addr 9009:5::2,
NSSA       0.0.0.2          2.2.2.2          0x80000004  1463  0x3627  60
  Prefix 4040::1/128
  Prefix-options 0x8, Metric 0, Type 2,
   Fwd addr 9009:5::2,
NSSA      *0.0.0.1          4.4.4.4          0x80000003    35  0x25f8  28
  Prefix ::/0
  Prefix-options 0x0, Metric 10, Type 1,
```

Meaning Device 4 is not sending type 7 (NSSA) LSAs for customer routes, 1010::1/128 and 2020::1/128. If you were to delete or deactivate the **no-nssa-abr** statement and then rerun the **show ospf3 database nssa detail** command, you would see that Device 4 is sending type 7 LSAs for 1010::1/128 and 2020::1/128.

Related Documentation

- Example: Configuring OSPFv3 Not-So-Stubby Areas on page 56
- Example: Configuring OSPFv3 Stub and Totally Stubby Areas on page 46

Example: Configuring OSPF Multiarea Adjacency

Multiarea Adjacency for OSPF

An area is a set of networks and hosts within an autonomous system (AS) that have been administratively grouped together. By default, a single interface can belong to only one OSPF area. However, in some situations, you might want to configure an interface to belong to more than one area. Doing so allows the corresponding link to be considered an intra-area link in multiple areas and to be preferred over other higher-cost intra-area paths. For example, you can configure an interface to belong to multiple areas with a high-speed backbone link between two area border routers (ABRs) so you can create multiarea adjacencies that belong to different areas.

In Junos OS Release 9.2 and later, you can configure a logical interface to belong to more than one OSPFv2 area. Support for OSPFv3 was introduced in Junos OS Release 9.4. As defined in RFC 5185, *OSPF Multi-Area Adjacency*, the ABRs establish multiple adjacencies belonging to different areas over the same logical interface. Each multiarea adjacency is announced as a point-to-point unnumbered link in the configured area by the routers connected to the link. For each area, one of the logical interfaces is treated as primary, and the remaining interfaces that are configured for the area are designated as secondary.

Any logical interface not configured as a secondary interface for an area is treated as the primary interface for that area. A logical interface can be configured as primary interface only for one area. For any other area for which you configure the interface, you must configure it as a secondary interface.

Example: Configuring Multiarea Adjacency for OSPF

This example shows how to configure multiarea adjacency for OSPF.

Requirements

Before you begin, plan your multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

By default, a single interface can belong to only one OSPF area. You can configure a single interface to belong in multiple OSPF areas. Doing so allows the corresponding link to be considered an intra-area link in multiple areas and to be preferred over other higher-cost intra-area paths. When configuring a secondary interface, consider the following:

- For OSPFv2, you cannot configure point-to-multipoint and nonbroadcast multiaccess (NBMA) network interfaces as a secondary interface because secondary interfaces are treated as a point-to-point unnumbered link.
- Secondary interfaces are supported for LAN interfaces (the primary interface can be a LAN interface, but any secondary interfaces are treated as point-to-point unnumbered links over the LAN). In this scenario, you must ensure that there are only two routing devices on the LAN or that there are only two routing devices on the LAN that have secondary interfaces configured for a specific OSPF area.
- Since the purpose of a secondary interface is to advertise a topological path through an OSPF area, you cannot configure a secondary interface or a primary interface with one or more secondary interfaces to be passive. Passive interfaces advertise their address, but do not run the OSPF protocol (adjacencies are not formed and hello packets are not generated).

- Any logical interface not configured as a secondary interface for an area is treated as a primary interface for that area. A logical interface can be configured as the primary interface only for one area. For any other area for which you configure the interface, you must configure it as a secondary interface.
- You cannot configure the **secondary** statement with the **interface all** statement.
- You cannot configure a secondary interface by its IP address.

In this example, you configure an interface to be in two areas, creating a multiarea adjacency with a link between two ABRs: ABR R1 and ABR R2. On each ABR, area 0.0.0.1 contains the primary interface and is the primary link between the ABRs, and area 0.0.0.2 contains the secondary logical interface, which you configure by including the **secondary** statement. You configure interface **so-0/0/0** on ABR R1 and interface **so-1/0/0** on ABR R2.

Configuration

CLI Quick Configuration

To quickly configure a secondary logical interface for an OSPF area, copy the following commands and paste them into the CLI.

Configuration on ABR R1:

```
[edit]
set interfaces so-0/0/0 unit 0 family inet address 192.168.8.45/30
set routing-options router-id 10.255.0.1
set protocols ospf area 0.0.0.1 interface so-0/0/0
set protocols ospf area 0.0.0.2 interface so-0/0/0 secondary
```

Configuration on ABR R2:

```
[edit]
set interfaces so-1/0/0 unit 0 family inet address 192.168.8.37/30
set routing-options router-id 10.255.0.2
set protocols ospf area 0.0.0.1 interface so-1/0/0
set protocols ospf area 0.0.0.2 interface so-1/0/0 secondary
```

Step-by-Step Procedure

To configure a secondary logical interface:

1. Configure the device interfaces.

   NOTE: For OSPFv3, on each interface specify the inet6 address family and include the IPv6 address.

   ```
   [edit]
   user@R1# set interfaces so-0/0/0 unit 0 family inet address 192.168.8.45/30
   ```

   ```
   [edit]
   user@R2# set interfaces so-1/0/0 unit 0 family inet address 192.168.8.37/30
   ```

2. Configure the router identifier.

   ```
   [edit]
   user@R1# set routing-options router-id 10.255.0.1
   ```



```
[edit]
user@R2# set routing-options router-id 10.255.0.2
```

3. On each ABR, configure the primary interface for the OSPF area.

   NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@R1# set protocols ospf 0.0.0.1 interface so-0/0/0

[edit ]
user@R2# set protocols ospf 0.0.0.2 interface so-1/0/0
```

4. On each ABR, configure the secondary interface for the OSPF area.

```
[edit ]
user@R1# set protocols ospf area 0.0.0.1 so-0/0/0 secondary

[edit ]
user@R2# set protocols ospf area 0.0.0.2 so-1/0/0 secondary
```

5. If you are done configuring the devices, commit the configuration.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# commit
```

Results

Confirm your configuration by entering the **show interfaces**, **show routing-options**, and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on ABR R1:

```
user@R1# show interfaces
so-0/0/0 {
  unit 0 {
    family inet {
      address 192.168.8.45/30;
    }
  }
}

user@R1# show routing-options
router-id 10.255.0.1;

user@R1# show protocols ospf
area 0.0.0.1 {
  interface so-0/0/0.0;
}
  area 0.0.0.2 {
    interface so-0/0/0.0 {
      secondary;
    }
  }
```

Configuration on ABR R2:

```
user@R2# show interfaces
so-0/0/0 {
  unit 0 {
    family inet {
      address 192.168.8.37/30;
    }
  }
}
```

```
user@R2# show routing-options
router-id 10.255.0.2;
```

```
user@R2# show protocols ospf
area 0.0.0.1 {
  interface so-1/0/0.0;
}
  area 0.0.0.2 {
    interface so-1/0/0.0 {
      secondary;
    }
  }
```

Verification

Confirm that the configuration is working properly.

- Verifying the Secondary Interface on page 80
- Verifying the Interfaces in the Area on page 80
- Verifying Neighbor Adjacencies on page 80

Verifying the Secondary Interface

Purpose Verify that the secondary interface appears for the configured area. The Secondary field displays if the interface is configured as a secondary interface. The output might also show the same interface listed in multiple areas.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Verifying the Interfaces in the Area

Purpose Verify the interfaces configured for the specified area.

Action From operational mode, enter the **show ospf interface area *area-id*** command for OSPFv2, and enter the **show ospf3 interface area *area-id*** command for OSPFv3..

Verifying Neighbor Adjacencies

Purpose Verify the primary and secondary neighbor adjacencies. The Secondary field displays if the neighbor is on a secondary interface.

Action From operational mode, enter the **show ospf neighbor detail** command for OSPFv2, and enter the **show ospf3 neighbor detail** command for OSPFv3.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Understanding OSPF Areas and Backbone Areas on page 27
- OSPF Configuration Overview on page 14

Example: Configuring a Multiarea Adjacency for OSPFv3

- Understanding Multiarea Adjacencies for OSPFv3 on page 81
- Example: Configuring a Multiarea Adjacency for OSPFv3 on page 81

Understanding Multiarea Adjacencies for OSPFv3

An area is a set of networks and hosts within an OSPFv3 domain that have been administratively grouped together. By default, a single interface can belong to only one OSPFv3 area. However, in some situations, you might want to configure an interface to belong to more than one area to avoid suboptimal routing. Doing so allows the corresponding link to be considered an intra-area link in multiple areas and to be preferred over higher-cost intra-area links.

In Junos OS Release 9.2 and later, you can configure an interface to belong to more than one OSPFv2 area. Support for OSPFv3 was introduced in Junos OS Release 9.4. As defined in RFC 5185, *OSPF Multi-Area Adjacency*, the ABRs establish multiple adjacencies belonging to different areas over the same logical interface. Each multiarea adjacency is announced as a point-to-point unnumbered link in the configured area by the routers connected to the link.

An interface is considered to be primarily in one area. When you configure the same interface in another area, it is considered to be secondarily in the other area. You designate the secondary area by including the **secondary** statement at the **[edit protocols ospf3 area *area-number* interface *interface-name*]** hierarchy level.

Example: Configuring a Multiarea Adjacency for OSPFv3

This example shows how to configure a multiarea adjacency for OSPFv3.

- Requirements on page 81
- Overview on page 82
- Configuration on page 83
- Verification on page 86

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

OSPFv3 intra-area paths are preferred over inter-area paths. In this example, Device R1 and Device R2 are area border routers (ABRs) with interfaces in both area 0 and in area 1. The link between Device R1 and R2 is in area 0 and is a high-speed link. The links in area 1 are lower speed.

If you want to forward some of area 1's traffic between Device R1 and Device R2 over the high-speed link, one method to accomplish this goal is to make the high-speed link a multiarea adjacency so that the link is part of both area 0 and area 1.

If the high-speed link between Device R1 and Device R2 remains in area 1 only, Device R1 always routes traffic to Device R4 and Device R5 through area 1 over the lower-speed links. Device R1 also uses the intra-area area 1 path through Device R3 to get to area 1 destinations downstream of Device R2.

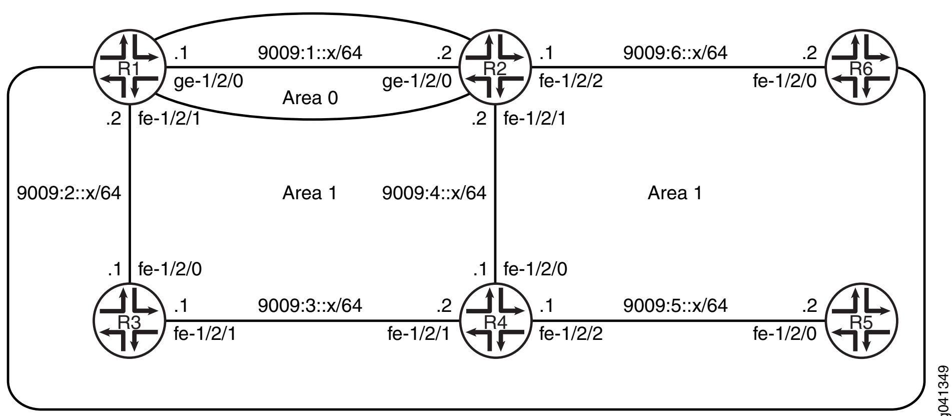
Clearly, this scenario results in suboptimal routing.

An OSPF virtual link cannot be used to resolve this issue without moving the link between Device R1 and Device R2 to area 1. You might not want to do this if the physical link belongs to the network's backbone topology.

The OSPF/OSPFv3 protocol extension described in RFC 5185, *OSPF Multi-Area Adjacency* resolves the issue, by allowing the link between Device R1 and Device R2 to be part of both the backbone area and area 1.

To create a multiarea adjacency, you configure an interface to be in two areas, with ge-1/2/0 on Device R1 configured in both area 0 and area 1, and ge-1/2/0 on Device R2 configured in both area 0 and area 1. On both Device R1 and Device R2, area 0 contains the primary interface and is the primary link between the devices. Area 1 contains the secondary logical interface, which you configure by including the **secondary** statement.

Figure 11: OSPFv3 Multiarea Adjacency



"CLI Quick Configuration" on page 83 shows the configuration for all of the devices in Figure 11 on page 82. The section "Step-by-Step Procedure" on page 84 describes the steps on Device R1 and Device R2.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device R1

```
set interfaces ge-1/2/0 unit 0 family inet6 address 9009:1::1/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:2::2/64
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
set interfaces lo0 unit 0 family inet6 address 1::1/128
set protocols ospf3 area 0.0.0.0 interface ge-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.1 interface ge-1/2/0.0 secondary
```

Device R2

```
set interfaces ge-1/2/0 unit 0 family inet6 address 9009:1::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
set interfaces fe-1/2/2 unit 0 family inet6 address 9009:6::2/64
set interfaces lo0 unit 0 family inet address 2.2.2.2/32
set interfaces lo0 unit 0 family inet6 address 2::2/128
set protocols ospf3 area 0.0.0.0 interface ge-1/2/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/2.0
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.1 interface ge-1/2/0.0 secondary
```

Device R3

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:2::1/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:3::1/64
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces lo0 unit 0 family inet6 address 3::3/128
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
```

Device R4

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:3::2/64
set interfaces fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
set interfaces fe-1/2/2 unit 0 family inet6 address 9009:5::1/64
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set interfaces lo0 unit 0 family inet6 address 4::4/128
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf3 area 0.0.0.1 interface fe-1/2/1.0
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/2.0
```

Device R5

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:5::2/64
set interfaces lo0 unit 0 family inet address 5.5.5.5/32
set interfaces lo0 unit 0 family inet6 address 5::5/128
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
```

Device R6

```
set interfaces fe-1/2/0 unit 0 family inet6 address 9009:6::2/64
set interfaces lo0 unit 0 family inet address 6.6.6.6/32
set interfaces lo0 unit 0 family inet6 address 6::6/128
```

```
set protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set protocols ospf3 area 0.0.0.1 interface fe-1/2/0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device R1:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@R1# set ge-1/2/0 unit 0 family inet6 address 9009:1::1/64
   user@R1# set fe-1/2/1 unit 0 family inet6 address 9009:2::2/64
   user@R1# set lo0 unit 0 family inet address 1.1.1.1/32
   user@R1# set lo0 unit 0 family inet6 address 1::1/128
   ```

2. Enable OSPFv3 on the interfaces that are in area 0.

   ```
   [edit protocols ospf3 area 0.0.0.0]
   user@R1# set interface ge-1/2/0.0
   user@R1# set interface lo0.0 passive
   ```

3. Enable OSPFv3 on the interface that is in area 1.

   ```
   [edit protocols ospf3 area 0.0.0.1]
   user@R1# set interface fe-1/2/1.0
   user@R1# set interface ge-1/2/0.0 secondary
   ```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device R2:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@R2# set ge-1/2/0 unit 0 family inet6 address 9009:1::2/64
   user@R2# set fe-1/2/1 unit 0 family inet6 address 9009:4::1/64
   user@R2# set fe-1/2/2 unit 0 family inet6 address 9009:6::2/64
   user@R2# set lo0 unit 0 family inet address 2.2.2.2/32
   user@R2# set lo0 unit 0 family inet6 address 2::2/128
   ```

2. Enable OSPFv3 on the interfaces that are in area 0.

   ```
   [edit protocols ospf3 area 0.0.0.0]
   user@R2# set interface ge-1/2/0.0
   user@R2# set interface lo0.0 passive
   ```

3. Enable OSPFv3 on the interface that is in area 1.

   ```
   [edit protocols ospf3 area 0.0.0.1]
   user@R2# set interface fe-1/2/2.0
   user@R2# set interface fe-1/2/1.0
   user@R2# set interface ge-1/2/0.0 secondary
   ```

Results From configuration mode, confirm your configuration by entering the **show interfaces** and **show protocols** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device R1

```
user@R1# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:1::1/64;
    }
  }
}
fe-1/2/1 {
  unit 0 {
    family inet6 {
      address 9009:2::2/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 1.1.1.1/32;
    }
    family inet6 {
      address 1::1/128;
    }
  }
}

user@R1# show protocols
ospf3 {
  area 0.0.0.0 {
    interface ge-1/2/0.0;
    interface lo0.0 {
      passive;
    }
  }
  area 0.0.0.1 {
    interface fe-1/2/1.0;
    interface ge-1/2/0.0 {
      secondary;
    }
  }
}
```

Device R2

```
user@R2# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet6 {
      address 9009:1::2/64;
    }
  }
}
fe-1/2/1 {
  unit 0 {
```

```
        family inet6 {
          address 9009:4::1/64;
        }
      }
    }
    fe-1/2/2 {
      unit 0 {
        family inet6 {
          address 9009:6::2/64;
        }
      }
    }
    lo0 {
      unit 0 {
        family inet {
          address 2.2.2.2/32;
        }
        family inet6 {
          address 2::2/128;
        }
      }
    }

    user@R2# show protocols
    ospf3 {
      area 0.0.0.0 {
        interface ge-1/2/0.0;
        interface lo0.0 {
          passive;
        }
      }
      area 0.0.0.1 {
        interface fe-1/2/2.0;
        interface fe-1/2/1.0;
        interface ge-1/2/0.0 {
          secondary;
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Flow of Traffic

Purpose Verify that traffic uses the high-speed link between Device R1 and Device R2 to reach destinations in area 1.

Action From operational mode on Device R1, use the **traceroute** command check the traffic flow to Device R5 and Device R6.

```
user@R1> traceroute 6::6
```



```
traceroute6 to 6::6 (6::6) from 9009:1::1, 64 hops max, 12 byte packets
 1  9009:1::2 (9009:1::2)  1.361 ms  1.166 ms  1.117 ms
 2  6::6 (6::6)  1.578 ms  1.484 ms  1.488 ms

user@R1> traceroute 5::5
traceroute6 to 5::5 (5::5) from 9009:1::1, 64 hops max, 12 byte packets
 1  9009:1::2 (9009:1::2)  1.312 ms  1.472 ms  1.132 ms
 2  9009:4::1 (9009:4::1)  1.137 ms  1.174 ms  1.126 ms
 3  5::5 (5::5)  1.591 ms  1.445 ms  1.441 ms
```

Meaning The traceroute output shows that traffic uses the 9009:1:: link between Device R1 and Device R2.

Verifying That the Traffic Flow Changes When You Remove the Multiarea Adjacency

Purpose Verify the results without the multiarea adjacency configured.

Action

1. Deactivate the backbone link interfaces in area 1.

   user@R1# **deactivate protocols ospf3 area 0.0.0.1 interface ge-1/2/0.0**
   user@R1# **commit**
   user@R2# **deactivate protocols ospf3 area 0.0.0.1 interface ge-1/2/0.0**
   user@R2# **commit**

2. From operational mode on Device R1, use the **traceroute** command check the traffic flow to Device R5 and Device R6.

   ```
   user@R1> traceroute 6::6
   traceroute6 to 6::6 (6::6) from 9009:2::2, 64 hops max, 12 byte packets
    1  9009:2::1 (9009:2::1)  1.314 ms  8.523 ms  8.310 ms
    2  9009:3::2 (9009:3::2)  1.166 ms  1.162 ms  1.172 ms
    3  9009:4::1 (9009:4::1)  1.386 ms  1.182 ms  1.138 ms
    4  6::6 (6::6)  1.605 ms  1.469 ms  1.438 ms
   ```

   ```
   user@R1> traceroute 5::5
   traceroute6 to 5::5 (5::5) from 9009:2::2, 64 hops max, 12 byte packets
    1  9009:2::1 (9009:2::1)  1.365 ms  1.174 ms  1.133 ms
    2  9009:3::2 (9009:3::2)  1.157 ms  1.198 ms  1.138 ms
    3  5::5 (5::5)  1.584 ms  1.461 ms  1.443 ms
   ```

Meaning Without the multiarea adjacency, the output shows suboptimal routing with traffic taking the path through the area 1 low-speed-links.

Related Documentation

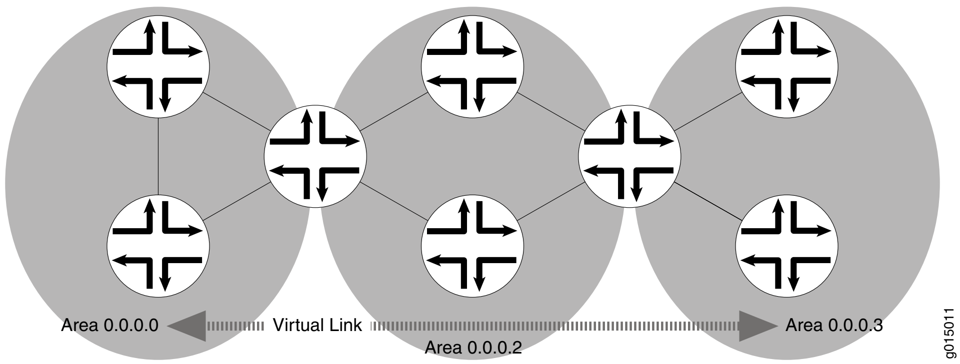
- Example: Configuring OSPF Multiarea Adjacency on page 76

Example: OSPF Virtual Links

Understanding OSPF Virtual Links

OSPF requires that all areas in an autonomous system (AS) must be physically connected to the backbone area (area 0). In large networks with many areas, in which direct connectivity between all areas and the backbone area is physically difficult or impossible, you can configure virtual links to connect noncontiguous areas. Virtual links use a transit area that contains two or more area border routers (ABRs) to pass network traffic from one adjacent area to another. The transit area must have full routing information and it cannot be a stub area. For example, Figure 12 on page 88 shows a virtual link between a noncontiguous area and the backbone area through an area connected to both.

Figure 12: OSPF Topology with a Virtual Link



In the topology shown in Figure 12 on page 88, a virtual link is established between area 0.0.0.3 and the backbone area through area 0.0.0.2. The virtual link transits area 0.0.0.2. All outbound traffic destined for other areas is routed through area 0.0.0.2 to the backbone area and then to the appropriate ABR. All inbound traffic destined for area 0.0.0.3 is routed to the backbone area and then through area 0.0.0.2.

Example: Configuring OSPF Virtual Links

This example shows how to configure an OSPF virtual link to connect noncontiguous areas.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

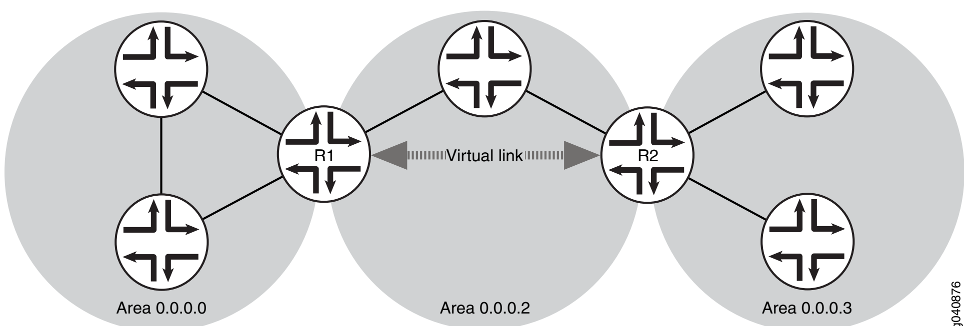
If any routing device on the backbone is not physically connected to the backbone, you must establish a virtual connection between that routing device and the backbone to connect the noncontiguous areas.

To configure an OSPF virtual link through an area, you specify the router ID (IP address) of the routing devices at each end of the virtual link. These routing devices must be area border routers (ABRs), with one that is physically connected to the backbone. You cannot configure virtual links through stub areas. You must also specify the number of the area through which the virtual link transits (also known as the transit area). You apply these settings to the backbone area (defined by the area 0.0.0.0) configuration on the ABRs that are part of the virtual link.

In this example, Device R1 and Device R2 are the routing devices at each end of the virtual link, with Device R1 physically connected to the backbone, as shown in Figure 13 on page 89. You configure the following virtual link settings:

- **neighbor-id**—Specifies the IP address of the routing device at the other end of the virtual link. In this example, Device R1 has a router ID of 192.168.0.5, and Device R2 has a router ID of 192.168.0.3.
- **transit-area**—Specifies the area identifier through which the virtual link transits. In this example, area 0.0.0.3 is not connected to the backbone, so you configure a virtual link session between area 0.0.0.3 and the backbone area through area 0.0.0.2. Area 0.0.0.2 is the transit area.

Figure 13: OSPF Virtual Link



Configuration

CLI Quick Configuration

- To quickly configure an OSPF virtual link on the local routing device (Device R1), copy the following commands and paste them into the CLI.

NOTE: You must configure both routing devices that are part of the virtual link and specify the applicable neighbor ID on each routing device.

```
[edit]
set routing-options router-id 192.168.0.5
```

```
set protocols ospf area 0.0.0.0 virtual-link neighbor-id 192.168.0.3 transit-area 0.0.0.2
```

- To quickly configure an OSPF virtual link on the remote routing device (Device R2), copy the following commands and paste them into the CLI.

```
[edit]
set routing-options router-id 192.168.0.3
set protocols ospf area 0.0.0.0 virtual-link neighbor-id 192.168.0.5 transit-area 0.0.0.2
```

Step-by-Step Procedure

To configure an OSPF virtual link on the local routing device (Device R1):

1. Configure the router ID.

```
[edit]
user@R1# set routing-options router-id 192.168.0.5
```

2. Enter OSPF configuration mode and specify OSPF area 0.0.0.0.

NOTE: For an OSPFv3 virtual link, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@R1# edit protocols ospf area 0.0.0.0
```

3. Configure an OSPF virtual link and specify the transit area 0.0.0.2.
This routing device must be an ABR that is physically connected to the backbone.

```
[edit protocols ospf area 0.0.0.0]
user@R1# set virtual-link neighbor-id 192.168.0.3 transit-area 0.0.0.2
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0]
user@R1# commit
```

Step-by-Step Procedure

To configure an OSPF virtual link on the remote ABR (Device R2, the routing device at the other end of the link):

1. Configure the router ID.

```
[edit]
user@R2# set routing-options router-id 192.168.0.3
```

2. Enter OSPF configuration mode and specify OSPF area 0.0.0.0.

NOTE: For an OSPFv3 virtual link, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@R2# edit protocols ospf area 0.0.0.0
```

3. Configure an OSPF virtual link on the remote ABR and specify the transit area 0.0.0.2.
This routing device is not physically connected to the backbone.

```
[edit protocols ospf area 0.0.0.0]
user@R2# set virtual-link neighbor-id 192.168.0.5 transit-area 0.0.0.2
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0]
user@R2# commit
```

Results

Confirm your configuration by entering the show **routing-options** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on the local routing device (Device R1):

```
user@R1#: show routing-options
router-id 192.168.0.5;

user@R1# show protocols ospf
area 0.0.0.0 {
  virtual-link neighbor-id 192.168.0.3 transit-area 0.0.0.2;
}
```

Configuration on the remote ABR (Device R2):

```
user@R2#: show routing-options
router-id 192.168.0.3;

user@R2# show protocols ospf
area 0.0.0.0 {
  virtual-link neighbor-id 192.168.0.5 transit-area 0.0.0.2;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying Entries in the Link-State Database on page 91
- Verifying OSPF Interface Status and Configuration on page 92

Verifying Entries in the Link-State Database

Purpose Verify that the entries in the OSPFv2 or OSPFv3 link-state database display. The Router field in the OSPFv2 output displays LSA information, including the type of link. If configured as a virtual link, the Type is Virtual. For each router link, the Type field in the OSPFv3 output displays the type of interface. If configured as a virtual link, the Type is Virtual.

Action From operational mode, enter the **show ospf database detail** command for OSPFv2, and enter the **show ospf3 database detail** command for OSPFv3.

Verifying OSPF Interface Status and Configuration

Purpose Verify that the OSPFv2 or OSPFv3 interface is configured and status displays. The Type field displays the type of interface. If the interface is configured as part of a virtual link, the Type is Virtual.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Example: Configuring OSPFv3 Virtual Links

This example shows how to configure OSPF version 3 (OSPFv3) with some areas that do not have a direct adjacency to the backbone area (area 0). When an area lacks an adjacency with area 0, a virtual link is required to connect to the backbone through a non-backbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub area.

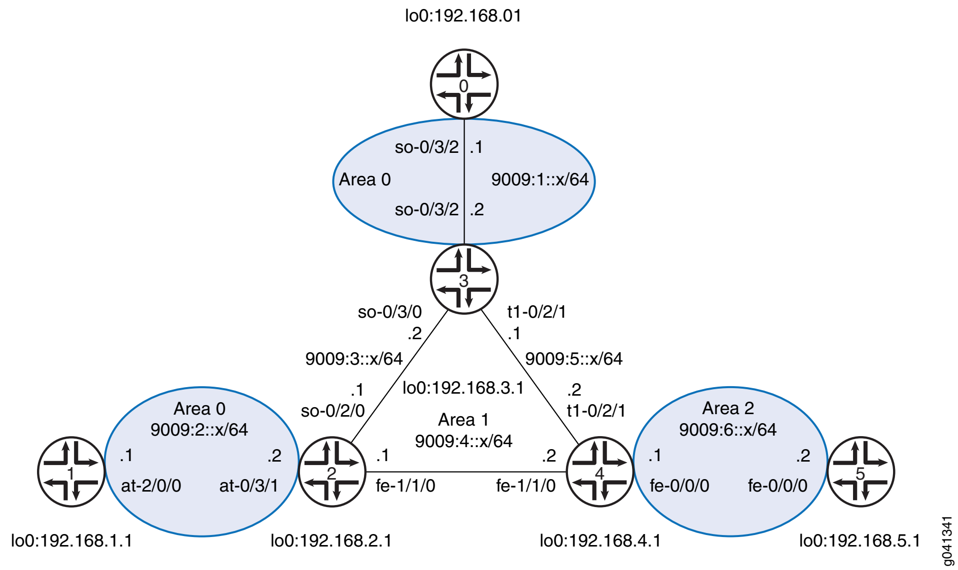
Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

Figure 14 on page 93 shows the topology used in this example.

Figure 14: OSPFv3 with Virtual Links



Device 0, Device 1, Device 2, and Device 3 are connected to the OSPFv3 backbone Area 0. Device 2, Device 3, and Device 4 connect to each other across Area 1. and Area 2 is located between Device 4 and Device 5. Because Device 5 does not have a direct adjacency to Area 0, a virtual link is required across Area 1 between Device 3 and Device 4. Similarly, because Device 0 and Device 1 have two separate Area 0 backbone sections, you need to configure a second virtual link across Area 1 between Device 2 and Device 3.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device 0

```
set logical-systems 0 interfaces so-0/3/2 unit 0 family inet6 address 9009:1::1/64
set logical-systems 0 interfaces lo0 unit 0 family inet address 192.168.0.1/32
set logical-systems 0 interfaces lo0 unit 0 family inet6 address feee::10:255:71:4/128
set logical-systems 0 protocols ospf3 area 0.0.0.0 interface so-0/3/2.0
set logical-systems 0 protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set logical-systems 0 routing-options router-id 192.168.0.1
```

Device 1

```
set logical-systems 1 interfaces at-2/0/0 atm-options vpi 0
set logical-systems 1 interfaces at-2/0/0 unit 0 family inet6 address 9009:2::1/64
set logical-systems 1 interfaces at-2/0/0 unit 0 vci 0.77
set logical-systems 1 interfaces lo0 unit 0 family inet address 192.168.1.1/32
set logical-systems 1 interfaces lo0 unit 0 family inet6 address feee::10:255:71:1/128
set logical-systems 1 protocols ospf3 area 0.0.0.0 interface at-2/0/0.0
set logical-systems 1 protocols ospf3 area 0.0.0.0 interface lo0.0 passive
set logical-systems 1 routing-options router-id 192.168.1.1
```

Device 2

```
set logical-systems 2 interfaces so-0/2/0 unit 0 family inet6 address 9009:3::1/64
set logical-systems 2 interfaces fe-1/1/0 unit 0 family inet6 address 9009:4::1/64
set logical-systems 2 interfaces at-0/3/1 atm-options vpi 0 maximum-vcs 1200
```

```
set logical-systems 2 interfaces at-0/3/1 unit 0 family inet6 address 9009:2::2/64
set logical-systems 2 interfaces at-0/3/1 unit 0 vci 0.77
set logical-systems 2 interfaces lo0 unit 0 family inet address 192.168.2.1/32
set logical-systems 2 interfaces lo0 unit 0 family inet6 address feee::10:255:71:11/128
set logical-systems 2 protocols ospf3 area 0.0.0.0 virtual-link neighbor-id 192.168.3.1
  transit-area 0.0.0.1
set logical-systems 2 protocols ospf3 area 0.0.0.0 interface at-0/3/1.0
set logical-systems 2 protocols ospf3 area 0.0.0.1 interface fe-1/1/0.0
set logical-systems 2 protocols ospf3 area 0.0.0.1 interface so-0/2/0.0
set logical-systems 2 protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set logical-systems 2 routing-options router-id 192.168.2.1
```

Device 3

```
set logical-systems 3 interfaces so-0/3/2 unit 0 family inet6 address 9009:1::2/64
set logical-systems 3 interfaces t1-0/2/1 unit 0 family inet6 address 9009:5::1/64
set logical-systems 3 interfaces so-0/3/0 unit 0 family inet6 address 9009:3::2/64
set logical-systems 3 interfaces lo0 unit 0 family inet address 192.168.3.1/32
set logical-systems 3 interfaces lo0 unit 0 family inet6 address feee::10:255:71:3/128
set logical-systems 3 protocols ospf3 area 0.0.0.1 interface so-0/3/0.0
set logical-systems 3 protocols ospf3 area 0.0.0.1 interface t1-0/2/1.0
set logical-systems 3 protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set logical-systems 3 protocols ospf3 area 0.0.0.0 virtual-link neighbor-id 192.168.2.1
  transit-area 0.0.0.1
set logical-systems 3 protocols ospf3 area 0.0.0.0 virtual-link neighbor-id 192.168.4.1
  transit-area 0.0.0.1
set logical-systems 3 protocols ospf3 area 0.0.0.0 interface so-0/3/2.0
set logical-systems 3 routing-options router-id 192.168.3.1
```

Device 4

```
set logical-systems 4 interfaces t1-0/2/1 unit 0 family inet6 address 9009:5::2/64
set logical-systems 4 interfaces fe-0/0/0 unit 0 family inet6 address 9009:6::1/64
set logical-systems 4 interfaces fe-1/1/0 unit 0 family inet6 address 9009:4::2/64
set logical-systems 4 interfaces lo0 unit 0 family inet address 192.168.4.1/32
set logical-systems 4 interfaces lo0 unit 0 family inet6 address feee::10:255:71:5/128
set logical-systems 4 protocols ospf3 area 0.0.0.1 interface fe-1/1/0.0
set logical-systems 4 protocols ospf3 area 0.0.0.1 interface t1-0/2/1.0
set logical-systems 4 protocols ospf3 area 0.0.0.1 interface lo0.0 passive
set logical-systems 4 protocols ospf3 area 0.0.0.2 interface fe-0/0/0.0
set logical-systems 4 protocols ospf3 area 0.0.0.0 virtual-link neighbor-id 192.168.3.1
  transit-area 0.0.0.1
set logical-systems 4 routing-options router-id 192.168.4.1
```

Device 5

```
set logical-systems 5 interfaces fe-0/0/0 unit 0 family inet6 address 9009:6::2/64
set logical-systems 5 interfaces lo0 unit 0 family inet address 192.168.5.1/32
set logical-systems 5 interfaces lo0 unit 0 family inet6 address feee::10:255:71:6/128
set logical-systems 5 protocols ospf3 area 0.0.0.2 interface fe-0/0/0.0
set logical-systems 5 protocols ospf3 area 0.0.0.2 interface lo0.0 passive
set logical-systems 5 routing-options router-id 192.168.5.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 0:

1. Configure the interfaces.

```
[edit interfaces]
user@0# set so-0/3/2 unit 0 family inet6 address 9009:1::1/64
user@0# set lo0 unit 0 family inet address 192.168.0.1/32
user@0# set lo0 unit 0 family inet6 address feee::10:255:71:4/128
```

2. Add the interfaces into Area 0 of the OSPFv3 process.

```
[edit protocols ospf3 area 0.0.0.0]
user@0# set interface so-0/3/2.0
user@0# set interface lo0.0 passive
```

3. Configure the router ID.

```
[edit routing-options]
user@0# set router-id 192.168.0.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 1:

1. Configure the interfaces.

```
[edit interfaces]
user@1# set at-2/0/0 atm-options vpi 0
user@1# set at-2/0/0 unit 0 family inet6 address 9009:2::1/64
user@1# set at-2/0/0 unit 0 vci 0.77
user@1# set lo0 unit 0 family inet address 192.168.1.1/32
user@1# set lo0 unit 0 family inet6 address feee::10:255:71:1/128
```

2. Add the interfaces into Area 0 of the OSPFv3 process.

```
[edit protocols ospf3 area 0.0.0.0]
user@1# set interface at-2/0/0.0
user@1# set interface lo0.0 passive
```

3. Configure the router ID.

```
[edit routing-options]
user@1# set router-id 192.168.1.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 2:

1. Configure the interfaces.

```
[edit interfaces]
user@2# set so-0/2/0 unit 0 family inet6 address 9009:3::1/64
user@2# set fe-1/1/0 unit 0 family inet6 address 9009:4::1/64
user@2# set at-0/3/1 atm-options vpi 0 maximum-vcs 1200
user@2# set at-0/3/1 unit 0 family inet6 address 9009:2::2/64
user@2# set at-0/3/1 unit 0 vci 0.77
user@2# set lo0 unit 0 family inet address 192.168.2.1/32
user@2# set lo0 unit 0 family inet6 address feee::10:255:71:11/128
```

2. Add the interfaces connected to Device 1, Device 3, and Device 4 into the OSPFv3 process.

   [edit protocols ospf3 area 0.0.0.0]
   user@2# **set interface at-0/3/1.0**
   [edit protocols ospf3 area 0.0.0.1]
   user@2# **set interface fe-1/1/0.0**
   user@2# **set interface so-0/2/0.0**
   user@2# **set interface lo0.0 passive**

3. Configure the virtual link to Device 3 through Area 1 so that Device 1 can access the discontiguous portion of the OSPF backbone found on Device 0.

   [edit protocols ospf3 area 0.0.0.0]
   user@2# **set virtual-link neighbor-id 192.168.3.1 transit-area 0.0.0.1**

4. Configure the router ID.

   [edit routing-options]
   user@2# **set router-id 192.168.2.1**

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 3:

1. Configure the interfaces.

   [edit interfaces]
   user@3# **set so-0/3/2 unit 0 family inet6 address 9009:1::2/64**
   user@3# **set t1-0/2/1 unit 0 family inet6 address 9009:5::1/64**
   user@3# **set so-0/3/0 unit 0 family inet6 address 9009:3::2/64**
   user@3# **set lo0 unit 0 family inet address 192.168.3.1/32**
   user@3# **set lo0 unit 0 family inet6 address feee::10:255:71:3/128**

2. For the OSPFv3 process on Device 3, configure the interfaces connected to Device 2 and Device 4 into Area 1 and the interface connected to Device 0 into Area 0.

   [edit protocols ospf3 area 0.0.0.1]
   user@3# **set interface so-0/3/0.0**
   user@3# **set interface t1-0/2/1.0**
   user@3# **set interface lo0.0 passive**
   [edit protocols ospf3 area 0.0.0.0]
   user@3# **set interface so-0/3/2.0**

3. Configure two virtual links through Area 1—one connecting to Device 2 and the second connecting to Device 4.

   The virtual links allow Device 5 to access the OSPF backbone, and connect the discontiguous sections of Area 0 located at Device 0 and Device 1.

   [edit protocols ospf3 area 0.0.0.0]
   user@3# **set virtual-link neighbor-id 192.168.2.1 transit-area 0.0.0.1**
   user@3# **set virtual-link neighbor-id 192.168.4.1 transit-area 0.0.0.1**

4. Configure the router ID.

   [edit routing-options]

```
user@3# set router-id 192.168.3.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 4:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@4# set t1-0/2/1 unit 0 family inet6 address 9009:5::2/64
   user@4# set fe-0/0/0 unit 0 family inet6 address 9009:6::1/64
   user@4# set fe-1/1/0 unit 0 family inet6 address 9009:4::2/64
   user@4# set lo0 unit 0 family inet address 192.168.4.1/32
   user@4# set lo0 unit 0 family inet6 address feee::10:255:71:5/128
   ```

2. On Device 4, add the connected interfaces into the OSPFv3 process.

   ```
   [edit protocols ospf3 area 0.0.0.1]
   user@4# set interface fe-1/1/0.0
   user@4# set interface t1-0/2/1.0
   user@4# set interface lo0.0 passive
   [edit protocols ospf3 area 0.0.0.2]
   user@4# set interface fe-0/0/0.0
   ```

3. Configure the virtual link to Device 3 through Area 1 so that Device 5 can access the OSPF backbone.

   ```
   [edit protocols ospf3 area 0.0.0.0]
   user@4# set virtual-link neighbor-id 192.168.3.1 transit-area 0.0.0.1
   ```

4. Configure the router ID.

   ```
   [edit routing-options]
   user@4# set router-id 192.168.4.1
   ```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device 5:

1. Configure the interfaces.

   ```
   [edit interfaces]
   user@5# set fe-0/0/0 unit 0 family inet6 address 9009:6::2/64
   user@5# set lo0 unit 0 family inet address 192.168.5.1/32
   user@5# set lo0 unit 0 family inet6 address feee::10:255:71:6/128
   ```

2. Add the interfaces into the OSPFv3 process.

   ```
   [edit protocols ospf3 area 0.0.0.2]
   user@5# set interface fe-0/0/0.0
   user@5# set interface lo0.0 passive
   ```

3. Configure the router ID.

   ```
   [edit routing-options]
   ```

user@5# **set router-id 192.168.5.1**

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device 0

```
user@0# show interfaces
so-0/3/2 {
   unit 0 {
      family inet6 {
         address 9009:1::1/64;
      }
   }
}
lo0 {
   unit 0 {
      family inet {
         address 192.168.0.1/32;
      }
      family inet6 {
         address feee::10:255:71:4/128;
      }
   }
}
user@0# show protocols
ospf3 {
   area 0.0.0.0 {
      interface so-0/3/2.0;
      interface lo0.0 {
         passive;
      }
   }
}
user@0# show routing-options
router-id 192.168.0.1;
```

Device 1

```
user@1# show interfaces
at-2/0/0 {
   atm-options {
      vpi 0;
   }
   unit 0 {
      family inet6 {
         address 9009:2::1/64;
      }
   }
}
lo0 {
   unit 0 {
      family inet {
         address 192.168.1.1/32;
      }
      family inet6 {
         address feee::10:255:71:1/128;
      }
```



```
    }
}
user@1# show protocols
ospf3 {
    area 0.0.0.0 {
        interface at-2/0/0.0;
        interface lo0.0 {
            passive;
        }
    }
}
user@1# show routing-options
router-id 192.168.1.1;
```

Device 2

```
user@2# show interfaces
so-0/2/0 {
    unit 0 {
        family inet6 {
            address 9009:3::1/64;
        }
    }
}
fe-1/1/0 {
    unit 0 {
        family inet6 {
            address 9009:4::1/64;
        }
    }
}
at-0/3/1 {
    atm-options {
        vpi 0 {
            maximum-vcs 1200;
        }
    }
    unit 0 {
        vci 0.77;
        family inet6 {
            address 9009:2::2/64;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.2.1/32;
        }
        family inet6 {
            address feee::10:255:71:11/128;
        }
    }
}
user@2# show protocols
ospf3 {
    area 0.0.0.0 {
        virtual-link neighbor-id 192.168.3.1 transit-area 0.0.0.1;
```

```
    interface at-0/3/1.0;
  }
  area 0.0.0.1 {
    interface fe-1/1/0.0;
    interface so-0/2/0.0;
    interface lo0.0 {
      passive;
    }
  }
}
user@2# show routing-options
router-id 192.168.2.1;
```

Device 3

```
user@3# show interfaces
so-0/3/2 {
  unit 0 {
    family inet6 {
      address 9009:1::2/64;
    }
  }
}
t1-0/2/1 {
  unit 0 {
    family inet6 {
      address 9009:5::1/64;
    }
  }
}
so-0/3/0 {
  unit 0 {
    family inet6 {
      address 9009:3::2/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.3.1/32;
    }
    family inet6 {
      address feee::10:255:71:3/128;
    }
  }
}
user@3# show protocols
ospf3 {
  area 0.0.0.1 {
    interface so-0/3/0.0;
    interface t1-0/2/1.0;
    interface lo0.0 {
      passive;
    }
  }
  area 0.0.0.0 {
    virtual-link neighbor-id 192.168.2.1 transit-area 0.0.0.1;
```



```
      virtual-link neighbor-id 192.168.4.1 transit-area 0.0.0.1;
      interface so-0/3/2.0;
    }
}
user@3# show routing-options
router-id 192.168.3.1;
```

Device 4

```
user@4# show interfaces
t1-0/2/1 {
  unit 0 {
    family inet6 {
      address 9009:5::2/64;
    }
  }
}
fe-0/0/0 {
  unit 0 {
    family inet6 {
      address 9009:6::1/64;
    }
  }
}
fe-1/1/0 {
  unit 0 {
    family inet6 {
      address 9009:4::2/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.4.1/32;
    }
    family inet6 {
      address feee::10:255:71:5/128;
    }
  }
}
user@4# show protocols
ospf3 {
  area 0.0.0.1 {
    interface fe-1/1/0.0;
    interface t1-0/2/1.0;
    interface lo0.0 {
      passive;
    }
  }
  area 0.0.0.2 {
    interface fe-0/0/0.0;
  }
  area 0.0.0.0 {
    virtual-link neighbor-id 192.168.3.1 transit-area 0.0.0.1;
  }
}
user@4# show routing-options
```

```
router-id 192.168.4.1;
```

Device 5

```
user@5# show interfaces
fe-0/0/0 {
  unit 0 {
    family inet6 {
      address 9009:6::2/64;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.5.1/32;
    }
    family inet6 {
      address feee::10:255:71:6/128;
    }
  }
}
user@5# show protocols
ospf3 {
  area 0.0.0.2 {
    interface fe-0/0/0.0;
    interface lo0.0 {
      passive;
    }
  }
}
user@5# show routing-options
router-id 192.168.5.1;
```

If you are done configuring the devices, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

To verify proper operation of OSPFv3 for IPv6, use the following commands:

- **show ospf3 interface**
- **show ospf3 neighbor**
- **show ospf3 database**
- **show ospf3 route**
- **show interfaces terse** (to see the IPv6 link local address assigned to the **lo0** interface)

NOTE: To view prefix information, you must use the **extensive** option with the **show ospf3 database** command.

Device 0 Status

Purpose Verify that Device 0 has learned the expected routes and has established the expected neighbor adjacencies.

In the **show ospf3 database** sample output, the stars indicate the “best” routes. These routes are the routes that are installed in the routing table.

Action

```
user@0> show ospf3 database
Area 0.0.0.0
 Type       ID               Adv Rtr          Seq          Age  Cksum  Len
Router     *0.0.0.0          192.168.0.1      0x8000008f  1858  0x6e21  40
Router      0.0.0.0          192.168.1.1      0x8000008f  1861  0x523d  40
Router      0.0.0.0          192.168.2.1      0x80000090  1918  0x9e62  56
Router      0.0.0.0          192.168.3.1      0x80000092  2104  0x46d   72
Router      0.0.0.0          192.168.4.1      0x8000008f  2012  0x7016  40
InterArPfx  0.0.0.1          192.168.2.1      0x80000093   231  0xfc5c  36
InterArPfx  0.0.0.2          192.168.2.1      0x80000093    43  0x156   36
InterArPfx  0.0.0.3          192.168.2.1      0x80000092  1731  0x31a4  44
InterArPfx  0.0.0.4          192.168.2.1      0x8000008f  2668  0xc51f  44
InterArPfx  0.0.0.5          192.168.2.1      0x80000091  2856  0xfa59  36
InterArPfx  0.0.0.6          192.168.2.1      0x80000090  2481  0xe3fb  44
InterArPfx  0.0.0.1          192.168.3.1      0x80000093   417  0xf562  36
InterArPfx  0.0.0.2          192.168.3.1      0x80000093  2854  0x84d   36
InterArPfx  0.0.0.3          192.168.3.1      0x80000092  1729  0xbc26  44
InterArPfx  0.0.0.4          192.168.3.1      0x8000008f  2667  0x2ca9  44
InterArPfx  0.0.0.5          192.168.3.1      0x80000091   229  0xe56e  36
InterArPfx  0.0.0.6          192.168.3.1      0x8000008f  2292  0xde01  44
InterArPfx  0.0.0.2          192.168.4.1      0x80000092   794  0xf461  36
InterArPfx  0.0.0.3          192.168.4.1      0x80000092   606  0xf85b  36
InterArPfx  0.0.0.4          192.168.4.1      0x80000091   419  0xfe54  36
InterArPfx  0.0.0.5          192.168.4.1      0x80000090  1825  0xd906  44
InterArPfx  0.0.0.6          192.168.4.1      0x8000008f  2669  0xf1eb  44
InterArPfx  0.0.0.7          192.168.4.1      0x80000091   981  0xbc95  36
InterArPfx  0.0.0.8          192.168.4.1      0x8000008f  2481  0x8f4f  44
InterArPfx  0.0.0.9          192.168.4.1      0x80000090  2294  0xf0dd  44
InterArPfx  0.0.0.10         192.168.4.1      0x8000008f   231  0xac5a  44
IntraArPfx *0.0.0.1          192.168.0.1      0x80000094  2858  0xbf9f  64
IntraArPfx  0.0.0.1          192.168.1.1      0x80000095  2861  0x87d6  64
IntraArPfx  0.0.0.1          192.168.2.1      0x80000096   793  0xc7bd  64
IntraArPfx  0.0.0.1          192.168.3.1      0x80000097  1167  0x93f0  64

interface so-0/3/2.0 Area 0.0.0.0
 Type       ID               Adv Rtr          Seq          Age  Cksum  Len
Link       *0.0.0.2          192.168.0.1      0x80000091   858  0xc0c7  56
Link        0.0.0.8          192.168.3.1      0x80000091  1354  0x84f9  56
user@0>  show ospf3 interface
Interface           State   Area            DR ID           BDR ID          Nbrs
lo0.0               DRother 0.0.0.0         0.0.0.0         0.0.0.0            0
so-0/3/2.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1


user@0>  show ospf3 neighbor
ID               Interface              State     Pri   Dead
192.168.3.1      so-0/3/2.0             Full      128     33
  Neighbor-address fe80::2a0:a514:0:24c

user@0>  show ospf3 route
Prefix                                        Path  Route      NH   Metric
                                              Type  Type       Type
192.168.1.1                                   Intra Router     IP   3
  NH-interface so-0/3/2.0
192.168.2.1                                   Intra Area BR    IP   2
  NH-interface so-0/3/2.0
192.168.3.1                                   Intra Area BR    IP   1
  NH-interface so-0/3/2.0
192.168.4.1                                   Intra Area BR    IP   2
  NH-interface so-0/3/2.0
9009:1::/64                                   Intra Network    IP   1
```



```
  NH-interface so-0/3/2.0
9009:1::2/128                     Intra Network    IP   1
  NH-interface so-0/3/2.0
9009:2::/64                       Intra Network    IP   3
  NH-interface so-0/3/2.0
9009:2::2/128                     Intra Network    IP   2
  NH-interface so-0/3/2.0
9009:3::/64                       Inter Network    IP   2
  NH-interface so-0/3/2.0
9009:4::/64                       Inter Network    IP   3
  NH-interface so-0/3/2.0
9009:5::/64                       Inter Network    IP   2
  NH-interface so-0/3/2.0
9009:6::/64                       Inter Network    IP   3
  NH-interface so-0/3/2.0
9009:6::1/128                     Inter Network    IP   2
  NH-interface so-0/3/2.0
feee::10:255:71:1/128             Intra Network    IP   3
  NH-interface so-0/3/2.0
feee::10:255:71:3/128             Inter Network    IP   1
  NH-interface so-0/3/2.0
feee::10:255:71:4/128             Intra Network    IP   0
  NH-interface lo0.0
feee::10:255:71:5/128             Inter Network    IP   2
  NH-interface so-0/3/2.0
feee::10:255:71:6/128             Inter Network    IP   3
  NH-interface so-0/3/2.0
feee::10:255:71:11/128            Inter Network    IP   2
  NH-interface so-0/3/2.0

user@0> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
so-0/3/2.0              up    up   inet6    9009:1::1/64
                                            fe80::2a0:a514:0:14c/64
lo0
lo0.0                   up    up   inet     192.168.0.1         --> 0/0
                                   inet6    fe80::2a0:a50f:fc56:14c
                                            feee::10:255:71:4
...
```

Meaning

Device 1 Status

Purpose Verify that Device 1 has learned the expected routes and has established the expected neighbor adjacencies.

Action

```
user@1> show ospf3 interface
Interface           State   Area            DR ID           BDR ID          Nbrs
lo0.0              DRother 0.0.0.0         0.0.0.0         0.0.0.0            0
at-2/0/0.0         PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
user@1> show ospf3 neighbor
ID               Interface              State     Pri   Dead
192.168.2.1      at-2/0/0.0             Full      128     37
  Neighbor-address fe80::2a0:a514:0:c4c

user@1>  show ospf3 database
Area 0.0.0.0
 Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Router      0.0.0.0          192.168.0.1      0x8000008f  2334  0x6e21  40
Router     *0.0.0.0          192.168.1.1      0x8000008f  2331  0x523d  40
Router      0.0.0.0          192.168.2.1      0x80000090  2390  0x9e62  56
Router      0.0.0.0          192.168.3.1      0x80000092  2578  0x46d   72
Router      0.0.0.0          192.168.4.1      0x8000008f  2486  0x7016  40
InterArPfx  0.0.0.1          192.168.2.1      0x80000093   703  0xfc5c  36
InterArPfx  0.0.0.2          192.168.2.1      0x80000093   515  0x156   36
InterArPfx  0.0.0.3          192.168.2.1      0x80000092  2203  0x31a4  44
InterArPfx  0.0.0.4          192.168.2.1      0x80000090   140  0xc320  44
InterArPfx  0.0.0.5          192.168.2.1      0x80000092   328  0xf85a  36
InterArPfx  0.0.0.6          192.168.2.1      0x80000090  2953  0xe3fb  44
InterArPfx  0.0.0.1          192.168.3.1      0x80000093   891  0xf562  36
InterArPfx  0.0.0.2          192.168.3.1      0x80000094   328  0x64e   36
InterArPfx  0.0.0.3          192.168.3.1      0x80000092  2203  0xbc26  44
InterArPfx  0.0.0.4          192.168.3.1      0x80000090   141  0x2aaa  44
InterArPfx  0.0.0.5          192.168.3.1      0x80000091   703  0xe56e  36
InterArPfx  0.0.0.6          192.168.3.1      0x8000008f  2766  0xde01  44
InterArPfx  0.0.0.2          192.168.4.1      0x80000092  1268  0xf461  36
InterArPfx  0.0.0.3          192.168.4.1      0x80000092  1080  0xf85b  36
InterArPfx  0.0.0.4          192.168.4.1      0x80000091   893  0xfe54  36
InterArPfx  0.0.0.5          192.168.4.1      0x80000090  2299  0xd906  44
InterArPfx  0.0.0.6          192.168.4.1      0x80000090   143  0xefec  44
InterArPfx  0.0.0.7          192.168.4.1      0x80000091  1455  0xbc95  36
InterArPfx  0.0.0.8          192.168.4.1      0x8000008f  2955  0x8f4f  44
InterArPfx  0.0.0.9          192.168.4.1      0x80000090  2768  0xf0dd  44
InterArPfx  0.0.0.10         192.168.4.1      0x8000008f   705  0xac5a  44
IntraArPfx  0.0.0.1          192.168.0.1      0x80000095   334  0xbda0  64
IntraArPfx *0.0.0.1          192.168.1.1      0x80000096   331  0x85d7  64
IntraArPfx  0.0.0.1          192.168.2.1      0x80000096  1265  0xc7bd  64
IntraArPfx  0.0.0.1          192.168.3.1      0x80000097  1641  0x93f0  64

interface at-2/0/0.0 Area 0.0.0.0
 Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Link       *0.0.0.2          192.168.1.1      0x80000091  1331  0xaecd  56
Link        0.0.0.8          192.168.2.1      0x80000091  1453  0x80f3  56

user@1>  show ospf3 route
Prefix                                       Path  Route      NH   Metric
                                             Type  Type       Type
192.168.0.1                                  Intra Router     IP   3
  NH-interface at-2/0/0.0
192.168.2.1                                  Intra Area BR    IP   1
  NH-interface at-2/0/0.0
192.168.3.1                                  Intra Area BR    IP   2
  NH-interface at-2/0/0.0
192.168.4.1                                  Intra Area BR    IP   3
  NH-interface at-2/0/0.0
9009:1::/64                                  Intra Network    IP   3
  NH-interface at-2/0/0.0
```



```
9009:1::2/128                              Intra Network    IP   2
  NH-interface at-2/0/0.0
9009:2::/64                                Intra Network    IP   1
  NH-interface at-2/0/0.0
9009:2::2/128                              Intra Network    IP   1
  NH-interface at-2/0/0.0
9009:3::/64                                Inter Network    IP   2
  NH-interface at-2/0/0.0
9009:4::/64                                Inter Network    IP   2
  NH-interface at-2/0/0.0
9009:5::/64                                Inter Network    IP   3
  NH-interface at-2/0/0.0
9009:6::/64                                Inter Network    IP   4
  NH-interface at-2/0/0.0
9009:6::1/128                              Inter Network    IP   3
  NH-interface at-2/0/0.0
feee::10:255:71:1/128                      Intra Network    IP   0
  NH-interface lo0.0
feee::10:255:71:3/128                      Inter Network    IP   2
  NH-interface at-2/0/0.0
feee::10:255:71:4/128                      Intra Network    IP   3
  NH-interface at-2/0/0.0
feee::10:255:71:5/128                      Inter Network    IP   2
  NH-interface at-2/0/0.0
feee::10:255:71:6/128                      Inter Network    IP   4
  NH-interface at-2/0/0.0
feee::10:255:71:11/128                     Inter Network    IP   1
  NH-interface at-2/0/0.0

user@1>  show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
at-2/0/0.0             up    up   inet6    9009:2::1/64
                                            fe80::2a0:a514:0:b4c/64
lo0
lo0.0                   up    up   inet     192.168.1.1         --> 0/0
                                   inet6    fe80::2a0:a50f:fc56:14c
                                            feee::10:255:71:1
...
```

Device 2 Status

Purpose

Verify that Device 2 has learned the expected routes and has established the expected neighbor adjacencies.

Action

```
user@2> show ospf3 interface
Interface           State   Area            DR ID           BDR ID          Nbrs
at-0/3/1.0         PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
vl-192.168.3.1      PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
lo0.0               DRother 0.0.0.1         0.0.0.0         0.0.0.0            0
so-0/2/0.0          PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1
fe-1/1/0.0          PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1

user@2>  show ospf3 neighbor
ID               Interface              State     Pri   Dead
192.168.1.1      at-0/3/1.0            Full      128    32
  Neighbor-address fe80::2a0:a514:0:b4c
192.168.3.1      vl-192.168.3.1         Full        0     35
  Neighbor-address 9009:3::2
192.168.3.1      so-0/2/0.0             Full      128     38
  Neighbor-address fe80::2a0:a514:0:74c
192.168.4.1      fe-1/1/0.0             Full      128     30
  Neighbor-address fe80::2a0:a514:0:a4c

user@2>  show ospf3 database
Area 0.0.0.0
 Type       ID                 Adv Rtr           Seq          Age  Cksum  Len
Router      0.0.0.0            192.168.0.1      0x8000008f  2771  0x6e21  40
Router      0.0.0.0            192.168.1.1      0x8000008f  2770  0x523d  40
Router     *0.0.0.0            192.168.2.1      0x80000090  2827  0x9e62  56
Router      0.0.0.0            192.168.3.1      0x80000093    15  0x26e   72
Router      0.0.0.0            192.168.4.1      0x8000008f  2923  0x7016  40
InterArPfx *0.0.0.1            192.168.2.1      0x80000093  1140  0xfc5c  36
InterArPfx *0.0.0.2            192.168.2.1      0x80000093   952  0x156   36
InterArPfx *0.0.0.3            192.168.2.1      0x80000092  2640  0x31a4  44
InterArPfx *0.0.0.4            192.168.2.1      0x80000090   577  0xc320  44
InterArPfx *0.0.0.5            192.168.2.1      0x80000092   765  0xf85a  36
InterArPfx *0.0.0.6            192.168.2.1      0x80000091   390  0xe1fc  44
InterArPfx  0.0.0.1            192.168.3.1      0x80000093  1328  0xf562  36
InterArPfx  0.0.0.2            192.168.3.1      0x80000094   765  0x64e   36
InterArPfx  0.0.0.3            192.168.3.1      0x80000092  2640  0xbc26  44
InterArPfx  0.0.0.4            192.168.3.1      0x80000090   578  0x2aaa  44
InterArPfx  0.0.0.5            192.168.3.1      0x80000091  1140  0xe56e  36
InterArPfx  0.0.0.6            192.168.3.1      0x80000090   203  0xdc02  44
InterArPfx  0.0.0.2            192.168.4.1      0x80000092  1705  0xf461  36
InterArPfx  0.0.0.3            192.168.4.1      0x80000092  1517  0xf85b  36
InterArPfx  0.0.0.4            192.168.4.1      0x80000091  1330  0xfe54  36
InterArPfx  0.0.0.5            192.168.4.1      0x80000090  2736  0xd906  44
InterArPfx  0.0.0.6            192.168.4.1      0x80000090   580  0xefec  44
InterArPfx  0.0.0.7            192.168.4.1      0x80000091  1892  0xbc95  36
InterArPfx  0.0.0.8            192.168.4.1      0x80000090   392  0x8d50  44
InterArPfx  0.0.0.9            192.168.4.1      0x80000091   205  0xeede  44
InterArPfx  0.0.0.10           192.168.4.1      0x8000008f  1142  0xac5a  44
IntraArPfx  0.0.0.1            192.168.0.1      0x80000095   771  0xbda0  64
IntraArPfx  0.0.0.1            192.168.1.1      0x80000096   770  0x85d7  64
IntraArPfx *0.0.0.1            192.168.2.1      0x80000096  1702  0xc7bd  64
IntraArPfx  0.0.0.1            192.168.3.1      0x80000097  2078  0x93f0  64

Area 0.0.0.1
 Type       ID                 Adv Rtr           Seq          Age  Cksum  Len
Router     *0.0.0.0            192.168.2.1      0x80000093    15  0x8f62  56
Router      0.0.0.0            192.168.3.1      0x80000093  2828  0x39b7  56
Router      0.0.0.0            192.168.4.1      0x80000092    16  0x8768  56
InterArPfx *0.0.0.1            192.168.2.1      0x80000094  1515  0xec6c  36
InterArPfx *0.0.0.3            192.168.2.1      0x80000090   202  0x994d  44
InterArPfx *0.0.0.4            192.168.2.1      0x8000008f  1327  0xd839  44
```



```
InterArPfx  0.0.0.1         192.168.3.1      0x80000094  1703  0xd781  36
InterArPfx  0.0.0.3         192.168.3.1      0x80000090   390  0xe002  44
InterArPfx  0.0.0.4         192.168.3.1      0x8000008f  1515  0xc34e  44
InterArPfx  0.0.0.1         192.168.4.1      0x80000093  1422  0x193b  36
InterArPfx  0.0.0.3         192.168.4.1      0x80000090   672  0xed1   44
InterArPfx  0.0.0.4         192.168.4.1      0x8000008f  1235  0xe824  44
IntraArPfx *0.0.0.1         192.168.2.1      0x80000097  2265  0x6bf1  76
IntraArPfx  0.0.0.1         192.168.3.1      0x80000099   953  0xadb8  76
IntraArPfx  0.0.0.1         192.168.4.1      0x80000098  2079  0x3c26  76

interface at-0/3/1.0 Area 0.0.0.0
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link        0.0.0.2         192.168.1.1      0x80000091  1770  0xaecd  56
Link       *0.0.0.8         192.168.2.1      0x80000091  1890  0x80f3  56

interface so-0/2/0.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link       *0.0.0.6         192.168.2.1      0x80000092  2452  0x6018  56
Link        0.0.0.7         192.168.3.1      0x80000092  2453  0x3a3d  56

interface fe-1/1/0.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link       *0.0.0.7         192.168.2.1      0x80000092  2077  0x8de7  56
Link        0.0.0.8         192.168.4.1      0x80000091  2172  0x8ce5  56

user@2>  show ospf3 route
Prefix                                       Path  Route      NH   Metric
                                             Type  Type       Type
192.168.0.1                                  Intra Router     IP   2
  NH-interface (null), NH-addr feee::10:255:71:3
192.168.1.1                                  Intra Router     IP   1
  NH-interface at-0/3/1.0
192.168.3.1                                  Intra Area BR    IP   1
  NH-interface so-0/2/0.0
192.168.4.1                                  Intra Area BR    IP   1
  NH-interface fe-1/1/0.0
9009:1::/64                                  Intra Network    IP   2
  NH-interface so-0/2/0.0
9009:1::2/128                                Intra Network    IP   1
  NH-interface so-0/2/0.0
9009:2::/64                                  Intra Network    IP   1
  NH-interface at-0/3/1.0
9009:2::2/128                                Intra Network    IP   0
  NH-interface at-0/3/1.0
9009:3::/64                                  Intra Network    IP   1
  NH-interface so-0/2/0.0
9009:4::/64                                  Intra Network    IP   1
  NH-interface fe-1/1/0.0
9009:5::/64                                  Intra Network    IP   2
  NH-interface so-0/2/0.0
  NH-interface fe-1/1/0.0
9009:6::/64                                  Inter Network    IP   2
  NH-interface fe-1/1/0.0
9009:6::1/128                                Inter Network    IP   1
  NH-interface fe-1/1/0.0
feee::10:255:71:1/128                        Intra Network    IP   1
  NH-interface at-0/3/1.0
feee::10:255:71:3/128                        Intra Network    IP   1
  NH-interface so-0/2/0.0
feee::10:255:71:4/128                        Intra Network    IP   2
  NH-interface so-0/2/0.0
```

```
feee::10:255:71:5/128                       Intra Network    IP   1
  NH-interface fe-1/1/0.0
feee::10:255:71:6/128                       Inter Network    IP   2
  NH-interface fe-1/1/0.0
feee::10:255:71:11/128                      Intra Network    IP   0
  NH-interface lo0.0

user@2>  show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
so-0/2/0.0               up    up   inet6    9009:3::1/64
                                             fe80::2a0:a514:0:84c/64
fe-1/1/0.0               up    up   inet6    9009:4::1/64
                                             fe80::2a0:a514:0:94c/64
at-0/3/1.0              up    up   inet6    9009:2::2/64
                                             fe80::2a0:a514:0:c4c/64
lo0
lo0.0                    up    up   inet     192.168.2.1         --> 0/0
                                    inet6    fe80::2a0:a50f:fc56:14c
                                             feee::10:255:71:11
...
```

Device 3 Status

Purpose Verify that Device 3 has learned the expected routes and has established the expected neighbor adjacencies.

Action

```
user@3> show ospf3 interface
Interface           State   Area            DR ID           BDR ID          Nbrs
so-0/3/2.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
vl-192.168.2.1      PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
vl-192.168.4.1      PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
lo0.0               DRother 0.0.0.1         0.0.0.0         0.0.0.0            0
t1-0/2/1.0          PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1
so-0/3/0.0          PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1
```

```
user@3> show ospf3 neighbor
ID               Interface              State     Pri   Dead
192.168.0.1      so-0/3/2.0             Full      128     31
  Neighbor-address fe80::2a0:a514:0:14c
192.168.2.1      vl-192.168.2.1         Full        0     33
  Neighbor-address 9009:3::1
192.168.4.1      vl-192.168.4.1         Full        0     38
  Neighbor-address 9009:5::2
192.168.4.1      t1-0/2/1.0             Full      128     35
  Neighbor-address fe80::2a0:a514:0:44c
192.168.2.1      so-0/3/0.0             Full      128     37
  Neighbor-address fe80::2a0:a514:0:84c
```

```
user@3>  show ospf3 database
Area 0.0.0.0
 Type       ID                Adv Rtr           Seq          Age  Cksum  Len
Router      0.0.0.0           192.168.0.1      0x80000090    11  0x6c22  40
Router      0.0.0.0           192.168.1.1      0x80000090    12  0x503e  40
Router      0.0.0.0           192.168.2.1      0x80000091    69  0x9c63  56
Router     *0.0.0.0           192.168.3.1      0x80000093   255  0x26e   72
Router      0.0.0.0           192.168.4.1      0x80000090   163  0x6e17  40
InterArPfx  0.0.0.1           192.168.2.1      0x80000093  1382  0xfc5c  36
InterArPfx  0.0.0.2           192.168.2.1      0x80000093  1194  0x156   36
InterArPfx  0.0.0.3           192.168.2.1      0x80000092  2882  0x31a4  44
InterArPfx  0.0.0.4           192.168.2.1      0x80000090   819  0xc320  44
InterArPfx  0.0.0.5           192.168.2.1      0x80000092  1007  0xf85a  36
InterArPfx  0.0.0.6           192.168.2.1      0x80000091   632  0xe1fc  44
InterArPfx *0.0.0.1           192.168.3.1      0x80000093  1568  0xf562  36
InterArPfx *0.0.0.2           192.168.3.1      0x80000094  1005  0x64e   36
InterArPfx *0.0.0.3           192.168.3.1      0x80000092  2880  0xbc26  44
InterArPfx *0.0.0.4           192.168.3.1      0x80000090   818  0x2aaa  44
InterArPfx *0.0.0.5           192.168.3.1      0x80000091  1380  0xe56e  36
InterArPfx *0.0.0.6           192.168.3.1      0x80000090   443  0xdc02  44
InterArPfx  0.0.0.2           192.168.4.1      0x80000092  1945  0xf461  36
InterArPfx  0.0.0.3           192.168.4.1      0x80000092  1757  0xf85b  36
InterArPfx  0.0.0.4           192.168.4.1      0x80000091  1570  0xfe54  36
InterArPfx  0.0.0.5           192.168.4.1      0x80000090  2976  0xd906  44
InterArPfx  0.0.0.6           192.168.4.1      0x80000090   820  0xefec  44
InterArPfx  0.0.0.7           192.168.4.1      0x80000091  2132  0xbc95  36
InterArPfx  0.0.0.8           192.168.4.1      0x80000090   632  0x8d50  44
InterArPfx  0.0.0.9           192.168.4.1      0x80000091   445  0xeede  44
InterArPfx  0.0.0.10          192.168.4.1      0x8000008f  1382  0xac5a  44
IntraArPfx  0.0.0.1           192.168.0.1      0x80000095  1011  0xbda0  64
IntraArPfx  0.0.0.1           192.168.1.1      0x80000096  1012  0x85d7  64
IntraArPfx  0.0.0.1           192.168.2.1      0x80000096  1944  0xc7bd  64
IntraArPfx *0.0.0.1           192.168.3.1      0x80000097  2318  0x93f0  64

Area 0.0.0.1
 Type       ID                Adv Rtr           Seq          Age  Cksum  Len
Router      0.0.0.0           192.168.2.1      0x80000093   257  0x8f62  56
Router     *0.0.0.0           192.168.3.1      0x80000094    68  0x37b8  56
Router      0.0.0.0           192.168.4.1      0x80000092   257  0x8768  56
```



```
InterArPfx  0.0.0.1         192.168.2.1      0x80000094  1757  0xec6c  36
InterArPfx  0.0.0.3         192.168.2.1      0x80000090   444  0x994d  44
InterArPfx  0.0.0.4         192.168.2.1      0x8000008f  1569  0xd839  44
InterArPfx *0.0.0.1         192.168.3.1      0x80000094  1943  0xd781  36
InterArPfx *0.0.0.3         192.168.3.1      0x80000090   630  0xe002  44
InterArPfx *0.0.0.4         192.168.3.1      0x8000008f  1755  0xc34e  44
InterArPfx  0.0.0.1         192.168.4.1      0x80000093  1663  0x193b  36
InterArPfx  0.0.0.3         192.168.4.1      0x80000090   913  0xed1   44
InterArPfx  0.0.0.4         192.168.4.1      0x8000008f  1476  0xe824  44
IntraArPfx  0.0.0.1         192.168.2.1      0x80000097  2507  0x6bf1  76
IntraArPfx *0.0.0.1         192.168.3.1      0x80000099  1193  0xadb8  76
IntraArPfx  0.0.0.1         192.168.4.1      0x80000098  2320  0x3c26  76

interface so-0/3/2.0 Area 0.0.0.0
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link        0.0.0.2         192.168.0.1      0x80000091  2011  0xc0c7  56
Link       *0.0.0.8         192.168.3.1      0x80000091  2505  0x84f9  56

interface t1-0/2/1.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link       *0.0.0.9         192.168.3.1      0x80000092  2130  0x1661  56
Link        0.0.0.7         192.168.4.1      0x80000092  2507  0x383f  56

interface so-0/3/0.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link        0.0.0.6         192.168.2.1      0x80000092  2694  0x6018  56
Link       *0.0.0.7         192.168.3.1      0x80000092  2693  0x3a3d  56

user@3>  show ospf3 route
Prefix                                       Path  Route      NH   Metric
                                             Type  Type       Type
192.168.0.1                                  Intra Router     IP   1
  NH-interface so-0/3/2.0
192.168.1.1                                  Intra Router     IP   2
  NH-interface (null), NH-addr feee::10:255:71:11
192.168.2.1                                  Intra Area BR    IP   1
  NH-interface so-0/3/0.0
192.168.4.1                                  Intra Area BR    IP   1
  NH-interface t1-0/2/1.0
9009:1::/64                                  Intra Network    IP   1
  NH-interface so-0/3/2.0
9009:1::2/128                                Intra Network    IP   0
  NH-interface so-0/3/2.0
9009:2::/64                                  Intra Network    IP   2
  NH-interface so-0/3/0.0
9009:2::2/128                                Intra Network    IP   1
  NH-interface so-0/3/0.0
9009:3::/64                                  Intra Network    IP   1
  NH-interface so-0/3/0.0
9009:4::/64                                  Intra Network    IP   2
  NH-interface so-0/3/0.0
  NH-interface t1-0/2/1.0
9009:5::/64                                  Intra Network    IP   1
  NH-interface t1-0/2/1.0
9009:6::/64                                  Inter Network    IP   2
  NH-interface t1-0/2/1.0
9009:6::1/128                                Inter Network    IP   1
  NH-interface t1-0/2/1.0
feee::10:255:71:1/128                        Intra Network    IP   2
  NH-interface so-0/3/0.0
feee::10:255:71:3/128                        Intra Network    IP   0
```

```
  NH-interface lo0.0
feee::10:255:71:4/128                      Intra Network    IP   1
  NH-interface so-0/3/2.0
feee::10:255:71:5/128                      Intra Network    IP   1
  NH-interface t1-0/2/1.0
feee::10:255:71:6/128                      Inter Network    IP   2
  NH-interface t1-0/2/1.0
feee::10:255:71:11/128                     Intra Network    IP   1
  NH-interface so-0/3/0.0

user@3>  show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
so-0/3/2.0              up    up   inet6    9009:1::2/64
                                            fe80::2a0:a514:0:24c/64
t1-0/2/1.0              up    up   inet6    9009:5::1/64
                                            fe80::2a0:a514:0:34c/64
so-0/3/0.0              up    up   inet6    9009:3::2/64
                                            fe80::2a0:a514:0:74c/64
lo0
lo0.0                   up    up   inet     192.168.3.1         --> 0/0
                                   inet6    fe80::2a0:a50f:fc56:14c
                                            feee::10:255:71:3
...
```

Device 4 Status

Purpose Verify that Device 4 has learned the expected routes and has established the expected neighbor adjacencies.

Action

user@4> **show ospf3 interface**

```
Interface           State   Area            DR ID           BDR ID          Nbrs
lo0.0              DRother 0.0.0.1         0.0.0.0         0.0.0.0            0
fe-1/1/0.0        PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1
t1-0/2/1.0         PtToPt  0.0.0.1         0.0.0.0         0.0.0.0            1
fe-0/0/0.0         PtToPt  0.0.0.2         0.0.0.0         0.0.0.0            1
vl-192.168.3.1     PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1
```

user@4> **show ospf3 neighbor**

```
ID               Interface              State     Pri   Dead
192.168.2.1      fe-1/1/0.0            Full      128    35
  Neighbor-address fe80::2a0:a514:0:94c
192.168.3.1      t1-0/2/1.0            Full      128     34
  Neighbor-address fe80::2a0:a514:0:34c
192.168.5.1      fe-0/0/0.0            Full      128     39
  Neighbor-address fe80::2a0:a514:0:64c
192.168.3.1      vl-192.168.3.1        Full        0     33
  Neighbor-address 9009:5::1
```

user@4> **show ospf3 database**

```
Area 0.0.0.0
 Type       ID                Adv Rtr          Seq          Age  Cksum  Len
Router      0.0.0.0          192.168.0.1      0x80000090   270  0x6c22  40
Router      0.0.0.0          192.168.1.1      0x80000090   271  0x503e  40
Router      0.0.0.0          192.168.2.1      0x80000091   328  0x9c63  56
Router      0.0.0.0          192.168.3.1      0x80000093   514  0x26e   72
Router     *0.0.0.0          192.168.4.1      0x80000090   420  0x6e17  40
InterArPfx  0.0.0.1          192.168.2.1      0x80000093  1641  0xfc5c  36
InterArPfx  0.0.0.2          192.168.2.1      0x80000093  1453  0x156   36
InterArPfx  0.0.0.3          192.168.2.1      0x80000093   141  0x2fa5  44
InterArPfx  0.0.0.4          192.168.2.1      0x80000090  1078  0xc320  44
InterArPfx  0.0.0.5          192.168.2.1      0x80000092  1266  0xf85a  36
InterArPfx  0.0.0.6          192.168.2.1      0x80000091   891  0xe1fc  44
InterArPfx  0.0.0.1          192.168.3.1      0x80000093  1827  0xf562  36
InterArPfx  0.0.0.2          192.168.3.1      0x80000094  1264  0x64e   36
InterArPfx  0.0.0.3          192.168.3.1      0x80000093   139  0xba27  44
InterArPfx  0.0.0.4          192.168.3.1      0x80000090  1077  0x2aaa  44
InterArPfx  0.0.0.5          192.168.3.1      0x80000091  1639  0xe56e  36
InterArPfx  0.0.0.6          192.168.3.1      0x80000090   702  0xdc02  44
InterArPfx *0.0.0.2          192.168.4.1      0x80000092  2202  0xf461  36
InterArPfx *0.0.0.3          192.168.4.1      0x80000092  2014  0xf85b  36
InterArPfx *0.0.0.4          192.168.4.1      0x80000091  1827  0xfe54  36
InterArPfx *0.0.0.5          192.168.4.1      0x80000091   233  0xd707  44
InterArPfx *0.0.0.6          192.168.4.1      0x80000090  1077  0xefec  44
InterArPfx *0.0.0.7          192.168.4.1      0x80000091  2389  0xbc95  36
InterArPfx *0.0.0.8          192.168.4.1      0x80000090   889  0x8d50  44
InterArPfx *0.0.0.9          192.168.4.1      0x80000091   702  0xeede  44
InterArPfx *0.0.0.10         192.168.4.1      0x8000008f  1639  0xac5a  44
IntraArPfx  0.0.0.1          192.168.0.1      0x80000095  1270  0xbda0  64
IntraArPfx  0.0.0.1          192.168.1.1      0x80000096  1271  0x85d7  64
IntraArPfx  0.0.0.1          192.168.2.1      0x80000096  2203  0xc7bd  64
IntraArPfx  0.0.0.1          192.168.3.1      0x80000097  2577  0x93f0  64

Area 0.0.0.1
 Type       ID                Adv Rtr          Seq          Age  Cksum  Len
Router      0.0.0.0          192.168.2.1      0x80000093   515  0x8f62  56
Router      0.0.0.0          192.168.3.1      0x80000094   327  0x37b8  56
Router     *0.0.0.0          192.168.4.1      0x80000092   514  0x8768  56
InterArPfx  0.0.0.1          192.168.2.1      0x80000094  2015  0xec6c  36
InterArPfx  0.0.0.3          192.168.2.1      0x80000090   702  0x994d  44
InterArPfx  0.0.0.4          192.168.2.1      0x8000008f  1827  0xd839  44
```



```
InterArPfx  0.0.0.1         192.168.3.1      0x80000094  2202  0xd781  36
InterArPfx  0.0.0.3         192.168.3.1      0x80000090   889  0xe002  44
InterArPfx  0.0.0.4         192.168.3.1      0x8000008f  2014  0xc34e  44
InterArPfx *0.0.0.1         192.168.4.1      0x80000093  1920  0x193b  36
InterArPfx *0.0.0.3         192.168.4.1      0x80000090  1170  0xed1   44
InterArPfx *0.0.0.4         192.168.4.1      0x8000008f  1733  0xe824  44
IntraArPfx  0.0.0.1         192.168.2.1      0x80000097  2765  0x6bf1  76
IntraArPfx  0.0.0.1         192.168.3.1      0x80000099  1452  0xadb8  76
IntraArPfx *0.0.0.1         192.168.4.1      0x80000098  2577  0x3c26  76

Area 0.0.0.2
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Router     *0.0.0.0         192.168.4.1      0x80000091    45  0x4741  40
Router      0.0.0.0         192.168.5.1      0x80000090   270  0x3a50  40
InterArPfx *0.0.0.1         192.168.4.1      0x80000094  2295  0xfa5a  36
InterArPfx *0.0.0.2         192.168.4.1      0x80000094  2108  0xfe54  36
InterArPfx *0.0.0.3         192.168.4.1      0x80000093   139  0xe7f6  44
InterArPfx *0.0.0.4         192.168.4.1      0x80000091  2483  0xda7a  36
InterArPfx *0.0.0.5         192.168.4.1      0x80000090   983  0xab35  44
InterArPfx *0.0.0.6         192.168.4.1      0x80000091   795  0xdc3   44
InterArPfx *0.0.0.7         192.168.4.1      0x80000090  1545  0xa2b2  36
InterArPfx *0.0.0.9         192.168.4.1      0x80000090  1358  0x9cb5  36
InterArPfx *0.0.0.11        192.168.4.1      0x80000090   608  0x8f49  44
InterArPfx *0.0.0.12        192.168.4.1      0x80000090   327  0x37a3  44
InterArPfx *0.0.0.13        192.168.4.1      0x8000008f  1452  0x689e  44
InterArPfx *0.0.0.14        192.168.4.1      0x8000008f  1264  0x6c98  44
IntraArPfx *0.0.0.1         192.168.4.1      0x80000098  2858  0x82f5  64
IntraArPfx  0.0.0.1         192.168.5.1      0x80000095  1270  0xf25a  64

interface fe-1/1/0.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link        0.0.0.7         192.168.2.1      0x80000092  2577  0x8de7  56
Link       *0.0.0.8         192.168.4.1      0x80000091  2670  0x8ce5  56

interface t1-0/2/1.0 Area 0.0.0.1
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link        0.0.0.9         192.168.3.1      0x80000092  2389  0x1661  56
Link       *0.0.0.7         192.168.4.1      0x80000092  2764  0x383f  56

interface fe-0/0/0.0 Area 0.0.0.2
 Type       ID              Adv Rtr           Seq         Age  Cksum  Len
Link       *0.0.0.6         192.168.4.1      0x80000092  2952  0x79fc  56
Link        0.0.0.2         192.168.5.1      0x80000091  2270  0xb1c7  56

user@4> show ospf3 route
Prefix                                    Path  Route      NH   Metric
                                          Type  Type       Type
192.168.0.1                               Intra Router     IP   2
  NH-interface (null), NH-addr feee::10:255:71:3
192.168.1.1                               Intra Router     IP   3
  NH-interface (null), NH-addr feee::10:255:71:3
192.168.2.1                               Intra Area BR    IP   1
  NH-interface fe-1/1/0.0
192.168.3.1                               Intra Area BR    IP   1
  NH-interface t1-0/2/1.0
192.168.5.1                               Intra Router     IP   1
  NH-interface fe-0/0/0.0
9009:1::/64                               Intra Network    IP   2
  NH-interface t1-0/2/1.0
9009:1::2/128                             Intra Network    IP   1
  NH-interface t1-0/2/1.0
```

```
9009:2::/64                                  Intra Network    IP   2
  NH-interface fe-1/1/0.0
9009:2::2/128                                Intra Network    IP   1
  NH-interface fe-1/1/0.0
9009:3::/64                                  Intra Network    IP   2
  NH-interface t1-0/2/1.0
  NH-interface fe-1/1/0.0
9009:4::/64                                  Intra Network    IP   1
  NH-interface fe-1/1/0.0
9009:5::/64                                  Intra Network    IP   1
  NH-interface t1-0/2/1.0
9009:6::/64                                  Intra Network    IP   1
  NH-interface fe-0/0/0.0
9009:6::1/128                                Intra Network    IP   0
  NH-interface fe-0/0/0.0
feee::10:255:71:1/128                        Intra Network    IP   2
  NH-interface fe-1/1/0.0
feee::10:255:71:3/128                        Intra Network    IP   1
  NH-interface t1-0/2/1.0
feee::10:255:71:4/128                        Intra Network    IP   2
  NH-interface t1-0/2/1.0
feee::10:255:71:5/128                        Intra Network    IP   0
  NH-interface lo0.0
feee::10:255:71:6/128                        Intra Network    IP   1
  NH-interface fe-0/0/0.0
feee::10:255:71:11/128                       Intra Network    IP   1
  NH-interface fe-1/1/0.0

user@4> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
t1-0/2/1.0              up    up   inet6    9009:5::2/64
                                            fe80::2a0:a514:0:44c/64
fe-0/0/0.0              up    up   inet6    9009:6::1/64
                                            fe80::2a0:a514:0:54c/64
fe-1/1/0.0             up    up   inet6    9009:4::2/64
                                            fe80::2a0:a514:0:a4c/64
lo0
lo0.0                   up    up   inet     192.168.4.1         --> 0/0
                                   inet6    fe80::2a0:a50f:fc56:14c
                                            feee::10:255:71:5
...
```

Device 5 Status

Purpose Verify that Device 5 has learned the expected routes and has established the expected neighbor adjacencies.

Action

```
user@5> show ospf3 interface
Interface           State    Area            DR ID           BDR ID          Nbrs
lo0.0               DRother 0.0.0.2         0.0.0.0         0.0.0.0            0
fe-0/0/0.0          PtToPt  0.0.0.2         0.0.0.0         0.0.0.0            1
user@5> show ospf3 neighbor
ID               Interface              State     Pri   Dead
192.168.4.1      fe-0/0/0.0             Full      128     34
  Neighbor-address fe80::2a0:a514:0:54c

user@5>  show ospf3 database
Area 0.0.0.2
 Type        ID               Adv Rtr           Seq         Age  Cksum  Len
Router       0.0.0.0          192.168.4.1      0x80000091   509  0x4741  40
Router      *0.0.0.0          192.168.5.1      0x80000090   732  0x3a50  40
InterArPfx   0.0.0.1          192.168.4.1      0x80000094  2759  0xfa5a  36
InterArPfx   0.0.0.2          192.168.4.1      0x80000094  2572  0xfe54  36
InterArPfx   0.0.0.3          192.168.4.1      0x80000093   603  0xe7f6  44
InterArPfx   0.0.0.4          192.168.4.1      0x80000091  2947  0xda7a  36
InterArPfx   0.0.0.5          192.168.4.1      0x80000090  1447  0xab35  44
InterArPfx   0.0.0.6          192.168.4.1      0x80000091  1259  0xdc3   44
InterArPfx   0.0.0.7          192.168.4.1      0x80000090  2009  0xa2b2  36
InterArPfx   0.0.0.9          192.168.4.1      0x80000090  1822  0x9cb5  36
InterArPfx   0.0.0.11         192.168.4.1      0x80000090  1072  0x8f49  44
InterArPfx   0.0.0.12         192.168.4.1      0x80000090   791  0x37a3  44
InterArPfx   0.0.0.13         192.168.4.1      0x8000008f  1916  0x689e  44
InterArPfx   0.0.0.14         192.168.4.1      0x8000008f  1728  0x6c98  44
IntraArPfx   0.0.0.1          192.168.4.1      0x80000099   322  0x80f6  64
IntraArPfx  *0.0.0.1          192.168.5.1      0x80000095  1732  0xf25a  64

interface fe-0/0/0.0 Area 0.0.0.2
 Type        ID               Adv Rtr           Seq         Age  Cksum  Len
Link         0.0.0.6          192.168.4.1      0x80000093   416  0x77fd  56
Link        *0.0.0.2          192.168.5.1      0x80000091  2732  0xb1c7  56

user@5>  show interfaces terse
Interface               Admin Link Proto    Local                 Remote
lt-1/2/0
fe-0/0/0.0              up    up   inet6    9009:6::2/64
                                            fe80::2a0:a514:0:64c/64
lo0
lo0.0                   up    up   inet     192.168.5.1         --> 0/0
                                   inet6    fe80::2a0:a50f:fc56:14c
                                            feee::10:255:71:6
...
```

Example: Disabling OSPFv2 Compatibility with RFC 1583

OSPFv2 Compatibility with RFC 1583 Overview

In the first implementation of OSPF (RFC1583, *OSPF Version 2*), the summary route assumes the cost of the granular route with the lowest cost. OSPF RFC 2328, *OSPF Version 2* changes the behavior so that the summary route assumes the cost of the granular route with the highest cost. OSPF readvertises the summary route whenever the cost of the summary changes. When using the default RFC 1583 behavior, this happens when the granular route with the lowest metric is changed or lost. When RFC 2328 is used, this happens when the granular route with the highest cost is changed or lost.

By default, the Junos OS implementation of OSPF is compatible with RFC 1583. This means that Junos OS maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table, rather than multiple intra-AS paths, if they are available. You can disable compatibility with RFC 1583. It is preferable to do so when the same external destination is advertised by AS boundary routers that belong to different OSPF areas. When you disable compatibility with RFC 1583, the OSPF routing table maintains the multiple intra-AS paths that are available, which the router uses to calculate AS external routes as defined in RFC 2328. Being able to use multiple available paths to calculate an AS external route can prevent routing loops.

Example: Disabling OSPFv2 Compatibility with RFC 1583

This example shows how to disable OSPFv2 compatibility with RFC 1583 on the routing device.

- Requirements on page 118
- Overview on page 118
- Configuration on page 118
- Verification on page 119

Requirements

No special configuration beyond device initialization is required before disabling OSPFv2 compatibility with RFC 1583.

Overview

The introduction of RFC 2328 changed the method used to calculate the routes in an OSPF network. By default, the Junos OS implementation of OSPFv2 is compatible with RFC 1583, so OSPF uses the minimum cost to determine the route to any of the networks within the specified range. When you disable RFC 1583 compatibility, OSPF uses the maximum cost to determine the route to any of the networks within the specified range. To minimize the potential for routing loops, configure the same RFC compatibility on all OSPF devices in an OSPF domain.

Configuration

CLI Quick Configuration

To quickly disable OSPFv2 compatibility with RFC 1583, copy the following command and paste it into the CLI. You configure this setting on all devices that are part of the OSPF domain.

```
[edit]
set protocols ospf no-rfc-1583
```

Step-by-Step Procedure

To disable OSPFv2 compatibility with RFC 1583:

1. Disable RFC 1583.

   ```
   [edit]
   user@host# set protocols ospf no-rfc-1583
   ```


2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

NOTE: Repeat this configuration on each routing device that participates in an OSPF routing domain.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

user@host# **show protocols ospf**
no-rfc-1583;

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Routes

Purpose Verify that the OSPF routing table maintains the intra-AS paths with the largest metric, which the router uses to calculate AS external routes.

Action From operational mode, enter the **show ospf route detail** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

CHAPTER 6

OSPF Interface Configuration

Examples: Configuring OSPF Interfaces

About OSPF Interfaces

To activate OSPF on a network, you must enable the OSPF protocol on one or more interfaces on each device within the network on which traffic is to travel. How you configure the interface depends on whether the interface is connected to a broadcast or point-to-point network, a point-to-multipoint network, a nonbroadcast multiaccess (NBMA) network, or across a demand circuit.

- A broadcast interface behaves as if the routing device is connected to a LAN.
- A point-to-point interface provides a connection between a single source and a single destination (there is only one OSPF adjacency).
- A point-to-multipoint interface provides a connection between a single source and multiple destinations.
- An NBMA interface behaves in a similar fashion to a point-to-multipoint interface, but you might configure an NBMA interface to interoperate with other equipment.
- A demand circuit is a connection on which you can limit traffic based on user agreements. The demand circuit can limit bandwidth or access time based on agreements between the provider and user.

You can also configure an OSPF interface to be passive, to operate in passive traffic engineering mode, or to be a peer interface.

- A passive interface advertises its address, but does not run the OSPF protocol (adjacencies are not formed and hello packets are not generated).
- An interface operating in OSPF passive traffic engineering mode floods link address information within the autonomous system (AS) and makes it available for traffic engineering calculations.
- A peer interface can be configured for OSPFv2 routing devices. A peer interface is required for Generalized MPLS (GMPLS) to transport traffic engineering information through a link separate from the control channel. You establish this separate link by configuring a peer interface. The peer interface name must match the Link Management Protocol (LMP) peer name. A peer interface is optional for a hierarchy of RSVP label-switched paths (LSPs). After you configure the forwarding adjacency, you can configure OSPFv2 to advertise the traffic engineering properties of a forwarding adjacency to a specific peer.

Point-to-point interfaces differ from multipoint in that only one OSPF adjacency is possible. (A LAN, for instance, can have multiple addresses and can run OSPF on each subnet simultaneously.) As such, when you configure a numbered point-to-point interface to OSPF by name, multiple OSPF interfaces are created. One, which is unnumbered, is the interface on which the protocol is run. An additional OSPF interface is created for each address configured on the interface, if any, which is automatically marked as passive.

For OSPFv3, one OSPF-specific interface must be created per interface name configured under OSPFv3. OSPFv3 does not allow interfaces to be configured by IP address.

Enabling OSPF on an interface (by including the **interface** statement), disabling it (by including the **disable** statement), and not actually having OSPF run on an interface (by including the **passive** statement) are mutually exclusive states.

NOTE: When you configure OSPFv2 on an interface, you must also include the **family inet** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level. When you configure OSPFv3 on an interface, you must also include the **family inet6** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level. In Junos OS Release 9.2 and later, you can configure OSPFv3 to support address families other than unicast IPv6.

Example: Configuring an Interface on a Broadcast or Point-to-Point Network

This example shows how to configure an OSPF interface on a broadcast or point-to-point network.

- Requirements on page 123
- Overview on page 123

- Configuration on page 123
- Verification on page 124

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

If the interface on which you are configuring OSPF supports broadcast mode (such as a LAN), or if the interface supports point-to-point mode (such as a PPP interface or a point-to-point logical interface on Frame Relay), you specify the interface by including the IP address or the interface name for OSPFv2, or only the interface name for OSPFv3. In Junos OS Release 9.3 and later, an OSPF point-to-point interface can be an Ethernet interface without a subnet. If you configure an interface on a broadcast network, designated router and backup designated router election is performed.

NOTE: **Using both the interface name and the IP address of the same interface produces an invalid configuration.**

In this example, you configure interface **ge-0/2/0** as an OSPFv2 interface in OSPF area 0.0.0.1.

Configuration

CLI Quick Configuration

To quickly configure an OSPF interface on a broadcast or point-to-point network, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces ge-0/2/0 unit 0 family inet address 10.0.0.1
set protocols ospf area 0.0.0.1 interface ge-0/2/0
```

Step-by-Step Procedure

To configure an OSPF interface on a broadcast or point-to-point network:

1. Configure the interface.

   NOTE: For an OSPFv3 interface, specify an IPv6 address.

   ```
   [edit]
   user@host# set interfaces ge-0/2/0 unit 0 family inet address 10.0.0.1
   ```

2. Create an OSPF area.

   NOTE: For an OSPFv3 interface, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.1
   ```

3. Assign the interface to the area.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# set interface ge-0/2/0
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
ge-0/2/0 {
   unit 0 {
      family inet {
         address 10.0.0.1/32;
      }
   }
}
```

```
user@host# show protocols ospf
area 0.0.0.1 {
   interface ge-0/2/0.0;
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces** and the **show protocols ospf3** commands.

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Interface

Purpose Verify the interface configuration. Depending on your deployment, the Type field might display LAN or P2P.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network

This example shows how to configure an OSPFv2 interface on a nonbroadcast multiaccess (NBMA) network.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

When you configure OSPFv2 on an NBMA network, you can use nonbroadcast mode rather than point-to-multipoint mode. Using this mode offers no advantages over point-to-multipoint mode, but it has more disadvantages than point-to-multipoint mode. Nevertheless, you might occasionally find it necessary to configure nonbroadcast mode to interoperate with other equipment. Because there is no autodiscovery mechanism, you must configure each neighbor.

Nonbroadcast mode treats the NBMA network as a partially connected LAN, electing designated and backup designated routers. All routing devices must have a direct connection to both the designated and backup designated routers, or unpredictable results occur.

When you configure the interface, specify either the IP address or the interface name. Using both the IP address and the interface name produces an invalid configuration. For nonbroadcast interfaces, specify the IP address of the nonbroadcast interface as the interface name.

In this example, you configure the Asynchronous Transfer Mode (ATM) interface **at-0/1/0** as an OSPFv2 interface in OSPF area 0.0.0.1, and you and specify the following settings:

- **interface-type nbma**—Sets the interface to run in NBMA mode. You must explicitly configure the interface to run in NBMA mode.
- **neighbor *address* <eligible>**—Specifies the IP address of the neighboring device. OSPF routing devices normally discover their neighbors dynamically by listening to the broadcast or multicast hello packets on the network. Because an NBMA network does not support broadcast (or multicast), the device cannot discover its neighbors

dynamically, so you must configure all the neighbors statically. To configure multiple neighbors, include multiple **neighbor** statements. If you want the neighbor to be a designated router, include the **eligible** keyword.

- **poll-interval**—Specifies the length of time, in seconds, before the routing device sends hello packets out of the interface before it establishes adjacency with a neighbor. Routing devices send hello packets for a longer interval on nonbroadcast networks to minimize the bandwidth required on slow WAN links. The range is from 1 through 255 seconds. By default, the device sends hello packets out the interface every 120 seconds before it establishes adjacency with a neighbor.

  Once the routing device detects an active neighbor, the hello packet interval changes from the time specified in the **poll-interval** statement to the time specified in the **hello-interval** statement.

Configuration

CLI Quick Configuration

To quickly configure an OSPFv2 interface on an NBMA network, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces at-0/1/0 unit 0 family inet address 192.0.2.1
set protocols ospf area 0.0.0.1 interface at-0/1/0.0 interface-type nbma
set protocols ospf area 0.0.0.1 interface at-0/1/0.0 neighbor 192.0.2.2 eligible
set protocols ospf area 0.0.0.1 interface at-0/1/0.0 poll-interval 130
```

Step-by-Step Procedure

To configure an OSPFv2 interface on an NBMA network:

1. Configure the interface.

   ```
   [edit]
   user@host# set interfaces at-0/1/0 unit 0 family inet address 192.0.2.1
   ```

2. Create an OSPF area.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.1
   ```

3. Assign the interface to the area.
   In this example, include the **eligible** keyword to allow the neighbor to be a designated router.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# set interface at-0/1/0 interface-type nbma neighbor 192.0.2.2 eligible
   ```

4. Configure the poll interval.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# set interface at-0/1/0 poll-interval 130
   ```

5. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# commit
   ```


Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
at-0/1/0 {
   unit 0 {
      family inet {
         address 192.0.2.1/32;
      }
   }
}
```

```
user@host# show protocols ospf
area 0.0.0.1 {
   interface at-0/1/0.0 {
      interface-type nbma;
      neighbor 192.0.2.2 eligible;
      poll-interval 130;
   }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Interface

Purpose Verify the interface configuration. Confirm that the Type field displays NBMA.

Action From operational mode, enter the **show ospf interface detail** command.

Example: Configuring an OSPFv2 Interface on a Point-to-Multipoint Network

This example shows how to configure an OSPFv2 interface on a point-to-multipoint network.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26

- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

When you configure OSPFv2 on a nonbroadcast multiaccess (NBMA) network, such as a multipoint Asynchronous Transfer Mode (ATM) or Frame Relay, OSPFv2 operates by default in point-to-multipoint mode. In this mode, OSPFv2 treats the network as a set of point-to-point links. Because there is no autodiscovery mechanism, you must configure each neighbor.

When you configure the interface, specify either the IP address or the interface name. Using both the IP address and the interface name produces an invalid configuration.

In this example, you configure ATM interface **at-0/1/0** as an OSPFv2 interface in OSPF area 0.0.0.1, and you and specify 192.0.2.1 as the neighbor's IP address.

Configuration

CLI Quick Configuration

To quickly configure an OSPFv2 interface on a point-to-multipoint network, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces at-0/1/0 unit 0 family inet address 192.0.2.2
set protocols ospf area 0.0.0.1 interface at-0/1/0 neighbor 192.0.2.1
```

Step-by-Step Procedure

To configure an OSPFv2 interface on a point-to-multipoint network:

1. Configure the interface.

```
[edit]
user@host# set interfaces at-0/1/0 unit 0 family inet address 192.0.2.2
```

2. Create an OSPF area.

```
[edit]
user@host# edit protocols ospf area 0.0.0.1
```

3. Assign the interface to the area and specify the neighbor.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface at-0/1/0 neighbor 192.0.2.1
```

   To configure multiple neighbors, include a **neighbor** statement for each neighbor.

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.1]
user@host# commit
```

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
```

```
at-0/1/0 {
   unit 0 {
      family inet {
         address 192.0.2.2/32;
      }
   }
}
user@host# show protocols ospf
area 0.0.0.1 {
   interface at-0/1/0.0 {
      neighbor 192.0.2.1;
   }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Interface

Purpose Verify the interface configuration. Confirm that the Type field displays P2MP.

Action From operational mode, enter the **show ospf interface detail** command.

Example: Configuring OSPF Demand Circuits

This example shows how to configure an OSPF demand circuit interface.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.

> NOTE: If you are using OSPF demand circuits over an ISDN link, you must configure an ISDN interface and enable dial-on-demand routing. See the *Junos OS Network Interfaces Library for Routing Devices*.

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.

- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

OSPF sends periodic hello packets to establish and maintain neighbor adjacencies and uses link-state advertisements (LSAs) to make routing calculations and decisions. OSPF support for demand circuits is defined in RFC 1793, *Extending OSPF to Support Demand Circuits*, and suppresses the periodic hello packets and LSAs. A demand circuit is a connection on which you can limit traffic based on user agreements. The demand circuit can limit bandwidth or access time based on agreements between the provider and user.

You configure demand circuits on an OSPF interface. When the interface becomes a demand circuit, all hello packets and LSAs are suppressed as soon as OSPF synchronization is achieved. LSAs have a DoNotAge bit that stops the LSA from aging and prevents periodic updates from being sent. Hello packets and LSAs are sent and received on a demand-circuit interface only when there is a change in the network topology. This reduces the amount of traffic through the OSPF interface.

Consider the following when configuring OSPF demand circuits:

- Periodic hellos are only suppressed on point-to-point and point-to-multipoint interfaces. If you configure demand circuits on an OSPF broadcast network or on an OSPF nonbroadcast multiaccess (NBMA) network, periodic hello packets are still sent.
- Demand circuit support on an OSPF point-to-multipoint interface resembles that for point-to-point interfaces. If you configure a point-to-multipoint interface as a demand circuit, the device negotiates hello suppression separately on each interface that is part of the point-to-multipoint network.

This example assumes that you have a point-to-point connection between two devices using SONET/SDH interfaces. A demand-circuit interface automatically negotiates the demand-circuit connection with its OSPF neighbor. If the neighbor does not support demand circuits, then no demand circuit connection is established.

In this example, you configure OSPF interface **so-0/1/0** in OSPF area 0.0.0.1 as a demand circuit.

Configuration

CLI Quick Configuration

To quickly configure an OSPF demand circuit interface, copy the following command and paste it into the CLI. You must configure both neighboring interfaces for OSPF demand circuits for the connection to be established.

```
[edit]
set protocols ospf area 0.0.0.1 interface so-0/1/0 demand-circuit
```

Step-by-Step Procedure

To configure an OSPF demand circuit interface on one neighboring interface:

1. Create an OSPF area.

NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit ]
user@host# edit protocols ospf area 0.0.0.1
```

2. Configure the neighboring interface as a demand circuit.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface so-0/1/0 demand-circuit
```

3. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.1]
user@host# commit
```

NOTE: Repeat this entire configuration on the other neighboring interface.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols
ospf {
  area 0.0.0.1 {
    interface so-0/1/0.0 {
      demand-circuit;
    }
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Status of Neighboring Interfaces

Purpose Verify information about the neighboring interface. When the neighbor is configured for demand circuits, a DC flag displays.

Action From operational mode, enter the **show ospf neighbor detail** command for OSPFv2, and enter the **show ospf3 neighbor detail** command for OSPFv3.

Example: Configuring a Passive OSPF Interface

This example shows how to configure a passive OSPF interface. A passive OSPF interface advertises its address but does not run the OSPF protocol.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

By default, OSPF must be configured on an interface for direct interface addresses to be advertised as interior routes. To advertise the direct interface addresses without actually running OSPF on that interface (adjacencies are not formed and hello packets are not generated), you configure that interface as a passive interface.

Enabling OSPF on an interface (by including the **interface** statement), disabling it (by including the **disable** statement), and not actually having OSPF run on an interface (by including the **passive** statement) are mutually exclusive states.

NOTE: If you do not want to see notifications for state changes in a passive OSPF interface, you can disable the OSPF traps for the interface by including the no-interface-state-traps statement. The no-interface-state-traps statement is supported only for OSPFv2.

In this example, you configure interface **ge-0/2/0** as a passive OSPF interface in area 0.0.0.1 by including the **passive** statement.

Configuration

CLI Quick Configuration

To quickly configure a passive OSPF interface, copy the following command and paste it into the CLI.

```
[edit]
```



```
set protocols ospf area 0.0.0.1 interface ge-0/2/0 passive
```

Step-by-Step Procedure

To configure a passive OSPF interface:

1. Create an OSPF area.

   NOTE: For an OSPFv3 interface, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.1
   ```

2. Configure the passive interface.

   ```
   [edit protocols ospf area 0.0.0.1 ]
   user@host# set interface ge-0/2/0 passive
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.1]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
  area 0.0.0.1 {
  interface ge-0/2/0.0 {
    passive;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Status of OSPF Interfaces

Purpose Verify the status of the OSPF interface. If the interface is passive, the Adj count field is 0 because no adjacencies have been formed. Next to this field, you might also see the word Passive.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Example: Configuring OSPFv2 Peer interfaces

This example shows how to configure an OSPFv2 peer interface.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.
- Configure Generalized MPLS per your network requirements. See *LMP Configuration Overview* in the *Junos OS MPLS Applications Library for Routing Devices*.

Overview

You can configure an OSPFv2 peer interface for many reasons, including when you configure Generalized MPLS (GMPLS). This example configures a peer interface for GMPLS. GMPLS requires traffic engineering information to be transported through a link separate from the control channel. You establish this separate link by configuring a peer interface. The OSPFv2 peer interface name must match the Link Management Protocol (LMP) peer name. You configure GMPLS and the LMP settings separately from OSPF.

This example assumes that GMPLS and the LMP peer named **oxc1** are already configured, and you need to configure the OSPFv2 peer interface in area 0.0.0.0.

Configuration

CLI Quick Configuration

To quickly configure an OSPFv2 peer interface, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 peer-interface oxc1
```

Step-by-Step Procedure

To configure a peer OSPFv2 interface used by the LMP:

1. Create an OSPF area.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
```


2. Configure the peer interface.

   [edit protocols ospf area 0.0.0.0]
   user@host# **set peer-interface oxc1**

3. If you are done configuring the device, commit the configuration.

   [edit protocols ospf area 0.0.0.0]
   user@host# **commit**

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
  area 0.0.0.0 {
  peer-interface oxc1;
}
```

Verification

Confirm that the configuration is working properly.

Verifying the Configured OSPFv2 Peer

Purpose Verify the status of the OSPFv2 peer. When an OSPFv2 peer is configured for GMPLS, the Peer Name field displays the name of the LMP peer that you created for GMPLS, which is also the configured OSPFv2 peer.

Action From operational mode, enter the **show link-management** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Example: Configuring Multiple Address Families for OSPFv3

Understanding Multiple Address Families for OSPFv3

By default, OSPFv3 supports only unicast IPv6 routes. In Junos OS Release 9.2 and later, you can configure OSPFv3 to support multiple address families, including IPv4 unicast, IPv4 multicast, and IPv6 multicast. This mutliple address family support allows OSPFv3 to support both IPv6 and IPv4 nodes. Junos OS maps each address family to a separate realm as defined in Internet draft draft-ietf-ospf-af-alt-06.txt, *Support for Address Families in OSPFv3*. Each realm maintains a separate set of neighbors and link-state database.

When you configure multiple address families for OSPFv3, there is a new instance ID field that allows multiple OSPFv3 protocol instances per link. This allows a single link to belong to multiple areas.

You configure each realm independently. We recommend that you configure an area and at least one interface for each realm.

These are the default import and export routing tables for each of the four address families:

- IPv6 unicast: **inet6.0**
- IPv6 multicast: **inet6.2**
- IPv4 unicast: **inet.0**
- IPv4 multicast: **inet.2**

With the exception of virtual links, all configurations supported for the default IPv6 unicast family are supported for the address families that have to be configured as realms.

Example: Configuring Multiple Address Families for OSPFv3

This example shows how to configure multiple address families for OSPFv3.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

By default, OSPFv3 supports unicast IPv6 routes, but you can configure OSPFv3 to support multiple address families. To support an address family other than unicast IPv6, you configure a realm that allows OSPFv3 to advertise IPv4 unicast, IPv4 multicast, or IPv6 multicast routes. Junos OS then maps each address family that you configure to a separate realm with its own set of neighbors and link-state database.

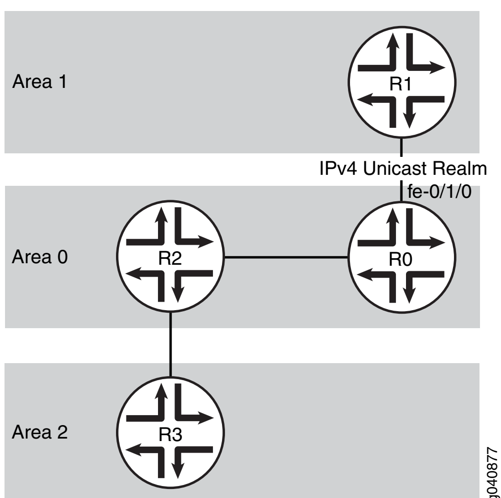
NOTE: By default, LDP synchronization is only supported for OSPFv2. If you configure an IPv4 unicast or IPv4 multicast realm, you can also configure LDP synchronization. Since LDP synchronization is only supported for IPv4, this support is only available for OSPFv3 if you configure an IPv4 realm.

When configuring OSPFv3 to support multiple address families, consider the following:

- You configure each realm independently. We recommend that you configure an area and at least one interface for each realm.
- OSPFv3 uses IPv6 link-local addresses as the source of hello packets and next hop calculations. As such, you must enable IPv6 on the link regardless of the additional realm you configure.

Figure 15 on page 137 shows a connection between Routers R0 and R1. In this example, you configure interface **fe-0/1/0** on Router R0 in area 0 to advertise IPv4 unicast routes, in addition to the default unicast IPv6 routes in area 1, by including the **realm ipv4-unicast** statement. Depending on your network requirements, you can also advertise IPv4 multicast routes by including the **realm-ipv4-multicast** statement, and you can advertise IPv6 multicast routes by including the **realm-ipv6-multicast** statement.

Figure 15: IPv4 Unicast Realm



Configuration

CLI Quick Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To quickly configure multiple address families for OSPFv3, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces fe-0/1/0 unit 0 family inet address 11.1.2.1/24
set interfaces fe-0/1/0 unit 0 family inet6
```

```
set protocols ospf3 area 0.0.0.0 interface fe-0/1/0
set protocols ospf3 realm ipv4-unicast area 0.0.0.0 interface fe-0/1/0
```

Step-by-Step Procedure

To configure multiple address families for OSPFv3:

1. Configure the device interface participating in OSPFv3.

   ```
   [edit]
   user@host# set interfaces fe-0/1/0 unit 0 family inet address 11.1.2.1/24
   user@host# set interfaces fe-0/1/0 unit 0 family inet6
   ```

2. Enter OSPFv3 configuration mode.

   ```
   [edit ]
   user@host# edit protocols ospf3
   ```

3. Add the interface you configured to the OSPFv3 area.

   ```
   [edit protocols ospf3 ]
   user@host# set area 0.0.0.0 interface fe-0/1/0
   ```

4. Configure an IPv4 unicast realm. This allows OSPFv3 to support both IPv4 unicast and IPv6 unicast routes.

   ```
   [edit protocols ospf3 ]
   user@host# set realm ipv4-unicast area 0.0.0.0 interface fe-0/1/0
   ```

5. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf3 ]
   user@host# commit
   ```

NOTE: Repeat this entire configuration on the neighboring device that is part of the realm.

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
  fe-0/1/0 {
  unit 0 {
    family inet {
      address 11.1.2.1/24;
    }
    family inet6;
  }
}

user@host# show protocols ospf3
realm ipv4-unicast {
  area 0.0.0.0 {
    interface fe-0/1/0.0;
  }
```



```
}
  area 0.0.0.0 {
    interface fe-0/1/0.0;
  }
```

Verification

Confirm that the configuration is working properly.

- Verifying the Link-State Database on page 139
- Verifying the Status of OSPFv3 Interfaces with Multiple Address Families on page 139

Verifying the Link-State Database

Purpose Verify the status of the link-state database for the configured realm, or address family.

Action From operational mode, enter the **show ospf3 database realm ipv4-unicast** command.

Verifying the Status of OSPFv3 Interfaces with Multiple Address Families

Purpose Verify the status of the interface for the specified OSPFv3 realm, or address family.

Action From operational mode, enter the **show ospf3 interface realm ipv4-unicast** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

CHAPTER 7

OSPF Route Control Configuration

Examples: Configuring OSPF Route Summarization

Understanding OSPF Route Summarization

Area border routers (ABRs) send summary link advertisements to describe the routes to other areas. Depending on the number of destinations, an area can get flooded with a large number of link-state records, which can utilize routing device resources. To minimize the number of advertisements that are flooded into an area, you can configure the ABR to coalesce, or summarize, a range of IP addresses and send reachability information about these addresses in a single link-state advertisement (LSA). You can summarize one or more ranges of IP addresses, where all routes that match the specified area range are filtered at the area boundary, and the summary is advertised in their place.

For an OSPF area, you can summarize and filter intra-area prefixes. All routes that match the specified area range are filtered at the area boundary, and the summary is advertised in their place. For an OSPF not-so-stubby area (NSSA), you can only coalesce or filter NSSA external (Type 7) LSAs before they are translated into AS external (Type 5) LSAs and enter the backbone area. All external routes learned within the area that do not fall into the range of one of the prefixes are advertised individually to other areas.

In addition, you can also limit the number of prefixes (routes) that are exported into OSPF. By setting a user-defined maximum number of prefixes, you prevent the routing device from flooding an excessive number of routes into an area.

Example: Summarizing Ranges of Routes in OSPF Link-State Advertisements

This example shows how to summarize routes sent into the backbone area.

Requirements

Before you begin:

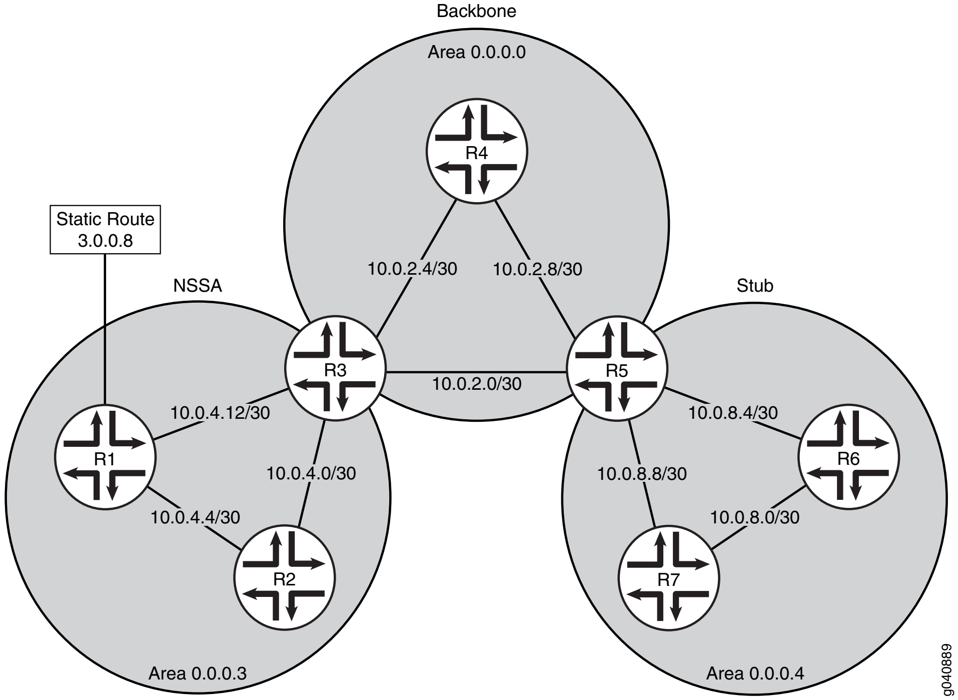
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a static route. See *Examples: Configuring Static Routes* in the *Junos OS Routing Protocols Library for Routing Devices*.

Overview

You can summarize a range of IP addresses to minimize the size of the backbone router's link-state database. All routes that match the specified area range are filtered at the area boundary, and the summary is advertised in their place.

Figure 16 on page 143 shows the topology used in this example. R5 is the ABR between area 0.0.0.4 and the backbone. The networks in area 0.0.0.4 are 10.0.8.4/30, 10.0.8.0/30, and 10.0.8.8/30, which can be summarized as 10.0.8.0/28. R3 is the ABR between NSSA area 0.0.0.3 and the backbone. The networks in area 0.0.0.3 are 10.0.4.4/30, 10.0.4.0/30, and 10.0.4.12/30, which can be summarized as 10.0.4.0/28. Area 0.0.0.3 also contains external static route 3.0.0.8 that you will prevent from flooding throughout the network.

Figure 16: Summarizing Ranges of Routes in OSPF



In this example, you configure the ABRs for route summarization by including the following settings:

- **area-range**—For an area, summarizes a range of IP addresses when sending summary intra-area link advertisements. For an NSSA, summarizes a range of IP addresses when sending NSSA link-state advertisements (Type 7 LSAs). The specified prefixes are used to aggregate external routes learned within the area when the routes are advertised to other areas.
- **network/mask-length**—Indicates the summarized IP address range and the number of significant bits in the network mask.
- **restrict**—On the NSSA ABR, prevents the configured summary from being advertised. In this example, we do not want to flood the external route outside of area 0.0.0.3.

Configuration

CLI Quick Configuration

- To quickly configure route summarization for an OSPF area, copy the following commands and paste them into the CLI. The following is the configuration on ABR R5:

```
[edit]
set interfaces fe-0/0/1 unit 0 family inet address 10.0.8.3
set interfaces fe-0/0/2 unit 0 family inet address 10.0.8.4
set interfaces fe-0/0/0 unit 0 family inet address 10.0.2.3
set interfaces fe-0/0/4 unit 0 family inet address 10.0.2.5
set protocols ospf area 0.0.0.4 stub
set protocols ospf area 0.0.0.4 interface fe-0/0/1
set protocols ospf area 0.0.0.4 interface fe-0/0/2
set protocols ospf area 0.0.0.0 interface fe-0/0/0
```



```
set protocols ospf area 0.0.0.0 interface fe-0/0/4
set protocols ospf area 0.0.0.4 area-range 10.0.8.0/28
```

- To quickly configure route summarization for an OSPF NSSA, copy the following commands and paste them into the CLI. The following is the configuration on ABR R3:

```
[edit]
set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.10
set interfaces fe-0/0/2 unit 0 family inet address 10.0.4.1
set interfaces fe-0/0/0 unit 0 family inet address 10.0.2.1
set interfaces fe-0/0/4 unit 0 family inet address 10.0.2.7
set protocols ospf area 0.0.0.3 interface fe-0/0/1
set protocols ospf area 0.0.0.3 interface fe-0/0/2
set protocols ospf area 0.0.0.0 interface fe-0/0/0
set protocols ospf area 0.0.0.0 interface fe-0/0/4
set protocols ospf area 0.0.0.3 area-range 10.0.4.0/28
set protocols ospf area 0.0.0.3 nssa
set protocols ospf area 0.0.0.3 nssa area-range 3.0.0.0/8 restrict
```

Step-by-Step Procedure

To summarize routes sent to the backbone area:

1. Configure the interfaces.

   NOTE: For OSPFv3, include IPv6 addresses.

```
[edit]
user@R5# set interfaces fe-0/0/1 unit 0 family inet address 10.0.8.3
user@R5# set interfaces fe-0/0/2 unit 0 family inet address 10.0.8.4
user@R5# set interfaces fe-0/0/0 unit 0 family inet address 10.0.2.3
user@R5# set interfaces fe-0/0/4 unit 0 family inet address 10.0.2.5
```

```
[edit]
user@R3# set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.10
user@R3# set interfaces fe-0/0/2 unit 0 family inet address 10.0.4.1
user@R3# set interfaces fe-0/0/0 unit 0 family inet address 10.0.2.1
user@R3# set interfaces fe-0/0/4 unit 0 family inet address 10.0.2.7
```

2. Configure the type of OSPF area.

   NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@R5# set protocols ospf area 0.0.0.4 stub
```

```
[edit]
user@R3# set protocols ospf area 0.0.0.3 nssa
```

3. Assign the interfaces to the OSPF areas.

```
user@R5# set protocols ospf area 0.0.0.4 interface fe-0/0/1
user@R5# set protocols ospf area 0.0.0.4 interface fe-0/0/2
```

user@R5# **set protocols ospf area 0.0.0.0 interface fe-0/0/0**
user@R5# **set protocols ospf area 0.0.0.0 interface fe-0/0/4**

user@R3# **set protocols ospf area 0.0.0.3 interface fe-0/0/1**
user@R3# **set protocols ospf area 0.0.0.3 interface fe-0/0/2**
user@R3# **set protocols ospf area 0.0.0.0 interface fe-0/0/0**
user@R3# **set protocols ospf area 0.0.0.0 interface fe-0/0/4**

4. Summarize the routes that are flooded into the backbone.

   [edit]
   user@R5# **set protocols ospf area 0.0.0.4 area-range 10.0.8.0/28**

   [edit]
   user@R3# **set protocols ospf area 0.0.0.3 area-range 10.0.4.0/28**

5. On ABR R3, restrict the external static route from leaving area 0.0.0.3.

   [edit]
   user@R3# **set protocols ospf area 0.0.0.3 nssa area-range 3.0.0.0/8 restrict**

6. If you are done configuring the devices, commit the configuration.

   [edit]
   user@host# **commit**

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on ABR R5:

```
user@R5# show interfaces
fe-0/0/0 {
  unit 0 {
    family inet {
      address 10.0.2.3/32;
    }
  }
}
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.8.3/32;
    }
  }
}
fe-0/0/2 {
  unit 0 {
    family inet {
      address 10.0.8.4/32;
    }
  }
}
fe-0/0/4 {
  unit 0 {
```

```
      family inet {
        address 10.0.2.5/32;
      }
    }
  }
  user@R5# show protocols ospf
  area 0.0.0.0 {
    interface fe-0/0/0.0;
    interface fe-0/0/4.0;
  }
    area 0.0.0.4 {
      stub;
      area-range 10.0.8.0/28;
      interface fe-0/0/1.0;
      interface fe-0/0/2.0;
    }
```

Configuration on ABR R3:

```
user@R3# show interfaces
fe-0/0/0 {
  unit 0 {
    family inet {
      address 10.0.2.1/32;
    }
  }
}
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.4.10/32;
    }
  }
}
fe-0/0/2 {
  unit 0 {
    family inet {
      address 10.0.4.1/32;
    }
  }
}
fe-0/0/4 {
  unit 0 {
    family inet {
      address 10.0.2.7/32;
    }
  }
}
user@R3t# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/0.0;
  interface fe-0/0/4.0;
}
area 0.0.0.3 {
  nssa {
```



```
        area-range 3.0.0.0/8 restrict;
    }
    area-range 10.0.4.0/28;
    interface fe-0/0/1.0;
    interface fe-0/0/2.0;
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces** and **show protocols ospf3** commands.

Verification

Confirm that the configuration is working properly.

Verifying the Summarized Route

Purpose Verify that the routes you configured for route summarization are being aggregated by the ABRs before the routes enter the backbone area. Confirm route summarization by checking the entries of the OSPF link-state database for the routing devices in the backbone.

Action From operational mode, enter the **show ospf database** command for OSPFv2, and enter the **show ospf3 database** command for OSPFv3.

Example: Limiting the Number of Prefixes Exported to OSPF

This example shows how to limit the number of prefixes exported to OSPF.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

By default, there is no limit to the number of prefixes (routes) that can be exported into OSPF. By allowing any number of routes to be exported into OSPF, the routing device can become overwhelmed and potentially flood an excessive number of routes into an area.

You can limit the number of routes exported into OSPF to minimize the load on the routing device and prevent this potential problem. If the routing device exceeds the configured prefix export value, the routing device purges the external prefixes and enters into an overload state. This state ensures that the routing device is not overwhelmed as it attempts to process routing information. The prefix export limit number can be a value from 0 through 4,294,967,295.

In this example, you configure a prefix export limit of 100,000 by including the **prefix-export-limit** statement.

Configuration

CLI Quick Configuration

To quickly limit the number of prefixes exported to OSPF, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf prefix-export-limit 100000
```

Step-by-Step Procedure

To limit the number of prefixes exported to OSPF:

1. Configure the prefix export limit value.

   NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf prefix-export-limit 100000
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
prefix-export-limit 100000;
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Prefix Export Limit

Purpose Verify the prefix export counter that displays the number or routes exported into OSPF.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** command for OSPFv3.

Configuring OSPF Refresh and Flooding Reduction in Stable Topologies

The OSPF standard requires that every link-state advertisement (LSA) be refreshed every 30 minutes. The Juniper Networks implementation refreshes LSAs every 50 minutes. By default, any LSA that is not refreshed expires after 60 minutes. This requirement can result in traffic overhead that makes it difficult to scale OSPF networks. You can override the default behavior by specifying that the DoNotAge bit be set in self-originated LSAs when they are initially sent by the router or switch. Any LSA with the DoNotAge bit set is reflooded only when a change occurs in the LSA. This feature thus reduces protocol traffic overhead while permitting any changed LSAs to be flooded immediately. Routers or switches enabled for flood reduction continue to send hello packets to their neighbors and to age self-originated LSAs in their databases.

The Juniper implementation of OSPF refresh and flooding reduction is based on RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*. However, the Juniper implementation does not include the forced-flooding interval defined in the RFC. Not implementing the forced-flooding interval ensures that LSAs with the DoNotAge bit set are reflooded only when a change occurs.

This feature is supported for the following:

- OSPFv2 and OSPFv3 interfaces
- OSPFv3 realms
- OSPFv2 and OSPFv3 virtual links
- OSPFv2 sham links
- OSPFv2 peer interfaces
- All routing instances supported by OSPF
- Logical systems

To configure flooding reduction for an OSPF interface, include the **flood-reduction** statement at the **[edit protocols (ospf | ospf3) area *area-id* interface *interface-id*]** hierarchy level.

NOTE: If you configure flooding reduction for an interface configured as a demand circuit, the LSAs are not initially flooded, but sent only when their content has changed. Hello packets and LSAs are sent and received on a demand-circuit interface only when a change occurs in the network topology.

In the following example, the OSPF interface **so-0/0/1.0** is configured for flooding reduction. As a result, all the LSAs generated by the routes that traverse the specified interface have the DoNotAge bit set when they are initially flooded, and LSAs are refreshed only when a change occurs.

```
[edit]
protocols ospf {
  area 0.0.0.0 {
    interface so-0/0/1.0 {
      flood-reduction;
    }
    interface lo0.0;
    interface so-0/0/0.0;
  }
}
```

NOTE: Beginning with Junos OS Release 12.2, you can configure a global default link-state advertisement (LSA) flooding interval in OSPF for self-generated LSAs by including the lsa-refresh-interval *minutes* statement at the **[edit protocols (ospf | ospf3)]** hierarchy level. The Juniper Networks implementation refreshes LSAs every 50 minutes. The range is 25 through 50 minutes. By default, any LSA that is not refreshed expires after 60 minutes.

If you have both the global LSA refresh interval configured for OSPF and OSPF flooding reduction configured for a specific interface in an OSPF area, the OSPF flood reduction configuration takes precedence for that specific interface.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Examples: Configuring OSPF Traffic Control

Understanding OSPF Traffic Control

Once a topology is shared across the network, OSPF uses the topology to route packets between network nodes. Each path between neighbors is assigned a cost based on the throughput, round-trip time, and reliability of the link. The sum of the costs across a particular path between hosts determines the overall cost of the path. Packets are then routed along the shortest path using the shortest-path-first (SPF) algorithm. Routes with lower total path metrics are preferred over those with higher path metrics.

You can use the following methods to control OSPF traffic:

- Control the cost of individual OSPF network segments
- Dynamically adjust OSPF interface metrics based on bandwidth
- Control OSPF route selection

Controlling the Cost of Individual OSPF Network Segments

OSPF uses the following formula to determine the cost of a route:

cost = reference-bandwidth / interface bandwidth

You can modify the reference-bandwidth value, which is used to calculate the default interface cost. The interface bandwidth value is not user-configurable and refers to the actual bandwidth of the physical interface.

By default, OSPF assigns a default cost metric of 1 to any link faster than 100 Mbps, and a default cost metric of 0 to the loopback interface (**lo0**). No bandwidth is associated with the loopback interface.

To control the flow of packets across the network, OSPF allows you to manually assign a cost (or metric) to a particular path segment. When you specify a metric for a specific OSPF interface, that value is used to determine the cost of routes advertised from that interface. For example, if all routers in the OSPF network use default metric values, and you increase the metric on one interface to 5, all paths through that interface have a calculated metric higher than the default and are not preferred.

NOTE: Any value you configure for the metric overrides the default behavior of using the reference-bandwidth value to calculate the route cost for that interface.

When there are multiple equal-cost routes to the same destination in a routing table, an equal-cost multipath (ECMP) set is formed. If there is an ECMP set for the active route, the Junos OS software uses a hash algorithm to choose one of the next-hop addresses in the ECMP set to install in the forwarding table.

You can configure Junos OS so that multiple next-hop entries in an ECMP set are installed in the forwarding table. Define a load-balancing routing policy by including one or more **policy-statement** configuration statements at the [**edit policy-options**] hierarchy level, with the action **load-balance per-packet**. Then apply the routing policy to routes exported from the routing table to the forwarding table.

Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth

You can specify a set of bandwidth threshold values and associated metric values for an OSPF interface or for a topology on an OSPF interface. When the bandwidth of an interface changes, the Junos OS automatically sets the interface metric to the value associated with the appropriate bandwidth threshold value. Junos OS uses the smallest configured bandwidth threshold value that is equal to or greater than the actual interface bandwidth to determine the metric value. If the interface bandwidth is greater than any of the configured bandwidth threshold values, the metric value configured for the interface is used instead of any of the bandwidth-based metric values configured. The ability to recalculate the metric for an interface when its bandwidth changes is especially useful for aggregate interfaces.

NOTE: You must also configure a metric for the interface when you enable bandwidth-based metrics.

Controlling OSPF Route Preferences

You can control the flow of packets through the network using route preferences. Route preferences are used to select which route is installed in the forwarding table when several protocols calculate routes to the same destination. The route with the lowest preference value is selected.

By default, internal OSPF routes have a preference value of 10, and external OSPF routes have a preference value of 150. Although the default settings are appropriate for most environments, you might want to modify the default settings if all of the routing devices in your OSPF network use the default preference values, or if you are planning to migrate from OSPF to a different interior gateway protocol (IGP). If all of the devices use the default route preference values, you can change the route preferences to ensure that the path through a particular device is selected for the forwarding table any time multiple equal-cost paths to a destination exist. When migrating from OSPF to a different IGP, modifying the route preferences allows you to perform the migration in a controlled manner.

Example: Controlling the Cost of Individual OSPF Network Segments

This example shows how to control the cost of individual OSPF network segments.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.

Overview

All OSPF interfaces have a cost, which is a routing metric that is used in the link-state calculation. Routes with lower total path metrics are preferred to those with higher path metrics. In this example, we explore how to control the cost of OSPF network segments.

By default, OSPF assigns a default cost metric of 1 to any link faster than 100 Mbps, and a default cost metric of 0 to the loopback interface (**lo0**). No bandwidth is associated with the loopback interface. This means that all interfaces faster than 100 Mbps have the same default cost metric of 1. If multiple equal-cost paths exist between a source and destination address, OSPF routes packets along each path alternately, in round-robin fashion.

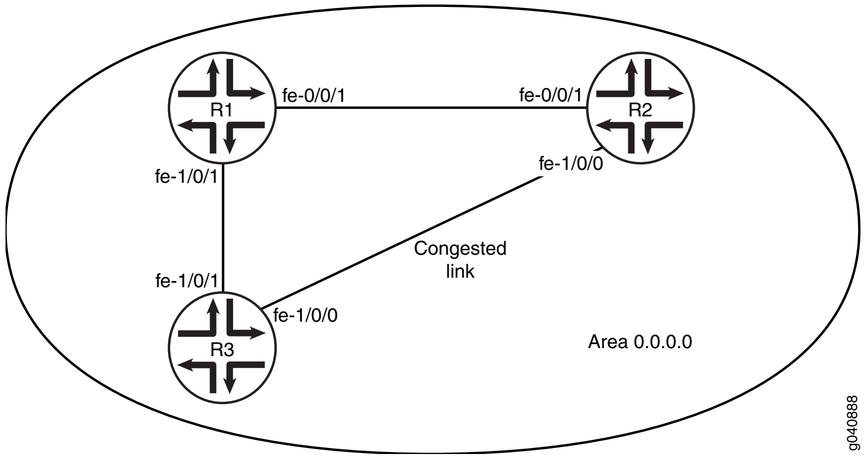
Having the same default metric might not be a problem if all of the interfaces are running at the same speed. If the interfaces operate at different speeds, you might notice that traffic is not routed over the fastest interface because OSPF equally routes packets across the different interfaces. For example, if your routing device has Fast Ethernet and Gigabit Ethernet interfaces running OSPF, each of these interfaces have a default cost metric of 1.

In the first example, you set the reference bandwidth to 10g (10 Gbps, as denoted by 10,000,000,000 bits) by including the **reference-bandwidth** statement. With this configuration, OSPF assigns the Fast Ethernet interface a default metric of 100, and the Gigabit Ethernet interface a metric of 10. Since the Gigabit Ethernet interface has the lowest metric, OSPF selects it when routing packets. The range is 9600 through 1,000,000,000,000 bits.

Figure 17 on page 154 shows three routing devices in area 0.0.0.0 and assumes that the link between Device R2 and Device R3 is congested with other traffic. You can also control the flow of packets across the network by manually assigning a metric to a particular path segment. Any value you configure for the metric overrides the default behavior of using the reference-bandwidth value to calculate the route cost for that interface. To prevent the traffic from Device R3 going directly to Device R2, you adjust the metric on the interface on Device R3 that connects with Device R1 so that all traffic goes through Device R1.

In the second example, you set the metric to 5 on interface **fe-1/0/1** on Device R3 that connects with Device R1 by including the **metric** statement. The range is 1 through 65,535.

Figure 17: OSPF Metric Configuration



Configuration

- Configuring the Reference Bandwidth on page 154
- Configuring a Metric for a Specific OSPF Interface on page 155

Configuring the Reference Bandwidth

CLI Quick Configuration

To quickly configure the reference bandwidth, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf reference-bandwidth 10g
```

Step-by-Step Procedure

To configure the reference bandwidth:

1. Configure the reference bandwidth to calculate the default interface cost.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf reference-bandwidth 10g
   ```

   TIP: As a shortcut in this example, you enter **10g** to specify 10 Gbps reference bandwidth. Whether you enter **10g** or **10000000000**, the output of **show protocols ospf** command displays 10 Gbps as **10g**, not **10000000000**.

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

NOTE: Repeat this entire configuration on all routing devices in a shared network.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
reference-bandwidth 10g;
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Configuring a Metric for a Specific OSPF Interface

CLI Quick Configuration

To quickly configure a metric for a specific OSPF interface, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-1/0/1 metric 5
```

Step-by-Step Procedure

To configure the metric for a specific OSPF interface:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Configure the metric of the OSPF network segment.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface fe-1/0/1 metric 5
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface fe-1/0/1.0 {
    metric 5;
  }
```

```
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the Configured Metric on page 156
- Verifying the Route on page 156

Verifying the Configured Metric

Purpose Verify the metric setting on the interface. Confirm that the Cost field displays the interface's configured metric (cost). When choosing paths to a destination, OSPF uses the path with the lowest cost.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Verifying the Route

Purpose When choosing paths to a destination, OSPF uses the path with the lowest total cost. Confirm that OSPF is using the appropriate path.

Action From operational mode, enter the **show route** command.

Example: Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth

This example shows how to dynamically adjust OSPF interface metrics based on bandwidth.

- Requirements on page 156
- Overview on page 157
- Configuration on page 157
- Verification on page 158

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.

Overview

You can specify a set of bandwidth threshold values and associated metric values for an OSPF interface. When the bandwidth of an interface changes, the Junos OS automatically sets the interface metric to the value associated with the appropriate bandwidth threshold value. When you configure bandwidth-based metric values, you typically configure multiple bandwidth and metric values.

In this example, you configure OSPF interface **ae0** for bandwidth-based metrics by including the **bandwidth-based-metrics** statement and the following settings:

- **bandwidth**—Specifies the bandwidth threshold in bits per second. The range is 9600 through 1,000,000,000,000,000.
- **metric**—Specifies the metric value to associate with a specific bandwidth value. The range is 1 through 65,535.

Configuration

CLI Quick Configuration

To quickly configure bandwidth threshold values and associated metric values for an OSPF interface, copy the following commands, remove any line breaks, and then paste the commands into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface ae0.0 metric 5
set protocols ospf area 0.0.0.0 interface ae0.0 bandwidth-based-metrics bandwidth 1g
   metric 60
set protocols ospf area 0.0.0.0 interface ae0.0 bandwidth-based-metrics bandwidth 10g
   metric 50
```

To configure the metric for a specific OSPF interface:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Configure the metric of the OSPF network segment.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface ae0 metric 5
   ```

3. Configure the bandwidth threshold values and associated metric values.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface ae0.0 bandwidth-based-metrics bandwidth 1g metric 60
   user@host# set interface ae0.0 bandwidth-based-metrics bandwidth 10g metric 50
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# commit
   ```


Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface ae0.0 {
    bandwidth-based-metrics {
      bandwidth 1g metric 60;
      bandwidth 10g metric 50;
    }
    metric 5;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Configured Metric

Purpose Verify the metric setting on the interface. Confirm that the Cost field displays the interface's configured metric (cost). When choosing paths to a destination, OSPF uses the path with the lowest cost.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Example: Controlling OSPF Route Preferences

This example shows how to control OSPF route selection in the forwarding table. This example also shows how you might control route selection if you are migrating from OSPF to another IGP.

Requirements

This example assumes that OSPF is properly configured and running in your network, and you want to control route selection because you are planning to migrate from OSPF to a different IGP.

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the IGP that you want to migrate to. See the *Junos OS Routing Protocols Library for Routing Devices*.

Overview

Route preferences are used to select which route is installed in the forwarding table when several protocols calculate routes to the same destination. The route with the lowest preference value is selected.

By default, internal OSPF routes have a preference value of 10, and external OSPF routes have a preference value of 150. You might want to modify this setting if you are planning to migrate from OSPF to a different IGP. Modifying the route preferences enables you to perform the migration in a controlled manner.

This example makes the following assumptions:

- OSPF is already running in your network.
- You want to migrate from OSPF to IS-IS.
- You configured IS-IS per your network requirements and confirmed it is working properly.

In this example, you increase the OSPF route preference values to make them less preferred than IS-IS routes by specifying 168 for internal OSPF routes and 169 for external OSPF routes. IS-IS internal routes have a preference of either 15 (for Level1) or 18 (for Level 2), and external routes have a preference of 160 (for Level 1) or 165 (for Level 2). In general, it is preferred to leave the new protocol at its default settings to minimize complexities and simplify any future addition of routing devices to the network. To modify the OSPF route preference values, configure the following settings:

- **preference**—Specifies the route preference for internal OSPF routes. By default, internal OSPF routes have a value of 10. The range is from 0 through 4,294967,295 (2^{32} – 1).
- **external-preference**—Specifies the route preference for external OSPF routes. By default, external OSPF routes have a value of 150. The range is from 0 through 4,294967,295 (2^{32} – 1).

Configuration

CLI Quick Configuration

To quickly configure the OSPF route preference values, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf preference 168 external-preference 169
```

To configure route selection:

1. Enter OSPF configuration mode and set the external and internal routing preferences.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf preference 168 external-preference 169
   ```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
preference 168;
external-preference 169;
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the Route on page 160

Verifying the Route

Purpose Verify that the IGP is using the appropriate route. After the new IGP becomes the preferred protocol (in this example, IS-IS), you should monitor the network for any issues. After you confirm that the new IGP is working properly, you can remove the OSPF configuration from the routing device by entering the **delete ospf** command at the **[edit protocols]** hierarchy level.

Action From operational mode, enter the **show route** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Example: Configuring OSPF Overload Mode

- OSPF Overload Function Overview on page 160
- Example: Configuring OSPF to Make Routing Devices Appear Overloaded on page 161

OSPF Overload Function Overview

If the time elapsed after the OSPF instance is enabled is less than the specified timeout, overload mode is set.

You can configure the local routing device so that it appears to be overloaded. An overloaded routing device determines it is unable to handle any more OSPF transit traffic, which results in sending OSPF transit traffic to other routing devices. OSPF traffic to directly attached interfaces continues to reach the routing device. You might configure overload mode for many reasons, including:

- If you want the routing device to participate in OSPF routing, but do not want it to be used for transit traffic. This could include a routing device that is connected to the network for analysis purposes, but is not considered part of the production network, such as network management routing devices.
- If you are performing maintenance on a routing device in a production network. You can move traffic off that routing device so network services are not interrupted during your maintenance window.

You configure or disable overload mode in OSPF with or without a timeout. Without a timeout, overload mode is set until it is explicitly deleted from the configuration. With a timeout, overload mode is set if the time elapsed since the OSPF instance started is less than the specified timeout.

A timer is started for the difference between the timeout and the time elapsed since the instance started. When the timer expires, overload mode is cleared. In overload mode, the router link-state advertisement (LSA) is originated with all the transit router links (except stub) set to a metric of 0xFFFF. The stub router links are advertised with the actual cost of the interfaces corresponding to the stub. This causes the transit traffic to avoid the overloaded routing device and to take paths around the routing device. However, the overloaded routing device's own links are still accessible.

NOTE: The routing device can also dynamically enter the overload state, regardless of configuring the device to appear overloaded. For example, if the routing device exceeds the configured OSPF prefix limit, the routing device purges the external prefixes and enters into an overload state. You can limit the number of routes exported into OSPF to minimize the load on the routing device and prevent this potential problem.

Example: Configuring OSPF to Make Routing Devices Appear Overloaded

This example shows how to configure a routing device running OSPF to appear to be overloaded.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

You can configure a local routing device running OSPF to appear to be overloaded, which allows the local routing device to participate in OSPF routing, but not for transit traffic. When configured, the transit interface metrics are set to the maximum value of 65535.

This example includes the following settings:

- **overload**—Configures the local routing device so it appears to be overloaded. You might configure this if you want the routing device to participate in OSPF routing, but do not want it to be used for transit traffic, or you are performing maintenance on a routing device in a production network.
- **timeout *seconds***—(Optional) Specifies the number of seconds at which the overload is reset. If no timeout interval is specified, the routing device remains in the overload state until the overload statement is deleted or a timeout is set. In this example, you configure 60 seconds as the amount of time the routing device remains in the overload state. By default, the timeout interval is 0 seconds (this value is not configured). The range is from 60 through 1800 seconds.

Configuration

CLI Quick Configuration

To quickly configure a local routing device to appear as overloaded, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf overload timeout 60
```

Step-by-Step Procedure

To configure a local routing device to appear overloaded:

1. Enter OSPF configuration mode.

NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@host edit protocols ospf
```

2. Configure the local routing device to be overloaded.

```
[edit protocols ospf]
user@host set overload
```

3. (Optional) Configure the number of seconds at which overload is reset.

```
[edit protocols ospf]
user@host set overload timeout 60
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration. The output includes the optional **timeout** statement.

```
user@host# show protocols ospf
overload timeout 60;
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying Traffic Has Moved Off Devices on page 163
- Verifying Transit Interface Metrics on page 163
- Verifying the Overload Configuration on page 164
- Verifying the Viable Next Hop on page 164

Verifying Traffic Has Moved Off Devices

Purpose Verify that the traffic has moved off the upstream devices.

Action From operational mode, enter the **show interfaces detail** command.

Verifying Transit Interface Metrics

Purpose Verify that the transit interface metrics are set to the maximum value of 65535 on the downstream neighboring device.

Action From operational mode, enter the **show ospf database router detail advertising-router *address*** command for OSPFv2, and enter the **show ospf3 database router detail advertising-router *address*** command for OSPFv3.

Verifying the Overload Configuration

Purpose Verify that overload is configured by reviewing the Configured overload field. If the overload timer is also configured, this field also displays the time that remains before it is set to expire.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and the **show ospf3 overview** command for OSPFv3.

Verifying the Viable Next Hop

Purpose Verify the viable next hop configuration on the upstream neighboring device. If the neighboring device is overloaded, it is not used for transit traffic and is not displayed in the output.

Action From operational mode, enter the **show route *address*** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Example: Configuring the OSPF Routing Algorithm

- Understanding the SPF Algorithm Options for OSPF on page 164
- Example: Configuring SPF Algorithm Options for OSPF on page 165

Understanding the SPF Algorithm Options for OSPF

OSPF uses the shortest-path-first (SPF) algorithm, also referred to as the Dijkstra algorithm, to determine the route to reach each destination. The SPF algorithm describes how OSPF determines the route to reach each destination, and the SPF options control the timers that dictate when the SPF algorithm runs. Depending on your network environment and requirements, you might want to modify the SPF options. For example, consider a large-scale environment with a large number of devices flooding link-state advertisements (LSAs) through out the area. In this environment, it is possible to receive a large number of LSAs to process, which can consume memory resources. By configuring the SPF options, you continue to adapt to the changing network topology, but you can minimize the amount of memory resources being used by the devices to run the SPF algorithm.

You can configure the following SPF options:

- The delay in the time between the detection of a topology change and when the SPF algorithm actually runs.

- The maximum number of times that the SPF algorithm can run in succession before the hold-down timer begins.
- The time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured number of times.

Example: Configuring SPF Algorithm Options for OSPF

This example shows how to configure the SPF algorithm options. The SPF options control the timers that dictate when the SPF algorithm runs.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

OSPF uses the SPF algorithm to determine the route to reach each destination. All routing devices in an area run this algorithm in parallel, storing the results in their individual topology databases. Routing devices with interfaces to multiple areas run multiple copies of the algorithm. The SPF options control the timers used by the SPF algorithm.

Before you modify any of the default settings, you should have a good understanding of your network environment and requirements.

This example shows how to configure the options for running the SPF algorithm. You include the **spf-options** statement and the following options:

- **delay**—Configures the amount of time (in milliseconds) between the detection of a topology and when the SPF actually runs. When you modify the delay timer, consider your requirements for network reconvergence. For example, you want to specify a timer value that can help you identify abnormalities in the network, but allow a stable network to reconverge quickly. By default, the SPF algorithm runs 200 milliseconds after the detection of a topology. The range is from 50 through 8000 milliseconds.

- **rapid-runs**—Configures the maximum number of times that the SPF algorithm can run in succession before the hold-down timer begins. By default, the number of SPF calculations that can occur in succession is 3. The range is from 1 through 10. Each SPF algorithm is run after the configured SPF delay. When the maximum number of SPF calculations occurs, the hold-down timer begins. Any subsequent SPF calculation is not run until the hold-down timer expires.
- **holddown**—Configures the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times. By default, the hold down time is 5000 milliseconds. The range is from 2000 through 20,000 milliseconds. If the network stabilizes during the holddown period and the SPF algorithm does not need to run again, the system reverts to the configured values for the **delay** and **rapid-runs** statements.

Configuration

CLI Quick Configuration

To quickly configure the SPF options, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf spf-options delay 210
set protocols ospf spf-options rapid-runs 4
set protocols ospf spf-options holddown 5050
```

Step-by-Step Procedure

To configure the SPF options:

1. Enter OSPF configuration mode.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf
   ```

2. Configure the SPF delay time.

   ```
   [edit protocols ospf]
   user@host# set spf-options delay 210
   ```

3. Configure the maximum number of times that the SPF algorithm can run in succession.

   ```
   [edit protocols ospf]
   user@host# set spf-options rapid-runs 4
   ```

4. Configure the SPF hold-down timer.

   ```
   [edit protocols ospf]
   user@host# set spf-options holddown 5050
   ```

5. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
spf-options {
  delay 210;
  holddown 5050;
  rapid-runs 4;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying SPF Options

Purpose Verify that SPF is operating per your network requirements. Review the SPF delay field, the SPF holddown field, and the SPF rapid runs fields.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** command for OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Example: Configuring Synchronization Between LDP and OSPF

- Synchronization Between LDP and IGPs Overview on page 167
- Example: Configuring Synchronization Between LDP and OSPF on page 168

Synchronization Between LDP and IGPs Overview

LDP is a protocol for distributing labels in non-traffic-engineered applications. Labels are distributed along the best path determined by the interior gateway protocol (IGP). If synchronization between LDP and the IGP is not maintained, the label-switch path (LSP) goes down. When LDP is not fully operational on a given link (a session is not established and labels are not exchanged), the IGP advertises the link with the maximum cost metric. The link is not preferred but remains in the network topology.

LDP synchronization is supported only on active point-to-point interfaces and LAN interfaces configured as point-to-point under the IGP. LDP synchronization is not supported during graceful restart.

Example: Configuring Synchronization Between LDP and OSPF

This example shows how to configure synchronization between LDP and OSPFv2.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

In this example, configure synchronization between LDP and OSPFv2 by performing the following tasks:

- Enable LDP on interface **so-1/0/3**, which is a member of OSPF area 0.0.0.0, by including the **ldp** statement at the **[edit protocols]** hierarchy level. You can configure one or more interfaces. By default, LDP is disabled on the routing device.
- Enable LDP synchronization by including the **ldp-synchronization** statement at the **[edit protocols ospf area *area-id* interface *interface-name*]** hierarchy level. This statement enables LDP synchronization by advertising the maximum cost metric until LDP is operational on the link.
- Configure the amount of time (in seconds) the routing device advertises the maximum cost metric for a link that is not fully operational by including the **hold-time** statement at the **[edit protocols ospf area *area-id* interface *interface-name* ldp-synchronization]** hierarchy level. If you do not configure the **hold-time** statement, the hold-time value defaults to infinity. The range is from 1 through 65,535 seconds. In this example, configure 10 seconds for the hold-time interval.

This example also shows how to disable synchronization between LDP and OSPFv2 by including the **disable** statement at the **[edit protocols ospf area *area-id* interface *interface-name* ldp-synchronization]** hierarchy level.

Configuration

Enabling Synchronization Between LDP and OSPFv2

CLI Quick Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To quickly enable synchronization between LDP and OSPFv2, copy the following commands, remove any line breaks, and then paste them into the CLI.

```
[edit]
set protocols ldp interface so-1/0/3
set protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-syncrhonization hold-time 10
```

Step-by-Step Procedure

To enable synchronization between LDP and OSPFv2:

1. Enable LDP on the interface.

   ```
   [edit]
   user@host# set protocols ldp interface so-1/0/3
   ```

2. Configure LDP synchronization and optionally configure a time period of 10 seconds to advertise the maximum cost metric for a link that is not fully operational.

   ```
   [edit ]
   user@host# edit protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-synchronization
   ```

3. Configure a time period of 10 seconds to advertise the maximum cost metric for a link that is not fully operational.

   ```
   [edit protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-synchronization ]
   user@host# set hold-time 10
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-synchronization]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ldp** and **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ldp
interface so-1/0/3.0;
```

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface so-1/0/3.0 {
    ldp-synchronization {
      hold-time 10;
    }
  }
}
```


Disabling Synchronization Between LDP and OSPFv2

CLI Quick Configuration

To quickly disable synchronization between LDP and OSPFv2, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-synchronization disable
```

Step-by-Step Procedure

To disable synchronization between LDP and OSPF:

1. Disable synchronization by including the **disable** statement.

   ```
   [edit ]
   user@host# set protocols ospf area 0.0.0.0 interface so-1/0/3 ldp-synchronization
     disable
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface so-1/0/3.0 {
    ldp-synchronization {
      disable;
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the LDP Synchronization State of the Interface

Purpose

Verify the current state of LDP synchronization on the interface. The LDP sync state displays information related to the current state, and the config holdtime field displays the configured hold-time interval.

Action

From operational mode, enter the **show ospf interface extensive** command.

Related Documentation

- OSPF Configuration Overview on page 14
- About OSPF Interfaces on page 121

Configuring OSPF Refresh and Flooding Reduction in Stable Topologies

The OSPF standard requires that every link-state advertisement (LSA) be refreshed every 30 minutes. The Juniper Networks implementation refreshes LSAs every 50 minutes. By default, any LSA that is not refreshed expires after 60 minutes. This requirement can result in traffic overhead that makes it difficult to scale OSPF networks. You can override the default behavior by specifying that the DoNotAge bit be set in self-originated LSAs when they are initially sent by the router or switch. Any LSA with the DoNotAge bit set is reflooded only when a change occurs in the LSA. This feature thus reduces protocol traffic overhead while permitting any changed LSAs to be flooded immediately. Routers or switches enabled for flood reduction continue to send hello packets to their neighbors and to age self-originated LSAs in their databases.

The Juniper implementation of OSPF refresh and flooding reduction is based on RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*. However, the Juniper implementation does not include the forced-flooding interval defined in the RFC. Not implementing the forced-flooding interval ensures that LSAs with the DoNotAge bit set are reflooded only when a change occurs.

This feature is supported for the following:

- OSPFv2 and OSPFv3 interfaces
- OSPFv3 realms
- OSPFv2 and OSPFv3 virtual links
- OSPFv2 sham links
- OSPFv2 peer interfaces
- All routing instances supported by OSPF
- Logical systems

To configure flooding reduction for an OSPF interface, include the **flood-reduction** statement at the **[edit protocols (ospf | ospf3) area *area-id* interface *interface-id*]** hierarchy level.

NOTE: **If you configure flooding reduction for an interface configured as a demand circuit, the LSAs are not initially flooded, but sent only when their content has changed. Hello packets and LSAs are sent and received on a demand-circuit interface only when a change occurs in the network topology.**

In the following example, the OSPF interface **so-0/0/1.0** is configured for flooding reduction. As a result, all the LSAs generated by the routes that traverse the specified interface have the DoNotAge bit set when they are initially flooded, and LSAs are refreshed only when a change occurs.

```
[edit]
protocols ospf {
```

```
    area 0.0.0.0 {
      interface so-0/0/1.0 {
        flood-reduction;
      }
      interface lo0.0;
      interface so-0/0/0.0;
    }
  }
```

NOTE: Beginning with Junos OS Release 12.2, you can configure a global default link-state advertisement (LSA) flooding interval in OSPF for self-generated LSAs by including the lsa-refresh-interval ***minutes*** statement at the **[edit protocols (ospf | ospf3)]** hierarchy level. The Juniper Networks implementation refreshes LSAs every 50 minutes. The range is 25 through 50 minutes. By default, any LSA that is not refreshed expires after 60 minutes.

If you have both the global LSA refresh interval configured for OSPF and OSPF flooding reduction configured for a specific interface in an OSPF area, the OSPF flood reduction configuration takes precedence for that specific interface.

Related Documentation

- flood-reduction on page 395
- lsa-refresh-interval on page 413

CHAPTER 8

OSPF Security Configuration

Examples: Configuring OSPF Authentication

Understanding OSPFv2 Authentication

All OSPFv2 protocol exchanges can be authenticated to guarantee that only trusted routing devices participate in the autonomous system's routing. By default, OSPFv2 authentication is disabled.

NOTE: **OSPFv3 does not have a built-in authentication method and relies on IP Security (IPsec) to provide this functionality.**

You can enable the following authentication types:

- Simple authentication—Authenticates by using a plain-text password that is included in the transmitted packet. The receiving routing device uses an authentication key (password) to verify the packet.
- MD5 authentication—Authenticates by using an encoded MD5 checksum that is included in the transmitted packet. The receiving routing device uses an authentication key (password) to verify the packet.

  You define an MD5 key for each interface. If MD5 is enabled on an interface, that interface accepts routing updates only if MD5 authentication succeeds. Otherwise, updates are rejected. The routing device only accepts OSPFv2 packets sent using the same key identifier (ID) that is defined for that interface.

- IPsec authentication (beginning with Junos OS Release 8.3)—Authenticates OSPFv2 interfaces, the remote endpoint of a sham link, and the OSPFv2 virtual link by using manual security associations (SAs) to ensure that a packet's contents are secure between the routing devices. You configure the actual IPsec authentication separately.

  NOTE: You can configure IPsec authentication together with either MD5 or simple authentication.

  The following restrictions apply to IPsec authentication for OSPFv2:

  - Dynamic Internet Key Exchange (IKE) SAs are not supported.
  - Only IPsec transport mode is supported. Tunnel mode is not supported.
  - Because only bidirectional manual SAs are supported, all OSPFv2 peers must be configured with the same IPsec SA. You configure a manual bidirectional SA at the **[edit security ipsec]** hierarchy level.
  - You must configure the same IPsec SA for all virtual links with the same remote endpoint address, for all neighbors on OSPF nonbroadcast multiaccess (NBMA) or point-to-multipoint links, and for every subnet that is part of a broadcast link.
  - OSPFv2 peer interfaces are not supported.

Because OSPF performs authentication at the area level, all routing devices within the area must have the same authentication and corresponding password (key) configured. For MD5 authentication to work, both the receiving and transmitting routing devices must have the same MD5 key. In addition, a simple password and MD5 key are mutually exclusive. You can configure only one simple password, but multiple MD5 keys.

As part of your security measures, you can change MD5 keys. You can do this by configuring multiple MD5 keys, each with a unique key ID, and setting the date and time to switch to the new key. Each unique MD5 key has a unique ID. The ID is used by the receiver of the OSPF packet to determine which key to use for authentication. The key ID, which is required for MD5 authentication, specifies the identifier associated with the MD5 key.

Understanding OSPFv3 Authentication

OSPFv3 does not have a built-in authentication method and relies on the IP Security (IPsec) suite to provide this functionality. IPsec provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. You can use IPsec to secure specific OSPFv3 interfaces and protect OSPFv3 virtual links.

NOTE:

You configure the actual IPsec authentication separately from your OSPFv3 configuration and then apply IPsec to the OSPFv3 interfaces or OSPFv3 virtual links.

OSPFv3 uses the IP authentication header (AH) and the IP Encapsulating Security Payload (ESP) portions of the IPsec Protocol to authenticate routing information between peers. AH can provide connectionless integrity and data origin authentication. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper-level protocol data. However, some IP header fields might change in transit. Because the value of these fields might not be predictable by the sender, they cannot be protected by AH. ESP can provide encryption and limited traffic flow confidentiality or connectionless integrity, data origin authentication, and an anti-replay service.

IPsec is based on security associations (SAs). An SA is a set of IPsec specifications that are negotiated between devices that are establishing an IPsec relationship. This simplex connection provides security services to the packets carried by the SA. These specifications include preferences for the type of authentication, encryption, and IPsec protocol to be used when establishing the IPsec connection. An SA is used to encrypt and authenticate a particular flow in one direction. Therefore, in normal bidirectional traffic, the flows are secured by a pair of SAs. An SA to be used with OSPFv3 must be configured manually and use transport mode. Static values must be configured on both ends of the SA.

Manual SAs require no negotiation between the peers. All values, including the keys, are static and specified in the configuration. Manual SAs statically define the security parameter index (SPI) values, algorithms, and keys to be used and require matching configurations on both end points (OSPFv3 peers). As a result, each peer must have the same configured options for communication to take place.

The actual choice of encryption and authentication algorithms is left to your IPsec administrator; however, we have the following recommendations:

- Use ESP with NULL encryption to provide authentication to the OSPFv3 protocol headers only. With NULL encryption, you are choosing not to provide encryption on OSPFv3 headers. This can be useful for troubleshooting and debugging purposes. For more information about NULL encryption, see RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*.
- Use ESP with non-NULL encryption for full confidentiality. With non-NULL encryption, you are choosing to provide encryption. For more information about NULL encryption, see RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*.
- Use AH to provide authentication to the OSPFv3 protocol headers, portions of the IPv6 header, and portions of the extension headers.

The following restrictions apply to IPsec authentication for OSPFv3:

- Dynamic Internet Key Exchange (IKE) security associations (SAs) are not supported.
- Only IPsec transport mode is supported. In transport mode, only the payload (the data you transfer) of the IP packet is encrypted and/or authenticated. Tunnel mode is not supported.

- Because only bidirectional manual SAs are supported, all OSPFv3 peers must be configured with the same IPsec SA. You configure a manual bidirectional SA at the **[edit security ipsec]** hierarchy level.
- You must configure the same IPsec SA for all virtual links with the same remote endpoint address.

Example: Configuring Simple Authentication for OSPFv2 Exchanges

This example shows how to enable simple authentication for OSPFv2 exchanges.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

Simple authentication uses a plain-text password that is included in the transmitted packet. The receiving routing device uses an authentication key (password) to verify the packet. Plain-text passwords are not encrypted and might be subject to packet interception. This method is the least secure and should only be used if network security is not your goal.

You can configure only one simple authentication key (password) on the routing device. The simple key can be from 1 through 8 characters and can include ASCII strings. If you include spaces, enclose all characters in quotation marks (“ “).

In this example, you specify OSPFv2 interface **so-0/1/0** in area 0.0.0.0, set the authentication type to simple-password, and define the key as PssWd4.

Configuration

CLI Quick Configuration

To quickly configure simple authentication, copy the following command, removing any line breaks, and then paste the command into the CLI. You must configure all routing devices within the area with the same authentication and corresponding password.

```
[edit]
set protocols ospf area 0.0.0.0 interface so-0/1/0 authentication simple-password PssWd4
```

Step-by-Step Procedure

To enable simple authentication for OSPFv2 exchanges:

1. Create an OSPF area.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Specify the interface.

   ```
   [edit protocols ospf area 0.0.0.0]
   user@host# edit interface so-0/1/0
   ```

3. Set the authentication type and the password.

   ```
   [edit protocols ospf area 0.0.0.0 interface so-0/1/0.0]
   user@host# set authentication simple-password PssWd4
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 interface so-0/1/0.0]
   user@host# commit
   ```

   NOTE: Repeat this entire configuration on all peer OSPFv2 routing devices in the area.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

NOTE: After you configure the password, you do not see the password itself. The output displays the encrypted form of the password you configured.

```
user@host# show protocols ospf
  area 0.0.0.0 {
  interface so-0/1/0.0 {
    authentication {
      simple-password "$9$-3dY4ZUHm5FevX-db2g"; ## SECRET-DATA
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

- Verifying the Configured Authentication Method on page 178

Verifying the Configured Authentication Method

Purpose Verify that the authentication method for sending and receiving OSPF protocol packets is configured. The Authentication Type field displays Password when configured for simple authentication.

Action From operational mode, enter the **show ospf interface** and the **show ospf overview** commands.

Example: Configuring MD5 Authentication for OSPFv2 Exchanges

This example shows how to enable MD5 authentication for OSPFv2 exchanges.

- Requirements on page 178
- Overview on page 178
- Configuration on page 179
- Verification on page 180

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

MD5 authentication uses an encoded MD5 checksum that is included in the transmitted packet. The receiving routing device uses an authentication key (password) to verify the packet.

You define an MD5 key for each interface. If MD5 is enabled on an interface, that interface accepts routing updates only if MD5 authentication succeeds. Otherwise, updates are rejected. The routing device only accepts OSPFv2 packets sent using the same key identifier (ID) that is defined for that interface.

In this example, you create the backbone area (area 0.0.0.0), specify OSPFv2 interface **so-0/2/0**, set the authentication type to md5, and then define the authentication key ID as 5 and the password as PssWd8.

Configuration

CLI Quick Configuration

To quickly configure MD5 authentication, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface so-0/2/0 authentication md5 5 key PssWd8
```

Step-by-Step Procedure

To enable MD5 authentication for OSPFv2 exchanges:

1. Create an OSPF area.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Specify the interface.

   ```
   [edit protocols ospf area 0.0.0.0]
   user@host# edit interface so-0/2/0
   ```

3. Configure MD5 authentication and set a key ID and an authentication password.

   ```
   [edit protocols ospf area 0.0.0.0 interface s0-0/2/0.0]
   user@host# set authentication md5 5 key PssWd8
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 interface s0-0/2/0.0]
   user@host# commit
   ```

   NOTE: Repeat this entire configuration on all peer OSPFv2 routing devices.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

NOTE: After you configure the password, you do not see the password itself. The output displays the encrypted form of the password you configured.

```
user@host# show protocols ospf
area 0.0.0.0 {
```



```
    interface so-0/2/0.0 {
      authentication {
        md5 5 key "$9$pXXhuIhreWx-wQF9puBEh"; ## SECRET-DATA
      }
    }
  }
```

Verification

Confirm that the configuration is working properly.

Verifying the Configured Authentication Method

Purpose Verify that the authentication method for sending and receiving OSPF protocol packets is configured. When configured for MD5 authentication, the Authentication Type field displays MD5, the Active key ID field displays the unique number you entered that identifies the MD5 key, and the Start time field displays the date as Start time 1970 Jan 01 00:00:00 PST. Do not be alarmed by this start time. This is the default start time that the routing device displays if the MD5 key is effective immediately.

Action From operational mode, enter the **show ospf interface** and the **show ospf overview** commands.

Example: Configuring a Transition of MD5 Keys on an OSPFv2 Interface

This example shows how to configure a transition of MD5 keys on an OSPFv2 interface.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

MD5 authentication uses an encoded MD5 checksum that is included in the transmitted packet. For MD5 authentication to work, both the receiving and transmitting routing devices must have the same MD5 key.

You define an MD5 key for each interface. If MD5 is enabled on an interface, that interface accepts routing updates only if MD5 authentication succeeds. Otherwise, updates are rejected. The routing device only accepts OSPFv2 packets sent using the same key identifier (ID) that is defined for that interface.

For increased security, you can configure multiple MD5 keys, each with a unique key ID, and set the date and time to switch to a new key. The receiver of the OSPF packet uses the ID to determine which key to use for authentication.

In this example, you configure new keys to take effect at 12:01 AM on the first day of the next three months on OSPFv2 interface **fe-0/0/1** in the backbone area (area 0.0.0.0), and you configure the following MD5 authentication settings:

- **md5**—Specifies the MD5 authentication key ID. The key ID can be set to any value between 0 and 255, with a default value of 0. The routing device only accepts OSPFv2 packets sent using the same key ID that is defined for that interface.
- **key**—Specifies the MD5 key. Each key can be a value from 1 through 16 characters long. Characters can include ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").
- **start-time**—Specifies the time to start using the MD5 key. This option enables you to configure a smooth transition mechanism for multiple keys. The start time is relevant for transmission but not for receiving OSPF packets.

NOTE: **You must set the same passwords and transition dates and times on all devices in the area so that OSPFv2 adjacencies remain active.**

Configuration

CLI Quick Configuration

To quickly configure multiple MD5 keys on an OSPFv2 interface, copy the following commands, remove any line breaks, and then paste the commands into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-0/1/0 authentication md5 1 key $2010HaL
set protocols ospf area 0.0.0.0 interface fe-0/1/0 authentication md5 2 key NeWpsswdFEB
  start-time 2011-02-01.00:01
set protocols ospf area 0.0.0.0 interface fe-0/1/0 authentication md5 3 key NeWpsswdMAR
  start-time 2011-03-01.00:01
set protocols ospf area 0.0.0.0 interface fe-0/1/0 authentication md5 4 key NeWpsswdAPR
  start-time 2011-04-01.00:01
```

Step-by-Step Procedure

To configure multiple MD5 keys on an OSPFv2 interface:

1. Create an OSPF area.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
```

2. Specify the interface.

```
[edit protocols ospf area 0.0.0.0]
user@host# edit interface fe-0/1/0
```

3. Configure MD5 authentication and set an authentication password and key ID.

```
[edit protocols ospf area 0.0.0.0 interface fe-0/1/0.0]
user@host# set authentication md5 1 key $2010HaL
```

4. Configure a new key to take effect at 12:01 AM on the first day of February, March, and April.

   You configure a new authentication password and key ID for each month.

   a. For the month of February, enter the following:

   ```
   [edit protocols ospf area 0.0.0.0 interface fe-0/1/0.0]
   user@host# set authentication md5 2 key NeWpsswdFEB start-time
     2011-02-01.00:01
   ```

   b. For the month of March, enter the following:

   ```
   [edit protocols ospf area 0.0.0.0 interface fe-0/1/0.0]
   user@host# set authentication md5 3 key NeWpsswdMAR start-time
     2011-03-01.00:01
   ```

   c. For the month of April, enter the following:

   ```
   [edit protocols ospf area 0.0.0.0 interface fe-0/1/0.0]
   user@host# set authentication md5 4 key NeWpsswdAPR start-time
     2011-04-01.00:01
   ```

5. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0 interface fe-0/1/0.0]
user@host# commit
```

NOTE: Repeat this entire configuration on all peer OSPFv2 routing devices.

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

NOTE: After you configure the password, you do not see the password itself. The output displays the encrypted form of the password you configured.

```
user@host# show protocols ospf
```



```
area 0.0.0.0 {
  interface fe-0/1/0.0 {
    authentication {
      md5 1 key "$9$wzs24JGDjk.2gfTQ3CAp0B1hy"; ## SECRET-DATA
      md5 2 key "$9$Q9gz39t1IcML7EcwgJZq.RhSylMN-b4oZDi" start-time
        "2011-2-1.00:01:00 -0800"; ## SECRET-DATA
      md5 3 key "$9$zjo2nCpIRSWXNhSs4ZG.mEcyreW2gaZGjCt" start-time
        "2011-3-1.00:01:00 -0800"; ## SECRET-DATA
      md5 4 key "$9$fQn90OReML1Rds4oiHBIEhSevMLXNVqm" start-time
        "2011-4-1.00:01:00 -0700"; ## SECRET-DATA
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the Configured Authentication Method

Purpose Verify that the authentication method for sending and receiving OSPF protocol packets is configured. When configured for MD5 authentication with a transition of keys, the Auth type field displays MD5, the Active key ID field displays the unique number you entered that identifies the MD5 key, and the Start time field displays the time at which the routing device starts using an MD5 key to authenticate OSPF packets transmitted on the interface you configured.

Action From operational mode, enter the **show ospf interface** and the **show ospf overview** commands.

Example: Configuring IPsec Authentication for an OSPF Interface

This example shows how to enable IP Security (IPsec) authentication for an OSPF interface.

Requirements

Before you begin:

- Configure the device interfaces. See the *Router Interfaces* or the *Junos OS Interfaces Configuration Guide for Security Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26

- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

You can use IPsec authentication for both OSPFv2 and OSPFv3. You configure the actual IPsec authentication separately and apply it to the applicable OSPF configuration.

OSPFv2

Beginning with Junos OS Release 8.3, you can use IPsec authentication to authenticate OSPFv2 interfaces, the remote endpoint of a sham link, and the OSPFv2 virtual link by using manual security associations (SAs) to ensure that a packet's contents are secure between the routing devices.

NOTE: You can configure IPsec authentication together with either MD5 or simple authentication.

To enable IPsec authentication, do one of the following:

- For an OSPFv2 interface, include the **ipsec-sa** ***name*** statement for a specific interface:

  interface *interface-name* ipsec-sa *name*;

- For a remote sham link, include the **ispec-sa** ***name*** statement for the remote end point of the sham link:

  sham-link-remote *address* ipsec-sa *name*;

  NOTE: If a Layer 3 VPN configuration has multiple sham links with the same remote endpoint IP address, you must configure the same IPsec security association for all the remote endpoints. You configure a Layer 3 VPN at the **[edit routing-instances *routing-instance-name* instance-type]** hierarchy level. For more information about Layer 3 VPNs, see the *Junos OS VPNs Library for Routing Devices*.

- For a virtual link, include the **ipsec-sa** ***name*** statement for a specific virtual link:

  virtual-link neighbor-id *router-id* transit-area *area-id* ipsec-sa *name*;

OSPFv3

OSPFv3 does not have a built-in authentication method and relies on IPsec to provide this functionality. You use IPsec authentication to secure OSPFv3 interfaces and protect OSPFv3 virtual links by using manual SAs to ensure that a packet's contents are secure between the routing devices.

To apply authentication, do one of the following:

- For an OSPFv3 interface, include the **ipsec-sa** ***name*** statement for a specific interface:

  interface *interface-name* ipsec-sa *name*;

- For a virtual link, include the **ipsec-sa** ***name*** statement for a specific virtual link:

  virtual-link neighbor-id *router-id* transit-area *area-id* ipsec-sa *name*;

Tasks to Complete for Both OSPFv2 and OSPFv3

In this example, you perform the following tasks:

1. Configure IPsec authentication. To do this, define a manual SA named **sa1** and specify the processing direction, the protocol used to protect IP traffic, the security parameter index (SPI), and the authentication algorithm and key.

   a. Configure the following option at the **[edit security ipsec security-association *sa-name* mode]** hierarchy level:

      transport—Specifies transport mode. This mode protects traffic when the communication endpoint and the cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not.

   b. Configure the following option at the **[edit security ipsec security-association *sa-name* manual direction]** hierarchy level:

      bidirectional—Defines the direction of IPsec processing. By specifying bidirectional, the same algorithms, keys, and security paramater index (SPI) values you configure are used in both directions.

   c. Configure the following options at the **[edit security ipsec security-association *sa-name* manual direction bidirectional]** hierarchy level:

      protocol—Defines the IPsec protocol used by the manual SA to protect IP traffic. You can specify either the authentication header (AH) or the Encapsulating Security Payload (ESP). If you specify AH, which you do in this example, you cannot configure encryption.

      spi—Configures the SPI for the manual SA. An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets. In this example, you specify 256.

      authentication—Configures the authentication algorithm and key. The **algorithm** option specifies the hash algorithm that authenticates packet data. In this example, you specify **hmac-md5-96**, which produces a 128-bit digest. The **key** option indicates the type of authentication key. In this example, you specify **ascii-text-key**, which is 16 ASCII characters for the **hmac-md5-96** algorithm.

2. Enable IPsec authentication on OSPF interface **so-0/2/0.0** in the backbone area (area 0.0.0.0) by including the name of the manual SA **sa1** that you configured at the **[edit security ipsec]** hierarchy level.

Configuration

Configuring Security Associations

CLI Quick Configuration

To quickly configure a manual SA to be used for IPsec authentication on an OSPF interface, copy the following commands, remove any line breaks, and then paste the commands into the CLI.

```
[edit]
set security ipsec security-association sa1
set security ipsec security-association sa1 mode transport
set security ipsec security-association sa1 manual direction bidirectional
set security ipsec security-association sa1 manual direction bidirectional protocol ah
set security ipsec security-association sa1 manual direction bidirectional spi 256
set security ipsec security-association sa1 manual direction bidirectional authentication
  algorithm hmac-md5-96 key ascii-text 123456789012abc
```

Step-by-Step Procedure

To configure a manual SA to be used on an OSPF interface:

1. Specify a name for the SA.

   ```
   [edit]
   user@host# edit security ipsec security-association sa1
   ```

2. Specify the mode of the SA.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# set mode transport
   ```

3. Configure the direction of the manual SA.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# set manual direction bidirectional
   ```

4. Configure the IPsec protocol to use.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# set manual direction bidirectional protocol ah
   ```

5. Configure the value of the SPI.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# set manual direction bidirectional spi 256
   ```

6. Configure the authentication algorithm and key.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# set manual direction bidirectional authentication algorithm
     hmac-md5-96 key ascii-text 123456789012abc
   ```

7. If you are done configuring the device, commit the configuration.

   ```
   [edit security ipsec security-association sa1 ]
   user@host# commit
   ```

NOTE: Repeat this entire configuration on all peer OSPF routing devices.

Results Confirm your configuration by entering the **show security ipsec** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

NOTE: After you configure the password, you do not see the password itself. The output displays the encrypted form of the password you configured.

```
user@host# show security ipsec
security-association sa1 {
  mode transport;
  manual {
    direction bidirectional {
      protocol ah;
      spi 256;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text "$9$AP5Hp1RcylMLxSygoZUHk1REhKMVwY2oJx7jHq.zF69A0OR";
          ## SECRET-DATA
      }
    }
  }
}
```

Enabling IPsec Authentication for an OSPF Interface

CLI Quick Configuration To quickly apply a manual SA used for IPsec authentication to an OSPF interface, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface so-0/2/0 ipsec-sa sa1
```

Step-by-Step Procedure To enable IPsec authentication for an OSPF interface:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Specify the interface.

   ```
   [edit protocols ospf area 0.0.0.0]
   ```

```
user@host# edit interface so-0/2/0
```

3. Apply the IPsec manual SA.

```
[edit protocols ospf area 0.0.0.0 interface so-0/2/0.0]
user@host# set ipsec-sa sa1
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0 interface so-0/2/0.0]
user@host# commit
```

NOTE: Repeat this entire configuration on all peer OSPF routing devices.

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface so-0/2/0.0 {
    ipsec-sa sa1;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the IPsec Security Association Settings on page 188
- Verifying the IPsec Security Association on the OSPF Interface on page 188

Verifying the IPsec Security Association Settings

Purpose Verify the configured IPsec security association settings. Verify the following information:

- The Security association field displays the name of the configured security association.
- The SPI field displays the value you configured.
- The Mode field displays transport mode.
- The Type field displays manual as the type of security association.

Action From operational mode, enter the **show ipsec security-associations** command.

Verifying the IPsec Security Association on the OSPF Interface

Purpose Verify that the IPsec security association that you configured has been applied to the OSPF interface. Confirm that the IPSec SA name field displays the name of the configured IPsec security association.

Action From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

CHAPTER 9

OSPF Routing Instances Configuration

Example: Configuring OSPF Routing Instances

Introduction to Routing Instances for OSPF

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the OSPF routing protocol parameters control the information in the routing tables. You can further install routes learned from OSPF routing instances into routing tables in the OSPF routing table group.

NOTE: **The default routing instance, master, refers to the main inet.0 routing table. The master routing instance is reserved and cannot be specified as a routing instance.**

You can configure the following types of routing instances:

- OSPFv2—Forwarding, Layer 2 virtual private network (VPN), nonforwarding, VPN routing and forwarding (VRF), virtual router, and virtual private LAN service (VPLS).
- OSPFv3—Nonforwarding, VRF, and virtual router.

Each routing instance has a unique name and a corresponding IP unicast table. For example, if you configure a routing instance with the name **my-instance**, the corresponding IP unicast table is **my-instance.inet.0**. All routes for **my-instance** are installed into **my-instance.inet.0**.

You can also configure multiple routing instances of OSPF.

Minimum Routing-Instance Configuration for OSPFv2

To configure a routing instance for OSPFv2, you must include at least the following statements in the configuration:

```
[edit]
routing-instances {
  routing-instance-name {
    interface interface-name;
    instance-type (forwarding | l2vpn | no-forwarding | virtual-router | vpls | vrf);
    route-distinguisher (as-number:number | ip-address:number);
    vrf-import [ policy-names ];
    vrf-export [ policy-names ];
    protocols {
      ospf {
        ... ospf-configuration ...
      }
    }
  }
}
```

NOTE: You can configure a logical interface under only one routing instance.

Minimum Routing-Instance Configuration for OSPFv3

To configure a routing instance for OSPFv3, you must include at least the following statements in the configuration:

```
[edit]
routing-instances {
  routing-instance-name {
    interface interface-name;
    instance-type (no-forwarding | virtual-router | vrf);
    vrf-import [ policy-names ];
    vrf-export [ policy-names ];
    protocols {
      ospf3 {
        ... ospf3-configuration ...
      }
    }
  }
}
```

NOTE: You can configure a logical interface under only one routing instance.

Multiple Routing Instances of OSPF

Multiple instances of OSPF are used for Layer 3 VPN implementations. The multiple instances of OSPF keep routing information for different VPNs separate. The VRF instance advertises routes from the customer edge (CE) router to the provider edge (PE) router and advertises routes from the PE router to the CE router. Each VPN receives only routing information belonging to that VPN.

You can create multiple instances of OSPF by including statements at the following hierarchy levels:

- **[edit routing-instances *routing-instance-name* (ospf | ospf3)]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* (ospf | ospf3)]**

Configuring OSPF Routing Table Groups

To install routes learned from OSPF routing instances into routing tables in the OSPF routing table group, include the **rib-group** statement:

```
rib-group group-name;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Example: Configuring Multiple Routing Instances of OSPF

This example shows how to configure multiple routing instances of OSPF.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26

Overview

When you configure multiple routing instances of OSPF, we recommend that you perform the following tasks:

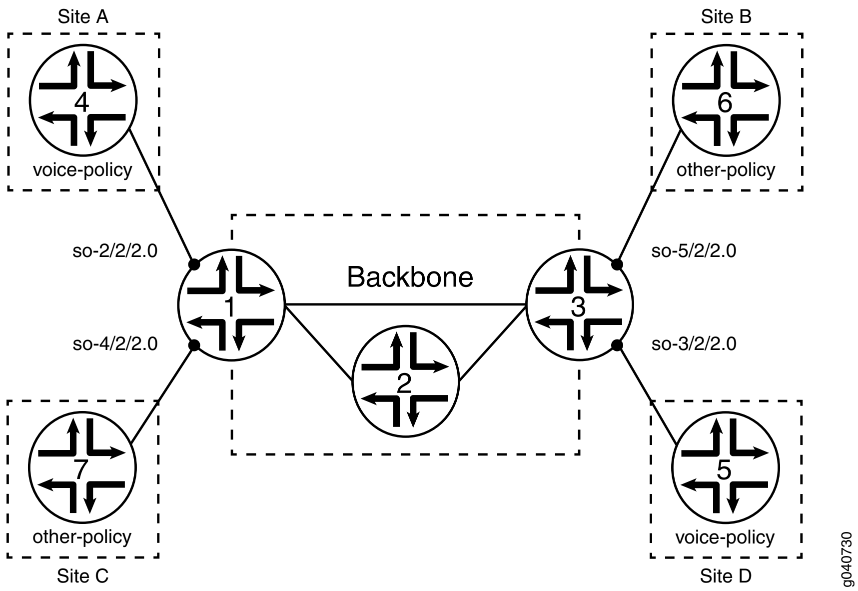
1. Configure the OSPFv2 or OSPFv3 default instance at the **[edit protocols (ospf | ospf3)]** and **[edit logical-systems *logical-system-name* protocols (ospf | ospf3)]** hierarchy levels with the statements needed for your network so that routes are installed in **inet.0** and in the forwarding table.
   Make sure to include the routing table group.
2. Configure an OSPFv2 or OSPFv3 routing instance for each additional OSPFv2 or OSPFv3 routing entity, configuring the following:
   - Interfaces
   - Routing options
   - OSPF protocol statements belonging to that entity
   - Routing table group
3. Configure a routing table group to install routes from the default route table, **inet.0**, into a routing instance's route table.
4. Configure a routing table group to install routes from a routing instance into the default route table, **inet.0**.

   NOTE: **Nonforwarding routing instances do not have forwarding tables that correspond to their routing tables.**

5. Create an export policy to export routes with a specific tag, and use that tag to export routes back into the instances. For more information, see the *Routing Policy Feature Guide for Routing Devices*.

Figure 18 on page 195 shows how you can use multiple routing instances of OSPFv2 or OSPFv3 to segregate prefixes within a large network. The network consists of three administrative entities: **voice-policy**, **other-policy**, and the default routing instance. Each entity is composed of several geographically separate sites that are connected by the backbone and managed by the backbone entity.

Figure 18: Configuration for Multiple Routing Instances



Sites A and D belong to the **voice-policy** routing instance. Sites B and C belong to the **other-policy** instance. Device 1 and Device 3 at the edge of the backbone connect the routing instances. Each runs a separate OSPF or OSPFv3 instance (one per entity).

Device 1 runs three OSPFv2 or OSPFv3 instances: one each for Site A (**voice-policy**), Site C (**other-policy**), and the backbone, otherwise known as the default instance. Device 3 also runs three OSPFv2 or OSPFv3 instances: one each for Site B (**other-policy**), Site D (**voice-policy**), and the backbone (default instance).

When Device 1 runs the OSPFv2 or OSPFv3 instances, the following occur:

- Routes from the default instance routing table are placed in the voice-policy and other-policy instance routing tables.
- Routes from the voice-policy routing instance are placed in the default instance routing table.
- Routes from the other-policy routing instance are placed in the default instance routing table.
- Routes from the voice-policy routing instance do not enter the other-policy instance routing table.
- Routes from the other-policy routing instance do not enter the voice-policy instance routing table.

Configuration

CLI Quick Configuration

To quickly configure multiple routing instances of OSPF, copy the following commands, remove any line breaks, and then paste the commands into the CLI.

Configuration on Device 1:

```
[edit]
set routing-instances voice-policy interface so-2/2/2
set routing-instances voice-policy protocols ospf rib-group voice-to-inet area 0.0.0.0
  interface so-2/2/2
set routing-instances other-policy interface so-4/2/2
set routing-instances other-policy protocols ospf rib-group other-to-inet area 0.0.0.0
  interface so-4/2/2
set routing-options rib-groups inet-to-voice-and-other import-rib [ inet.0 voice-policy.inet.0
  other-policy.inet.0 ]
set routing-options rib-groups voice-to-inet import-rib [ voice-policy.inet.0 inet.0 ]
set routing-options rib-groups other-to-inet import-rib [ other-policy.inet.0 inet.0 ]
set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-2/2/2
set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-4/2/2
```

Configuration on Device 3:

```
[edit]
set routing-instances voice-policy interface so-3/2/2
set routing-instances voice-policy protocols ospf rib-group voice-to-inet area 0.0.0.0
  interface so-3/2/2
set routing-instances other-policy interface so-5/2/2
set routing-instances other-policy protocols ospf rib-group other-to-inet area 0.0.0.0
  interface so-5/2/2
set routing-options rib-groups inet-to-voice-and-other import-rib [ inet.0 voice-policy.inet.0
  other-policy.inet.0 ]
set routing-options rib-groups voice-to-inet import-rib [ voice-policy.inet.0 inet.0 ]
set routing-options rib-groups other-to-inet import-rib [ other-policy.inet.0 inet.0 ]
set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-3/2/2
set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-5/2/2
```

Step-by-Step Procedure

To configure multiple routing instances of OSPF:

1. Configure the routing instances for **voice-policy** and **other-policy**.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit routing-instances protocols]** hierarchy level.

   ```
   [edit]
   user@D1# set routing-instances voice-policy interface so-2/2/2
   user@D1# set routing-instances voice-policy protocols ospf rib-group voice-to-inet
     area 0.0.0.0 interface so-2/2/2
   user@D1# set routing-instances other-policy interface so-4/2/2
   user@D1# set routing-instances other-policy protocols ospf rib-group other-to-inet
     area 0.0.0.0 interface so-4/2/2
   ```

   ```
   [edit]
   user@D3# set routing-instances voice-policy interface so-3/2/2
   user@D3# set routing-instances voice-policy protocols ospf rib-group voice-to-inet
     area 0.0.0.0 interface so-3/2/2
   user@D3#set routing-instances other-policy interface so-5/2/2
   user@D3# set routing-instances other-policy protocols ospf rib-group other-to-inet
     area 0.0.0.0 interface so-5/2/2
   ```


2. Configure the routing table group **inet-to-voice-and-other** to take routes from **inet.0** (default routing table) and place them in the **voice-policy.inet.0** and **other-policy.inet.0** routing tables.

   [edit]
   user@D1# **set routing-options rib-groups inet-to-voice-and-other import-rib [inet.0 voice-policy.inet.0 other-policy.inet.0]**

   [edit]
   user@D3# **set routing-options rib-groups inet-to-voice-and-other import-rib [inet.0 voice-policy.inet.0 other-policy.inet.0]**

3. Configure the routing table group **voice-to-inet** to take routes from **voice-policy.inet.0** and place them in the **inet.0** default routing table.

   [edit]
   user@D1# **set routing-options rib-groups voice-to-inet import-rib [voice-policy.inet.0 inet.0]**

   [edit]
   user@D3# **set routing-options rib-groups voice-to-inet import-rib [voice-policy.inet.0 inet.0]**

4. Configure the routing table group **other-to-inet** to take routes from **other-policy.inet.0** and place them in the **inet.0** default routing table.

   [edit]
   user@D1# **set routing-options rib-groups other-to-inet import-rib [other-policy.inet.0 inet.0]**

   [edit]
   user@D3# **set routing-options rib-groups other-to-inet import-rib [other-policy.inet.0 inet.0]**

5. Configure the default OSPF instance.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit routing-instances protocols]** hierarchy level.

   [edit]
   user@D1# **set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-2/2/2**
   user@D1# **set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-4/2/2**

   [edit]
   user@D3# **set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-3/2/2**
   user@D3# **set protocols ospf rib-group inet-to-voice-and-other area 0.0.0.0 interface so-5/2/2**

6. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Results Confirm your configuration by entering the **show routing-instances**, **show routing-options**, and **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on Device 1:

```
user@D1# show routing-instances
voice-policy {
   interface so-2/2/2.0;
   protocols {
      ospf {
         rib-group voice-to-inet;
         area 0.0.0.0 {
            interface so-2/2/2.0;
         }
      }
   }
}
other-policy {
   interface so-4/2/2.0;
   protocols {
      ospf {
         rib-group other-to-inet;
         area 0.0.0.0 {
            interface so-4/2/2.0;
         }
      }
   }
}
```

```
user@D1# show routing-options
rib-groups {
   inet-to-voice-and-other {
      import-rib [ inet.0 voice-policy.inet.0 other-policy.inet.0 ];
   }
   voice-to-inet {
      import-rib [ voice-policy.inet.0 inet.0 ];
   }
   other-to-inet {
      import-rib [ other-policy.inet.0 inet.0 ];
   }
}
```

```
user@D1# show protocols ospf
rib-group inet-to-voice-and-other;
area 0.0.0.0 {
   interface so-2/2/2.0;
   interface so-4/2/2.0;
}
```

Configuration on Device 3:

```
user@D3# show routing-instances
voice-policy {
   interface so-3/2/2.0;
   protocols {
      ospf {
```



```
            rib-group voice-to-inet;
            area 0.0.0.0 {
                interface so-3/2/2.0;
            }
        }
    }
}
other-policy {
    interface so-5/2/2.0;
    protocols {
        ospf {
            rib-group other-to-inet;
            area 0.0.0.0 {
                interface so-5/2/2.0;
            }
        }
    }
}
```

```
user@D3# show routing-options
rib-groups {
    inet-to-voice-and-other {
        import-rib [ inet.0 voice-policy.inet.0 other-policy.inet.0 ];
    }
    voice-to-inet {
        import-rib [ voice-policy.inet.0 inet.0 ];
    }
    other-to-inet {
        import-rib [ other-policy.inet.0 inet.0 ];
    }
}
```

```
user@D3# show protocols ospf
rib-group inet-to-voice-and-other;
area 0.0.0.0 {
    interface so-3/2/2.0;
    interface so-5/2/2.0;
}
```

To confirm your OSPFv3 configuration, enter the **show routing-instances**, **show routing-options**, and **show protocols ospf3** commands.

Verification

Confirm that the configuration is working properly.

Verifying the Routing Instances

Purpose Verify the configured routing instance settings.

Action From operational mode, enter the **show route instance detail** command.

Related Documentation

- OSPF Overview on page 4
- *Routing Instances Overview* in the *Routing Policy Feature Guide for Routing Devices*

CHAPTER 10

OSPF Fault Detection Configuration

Example: Configuring OSPF Timers

OSPF Timers Overview

OSPF routing devices constantly track the status of their neighbors, sending and receiving hello packets that indicate whether each neighbor still is functioning, and sending and receiving link-state advertisement (LSA) and acknowledgment packets. OSPF sends packets and expects to receive packets at specified intervals.

You configure OSPF timers on the interface of the routing device participating in OSPF. Depending on the timer, the configured interval must be the same on all routing devices on a shared network (area).

You can configure the following OSPF timers:

- Hello interval—Routing devices send hello packets at a fixed interval on all interfaces, including virtual links, to establish and maintain neighbor relationships. The hello interval specifies the length of time, in seconds, before the routing device sends a hello packet out of an interface. This interval must be the same on all routing devices on a shared network. By default, the routing device sends hello packets every 10 seconds (broadcast and point-to-point networks) and 30 seconds (nonbroadcast multiple access (NBMA) networks).
- Poll interval—(OSPFv2, Nonbroadcast networks only) Routing devices send hello packets for a longer interval on nonbroadcast networks to minimize the bandwidth required on slow WAN links. The poll interval specifies the length of time, in seconds, before the routing device sends hello packets out of the interface before establishing adjacency with a neighbor. By default, the routing device sends hello packets every 120 seconds until active neighbors are detected.

Once the routing device detects an active neighbor, the hello packet interval changes from the time specified in the poll interval to the time specified in the hello interval.

- LSA retransmission interval—When a routing device sends LSAs to its neighbors, the routing device expects to receive an acknowledgment packet from each neighbor within a certain amount of time. The LSA retransmission interval specifies the length of time, in seconds, that the routing device waits to receive an LSA packet before retransmitting the LSA to an interface's neighbors. By default, the routing device waits 5 seconds for an acknowledgment before retransmitting the LSA.
- Dead interval—If a routing device does not receive a hello packet from a neighbor within a fixed amount of time, the routing device modifies its topology database to indicate that the neighbor is nonoperational. The dead interval specifies the length of time, in seconds, that the routing device waits before declaring that a neighboring routing device is unavailable. This is an interval during which the routing device receives no hello packets from the neighbor. This interval must be the same on all routing devices on a shared network. By default, this interval is four times the default hello interval, which is 40 seconds (broadcast and point-to-point networks) and 120 seconds (NBMA networks).
- Transit delay—Before a link-state update packet is propagated out of an interface, the routing device must increase the age of the packet. The transit delay sets the estimated time required to transmit a link-state update on the interface. By default, the transit delay is 1 second. You should never have to modify the transit delay time.

Example: Configuring OSPF Timers

This example shows how to configure the OSPF timers.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

The default OSPF timer settings are optimal for most networks. However, depending on your network requirements, you might need to modify the timer settings. This example explains why you might need to modify the following timers:

- Hello interval
- Dead interval
- LSA retransmission interval
- Transit delay

Hello Interval and Dead Interval

The hello interval and the dead interval optimize convergence times by efficiently tracking neighbor status. By lowering the values of the hello interval and the dead interval, you can increase the convergence of OSPF routes if a path fails. These intervals must be the same on all routing devices on a shared network. Otherwise, OSPF cannot establish the appropriate adjacencies.

In the first example, you lower the hello interval to 2 seconds and the dead interval to 8 seconds on point-to-point OSPF interfaces **fe-0/0/1** and **fe-1/0/1** in area 0.0.0.0 by configuring the following settings:

- **hello-interval**—Specifies the length of time, in seconds, before the routing device sends a hello packet out of an interface. By default, the routing device sends hello packets every 10 seconds. The range is from 1 through 255 seconds.
- **dead-interval**—Specifies the length of time, in seconds, that the routing device waits before declaring that a neighboring routing device is unavailable. This is an interval during which the routing device receives no hello packets from the neighbor. By default, the routing device waits 40 seconds (four times the hello interval). The range is 1 through 65,535 seconds.

LSA Retransmission Interval

The link-state advertisement (LSA) retransmission interval optimizes the sending and receiving of LSA and acknowledgement packets. You must configure the LSA retransmission interval to be equal to or greater than 3 seconds to avoid triggering a retransmit trap because the Junos OS delays LSA acknowledgments by up to 2 seconds. If you have a virtual link, you might find increased performance by increasing the value of the LSA retransmission interval.

In the second example, you increase the LSA retransmission timer to 8 seconds on OSPF interface **fe-0/0/1** in area 0.0.0.1 by configuring the following setting:

- **retransmit-interval**—Specifies the length of time, in seconds, that the routing device waits to receive an LSA packet before retransmitting LSA to an interface's neighbors. By default, the routing device retransmits LSAs to its neighbors every 5 seconds. The range is from 1 through 65,535 seconds.

Transit Delay

The transit delay sets the time the routing device uses to age a link-state update packet. If you have a slow link (for example, one with an average propagation delay of multiple seconds), you should increase the age of the packet by a similar amount. Doing this ensures that you do not receive a packet back that is younger than the original copy.

In the final example, you increase the transit delay to 2 seconds on OSPF interface **fe-1/0/1** in area 0.0.0.1. By configuring the following setting, this causes the routing device to age the link-state update packet by 2 seconds:

- **transit-delay**—Sets the estimated time required to transmit a link-state update on the interface. You should never have to modify the transit delay time. By default, the routing device ages the packet by 1 second. The range is from 1 through 65,535 seconds.

Configuration

Configuring the Hello Interval and the Dead Interval

CLI Quick Configuration

To quickly configure the hello and dead intervals, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-0/0/1 hello-interval 2
set protocols ospf area 0.0.0.0 interface fe-0/0/1 dead-interval 8
set protocols ospf area 0.0.0.0 interface fe-1/0/1 hello-interval 2
set protocols ospf area 0.0.0.0 interface fe-1/0/1 dead-interval 8
```

Step-by-Step Procedure

To configure the hello and dead intervals:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Specify the interfaces.


```
[edit protocols ospf area 0.0.0.0]
user@host# set interface fe-0/0/1
user@host# set interface fe-1/0/1
```

3. Configure the hello interval.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# set interface fe-0/0/1 hello-interval 2
user@host# set interface fe-1/0/1 hello-interval 2
```

4. Configure the dead interval.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# set interface fe-0/0/1 dead-interval 8
user@host# set interface fe-1/0/1 dead-interval 8
```

5. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# commit
```

NOTE: Repeat this entire configuration on all routing devices in a shared network.

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/1.0 {
    hello-interval 2;
    dead-interval 8;
  }
  interface fe-1/0/1.0 {
    hello-interval 2;
    dead-interval 8;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Controlling the LSA Retransmission Interval

CLI Quick Configuration To quickly configure the LSA retransmission interval, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.1 interface fe-0/0/1 retransmit-interval 8
```

Step-by-Step Procedure To configure the LSA retransmission interval:

1. Create an OSPF area.

NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@host# edit protocols ospf area 0.0.0.1
```

2. Specify the interface.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface fe-0/0/1
```

3. Configure the LSA retransmission interval.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# set interface fe-0/0/1 retransmit-interval 8
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.1]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.1 {
  interface fe-0/0/1.0 {
    retransmit-interval 8;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Specifying the Transit Delay

CLI Quick Configuration To quickly configure the transit delay, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.1 interface fe-1/0/1 transit-delay 2
```

Step-by-Step Procedure To configure the transit delay:

1. Create an OSPF area.

NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@host# edit protocols ospf area 0.0.0.1
```


2. Specify the interface.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface fe-1/0/1
```

3. Configure the transit delay.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# set interface fe-1/0/1 transit-delay 2
```

4. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.1 {
  interface fe-1/0/1.0 {
    transit-delay 2;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Timer Configuration

Purpose Verify that the interface for OSPF or OSPFv3 has been configured with the applicable timer values. Confirm that the Hello field, the Dead field, and the ReXmit field display the values that you configured.

Action From operational mode, enter the **show ospf interface detail** for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

Example: Configuring BFD for OSPF

- BFD for OSPF Overview on page 207
- Example: Configuring BFD for OSPF on page 210

BFD for OSPF Overview

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchange BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. The BFD failure detection timers have shorter time limits than the OSPF failure detection mechanisms, so they provide faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the **clear bfd adaptation** command to return BFD interval timers to their configured values. The **clear bfd adaptation** command is hitless, meaning that the command does not affect traffic flow on the routing device.

NOTE: BFD is supported for OSPFv3 in Junos OS Release 9.3 and later.

You can configure the following BFD protocol settings:

- **detection-time threshold**—Threshold for the adaptation of the detection time. When the BFD session detection time adapts to a value equal to or greater than the configured threshold, a single trap and a single system log message are sent.
- **full-neighbors-only**—Ability to establish BFD sessions only for OSPF neighbors with full neighbor adjacency. The default behavior is to establish BFD sessions for all OSPF neighbors. This setting is available in Junos OS Release 9.5 and later.
- **minimum-interval**—Minimum transmit and receive interval for failure detection. This setting configures both the minimum interval after which the local routing device transmits hello packets and the minimum interval after which the routing device expects to receive a reply from the neighbor with which it has established a BFD session. Both intervals are in milliseconds. You can also specify the minimum transmit and receive intervals separately using the **transmit-interval minimum-interval** and **minimum-receive-interval** statements.

NOTE: BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. Without NSR, Routing Engine-based sessions can have a minimum interval of 100 ms. In OSPFv3, BFD is always based in the Routing Engine, meaning that BFD is not distributed. For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

- **minimum-receive-interval**—Minimum receive interval for failure detection. This setting configures the minimum receive interval, in milliseconds, after which the routing device expects to receive a hello packet from a neighbor with which it has established a BFD session. You can also specify the minimum receive interval using the **minimum-interval** statement.
- **multiplier**—Multiplier for hello packets. This setting configures the number of hello packets that are not received by a neighbor, which causes the originating interface to be declared down. By default, three missed hello packets cause the originating interface to be declared down.
- **no-adaptation**—Disables BFD adaption. This setting disables BFD sessions from adapting to changing network conditions. This setting is available in Junos OS Release 9.0 and later.

NOTE: We recommend that you do not disable BFD adaptation unless it is preferable not to have BFD adaptation in your network.

- **transmit-interval minimum-interval**—Minimum transmit interval for failure detection. This setting configures the minimum transmit interval, in milliseconds, at which the local routing device transmits hello packets to the neighbor with which it has established a BFD session. You can also specify the minimum transmit interval using the **minimum-interval** statement.

- **transmit-interval threshold**—Threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system log message are sent. The threshold value must be greater than the minimum transmit interval. If you attempt to commit a configuration with a threshold value less than the minimum transmit interval, the routing device displays an error and does not accept the configuration.
- **version**—BFD version. This setting configures the BFD version used for detection. You can explicitly configure BFD version 1, or the routing device can automatically detect the BFD version. By default, the routing device automatically detects the BFD version automatically, which is either 0 or 1.

You can also trace BFD operations for troubleshooting purposes.

Example: Configuring BFD for OSPF

This example shows how to configure the Bidirectional Forwarding Detection (BFD) protocol for OSPF.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26.
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

An alternative to adjusting the OSPF hello interval and dead interval settings to increase route convergence is to configure BFD. The BFD protocol is a simple hello mechanism that detects failures in a network. The BFD failure detection timers have shorter timer limits than the OSPF failure detection mechanisms, thereby providing faster detection.

BFD is useful on interfaces that are unable to detect failure quickly, such as Ethernet interfaces. Other interfaces, such as SONET interfaces, already have built-in failure detection. Configuring BFD on those interfaces is unnecessary.

You configure BFD on a pair of neighboring OSPF interfaces. Unlike the OSPF hello interval and dead interval settings, you do not have to enable BFD on all interfaces in an OSPF area.

In this example, you enable failure detection by including the **bfd-liveness-detection** statement on the neighbor OSPF interface **fe-0/1/0** in area 0.0.0.0 and configure the BFD packet exchange interval to 300 milliseconds, configure 4 as the number of missed hello packets that causes the originating interface to be declared down, and configure BFD sessions only for OSPF neighbors with full neighbor adjacency by including the following settings:

- **full-neighbors-only**—In Junos OS Release 9.5 and later, configures the BFD protocol to establish BFD sessions only for OSPF neighbors with full neighbor adjacency. The default behavior is to establish BFD sessions for all OSPF neighbors.
- **minimum-interval**—Configures the minimum interval, in milliseconds, after which the local routing device transmits hello packets as well as the minimum interval after which the routing device expects to receive a reply from the neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds. You can also specify the minimum transmit and receive intervals separately using the **transmit-interval minimum-interval** and **minimum-receive-interval** statements.

NOTE: BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

- **multiplier**—Configures the number of hello packets not received by a neighbor that causes the originating interface to be declared down. By default, three missed hello packets cause the originating interface to be declared down. You can configure a value in the range from 1 through 255.

Configuration

CLI Quick Configuration

To quickly configure the BFD protocol for OSPF, copy the following commands, remove any line breaks, and then paste the commands into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection minimum-interval
  300
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection multiplier 4
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection full-neighbors-only
```

Step-by-Step Procedure

To configure the BFD protocol for OSPF on one neighboring interface:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Specify the interface.

   ```
   [edit protocols ospf area 0.0.0.0]
   user@host# set interface fe-0/0/1
   ```

3. Specify the minimum transmit and receive intervals.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface fe-0/0/1 bfd-liveness-detection minimum-interval 300
   ```

4. Configure the number of missed hello packets that cause the originating interface to be declared down.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface fe-0/0/1 bfd-liveness-detection multiplier 4
   ```

5. Configure BFD sessions only for OSPF neighbors with full neighbor adjacency.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# set interface fe-0/0/1 bfd-liveness-detection full-neighbors-only
   ```

6. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0 ]
   user@host# commit
   ```

   NOTE: Repeat this entire configuration on the other neighboring interface.

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/1.0 {
    bfd-liveness-detection {
      minimum-interval 300;
      multiplier 4;
      full-neighbors-only;
    }
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the BFD Sessions

Purpose Verify that the OSPF interfaces have active BFD sessions, and that session components have been configured correctly.

Action From operational mode, enter the **show bfd session detail** command.

Meaning The output displays information about the BFD sessions.

- The Address field displays the IP address of the neighbor.
- The Interface field displays the interface you configured for BFD.
- The State field displays the state of the neighbor and should show Full to reflect the full neighbor adjacency that you configured.
- The Transmit Interval field displays the time interval you configured to send BFD packets.
- The Multiplier field displays the multiplier you configured.

Related Documentation

- OSPF Configuration Overview on page 14
- BFD Authentication for OSPF Overview on page 214

Example: Configuring BFD Authentication for OSPF

- BFD Authentication for OSPF Overview on page 214
- Configuring BFD Authentication for OSPF on page 215

BFD Authentication for OSPF Overview

Bidirectional Forwarding Detection (BFD) enables rapid detection of communication failures between adjacent systems. By default, authentication for BFD sessions is disabled. However, when you run BFD over Network Layer protocols, the risk of service attacks can be significant. We strongly recommend using authentication if you are running BFD over multiple hops or through insecure tunnels. Beginning with Junos OS Release 9.6, Junos OS supports authentication for BFD sessions running over OSPFv2. BFD authentication is not supported on MPLS OAM sessions. BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.

You authenticate BFD sessions by specifying an authentication algorithm and keychain, and then associating that configuration information with a security authentication keychain using the keychain name.

The following sections describe the supported authentication algorithms, security keychains, and level of authentication that can be configured:

BFD Authentication Algorithms

Junos OS supports the following algorithms for BFD authentication:

- **simple-password**—Plain-text password. One to 16 bytes of plain text are used to authenticate the BFD session. One or more passwords can be configured. This method is the least secure and should be used only when BFD sessions are not subject to packet interception.
- **keyed-md5**—Keyed Message Digest 5 hash algorithm for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed MD5 uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. With this method, packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than or equal to the last sequence number received. Although more secure than a simple password, this method is vulnerable to replay attacks. Increasing the rate at which the sequence number is updated can reduce this risk.
- **meticulous-keyed-md5**—Meticulous keyed Message Digest 5 hash algorithm. This method works in the same manner as keyed MD5, but the sequence number is updated with every packet. Although more secure than keyed MD5 and simple passwords, this method might take additional time to authenticate the session.
- **keyed-sha-1**—Keyed Secure Hash Algorithm I for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed SHA uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. The key is not carried within the packets. With this method,

packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than the last sequence number received.

- **meticulous-keyed-sha-1**—Meticulous keyed Secure Hash Algorithm I. This method works in the same manner as keyed SHA, but the sequence number is updated with every packet. Although more secure than keyed SHA and simple passwords, this method might take additional time to authenticate the session.

NOTE: Nonstop active routing (NSR) is not supported with the meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

Security Authentication Keychains

The security authentication keychain defines the authentication attributes used for authentication key updates. When the security authentication keychain is configured and associated with a protocol through the keychain name, authentication key updates can occur without interrupting routing and signaling protocols.

The authentication keychain contains one or more keychains. Each keychain contains one or more keys. Each key holds the secret data and the time at which the key becomes valid. The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

BFD allows multiple clients per session, and each client can have its own keychain and algorithm defined. To avoid confusion, we recommend specifying only one security authentication keychain.

Strict Versus Loose Authentication

By default, strict authentication is enabled and authentication is checked at both ends of each BFD session. Optionally, to smooth migration from nonauthenticated sessions to authenticated sessions, you can configure *loose checking*. When loose checking is configured, packets are accepted without authentication being checked at each end of the session. This feature is intended for transitional periods only.

Configuring BFD Authentication for OSPF

Beginning with Junos OS Release 9.6, you can configure authentication for BFD sessions running over OSPFv2. Routing instances are also supported.

The following sections provide instructions for configuring and viewing BFD authentication on OSPF:

Configuring BFD Authentication Parameters

Only three steps are needed to configure authentication on a BFD session:

1. Specify the BFD authentication algorithm for the OSPFv2 protocol.
2. Associate the authentication keychain with the OSPFv2 protocol.
3. Configure the related security authentication keychain.

To configure BFD authentication:

1. Specify the algorithm (**keyed-md5**, **keyed-sha-1**, **meticulous-keyed-md5**, **meticulous-keyed-sha-1**, or **simple-password**) to use for BFD authentication on an OSPF route or routing instance.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.1 interface if2-ospf bfd-liveness-detection
     authentication algorithm keyed-sha-1
   ```

   NOTE: Nonstop active routing (NSR) is not supported with meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

2. Specify the keychain to be used to associate BFD sessions on the specified OSPF route or routing instance with the unique security authentication keychain attributes.

   This keychain should match the keychain name configured at the **[edit security authentication key-chains]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.1 interface if2-ospf bfd-liveness-detection
     authentication keychain bfd-ospf
   ```

   NOTE: The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

3. Specify the unique security authentication information for BFD sessions:

   - The matching keychain name as specified in Step 2.
   - At least one key, a unique integer between 0 and 63. Creating multiple keys enables multiple clients to use the BFD session.
   - The secret data used to allow access to the session.
   - The time at which the authentication key becomes active, in the format *yyyy-mm-dd.hh:mm:ss*.

   ```
   [edit security]
   ```

```
user@host# authentication-key-chains key-chain bfd-ospf key 53 secret
  $9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm start-time 2009-06-14.10:00:00
```

4. (Optional) Specify loose authentication checking if you are transitioning from nonauthenticated sessions to authenticated sessions.

```
[edit]
user@host> set protocols ospf interface if2-ospf bfd-liveness-detection authentication
  loose-check
```

5. (Optional) View your configuration using the **show bfd session detail** or **show bfd session extensive** command.

6. Repeat the steps in this procedure to configure the other end of the BFD session.

NOTE: BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.

Viewing Authentication Information for BFD Sessions

You can view the existing BFD authentication configuration using the **show bfd session detail** and **show bfd session extensive** commands.

The following example shows BFD authentication configured for the **if2-ospf** BGP group. It specifies the keyed SHA-1 authentication algorithm and a keychain name of **bfd-ospf**. The authentication keychain is configured with two keys. Key **1** contains the secret data "**9ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm**" and a start time of June 1, 2009, at 9:46:02 AM PST. Key **2** contains the secret data "**9a5jiKW9l.reP38ny.TszF2/9**" and a start time of June 1, 2009, at 3:29:20 PM PST.

```
[edit protocols ospf]
area 0.0.0.1 {
  interface if2-ospf {
    bfd-liveness-detection {
      authentication {
        algorithm keyed-sha-1;
        key-chain bfd-ospf;
      }
    }
  }
}
[edit security]
authentication key-chains {
  key-chain bfd-ospf {
    key 1 {
      secret "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm";
      start-time "2009-6-1.09:46:02 -0700";
    }
    key 2 {
      secret "$9$a5jiKW9l.reP38ny.TszF2/9";
      start-time "2009-6-1.15:29:20 -0700";
    }
  }
}
```

If you commit these updates to your configuration, you see output similar to the following. In the output for the **show bfd session detail** command, **Authenticate** is displayed to indicate that BFD authentication is configured.

show bfd session detail

```
user@host# show bfd session detail
                                                  Detect   Transmit
Address                  State     Interface      Time     Interval  Multiplier
10.9.1.33            Up        so-7/1/0.0          0.600     0.200      3
  Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3, Authenticate
  Session up time 3d 00:34
  Local diagnostic None, remote diagnostic None
  Remote state Up, version 1
  Replicated

1 sessions, 1 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps
```

For more information about the configuration, use the **show bfd session extensive** command. The output for this command provides the keychain name, the authentication algorithm and mode for each client in the session, and the overall BFD authentication configuration status, keychain name, and authentication algorithm and mode.

show bfd session extensive

```
user@host# show bfd session extensive
                                                  Detect   Transmit
Address                  State     Interface      Time     Interval  Multiplier
10.9.1.33            Up        so-7/1/0.0          0.600     0.200      3
  Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3, Authenticate
       keychain bfd-ospf, algo keyed-md5, mode loose

  Session up time 3d 00:34
  Local diagnostic None, remote diagnostic None
  Remote state Up, version 1
  Replicated
  Min async interval 0.200, min slow interval 1.000
  Adaptive async tx interval 0.200, rx interval 0.200
  Local min tx interval 0.200, min rx interval 0.200, multiplier 3
  Remote min tx interval 0.100, min rx interval 0.100, multiplier 3
  Threshold transmission interval 0.000, Threshold for detection time 0.000
  Local discriminator 11, remote discriminator 80
  Echo mode disabled/inactive
 Authentication enabled/active, keychain bfd-ospf, algo keyed-sha-1, mode strict
1 sessions, 1 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps
```

Related Documentation

- OSPF Configuration Overview on page 14
- BFD for OSPF Overview on page 207

CHAPTER 11

OSPF Redundancy Features Configuration

Examples: Configuring Graceful Restart for OSPF

Graceful Restart for OSPF Overview

Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition. During a graceful restart, the restarting device and its neighbors continue forwarding packets without disrupting network performance. Because neighboring devices assist in the restart (these neighbors are called *helper routers*), the restarting device can quickly resume full operation without recalculating algorithms.

NOTE: On a broadcast link with a single neighbor, when the neighbor initiates an OSPFv3 graceful restart operation, the restart might be terminated at the point when the local routing device assumes the role of a helper. A change in the LSA is considered a topology change, which terminates the neighbor's restart operation.

Graceful restart is disabled by default. You can globally enable graceful restart for all routing protocols by including the **graceful-restart** statement at the **[edit routing-options]** hierarchy level. To enable graceful restart specifically for OSPF, first you need to globally enable graceful restart for all routing protocols.

This topic describes the following information:

Helper Mode for Graceful Restart

When a device enabled for OSPF graceful restart restarts, it retains routes learned before the restart in its forwarding table. The device does not allow new OSPF link-state advertisements (LSAs) to update the routing table. This device continues to forward traffic to other OSPF neighbors (or helper routers), and sends only a limited number of LSAs during the restart period. To reestablish OSPF adjacencies with neighbors, the restarting device must send a grace LSA to all neighbors. In response, the helper routers enter helper mode (the ability to assist a neighboring device attempting a graceful restart) and send an acknowledgment back to the restarting device. If there are no topology changes, the helper routers continue to advertise LSAs as if the restarting device had remained in continuous OSPF operation.

NOTE: Helper mode is enabled by default when you start the routing platform, even if graceful restart is not enabled. You can disable helper mode specifically for OSPF.

When the restarting device receives replies from all the helper routers, the restarting device selects routes, updates the forwarding table, and discards the old routes. At this point, full OSPF adjacencies are reestablished and the restarting device receives and processes OSPF LSAs as usual. When the helper routers no longer receive grace LSAs from the restarting device or when the topology of the network changes, the helper routers also resume normal operation.

Beginning with Junos OS Release 11.4, you can configure restart signaling-based helper mode for OSPFv2 graceful restart configurations. The Junos OS implementation is based on RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*, RFC 4812, *OSPF Restart Signaling*, and RFC 4813, *OSPF Link-Local Signaling*. In restart signaling-based helper mode implementations, the restarting device informs its restart status to its neighbors only after the restart is complete. When the restart is complete, the restarting device sends hello messages to its helper routers with the restart signal (RS) bit set in the hello packet header. When a helper router receives a hello packet with the RS bit set in the header, the helper router returns a hello message to the restarting device. The reply hello message from the helper router contains the ResyncState flag and the ResyncTimeout timer that enable the restarting device to keep track of the helper routers that are syncing up with it. When all helpers complete the synchronization, the restarting device exits the restart mode.

NOTE: Restart signaling-based graceful restart helper mode is not supported for OSPFv3 configurations.

Planned and Unplanned Graceful Restart

OSPF supports two types of graceful restart: planned and unplanned. During a planned restart, the restarting routing device informs the neighbors before restarting. The neighbors act as if the routing device is still within the network topology, and continue forwarding traffic to the restarting routing device. A grace period is set to specify when the neighbors should consider the restarting routing device as part of the topology. During an unplanned restart, the routing device restarts without warning.

Example: Configuring Graceful Restart for OSPF

This example shows how to configure graceful restart specifically for OSPF.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

Graceful restart enables a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition. During a graceful restart, the restarting routing device and its neighbors continue forwarding packets without disrupting network performance. By default, graceful restart is disabled. You can globally enable graceful restart for all routing protocols by including the **graceful-restart** statement at the **[edit routing-options]** hierarchy level, or you can enable graceful restart specifically for OSPF by including the **graceful-restart** statement at the **[edit protocols (ospf|ospf3)]** hierarchy level.

The first example shows how to enable graceful restart and configure the optional settings for the grace period interval. In this example, interfaces **fe-1/1/1** and **fe-1/1/2** are in OSPF area 0.0.0.0, and you configure those interfaces for graceful restart. The grace period interval for OSPF graceful restart is determined as equal to or less than the sum of the **notify-duration** time interval and the **restart-duration** time interval. The grace period is the number of seconds that the routing device's neighbors continue to advertise the routing device as fully adjacent, regardless of the connection state between the routing device and its neighbors.

The **notify-duration** statement configures how long (in seconds) the routing device notifies helper routers that it has completed graceful restart by sending purged grace link-state advertisements (LSAs) over all interfaces. By default, the routing device sends grace LSAs for 30 seconds. The range is from 1 through 3600 seconds.

The **restart-duration** statement configures the amount of time the routing device waits (in seconds) to complete reacquisition of OSPF neighbors from each area. By default, the routing device allows 180 seconds. The range is from 1 through 3600 seconds.

The second example shows how to disable graceful restart for OSPF by including the **disable** statement.

Configuration

Enabling Graceful Restart for OSPF

CLI Quick Configuration

To quickly enable graceful restart for OSPF, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
set interfaces fe-1/1/2 unit 0 family inet address 10.0.0.5
set protocols ospf area 0.0.0.0 interface fe-1/1/1
set protocols ospf area 0.0.0.0 interface fe-1/1/2
set routing-options graceful-restart
set protocols ospf graceful-restart restart-duration 190
set protocols ospf graceful-restart notify-duration 40
```

Step-by-Step Procedure

To enable graceful restart for OSPF:

1. Configure the interfaces.

   NOTE: For OSPFv3, use IPv6 addresses.

   ```
   [edit]
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.5
   ```

2. Configure OSPF on the interfaces.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/1
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/2
   ```

3. Configure graceful restart globally

```
[edit]
user@host#edit routing-options graceful-restart
```

4. Configure OSPF graceful restart.

```
[edit]
user@host# edit protocols ospf graceful-restart
```

5. (Optional) Configure the restart duration time.

```
[edit protocols ospf graceful-restart]
user@host# set restart-duration 190
```

6. (Optional) Configure the notify duration time.

```
[edit protocols ospf graceful-restart]
user@host# set notify-duration 40
```

7. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf graceful-restart]
user@host# commit
```

Results Confirm your configuration by entering the **show interfaces** and **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
fe-1/1/1 {
  unit 0 {
    family inet {
      address 10.0.0.4/32;
    }
  }
}
fe-1/1/2 {
  unit 0 {
    family inet {
      address 10.0.0.5/32;
    }
  }
}
user@host# show protocols ospf
graceful-restart {
  restart-duration 190;
  notify-duration 40;
}
area 0.0.0.0 {
  interface fe-1/1/1.0;
  interface fe-1/1/2.0;
}
```

To confirm an OSPFv3 configuration, enter the **show interfaces** and the **show protocols ospf3** commands.

Disabling Graceful Restart for OSPF

CLI Quick Configuration

To quickly disable graceful restart for OSPF, copy the following command and paste it into the CLI.

```
[edit]
user@host# set protocols ospf graceful-restart disable
```

Step-by-Step Procedure

To disable graceful restart for OSPF:

1. Disable graceful restart for the OSPF protocol only.

   This command does not affect the global graceful restart configuration setting.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf graceful-restart disable
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
graceful-restart disable;
```

To confirm an OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

- Verifying the OSPF Graceful Restart Configuration on page 224
- Verifying Graceful Restart Status on page 225

Verifying the OSPF Graceful Restart Configuration

Purpose

Verify information about your OSPF graceful restart configuration.

Action

From operational mode, enter the **show ospf overview** command for OSPFv2. Enter the **show ospf3 overview** command for OSPFv3.

Meaning

The Restart field displays the status of graceful restart as either enabled or disabled. The Restart duration field displays how much time the restarted routing device requires to complete reacquisition of OSPF neighbors. The Restart grace period field displays how much time the neighbors should consider the restarted routing device as part of the topology.

Verifying Graceful Restart Status

Purpose Verify the status of graceful restart.

Action From operational mode, enter the **show route instance detail** command.

Meaning The Restart State field displays Pending if the restart has not been completed or Complete if the restart has finished. The Path selection timeout field indicates the amount of time remaining until graceful restart is declared complete. There is a more detailed Restart State field that displays a list of protocols that have or have not yet completed graceful restart for the specified routing table.

Example: Configuring the Helper Capability Mode for OSPFv2 Graceful Restart

This example shows how to disable and reenable the helper mode capability for OSPFv2 graceful restart.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

The OSPF graceful restart helper capability assists a neighboring routing device attempting a graceful restart. By default, the helper capability is globally enabled when you start the routing platform. This means that the helper capability is enabled when you start OSPF, even if graceful restart is not globally enabled or specifically enabled for OSPF. You can further modify your graceful restart configuration to disable the helper capability.

Beginning with Junos OS Release 11.4, you can configure restart signaling-based helper mode for OSPFv2 graceful restart configurations. Both the standard and restart signaling-based helper modes are enabled by default.

In the first example, interfaces **fe-1/1/1** and **fe-1/1/2** are in OSPFv2 area 0.0.0.0, and you configure those interfaces for graceful restart. You then disable the standard OSPFv2 graceful restart helper capability by including the **helper-disable standard** statement. This configuration is useful if you have an environment that contains other vendor equipment that is configured for restart signaling-based graceful restart.

NOTE: The **helper-disable** statement and the **no-strict-lsa-checking** statement cannot be configured at the same time. If you attempt to configure both statements at the same time, the routing device displays a warning message when you enter the **show protocols ospf** command.

The second example shows how to reenable the standard OSPFv2 restart helper capability that you disabled in the first example.

Configuration

- Disabling Helper Mode for OSPFv2 on page 226
- Reenabling Helper Mode for OSPFv2 on page 227

Disabling Helper Mode for OSPFv2

CLI Quick Configuration

To quickly enable graceful restart for OSPFv2 with helper mode disabled, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
set interfaces fe-1/1/2 unit 0 family inet address 10.0.0.5
set protocols ospf area 0.0.0.0 interface fe-1/1/1
set protocols ospf area 0.0.0.0 interface fe-1/1/2
set protocols ospf graceful-restart helper-disable standard
```

Step-by-Step Procedure

To enable graceful restart for OSPFv2 with helper mode disabled:

1. Configure the interfaces.

   ```
   [edit]
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.5
   ```

2. Configure OSPFv2 on the interfaces

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/1
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/2
   ```

3. Disable the OSPFv2 graceful restart helper capability.
   If you disable the OSPFv2 graceful restart helper capability, you cannot disable strict LSA checking.

   ```
   [edit]
   ```

```
user@host# set protocols ospf graceful-restart helper-disable standard
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Results Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
fe-1/1/1 {
  unit 0 {
    family inet {
      address 10.0.0.4/32;
    }
  }
}
fe-1/1/2 {
  unit 0 {
    family inet {
      address 10.0.0.5/32;
    }
  }
}
user@host# show protocols ospf
graceful-restart {
  helper-disable {
    standard;
  }
}
area 0.0.0.0 {
  interface fe-1/1/1.0;
  interface fe-1/1/2.0;
}
```

Reenabling Helper Mode for OSPFv2

CLI Quick Configuration To quickly reenable standard helper-mode for OSPFv2, copy the following command and paste it into the CLI.

```
[edit]
delete protocols ospf graceful-restart helper-disable standard
```

NOTE: To reenable restart signaling-based helper mode, include the **restart-signaling** statement. To reenable both standard and restart signaling-based helper mode, include the **both** statement.

Step-by-Step Procedure To reenable standard helper mode for OSPFv2:

1. Delete the standard helper-mode statement from the OSPFv2 configuration.

[edit]
user@host# **delete protocols ospf graceful-restart helper-disable standard**

2. If you are done configuring the device, commit the configuration.

[edit]
user@host# **commit**

Results After you reenable standard helper mode, the **show protocols ospf** command no longer displays the graceful restart configuration.

Verification

Confirm that the configuration is working properly.

Verifying the OSPFv2 Graceful Restart Configuration

Purpose Verify information about your OSPFv2 graceful restart configuration. The Restart field displays the status of graceful restart as either enabled or disabled, the Graceful restart helper mode field displays the status of the standard helper mode capability as enabled or disabled, and the Restart-signaling helper mode field displays the status of the restart signaling-based helper mode as enabled or disabled. By default, both standard and restart signaling-based helper modes are enabled.

Action From operational mode, enter the **show ospf overview** command.

Verifying Graceful Restart Status

Purpose Verify the status of graceful restart. The Restart State field displays Pending if the restart has not completed, or Complete if the restart has finished. The Path selection timeout field indicates the amount of time remaining until graceful restart is declared complete. There is a more detailed Restart State field that displays a list of protocols that have completed graceful restart or have not yet completed graceful restart for the specified routing table.

Action From operational mode, enter the **show route instance detail** command.

Example: Configuring the Helper Capability Mode for OSPFv3 Graceful Restart

This example shows how to disable and reenable the helper mode capability for OSPFv3 graceful restart.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

The OSPF graceful restart helper capability assists a neighboring routing device attempting a graceful restart. By default, the helper capability is globally enabled when you start the routing platform. This means that the helper capability is enabled when you start OSPF, even if graceful restart is not globally enabled or specifically enabled for OSPF. You can further modify your graceful restart configuration to disable the helper capability.

In the first example, interfaces **fe-1/1/1** and **fe-1/1/2** are in OSPFv3 area 0.0.0.0, and you configure those interfaces for graceful restart. You then disable the OSPFv3 graceful restart helper capability by including the **helper-disable** statement.

NOTE: The **helper-disable** statement and the **no-strict-lsa-checking** statement cannot be configured at the same time. If you attempt to configure both statements at the same time, the routing device displays a warning message when you enter the **show protocols ospf** command.

The second example shows how to reenable the OSPFv3 restart helper capability that you disabled in the first example.

Configuration

Disabling Helper Mode for OSPFv3

CLI Quick Configuration

To quickly enable graceful restart for OSPFv3 with helper mode disabled, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces fe-1/1/1 unit 0 family inet6 address 2002:0a00:0004::
set interfaces fe-1/1/2 unit 0 family inet6 address 2002:0a00:0005::
set protocols ospf3 area 0.0.0.0 interface fe-1/1/1
set protocols ospf3 area 0.0.0.0 interface fe-1/1/2
set protocols ospf3 graceful-restart helper-disable
```


Step-by-Step Procedure

To enable graceful restart for OSPFv3 with helper mode disabled:

1. Configure the interfaces.

   ```
   [edit]
   user@host# set interfaces fe-1/1/1 unit 0 family inet6 address 2002:0a00:0004::
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 2002:0a00:0005::
   ```

2. Configure OSPFv3 on the interfaces

   ```
   [edit]
   user@host# set protocols ospf3 area 0.0.0.0 interface fe-1/1/1
   user@host# set protocols ospf3 area 0.0.0.0 interface fe-1/1/2
   ```

3. Disable the OSPFv3 graceful restart helper capability.
   If you disable the OSPFv3 graceful restart helper capability, you cannot disable strict LSA checking.

   ```
   [edit]
   user@host# set protocols ospf3 graceful-restart helper-disable
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf3** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
fe-1/1/1 {
  unit 0 {
    family inet6 {
      address 2002:0a00:0004::/128;
    }
  }
}
fe-1/1/2 {
  unit 0 {
    family inet6 {
      address 2002:0a00:0005::/128;
    }
  }
}
user@host# show protocols ospf3
graceful-restart {
  helper-disable;
}
area 0.0.0.0 {
  interface fe-1/1/1.0;
  interface fe-1/1/2.0;
}
```


Reenabling Helper Mode for OSPFv3

CLI Quick Configuration

To quickly reenable helper-mode for OSPFv3, copy the following command and paste it into the CLI.

```
[edit]
delete protocols ospf3 graceful-restart helper-disable
```

Step-by-Step Procedure

To reenable helper mode for OSPFv3:

1. Delete the standard helper-mode statement from the OSPFv3 configuration.

   ```
   [edit]
   user@host# delete protocols ospf3 graceful-restart helper-disable
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results

After you reenable standard helper mode, the **show protocols ospfs** command no longer displays the graceful restart configuration.

Verification

Confirm that the configuration is working properly.

- Verifying the OSPFv3 Graceful Restart Configuration on page 231
- Verifying Graceful Restart Status on page 231

Verifying the OSPFv3 Graceful Restart Configuration

Purpose

Verify information about your OSPFv3 graceful restart configuration. The Restart field displays the status of graceful restart as either enabled or disabled, and the Helper mode field displays the status of the helper mode capability as either enabled or disabled.

Action

From operational mode, enter the **show ospf3 overview** command.

Verifying Graceful Restart Status

Purpose

Verify the status of graceful restart. The Restart State field displays Pending if the restart has not completed, or Complete if the restart has finished. The Path selection timeout field indicates the amount of time remaining until graceful restart is declared complete. There is a more detailed Restart State field that displays a list of protocols that have completed graceful restart or have not yet completed graceful restart for the specified routing table.

Action

From operational mode, enter the **show route instance detail** command.

Example: Disabling Strict LSA Checking for OSPF Graceful Restart

This example shows how to disable strict link-state advertisement (LSA) checking for OSPF graceful restart.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

You can disable strict LSA checking to prevent the termination of graceful restart by a helping router. You might configure this option for interoperability with other vendor devices. The OSPF graceful restart helper capability must be enabled if you disable strict LSA checking. By default, LSA checking is enabled.

In this example, interfaces **fe-1/1/1** and **fe-1/1/2** are in OSPF area 0.0.0.0, and you configure those interfaces for graceful restart. You then disable strict LSA checking by including the **no-strict-lsa-checking** statement.

NOTE: The **helper-disable** statement and the **no-strict-lsa-checking** statement cannot be configured at the same time. If you attempt to configure both statements at the same time, the routing device displays a warning message when you enter the **show protocols ospf** command.

Configuration

CLI Quick Configuration

To quickly enable graceful restart for OSPF with strict LSA checking disabled, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
set interfaces fe-1/1/2 unit 0 family inet address 10.0.0.5
```

```
set protocols ospf area 0.0.0.0 interface fe-1/1/1
set protocols ospf area 0.0.0.0 interface fe-1/1/2
set protocols ospf graceful-restart no-strict-lsa-checking
```

Step-by-Step Procedure

To enable graceful restart for OSPF with strict LSA checking disabled:

1. Configure the interfaces.

   NOTE: For OSPFv3, use IPv6 addresses.

   ```
   [edit]
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.4
   user@host# set interfaces fe-1/1/1 unit 0 family inet address 10.0.0.5
   ```

2. Configure OSPF on the interfaces

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/1
   user@host# set protocols ospf area 0.0.0.0 interface fe-1/1/2
   ```

3. Disable strict LSA checking.
   If you disable the strict LSA checking, OSPF graceful restart helper capability must be enabled (which is the default behavior).

   ```
   [edit]
   user@host# set protocols ospf graceful-restart no-strict-lsa-checking
   ```

4. If you are done configuring the device, commit the configuration.

   ```
   [edit ]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
fe-1/1/1 {
  unit 0 {
    family inet {
      address 10.0.0.4/32;
    }
  }
}
fe-1/1/2 {
  unit 0 {
    family inet {
      address 10.0.0.5/32;
```

```
        }
      }
    }
    user@host# show protocols ospf
    graceful-restart {
      no-strict-lsa-checking;
    }
    area 0.0.0.0 {
      interface fe-1/1/1.0;
      interface fe-1/1/2.0;
    }
```

To confirm your OSPFv3 configuration, enter the **show interfaces** and the **show protocols ospf3** commands.

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Graceful Restart Configuration

Purpose Verify information about your OSPF graceful restart configuration. The Restart field displays the status of graceful restart as either enabled or disabled.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** command for OSPFv3.

Verifying Graceful Restart Status

Purpose Verify the status of graceful restart. The Restart State field displays Pending if the restart has not completed, or Complete if the restart has finished. The Path selection timeout field indicates the amount of time remaining until graceful restart is declared complete. There is a more detailed Restart State field that displays a list of protocols that have completed graceful restart or have not yet completed graceful restart for the specified routing table.

Action From operational mode, enter the **show route instance detail** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14
- *Graceful Restart Concepts* in the *Junos OS High Availability Library for Routing Devices*

Examples: Configuring Loop-Free Alternate Routes for OSPF

Loop-Free Alternate Routes for OSPF Overview

Support for OSPF loop-free alternate routes essentially adds IP fast-reroute capability for OSPF. Junos OS precomputes loop-free backup routes for all OSPF routes. These backup routes are preinstalled in the Packet Forwarding Engine, which performs a local repair and implements the backup path when the link for a primary next hop for a particular route is no longer available. With local repair, the Packet Forwarding Engine can correct a path failure before it receives precomputed paths from the Routing Engine. Local repair reduces the amount of time needed to reroute traffic to less than 50 milliseconds. In contrast, global repair can take up to 800 milliseconds to compute a new route. Local repair enables traffic to continue to be routed using a backup path until global repair is able to calculate a new route.

A loop-free path is one that does not forward traffic back through the routing device to reach a given destination. That is, a neighbor whose shortest path first to the destination traverses the routing device that is not used as a backup route to that destination. To determine loop-free alternate paths for OSPF routes, Junos OS runs shortest-path-first (SPF) calculations on each one-hop neighbor. You can enable support for alternate loop-free routes on any OSPF interface. Because it is common practice to enable LDP on an interface for which OSPF is already enabled, this feature also provides support for LDP label-switched paths (LSPs.)

NOTE: **If you enable support for alternate loop-free routes on an interface configured for both LDP and OSPF, you can use the traceroute command to trace the active path to the primary next hop.**

The level of backup coverage available through OSPF routes depends on the actual network topology and is typically less than 100 percent for all destinations on any given routing device. You can extend backup coverage to include RSVP LSP paths.

Junos OS provides two mechanisms for route redundancy for OSPF through alternate loop-free routes:

- Link protection—Offers per-link traffic protection. Use link protection when you assume that only a single link might become unavailable but that the neighboring node on the primary path would still be available through another interface.
- Node-link protection—Establishes an alternate path through a different routing device altogether. Use node-link protection when you assume that access to a node is lost when a link is no longer available. As a result, Junos OS calculates a backup path that avoids the primary next-hop routing device.

When you enable link protection or node-link protection on an OSPF interface, Junos OS creates an alternate path to the primary next hop for all destination routes that traverse a protected interface.

Configuring Link Protection for OSPF

You can configure link protection for any interface for which OSPF is enabled. When you enable link protection, Junos OS creates an alternate path to the primary next hop for all destination routes that traverse a protected interface. Use link protection when you assume that only a single link might become unavailable but that the neighboring node would still be available through another interface.

Link protection is supported on:

- OSPFv2 and OSPFv3 interfaces
- OSPFv3 unicast realms
- OSPFv2 unicast topologies, except for multicast topologies
- All routing instances supported by OSPFv2 and OSPFv3
- Logical systems

To configure link protection for an OSPF interface:

- Include the **link-protection** statement at the **[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*]** hierarchy level.

BEST PRACTICE: **When you configure link protection for OSPF, you must also configure a per-packet load-balancing routing policy to ensure that the routing protocol process installs all the next hops for a given route in the routing table.**

In the following example, the OSPF interface **so-0/0/0.0** in area 0.0.0.0 is configured for link protection. If a link for a destination route that traverses this interface becomes unavailable, Junos OS creates a loop-free backup path through another interface on the neighboring node, thus avoiding the link that is no longer available.

```
[edit]
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0 {
        link-protection;
      }
    }
  }
}
```

Configuring Node-Link Protection for OSPF

You can configure node-link protection on any interface for which OSPF is enabled. Node-link protection establishes an alternative path through a different routing device altogether for all destination routes that traverse a protected interface. Node-link protection assumes that the entire routing device, or node, has failed. Junos OS therefore calculates a backup path that avoids the primary next-hop routing device.

Node-link protection is supported on:

- OSPFv2 and OSPFv3 interfaces
- OSPFv3 unicast realms
- OSPFv2 unicast topologies
- All routing instances supported by OSPFv2 and OSPFv3
- Logical systems

To configure node-link protection for an OSPF interface:

- Include the **node-link-protection** statement at the **[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*]** hierarchy level.

BEST PRACTICE: **You must also configure a per-packet load-balancing routing policy to ensure that the routing protocol process installs all the next hops for a given route in the routing table.**

In the following example, the OSPF interface **so-0/0/0.0** in area 0.0.0.0 is configured for node-link protection. If a link for a destination route that traverses this interface becomes unavailable, Junos OS creates a loop-free backup path through a different routing device altogether, thus avoiding the primary next-hop routing device.

```
[edit]
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0 {
        node-link-protection;
      }
    }
  }
}
```

Excluding an OSPF Interface as a Backup for a Protected Interface

By default, all OSPF interfaces that belong to the default instance or to a specific routing instance are eligible as a backup interface for interfaces configured with link-protection or node-link protection. You can specify that any OSPF interface be excluded from functioning as a backup interface to protected interfaces.

To exclude an OSPF interface as a backup interface for a protected interface:

- Include the **no-eligible-backup** statement at the **[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*]** hierarchy level.

In the following example, interface **so-0/0/0.0** has been configured to prohibit backup traffic for traffic destined for a protected interface. This means that if a neighboring next-hop path or node for a protected interface fails, interface **so-0/0/0.0** cannot be used to transmit traffic to a backup path.

```
[edit]
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0 {
        no-eligible-backup;
      }
    }
  }
}
```

Configuring Backup SPF Options for Protected OSPF Interfaces

By default, if at least one OSPF interface is configured for link-protection or node-link protection, Junos OS calculates backup next hops for all the topologies in an OSPF instance. You can configure the following backup shortest-path-first (SPF) options to override the default behavior:

- Disable the calculation of backup next hops for an OSPF instance or a specific topology in an instance.
- Prevent the installation of backup next hops in the routing table or the forwarding table for an OSPF instance or a specific topology in an instance.
- Limit the calculation of backup next hops to a subset of paths as defined in RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*.

You can disable the backup SPF algorithm for an OSPF instance or specific topology in an instance. Doing so prevents the calculation of backup next hops for that OSPF instance or topology.

To disable the calculation of backup next hops for an OSPF instance or topology:

- Include the **disable** statement at the **[edit protocols (ospf | ospf3) backup-spf-options]** or **[edit protocols ospf backup-spf-options topology *topology-name*]** hierarchy level.

In the following example, the calculation of backup next hops is disabled for the OSPF topology **voice**:

```
[edit]
protocols {
    ospf {
        topology voice {
            backup-spf-options {
                disable;
            }
        }
    }
}
```

You can configure the routing device to prevent the installation of backup next hops in the routing table or the forwarding table for an OSPF instance, or a specific topology in an OSPF instance. The SPF algorithm continues to calculate backup next hops, but they are not installed.

To prevent the routing device from installing backup next hops in the routing table or the forwarding table:

- Include the **no-install** statement at the **[edit protocols (ospf | ospf3) backup-spf-options]** or the **[edit protocols ospf topology *topology-name*]** hierarchy level.

In the following example, backup next hops for the OSPF topology **voice** are not installed in the routing table or forwarding table. Any calculated backup next hops for other OSPF instances or topologies continue to be installed.

```
[edit]
protocols {
    ospf {
        topology voice {
            backup-spf-options {
                no-install;
            }
        }
    }
}
```

You can limit the calculation of backup next hops to *downstream paths*, as defined in RFC 5286. You can specify for Junos OS to use only downstream paths as backup next hops for protected interfaces for an OSPF instance or a specific topology in an OSPF instance. In a downstream path, the distance from the backup neighbor to the destination must be smaller than the distance from the calculating routing device to the destination. Using only downstream paths as loop-free alternate paths for protected interfaces ensures that these paths do not result in microloops. However, you might experience less than optimal backup coverage for your network.

To limit the calculation of backup next hops to downstream paths:

- Include the **downstream-paths-only** statement at the **[edit protocols (ospf | ospf3) backup-spf-options]** or **[edit protocols ospf backup-spf-options topology *topology-name*]** hierarchy level.

In the following example, only downstream paths are calculated as backup next hops for the topology **voice**:

```
[edit]
protocols {
  ospf {
    topology voice {
      backup-spf-options {
        downstream-paths-only;
      }
    }
  }
}
```

Configuring RSVP Label-Switched Paths as Backup Paths for OSPF

When configuring an OSPF interface for link protection or node-link protection, relying on the shortest-path-first (SPF) calculation of backup paths for one-hop neighbors might result in less than 100 percent backup coverage for a specific network topology. You can enhance coverage of OSPF and LDP label-switched-paths (LSPs) by configuring RSVP LSPs as backup paths.

When configuring an LSP, you must specify the IP address of the egress router.

NOTE: RSVP LSPs can be used as backup paths only for the default topology for OSPFv2 and not for a configured topology. Additionally, RSVP LSP cannot be used a backup paths for non-default instances for OSPFv2 or OSPFv3.

To configure a specific RSVP LSP as a backup path:

1. Include the **backup** statement at the **[edit protocols mpls labeled-switched-path *lsp-name*]** hierarchy level.
2. Specify the address of the egress router by including the **to *ip-address*** statement at the **[edit protocols mpls label-switched-path]** hierarchy level.

In the following example, the RSVP LSP **f-to-g** is configured as a backup LSP for protected OSPF interfaces. The egress router is configured with the IP address **192.168.1.4**.

```
[edit]
protocols {
  mpls {
    label-switched-path f-to-g {
      to 192.168.1.4;
      backup;
    }
  }
```

```
}
```

Related Documentation

- OSPF Configuration Overview on page 14

CHAPTER 12

OSPF Traffic Engineering Configuration

Examples: Configuring OSPF Traffic Engineering

OSPF Support for Traffic Engineering

Traffic engineering allows you to control the path that data packets follow, bypassing the standard routing model, which uses routing tables. Traffic engineering moves flows from congested links to alternate links that would not be selected by the automatically computed destination-based shortest path.

To help provide traffic engineering and MPLS with information about network topology and loading, extensions have been added to the Junos OS implementation of OSPF. When traffic engineering is enabled on the routing device, you can enable OSPF traffic engineering support. When you enable traffic engineering for OSPF, the shortest-path-first (SPF) algorithm takes into account the various label-switched paths (LSPs) configured under MPLS and configures OSPF to generate opaque link-state advertisements (LSAs) that carry traffic engineering parameters. The parameters are used to populate the traffic engineering database. The traffic engineering database is used exclusively for calculating explicit paths for the placement of LSPs across the physical topology. The Constrained Shortest Path First (CSPF) algorithm uses the traffic engineering database to compute the paths that MPLS LSPs take. RSVP uses this path information to set up LSPs and to reserve bandwidth for them.

By default, traffic engineering support is disabled. To enable traffic engineering, include the **traffic-engineering** statement. You can also configure the following OSPF traffic engineering extensions:

- **advertise-unnumbered-interfaces**—(OSPFv2 only) Advertises the link-local identifier in the link-local traffic engineering LSA packet. This statement must be included on both ends of an unnumbered link to allow an ingress LER to update the link in its traffic engineering database and use it for CSPF calculations. The link-local identifier is then used by RSVP to signal unnumbered interfaces as defined in RFC 3477, *Signalling Unnumbered Links in Resource Reservation Protocol - Traffic Engineering (RSVP-TE)*.
- **credibility-protocol-preference**—(OSPFv2 only) Assigns a credibility value to OSPF routes in the traffic engineering database. By default, Junos OS prefers IS-IS routes in the traffic engineering database over other interior gateway protocol (IGP) routes even if the routes of another IGP are configured with a lower, that is, more preferred, preference value. The traffic engineering database assigns a credibility value to each IGP and prefers the routes of the IGP with the highest credibility value. In Junos OS Release 9.4 and later, you can configure OSPF to take protocol preference into account to determine the traffic engineering database credibility value. When protocol preference is used to determine the credibility value, IS-IS routes are not automatically preferred by the traffic engineering database, depending on your configuration.
- **ignore-lsp-metrics**—Ignores RSVP LSP metrics in OSPF traffic engineering shortcut calculations or when you configure LDP over RSVP LSPs. This option avoids mutual dependency between OSPF and RSVP, eliminating the time period when the RSVP metric used for tunneling traffic is not up to date. In addition, If you are using RSVP for traffic engineering, you can run LDP simultaneously to eliminate the distribution of external routes in the core. The LSPs established by LDP are tunneled through the LSPs established by RSVP. LDP effectively treats the traffic-engineered LSPs as single hops.
- **multicast-rpf-routes**—(OSPFv2 only) Installs unicast IPv4 routes (not LSPs) in the multicast routing table (**inet.2**) for multicast reverse-path forwarding (RPF) checks. The **inet.2** routing table consists of unicast routes used for multicast RPF lookup. RPF is an antispoofing mechanism used to check if the packet is coming in on an interface that is also sending data back to the packet source.
- **no-topology**—(OSPFv2 only) To disable the dissemination of link-state topology information. If disabled, traffic engineering topology information is no longer distributed within the OSPF area.
- **shortcuts**—Configures OSPF to use MPLS LSPs as shortcut next hops. By default, shortcut routes calculated through OSPFv2 are installed in the **inet.3** routing table, and shortcut routes calculated through OSPFv3 are installed in the **inet6.3** routing table.

NOTE: Whenever possible, use OSPF IGP shortcuts configured at the **[edit protocols mpls traffic-engineering bgp-igp]** hierarchy level instead of traffic engineering shortcuts configured at the **[edit protocols (ospf | ospf3) traffic-engineering shortcuts]** hierarchy level.

If you configure OSPF IGP shortcuts, **inet.3** routes are moved into the **inet.0** routing table. In addition, you can verify the data path using **ping** or **traceroute** commands since the ping and traceroute packets get tunneled into the LSP. In case of a VPN enabled device, we recommend using **[edit protocols mpls traffic-engineering bgp-igp-both-ribs]** because BGP next-hop resolution for VPN prefixes relies on entries in the **inet.3** table.

If you configure traffic engineering shortcuts, OSPF treats the MPLS LSP as a candidate next hop and installs the routes in the **inet.3** (for OSPFv2) and **inet6.3** (for OSPFv3) routing tables. The only use for these tables is to allow BGP to perform next-hop resolution. In addition, you cannot verify the data path of these routes using **ping or traceroute** commands because the ping and traceroute packets get tunneled into the LSP.

- **lsp-metric-info-summary**—Advertises the LSP metric in summary LSAs to treat the LSP as a link. This configuration allows other routing devices in the network to use this LSP. To accomplish this, you need to configure MPLS and OSPF traffic engineering to advertise the LSP metric in summary LSAs.

When you enable traffic engineering on the routing device, you can also configure an OSPF metric that is used exclusively for traffic engineering. The traffic engineering metric is used for information injected into the traffic engineering database. Its value does not affect normal OSPF forwarding.

CAUTION: When the OSPF traffic engineering configuration is considerably modified, the routing table entries are deleted and the routing table is recreated. Changes to configuration that can cause this behavior include enabling or disabling:

- Traffic engineering shortcuts
- IGP shortcuts
- LDP tunneling
- Multiprotocol LSP
- Advertise summary metrics
- Multicast RPF routes

Example: Enabling OSPF Traffic Engineering Support

This example shows how to enable OSPF traffic engineering support to advertise the label-switched path (LSP) metric in summary link-state advertisements (LSAs).

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure BGP per your network requirements. See the *Junos OS Routing Protocols Library for Routing Devices*
- Configure MPLS per your network requirements. See the *Junos OS MPLS Applications Library for Routing Devices*.

Overview

You can configure OSPF to treat an LSP as a link and have other routing devices in the network use this LSP. To accomplish this, you configure MPLS and OSPF traffic engineering to advertise the LSP metric in summary LSAs.

In this example, there are four routing devices in area 0.0.0.0, and you want OSPF to treat the LSP named R1-to-R4 that goes from the ingress Device R1 to the egress Device R4 as a link.

For OSPF, you enable traffic engineering on all four routing devices in the area by including the **traffic-engineering** statement. This configuration ensures that the shortest-path-first (SPF) algorithm takes into account the LSPs configured under MPLS and configures OSPF to generate LSAs that carry traffic engineering parameters. You further ensure that OSPF uses the MPLS LSP as the next hop and advertises the LSP metric in summary LSAs, by including the optional **shortcuts lsp-metric-into-summary** statement on the ingress Device R1.

For MPLS, you enable traffic engineering so that MPLS performs traffic engineering on both BGP and IGP destinations by including the **traffic-engineering bgp-igp** statement, and you include the LSP named R1-to-R4 by including the **label-switched-path *lsp-path-name* to *address*** statement on the ingress Device R1. The address specified in the **to** statement on the ingress Device R1 must match the router ID of the egress Device R4 for the LSP to function as a direct link to the egress routing device and to be used as input to the OSPF SPF calculations. In this example, the router ID of the egress Device R4 is 10.0.0.4.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

CLI Quick Configuration

To quickly enable OSPF traffic engineering support to advertise the LSP metric in summary LSAs, copy the following commands and paste them into the CLI.

Configuration on R1:

```
[edit]
set routing-options router-id 10.0.0.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf traffic-engineering shortcuts lsp-metric-into-summary
set protocols mpls traffic-engineering bgp-igp
set protocols mpls label-switched-path R1-to-R4 to 10.0.0.4
```

Configuration on R2:

```
[edit]
set routing-options router-id 10.0.0.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf traffic-engineering
```

Configuration on R3:

```
[edit]
set routing-options router-id 10.0.0.3
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf traffic-engineering
```

Configuration on R4:

```
[edit]
set routing-options router-id 10.0.0.4
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf traffic-engineering
```

Step-by-Step Procedure

To enable OSPF traffic engineering support to advertise LSP metrics in summary LSAs:

1. Configure the router ID.

   ```
   [edit]
   user@R1# set routing-options router-id 10.0.0.1
   ```

   ```
   [edit]
   user@R2# set routing-options router-id 10.0.0.2
   ```

   ```
   [edit]
   user@R3# set routing-options router-id 10.0.0.3
   ```

   ```
   [edit]
   user@R4# set routing-options router-id 10.0.0.4
   ```

2. Configure the OSPF area and add the interfaces.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   [edit]
   user@R1# **set protocols ospf area 0.0.0.0 interface all**
   user@R1# **set protocols ospf area 0.0.0.0 interface fxp0.0 disable**

   [edit]
   user@R2# **set protocols ospf area 0.0.0.0 interface all**
   user@R2# **set protocols ospf area 0.0.0.0 interface fxp0.0 disable**

   [edit]
   user@R3# **set protocols ospf area 0.0.0.0 interface all**
   user@R3# **set protocols ospf area 0.0.0.0 interface fxp0.0 disable**

   [edit]
   user@R4# **set protocols ospf area 0.0.0.0 interface all**
   user@R4# **set protocols ospf area 0.0.0.0 interface fxp0.0 disable**

3. Enable OSPF traffic engineering.

   [edit]
   user@R1 **set protocols ospf traffic-engineering shortcuts** lsp-metric-into-summary

   [edit]
   user@R2 **set protocols ospf** traffic-engineering

   [edit]
   user@R3 **set protocols ospf traffic-engineering**

   [edit]
   user@R4 **set protocols ospf traffic-engineering**

4. On Device R1, configure MPLS traffic engineering.

   [edit]
   user@R1 **set protocol mpls traffic-engineering bgp-igp**
   user@R1 **set protocols mpls label-switched-path R1-to-R4 to 10.0.0.4**

5. If you are done configuring the devices, commit the configuration.

   [edit]
   user@host# **commit**

Results Confirm your configuration by entering the **show routing-options**, **show protocols ospf**, and **show protocols mpls** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Output for R1:

```
user@host# show routing-options
router-id 10.0.0.1;

user@host# show protocols ospf
  traffic-engineering {
    shortcuts lsp-metric-into-summary;
```



```
    }
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
user@host# show protocols mpls
    traffic-engineering bgp-igp;
    label-switched-path R1-to-R4 {
        to 10.0.0.4;
}
```

Output for R2:

```
user@host# show routing-options
router-id 10.0.0.2;
user@host# show protocols ospf
    traffic-engineering;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
```

Output for R3:

```
user@host# show routing-options
router-id 10.0.0.3;
user@host# show protocols ospf
    traffic-engineering;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
```

Output for R4:

```
user@host# show routing-options
router-id 10.0.0.4;
user@host# show protocols ospf
    traffic-engineering;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
```

To confirm your OSPFv3 configuration, enter the **show routing-options**, **show protocols ospf3**, and **show protocols mpls** commands.

Verification

Confirm that the configuration is working properly.

Verifying the Traffic Engineering Capability for OSPF

Purpose Verify that traffic engineering has been enabled for OSPF. By default, traffic engineering is disabled.

Action From operational mode, enter the **show ospf overview** command for OSPFv2, and enter the **show ospf3 overview** for OSPFv3.

Verifying OSPF Entries in the Traffic Engineering Database

Purpose Verify the OSPF information in the traffic engineering database. The Protocol field displays OSPF and the area from which the information was learned.

Action From operational mode, enter the **show ted database** command.

Verifying That the Traffic Engineering Database Is Learning Node Information from OSPF

Purpose Verify that OSPF is reporting node information. The Protocol name field displays OSPF and the area from which the information was learned.

Action From operational mode, enter the **show ted protocol** command.

Example: Configuring the Traffic Engineering Metric for a Specific OSPF Interface

This example shows how to configure the OSPF metric value used for traffic engineering.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure OSPF for traffic engineering. See "Example: Enabling OSPF Traffic Engineering Support" on page 246

Overview

You can configure an OSPF metric that is used exclusively for traffic engineering. To modify the default value of the traffic engineering metric, include the **te-metric** statement. The OSPF traffic engineering metric does not affect normal OSPF forwarding. By default, the traffic engineering metric is the same value as the OSPF metric. The range is 1 through 65,535.

In this example, you configure the OSPF traffic engineering metric on OSPF interface **fe-0/1/1** in area 0.0.0.0.

Configuration

CLI Quick Configuration

To quickly configure the OSPF traffic engineering metric for a specific interface, copy the following command and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-0/1/1 te-metric 10
```

Step-by-Step Procedure

To configure an OSPF traffic engineering metric for a specific interface used only for traffic engineering:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf area 0.0.0.0
   ```

2. Configure the traffic engineering metric of the OSPF network segments.

   ```
   [edit protocols ospf area 0.0.0.0]
   user@host set interface fe-0/1/1 te-metric 10
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf area 0.0.0.0]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface fe-0/1/1.0 {
    te-metric 10;
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Configured Traffic Engineering Metric

Purpose Verify the traffic engineering metric value. Confirm that Metric field displays the configured traffic engineering metric.

Action From operational mode, enter the **show ted database extensive** command.

Related Documentation

- OSPF Configuration Overview on page 14
- *Junos OS MPLS Applications Library for Routing Devices*

Example: Configuring OSPF Passive Traffic Engineering Mode

OSPF Passive Traffic Engineering Mode

Ordinarily, interior routing protocols such as OSPF are not run on links between autonomous systems. However, for inter-AS traffic engineering to function properly, information about the inter-AS link—in particular, the address on the remote interface—must be made available inside the autonomous system (AS). This information is not normally included either in the external BGP (EBGP) reachability messages or in the OSPF routing advertisements.

To flood this link address information within the AS and make it available for traffic engineering calculations, you must configure OSPF passive mode for traffic engineering on each inter-AS interface. You must also supply the remote address for OSPF to distribute and include it in the traffic engineering database. OSPF traffic engineering mode allows MPLS label-switched paths (LSPs) to dynamically discover OSPF AS boundary routers and to allow routers to establish a traffic engineering LSP across multiple autonomous systems.

Example: Configuring OSPF Passive Traffic Engineering Mode

This example shows how to configure OSPF passive mode for traffic engineering on an inter-AS interface. The AS boundary router link between the EBGP peers must be a directly connected link and must be configured as a passive traffic engineering link.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure BGP per your network requirements. See the *Junos OS Routing Protocols Library for Routing Devices*.
- Configure the LSP per your network requirements. See the *Junos OS MPLS Applications Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29.
- Configure a multiarea OSPF network. See "Example: Configuring a Multiarea OSPF Network" on page 31.

Overview

You can configure OSPF passive mode for traffic engineering on an inter-AS interface. The address used for the remote node of the OSPF passive traffic engineering link must be the same as the address used for the EBGP link. In this example, you configure interface **so-1/1/0** in area 0.0.0.1 as the inter-AS link to distribute traffic engineering information with OSPF within the AS and include the following settings:

- **passive**—Advertises the direct interface addresses on an interface without actually running OSPF on that interface. A passive interface is one for which the address information is advertised as an internal route in OSPF, but on which the protocol does not run.
- **traffic-engineering**—Configures an interface in OSPF passive traffic-engineering mode to enable dynamic discovery of OSPF AS boundary routers. By default, OSPF passive traffic-engineering mode is disabled.
- **remote-node-id**—Specifies the IP address at the far end of the inter-AS link. In this example, the remote IP address is 192.168.207.2.

Configuration

To quickly configure OSPF passive mode for traffic engineering, copy the following command, remove any line breaks, and paste it into the CLI.

```
[edit]
set protocols ospf area 0.0.0.1 interface so-1/1/0 passive traffic-engineering remote-node-id
  192.168.207.2
```

Step-by-Step Procedure

To configure OSPF passive traffic engineering mode:

1. Create an OSPF area.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.1
   ```

2. Configure interface **so-1/1/0** as a passive interface configured for traffic engineering, and specify the IP address at the far end of the inter-AS link.

   ```
   [edit protocols ospf area 0.0.0.1]
   user@host# set interface so-1/1/0 passive traffic-engineering remote-node-id
     192.168.207.2
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.1 {
  interface so-1/1/0.0 {
    passive {
      traffic-engineering {
        remote-node-id 192.168.207.2;
      }
    }
  }
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying the Status of OSPF Interfaces

Purpose

Verify the status of OSPF interfaces. If the interface is passive, the Adj count field is 0 because no adjacencies have been formed. Next to this field, you might also see the word Passive.

Action

From operational mode, enter the **show ospf interface detail** command for OSPFv2, and enter the **show ospf3 interface detail** command for OSPFv3.

Related Documentation

- OSPF Configuration Overview on page 14
- About OSPF Interfaces on page 121

- *Junos OS MPLS Applications Library for Routing Devices*

Example: Advertising Label-Switched Paths into OSPFv2

Advertising Label-Switched Paths into OSPFv2

One main reason to configure label-switched paths (LSPs) in your network is to control the shortest path between two points on the network. You can advertise LSPs into OSPFv2 as point-to-point links so that all participating routing devices can take the LSP into account when performing SPF calculations. The advertisement contains a local address (the **from** address of the LSP), a remote address (the **to** address of the LSP), and a metric with the following precedence:

1. Use the LSP metric defined under OSPFv2.
2. Use the LSP metric configured for the label-switched path under MPLS.
3. If you do not configure any of the above, use the default OSPFv2 metric of 1.

NOTE: If you want an LSP that is announced into OSPFv2 to be used in SPF calculations, there must be a reverse link (that is, a link from the tail end of the LSP to the head end). You can accomplish this by configuring an LSP in the reverse direction and also announcing it in OSPFv2.

Example: Advertising Label-Switched Paths into OSPFv2

This example shows how to advertise LSPs into OSPFv2.

Requirements

Before you begin, configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.

Overview

To advertise an LSP into OSPFv2, you define the LSP and configure OSPFv2 to route traffic using the LSP. By doing this, you can use the LSP to control the shortest path between two points on the network. You might choose to do this if you want to have

OSPF traffic routed along the LSP instead of having OSPF use the default best-effort routing.

In this example, you configure the following to advertise an LSP into OSPFv2:

- BGP

  For all routing devices, configure the local AS number 65000 and define the IBGP group that recognizes the specified BGP systems as peers. All members are internal to the local AS, so you configure an internal group with a full list of peers. You also include the peer AS group, which is the same as the local AS number that you configure.

- MPLS

  For all routing devices, configure the protocol family on each transit logical interface and enable MPLS on all interfaces, except for the management interface (**fxp0.0**). Specify the **mpls** protocol family type.

- RSVP

  For all routing devices, enable RSVP on all interfaces, except for the management interface (**fxp0.0**). You enable RSVP on the devices in this network to ensure that the interfaces can signal the LSP.

- OSPFv2

  For all routing devices, use the loopback address to assign the router ID, administratively group all of the devices into OSPF area 0.0.0.0, add all of the interfaces participating in OSPF to area 0.0.0.0, and disable OSPF on the management interface (**fxp0.0**).

- Label-switched path

  On the ingress routing device R1, which is the beginning (or head end) of the LSP, configure an LSP with an explicit path. The explicit path indicates that the LSP must go to the next specified IP address in the path without traversing other nodes. In this example, you create an LSP named R1-to-R6, and you specify the IP address of the egress routing device R6.

- Advertise the LSP in OSPFv2

  On the ingress routing device R1, you advertise the LSP as a point-to-point link into OSPFv2. You can optionally assign a metric to have the LSP be the more or less preferred path to the destination.

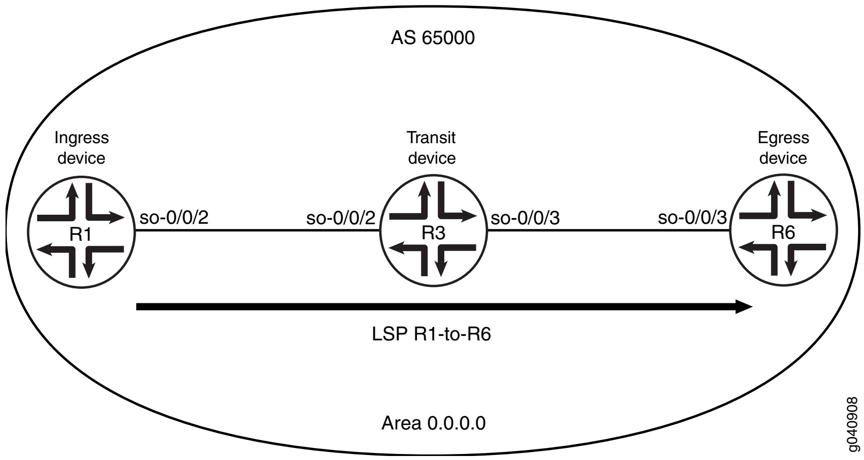
Figure 19 on page 257 shows a sample network topology that consists of the following:

- BGP is configured on all routing devices, with one local autonomous system (AS) 65000 that contains three routing devices:
  - R1—Device R1 is the ingress device with a router ID of 10.0.0.1. Interface **so-0/0/2** connects to Device R3.
  - R3—Device R3 is the transit device with a router ID of 10.0.0.3. Interface **so-0/0/2** connects to Device R1, and interface **so-0/0/3** connects to Device R6.

- R6—Device R6 is the egress device with a router ID of 10.0.0.6. Interface **so-0/0/3** connects to Device R3.

- OSPFv2 is configured on all routing devices.
- MPLS and RSVP are enabled on all routing devices.
- One RSVP-signaled LSP is configured on Device R1.

Figure 19: Advertising an LSP into OSPFv2



Configuration

The following examples require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure the devices to advertise an LSP into OSPFv2, perform the following tasks:

- Configuring BGP on page 257
- Configuring MPLS on page 259
- Configuring RSVP on page 261
- Configuring OSPF on page 263
- Configuring the LSP on page 265
- Advertising the LSP into OSPFv2 on page 265

Configuring BGP

CLI Quick Configuration

To quickly configure BGP on each routing device, copy the following commands and paste them into the CLI.

Configuration on Device R1:

```
[edit]
set routing-options autonomous-system 65000
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 10.0.0.1
set protocols bgp group internal-peers neighbor 10.0.0.3
```

```
set protocols bgp group internal-peers neighbor 10.0.0.6
set protocols bgp group internal-peers peer-as 65000
```

Configuration on Device R3:

```
[edit]
set routing-options autonomous-system 65000
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 10.0.0.3
set protocols bgp group internal-peers neighbor 10.0.0.1
set protocols bgp group internal-peers neighbor 10.0.0.6
set protocols bgp group internal-peers peer-as 65000
```

Configuration on Device R6:

```
[edit]
set routing-options autonomous-system 65000
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 10.0.0.6
set protocols bgp group internal-peers neighbor 10.0.0.1
set protocols bgp group internal-peers neighbor 10.0.0.3
set protocols bgp group internal-peers peer-as 65000
```

Step-by-Step Procedure

To configure BGP:

1. On each routing device, configure the local AS number.

```
[edit]
user@R1# set routing-options autonomous-system 65000

[edit]
user@R3# set routing-options autonomous-system 65000

[edit]
user@R6# set routing-options autonomous-system 65000
```

2. On each routing device, configure the internal BGP neighbor connections.

```
[edit]
user@R1# set protocols bgp group internal-peers type internal
user@R1# set protocols bgp group internal-peers local-address 10.0.0.1
user@R1# set protocols bgp group internal-peers neighbor 10.0.0.3
user@R1# set protocols bgp group internal-peers neighbor 10.0.0.6
user@R1# set protocols bgp group internal-peers peer-as 65000

[edit]
user@R3# set protocols bgp group internal-peers type internal
user@R3# set protocols bgp group internal-peers local-address 10.0.0.3
user@R3# set protocols bgp group internal-peers neighbor 10.0.0.1
user@R3# set protocols bgp group internal-peers neighbor 10.0.0.6
user@R3# set protocols bgp group internal-peers peer-as 65000

[edit]
user@R6# set protocols bgp group internal-peers type internal
user@R6# set protocols bgp group internal-peers local-address 10.0.0.6
user@R6# set protocols bgp group internal-peers neighbor 10.0.0.1
user@R6# set protocols bgp group internal-peers neighbor 10.0.0.3
user@R6# set protocols bgp group internal-peers peer-as 65000
```

3. If you are done configuring the devices, commit the configuration.

```
[edit]
user@host# commit
```

Results Confirm your configuration by entering the **show routing-options** and **show protocols bgp** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on R1:

```
user@R1# show routing-options
autonomous-system 65000;

user@R1# show protocols bgp
group internal-peers {
   type internal;
   local-address 10.0.0.1;
   peer-as 65000;
   neighbor 10.0.0.3;
   neighbor 10.0.0.6;
}
```

Configuration on R3:

```
user@R3# show routing-options
autonomous-system 65000;

user@R3# show protocols bgp
group internal-peers {
   type internal;
   local-address 10.0.0.3;
   peer-as 65000;
   neighbor 10.0.0.1;
   neighbor 10.0.0.6;
}
```

Configuration on R6:

```
user@R6# show routing-options
autonomous-system 65000;

user@R6# show protocols bgp
group internal-peers {
   type internal;
   local-address 10.0.0.6;
   peer-as 65000;
   neighbor 10.0.0.1;
   neighbor 10.0.0.3;
}
```

Configuring MPLS

CLI Quick Configuration To quickly configure MPLS on all of the routing devices in AS 65000, copy the following commands and paste them into the CLI.

Configuration on Device R1:

```
[edit]
```

```
set interfaces so-0/0/2 unit 0 family mpls
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
```

Configuration on Device R3:

```
[edit]
set interfaces so-0/0/2 unit 0 family mpls
set interfaces so-0/0/3 unit 0 family mpls
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
```

Configuration on Device R6:

```
[edit]
set interfaces so-0/0/3 unit 0 family mpls
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
```

Step-by-Step Procedure

To configure MPLS:

1. Configure the transit interfaces for MPLS.

   ```
   [edit ]
   user@R1# set interfaces so-0/0/2 unit 0 family mpls
   ```

   ```
   [edit ]
   user@R3# set interfaces so-0/0/2 unit 0 family mpls
   user@R3# set interfaces so-0/0/3 unit 0 family mpls
   ```

   ```
   [edit ]
   user@R6# set interfaces so-0/0/3 unit 0 family mpls
   ```

2. Enable MPLS.

   ```
   [edit ]
   user@R1# set protocols mpls interface all
   ```

   ```
   [edit ]
   user@R3# set protocols mpls interface all
   ```

   ```
   [edit ]
   user@R6# set protocols mpls interface all
   ```

3. Disable MPLS on the management interface (**fxp0.0**).

   ```
   [edit ]
   user@R1# set protocols mpls interface fxp0.0 disable
   ```

   ```
   [edit ]
   user@R3# set protocols mpls interface fxp0.0 disable
   ```

   ```
   [edit ]
   user@R6# set protocols mpls interface fxp0.0 disable
   ```

4. If you are done configuring the devices, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Results Confirm your configuration by entering the **show interfaces** and **show protocols mpls** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on Device R1:

```
user@R1# show interfaces
so-0/0/2 {
   unit 0 {
      family mpls;
   }
}
```

```
user@R1# show protocols mpls
interface all;
interface fxp0.0 {
   disable;
}
```

Configuration on Device R3:

```
user@R3# show interfaces
so-0/0/2 {
   unit 0 {
      family mpls;
   }
}
so-0/0/3 {
   unit 0 {
      family mpls;
   }
}
```

```
user@R3# show protocols mpls
interface all;
interface fxp0.0 {
   disable;
}
```

Configuration on Device R6:

```
user@R6# show interfaces
so-0/0/3 {
   unit 0 {
      family mpls;
   }
}
```

```
user@R6# show protocols mpls
interface all;
interface fxp0.0 {
   disable;
}
```

Configuring RSVP

CLI Quick Configuration To quickly configure RSVP on all of the routing devices in AS 65000, copy the following commands and paste them into the CLI.

Configuration on Device R1:

```
[edit]
set protocols rsvp interface so-0/0/2
set protocols rsvp interface fxp0.0 disable
```

Configuration on Device R3:

```
[edit]
set protocols rsvp interface so-0/0/2
set protocols rsvp interface so-0/0/3
set protocols rsvp interface fxp0.0 disable
```

Configuration on Device R6:

```
[edit]
set protocols rsvp interface so-0/0/3
set protocols rsvp interface fxp0.0 disable
```

Step-by-Step Procedure

To configure RSVP:

1. Enable RSVP.

```
[edit ]
user@R1# set protocols rsvp interface so-0/0/2
```

```
[edit ]
user@R3# set protocols rsvp interface so-0/0/2
user@R3# set protocols rsvp interface so-0/0/3
```

```
[edit ]
user@R6# set protocols rsvp interface so-0/0/3
```

2. Disable RSVP on the management interface (**fxp0.0**).

```
[edit ]
user@R1# set protocols rsvp interface fxp0.0 disable
```

```
[edit ]
user@R3# set protocols rsvp interface fxp0.0 disable
```

```
[edit ]
user@R6# set protocols rsvp interface fxp0.0 disable
```

3. If you are done configuring the devices, commit the configuration.

```
[edit]
user@host# commit
```

Results

Confirm your configuration by entering the **show protocols rsvp** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on Device R1:

```
user@R1# show protocols rsvp
interface so-0/0/2.0;
interface fxp0.0 {
  disable;
}
```


Configuration on Device R3:

```
user@R3# show protocols rsvp
interface so-0/0/2.0;
interface so-0/0/3.0;
interface fxp0.0 {
    disable;
}
```

Configuration on Device R6:

```
user@R3# show protocols rsvp
interface so-0/0/3.0;
interface fxp0.0 {
    disable;
}
```

Configuring OSPF

CLI Quick Configuration

To quickly configure OSPF, copy the following commands and paste them into the CLI.

Configuration on Device R1:

```
[edit]
set routing-options router-id 10.0.0.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

Configuration on Device R3:

```
[edit]
set routing-options router-id 10.0.0.3
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

Configuration on Device R6:

```
[edit]
set routing-options router-id 10.0.0.6
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

Step-by-Step Procedure

To configure OSPF:

1. Configure the router ID.

```
[edit]
user@R1# set routing-options router-id 10.0.0.1

[edit]
user@R3# set routing-options router-id 10.0.0.3

[edit]
user@R6# set routing-options router-id 10.0.0.6
```

2. Configure the OSPF area and the interfaces.

```
[edit]
user@R1# set protocols ospf area 0.0.0.0 interface all
```

```
[edit]
user@R3# set protocols ospf area 0.0.0.0 interface all
```

```
[edit]
user@R6# set protocols ospf area 0.0.0.0 interface all
```

3. Disable OSPF on the management interface (**fxp0.0**).

```
[edit]
user@R1# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

```
[edit]
user@R3# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

```
[edit]
user@R6# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
```

4. If you are done configuring the devices, commit the configuration.

```
[edit ]
user@host# commit
```

Results Confirm your configuration by entering the **show routing-options** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Configuration on Device R1:

```
user@R1# show routing-options
router-id 10.0.0.1;
```

```
user@R1# show protocols ospf
area 0.0.0.0 {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
```

Configuration on Device R3:

```
user@R3# show routing-options
router-id 10.0.0.3;
```

```
user@R3# show protocols ospf
area 0.0.0.0 {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
```

Configuration on Device R6:

```
user@R6# show routing-options
router-id 10.0.0.6;
```

```
user@R6# show protocols ospf
area 0.0.0.0 {
  interface all;
```



```
    interface fxp0.0 {
      disable;
    }
  }
```

Configuring the LSP

CLI Quick Configuration

To quickly configure the LSP on the ingress routing device Router R1, copy the following command and paste it into the CLI.

```
[edit]
set protocols mpls label-switched-path R1-to-R6 to 10.0.0.6
```

Step-by-Step Procedure

To configure the LSP on Device R1:

1. Enter MPLS configuration mode.

   ```
   [edit]
   user@R1# edit protocols mpls
   ```

2. Create the LSP.

   ```
   [edit protocols mpls]
   user@R1# set label-switched-path R1-to-R6 to 10.0.0.6
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit ]
   user@R1# commit
   ```

Results

Confirm your configuration by entering the **show protocols mpls** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show protocols mpls
label-switched-path R1-to-R6 {
  to 10.0.0.6;
}
```

Advertising the LSP into OSPFv2

CLI Quick Configuration

To quickly advertise the LSP into OSPFv2 and optionally include a metric for the LSP on Device R1, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf area 0.0.0.0 label-switched-path R1-to-R6
set protocols ospf area 0.0.0.0 label-switched-path R1-to-R6 metric 2
```

Step-by-Step Procedure

To advertise the LSP into OSPFv2 on Router R1:

1. Enter OSPF configuration mode.

   ```
   [edit]
   user@R1# edit protocols ospf
   ```

2. Include the **label-switched-path** statement, and specify the LSP R1-to-R6 that you created.

```
[edit protocols ospf]
user@R1# set protocols ospf area 0.0.0.0 label-switched-path R1-to-R6
```

3. (Optional) Specify a metric for the LSP.

```
[edit ]
user@R1# set protocols ospf area 0.0.0.0 label-switched-path R1-to-R6 metric 2
```

4. If you are done configuring the device, commit the configuration.

```
[edit ]
user@R1# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show protocols ospf
area 0.0.0.0 {
  label-switched-path R1-to-R6 {
    metric 2;
  }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Neighbor

Purpose Verify that another neighbor is listed and is reachable over the LSP. The interface field indicates the name of the LSP.

Action From operational mode, enter the **show ospf neighbor** command.

Related Documentation

- OSPF Configuration Overview on page 14
- *Junos OS MPLS Applications Library for Routing Devices*

CHAPTER 13

OSPFv2 Sham Link Configuration

Example: Configuring OSPFv2 Sham Links

OSPFv2 Sham Links Overview

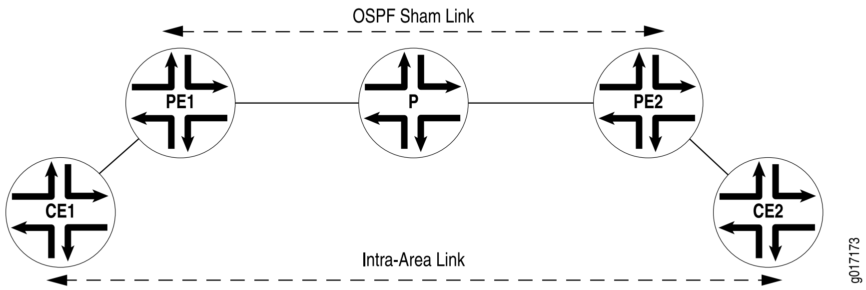
You can create an intra-area link or sham link between two provider edge (PE) routing devices so that the VPN backbone is preferred over the back-door link. A back-door link is a backup link that connects customer edge (CE) devices in case the VPN backbone is unavailable. When such a backup link is available and the CE devices are in the same OSPF area, the default behavior is to prefer this backup link over the VPN backbone. This is because the backup link is considered an intra-area link, while the VPN backbone is always considered an interarea link. Intra-area links are always preferred over interarea links.

The sham link is an unnumbered point-to-point intra-area link between PE devices. When the VPN backbone has a sham intra-area link, this sham link can be preferred over the backup link if the sham link has a lower OSPF metric than the backup link.

The sham link is advertised using Type 1 link-state advertisements (LSAs). Sham links are valid only for routing instances and OSPFv2.

Each sham link is identified by the combination of a local endpoint address and a remote endpoint address. Figure 20 on page 268 shows an OSPFv2 sham link. Router CE1 and Router CE2 are located in the same OSPFv2 area. These customer edge (CE) routing devices are linked together by a Layer 3 VPN over Router PE1 and Router PE2. In addition, Router CE1 and Router CE2 are connected by an intra-area link used as a backup.

Figure 20: OSPFv2 Sham Link



OSPFv2 treats the link through the Layer 3 VPN as an interarea link. By default, OSPFv2 prefers intra-area links to interarea links, so OSPFv2 selects the backup intra-area link as the active path. This is not acceptable in a configuration where the intra-area link is not the expected primary path for traffic between the CE routing devices. You can configure the metric for the sham link to ensure that the path over the Layer 3 VPN is preferred to a backup path over an intra-area link connecting the CE routing devices.

For the remote endpoint, you can configure the OSPFv2 interface as a demand circuit, configure IPsec authentication (you configure the actual IPsec authentication separately), and define the metric value.

You should configure an OSPFv2 sham link under the following circumstances:

- Two CE routing devices are linked together by a Layer 3 VPN.
- These CE routing devices are in the same OSPFv2 area.
- An intra-area link is configured between the two CE routing devices.

If there is no intra-area link between the CE routing devices, you do not need to configure an OSPFv2 sham link.

NOTE: **In Junos OS Release 9.6 and later, an OSPFv2 sham link is installed in the routing table as a hidden route. Additionally, a BGP route is not exported to OSPFv2 if a corresponding OSPF sham link is available.**

Example: Configuring OSPFv2 Sham Links

This example shows how to enable OSPFv2 sham links on a PE routing device.

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

The sham link is an unnumbered point-to-point intra-area link and is advertised by means of a type 1 link-state advertisement (LSA). Sham links are valid only for routing instances and OSPFv2.

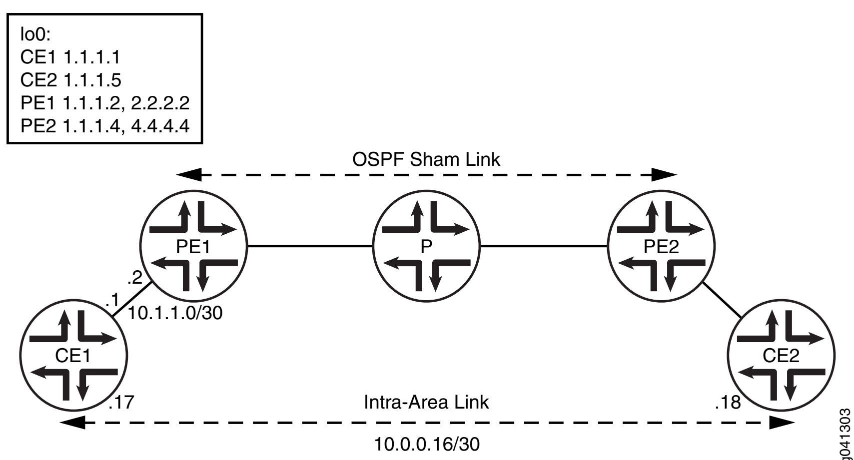
Each sham link is identified by a combination of the local endpoint address and a remote endpoint address and the OSPFv2 area to which it belongs. You manually configure the sham link between two PE devices, both of which are within the same VPN routing and forwarding (VRF) routing instance, and you specify the address for the local end point of the sham link. This address is used as the source for the sham link packets and is also used by the remote PE routing device as the sham link remote end point. You can also include the optional **metric** option to set a metric value for the remote end point. The metric value specifies the cost of using the link. Routes with lower total path metrics are preferred over those with higher path metrics.

To enable OSPFv2 sham links on a PE routing device:

- Configure an extra loopback interface on the PE routing device.
- Configure the VRF routing instance that supports Layer 3 VPNs on the PE routing device, and associate the sham link with an existing OSPF area. The OSPFv2 sham link configuration is also included in the routing instance. You configure the sham link's local endpoint address, which is the loopback address of the local VPN, and the remote endpoint address, which is the loopback address of the remote VPN. In this example, the VRF routing instance is named red.

Figure 21 on page 269 shows an OSPFv2 sham link.

Figure 21: OSPFv2 Sham Link Example



The devices in the figure represent the following functions:

- CE1 and CE2 are the customer edge devices.
- PE1 and PE2 are the provider edge devices.

- P is the provider device.

"CLI Quick Configuration" on page 270 shows the configuration for all of the devices in Figure 21 on page 269. The section "Step-by-Step Procedure" on page 272describes the steps on Device PE1.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

CE1

```
set interfaces fe-1/2/0 unit 0 family inet address 10.1.1.1/30
set interfaces fe-1/2/0 unit 0 family mpls
set interfaces fe-1/2/1 unit 0 family inet address 10.0.0.17/30
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
set protocols ospf area 0.0.0.0 interface fe-1/2/0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-1/2/1.0 metric 100
set policy-options policy-statement send-direct from protocol direct
set policy-options policy-statement send-direct then accept
set routing-options router-id 1.1.1.1
set routing-options autonomous-system 1
```

PE1

```
set interfaces fe-1/2/0 unit 0 family inet address 10.1.1.2/30
set interfaces fe-1/2/0 unit 0 family mpls
set interfaces fe-1/2/1 unit 0 family inet address 10.1.1.5/30
set interfaces fe-1/2/1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 1.1.1.2/32
set interfaces lo0 unit 1 family inet address 2.2.2.2/32
set protocols mpls interface fe-1/2/1.0
set protocols bgp group toR4 type internal
set protocols bgp group toR4 local-address 1.1.1.2
set protocols bgp group toR4 family inet-vpn unicast
set protocols bgp group toR4 neighbor 1.1.1.4
set protocols ospf area 0.0.0.0 interface fe-1/2/1.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface fe-1/2/1.0
set protocols ldp interface lo0.0
set policy-options policy-statement bgp-to-ospf term 1 from protocol bgp
set policy-options policy-statement bgp-to-ospf term 1 then accept
set policy-options policy-statement bgp-to-ospf term 2 then reject
set routing-instances red instance-type vrf
set routing-instances red interface fe-1/2/0.0
set routing-instances red interface lo0.1
set routing-instances red route-distinguisher 2:1
set routing-instances red vrf-target target:2:1
set routing-instances red protocols ospf export bgp-to-ospf
set routing-instances red protocols ospf sham-link local 2.2.2.2
set routing-instances red protocols ospf area 0.0.0.0 sham-link-remote 4.4.4.4 metric
  10
set routing-instances red protocols ospf area 0.0.0.0 interface fe-1/2/0.0
set routing-instances red protocols ospf area 0.0.0.0 interface lo0.1
set routing-options router-id 1.1.1.2
```

```
set routing-options autonomous-system 2
```

P

```
set interfaces fe-1/2/0 unit 0 family inet address 10.1.1.6/30
set interfaces fe-1/2/0 unit 0 family mpls
set interfaces fe-1/2/1 unit 0 family inet address 10.1.1.9/30
set interfaces fe-1/2/1 unit 0 family mpls
set interfaces lo0 unit 3 family inet address 1.1.1.3/32
set protocols mpls interface all
set protocols ospf area 0.0.0.0 interface lo0.3 passive
set protocols ospf area 0.0.0.0 interface all
set protocols ldp interface all
set routing-options router-id 1.1.1.3
```

PE2

```
set interfaces fe-1/2/0 unit 0 family inet address 10.1.1.10/30
set interfaces fe-1/2/0 unit 0 family mpls
set interfaces fe-1/2/1 unit 0 family inet address 10.1.1.13/30
set interfaces fe-1/2/1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 1.1.1.4/32
set interfaces lo0 unit 1 family inet address 4.4.4.4/32
set protocols mpls interface fe-1/2/0.0
set protocols bgp group toR2 type internal
set protocols bgp group toR2 local-address 1.1.1.4
set protocols bgp group toR2 family inet-vpn unicast
set protocols bgp group toR2 neighbor 1.1.1.2
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-1/2/0.0
set protocols ldp interface fe-1/2/0.0
set protocols ldp interface lo0.0
set policy-options policy-statement bgp-to-ospf term 1 from protocol bgp
set policy-options policy-statement bgp-to-ospf term 1 then accept
set policy-options policy-statement bgp-to-ospf term 2 then reject
set routing-instances red instance-type vrf
set routing-instances red interface fe-1/2/1.0
set routing-instances red interface lo0.1
set routing-instances red route-distinguisher 2:1
set routing-instances red vrf-target target:2:1
set routing-instances red protocols ospf export bgp-to-ospf
set routing-instances red protocols ospf sham-link local 4.4.4.4
set routing-instances red protocols ospf area 0.0.0.0 sham-link-remote 2.2.2.2 metric 10
set routing-instances red protocols ospf area 0.0.0.0 interface fe-1/2/1.0
set routing-instances red protocols ospf area 0.0.0.0 interface lo0.1
set routing-options router-id 1.1.1.4
set routing-options autonomous-system 2
```

CE2

```
set interfaces fe-1/2/0 unit 14 family inet address 10.1.1.14/30
set interfaces fe-1/2/0 unit 14 family mpls
set interfaces fe-1/2/0 unit 18 family inet address 10.0.0.18/30
set interfaces lo0 unit 5 family inet address 1.1.1.5/32
set protocols ospf area 0.0.0.0 interface fe-1/2/0.14
set protocols ospf area 0.0.0.0 interface lo0.5 passive
set protocols ospf area 0.0.0.0 interface fe-1/2/0.18
set policy-options policy-statement send-direct from protocol direct
set policy-options policy-statement send-direct then accept
set routing-options router-id 1.1.1.5
set routing-options autonomous-system 3
```


Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure OSPFv2 sham links on each PE device:

1. Configure the interfaces, including two loopback interfaces.

```
[edit interfaces]
user@PE1# set fe-1/2/0 unit 0 family inet address 10.1.1.2/30
user@PE1# set fe-1/2/0 unit 0 family mpls
user@PE1# set fe-1/2/1 unit 0 family inet address 10.1.1.5/30
user@PE1# set fe-1/2/1 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 1.1.1.2/32
user@PE1# set lo0 unit 1 family inet address 2.2.2.2/32
```

2. Configure MPLS on the core-facing interface.

```
[edit protocols mpls]
user@PE1# set interface fe-1/2/1.0
```

3. Configure internal BGP (IBGP).

```
[edit ]
user@PE1# set protocols bgp group toR4 type internal
user@PE1# set protocols bgp group toR4 local-address 1.1.1.2
user@PE1# set protocols bgp group toR4 family inet-vpn unicast
user@PE1# set protocols bgp group toR4 neighbor 1.1.1.4
```

4. Configure OSPF on the core-facing interface and on the loopback interface that is being used in the main instance.

```
[edit protocols ospf area 0.0.0.0]
user@PE1# set interface fe-1/2/1.0
user@PE1# set interface lo0.0 passive
```

5. Configure LDP or RSVP on the core-facing interface and on the loopback interface that is being used in the main instance.

```
[edit protocols ldp]
user@PE1# set interface fe-1/2/1.0
user@PE1# set interface lo0.0
```

6. Configure a routing policy for use in the routing instance.

```
[edit policy-options policy-statement bgp-to-ospf]
user@PE1# set term 1 from protocol bgp
user@PE1# set term 1 then accept
user@PE1# set term 2 then reject
```

7. Configure the routing instance.

```
[edit routing-instances red]
user@PE1# set instance-type vrf
user@PE1# set interface fe-1/2/0.0
user@PE1# set route-distinguisher 2:1
user@PE1# set vrf-target target:2:1
user@PE1# set protocols ospf export bgp-to-ospf
user@PE1# set protocols ospf area 0.0.0.0 interface fe-1/2/0.0
```

8. Configure the OSPFv2 sham link.

   Include the extra loopback interface in the routing instance and also in the OSPF configuration.

   Notice that the metric on the sham-link interface is set to 10. On Device CE1's backup OSPF link, the metric is set to 100. This causes the sham link to be the preferred link.

   ```
   [edit routing-instances red]
   user@PE1# set interface lo0.1
   user@PE1# set protocols ospf sham-link local 2.2.2.2
   user@PE1# set protocols ospf area 0.0.0.0 sham-link-remote 4.4.4.4 metric 10
   user@PE1# set protocols ospf area 0.0.0.0 interface lo0.1
   ```

9. Configure the autonomous system (AS) number and the router ID.

   ```
   [edit routing-options]
   user@PE1# set router-id 1.1.1.2
   user@PE1# set autonomous-system 2
   ```

10. If you are done configuring the device, commit the configuration.

    ```
    [edit]
    user@R1# commit
    ```

Results Confirm your configuration by entering the **show interfaces** and the **show routing-instances** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Output for PE1:

```
user@PE1# show interfaces
fe-1/2/0 {
  unit 0{
    family inet {
      address 10.1.1.2/30;
    }
    family mpls;
  }
}
fe-1/2/1 {
  unit 0 {
    family inet {
      address 10.1.1.5/30;
    }
    family mpls;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 1.1.1.2/32;
    }
  }
  unit 1 {
    family inet {
```

```
            address 2.2.2.2/32;
        }
    }
}
user@PE1# show protocols
mpls {
    interface fe-1/2/1.0;
}
bgp {
    group toR4 {
        type internal;
        local-address 1.1.1.2;
        family inet-vpn {
            unicast;
        }
        neighbor 1.1.1.4;
    }
}
ospf {
    area 0.0.0.0 {
        interface fe-1/2/1.0;
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface fe-1/2/1.0;
    interface lo0.0;
}
user@PE1# show policy-options
policy-statement bgp-to-ospf {
    term 1 {
        from protocol bgp;
        then accept;
    }
    term 2 {
        then reject;
    }
}
user@PE1# show routing-instances
red {
    instance-type vrf;
    interface fe-1/2/0.0;
    interface lo0.1;
    route-distinguisher 2:1;
    vrf-target target:2:1;
    protocols {
        ospf {
            export bgp-to-ospf;
            sham-link local 2.2.2.2;
            area 0.0.0.0 {
                sham-link-remote 4.4.4.4 metric 10;
                interface fe-1/2/0.0;
```



```
                interface lo0.1;
            }
        }
    }
}
```

user@PE1# **show routing-options**
router-id 1.1.1.2;
autonomous-system 2;

Verification

Confirm that the configuration is working properly.

- Verifying the Sham Link Interfaces on page 275
- Verifying the Local and Remote End Points of the Sham Link on page 275
- Verifying the Sham Link Adjacencies on page 276
- Verifying the Link-State Advertisement on page 276
- Verifying the Path Selection on page 276

Verifying the Sham Link Interfaces

Purpose Verify the sham link interface. The sham link is treated as an interface in OSPFv2, with the named displayed as **shamlink.<unique identifier>**, where the unique identifier is a number. For example, **shamlink.0**. The sham link appears as a point-to-point interface.

Action From operational mode, enter the **show ospf interface instance *instance-name*** command.

```
user@PE1> show ospf interface instance red
Interface           State    Area            DR ID           BDR ID          Nbrs
lo0.1              DR       0.0.0.0         2.2.2.2         0.0.0.0            0
fe-1/2/0.0          PtToPt  0.0.0.0          0.0.0.0         0.0.0.0            1
shamlink.0          PtToPt  0.0.0.0          0.0.0.0         0.0.0.0            1
```

Verifying the Local and Remote End Points of the Sham Link

Purpose Verify the local and remote end points of the sham link. The MTU for the sham link interface is always zero.

Action From operational mode, enter the **show ospf interface instance *instance-name* detail** command.

```
user@PE1> show ospf interface shamlink.0 instance red
Interface           State    Area            DR ID           BDR ID          Nbrs
shamlink.0          PtToPt  0.0.0.0          0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 0, Cost: 10
  Local: 2.2.2.2, Remote: 4.4.4.4
  Adj count: 1
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Protection type: None, No eligible backup
  Topology default (ID 0) -> Cost: 10
```

Verifying the Sham Link Adjacencies

Purpose Verify the adjacencies between the configured sham links.

Action From operational mode, enter the **show ospf neighbor instance** ***instance-name*** command.

```
user@PE1> show ospf neighbor instance red
Address          Interface              State     ID               Pri  Dead
10.1.1.1         fe-1/2/0.0             Full      1.1.1.1          128    35
4.4.4.4          shamlink.0             Full      4.4.4.4            0    31
```

Verifying the Link-State Advertisement

Purpose Verify that the router LSA originated by the instance carries the sham link adjacency as an unnumbered point-to-point link. The link data for sham links is a number ranging from 0x80010000 through 0x8001ffff.

Action From operational mode, enter the **show ospf database instance** ***instance-name*** command.

```
user@PE1> show ospf database instance red

    OSPF database, Area 0.0.0.0
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   1.1.1.1          1.1.1.1          0x80000009  1803  0x22 0x6ec7   72
Router   1.1.1.5          1.1.1.5          0x80000007    70  0x22 0x2746   72
Router  *2.2.2.2          2.2.2.2          0x80000006    55  0x22 0xda6b   60
Router   4.4.4.4          4.4.4.4          0x80000005    63  0x22 0xb19    60
Network  10.0.0.18        1.1.1.5          0x80000002    70  0x22 0x9a71   32
    OSPF AS SCOPE link state database
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Extern   2.2.2.2          4.4.4.4          0x80000002    72  0xa2 0x343    36
Extern  *4.4.4.4          2.2.2.2          0x80000002    71  0xa2 0xe263   36
```

Verifying the Path Selection

Purpose Verify that the Layer 3 VPN path is used instead of the backup path.

Action From operational mode, enter the **traceroute** command from Device CE1 to Device CE2.

```
user@CE1> traceroute 1.1.1.5

traceroute to 1.1.1.5 (1.1.1.5), 30 hops max, 40 byte packets
 1  10.1.1.2 (10.1.1.2)  1.930 ms  1.664 ms  1.643 ms
 2  * * *
 3  10.1.1.10 (10.1.1.10)  2.485 ms  1.435 ms  1.422 ms
     MPLS Label=299808 CoS=0 TTL=1 S=1
 4  1.1.1.5 (1.1.1.5)  1.347 ms  1.362 ms  1.329 ms
```

Meaning The traceroute operation shows that the Layer 3 VPN is the preferred path. If you were to remove the sham link or if you were to modify the OSPF metric to prefer that backup path, the traceroute would show that the backup path is preferred.

Related Documentation

- OSPF Configuration Overview on page 14
- *Junos OS VPNs Library for Routing Devices*

CHAPTER 14

OSPF Database Protection Configuration

Example: Configuring OSPF Database Protection

OSPF Database Protection Overview

OSPF database protection allows you to limit the number of link-state advertisements (LSAs) not generated by the local router in a given OSPF routing instance, helping to protect the link-state database from being flooded with excessive LSAs. This feature is particularly useful if VPN routing and forwarding is configured on your provider edge and customer edge routers using OSPF as the routing protocol. An overrun link-state database on the customer edge router can exhaust resources on the provider edge router and impact the rest of the service provider network.

When you enable OSPF database protection, the maximum number of LSAs you specify includes all LSAs whose advertising router ID is not equal to the local router ID (nonself-generated LSAs). These might include external LSAs as well as LSAs with any scope such as the link, area, and autonomous system (AS).

Once the specified maximum LSA count is exceeded, the database typically enters into the ignore state. In this state, all neighbors are brought down, and nonself-generated LSAs are destroyed. In addition, the database sends out hellos but ignores all received packets. As a result, the database does not form any full neighbors, and therefore does not learn about new LSAs. However, if you have configured the **warning-only** option, only a warning is issued and the database does not enter the ignore state but continues to operate as before.

You can also configure one or more of the following options:

- A warning threshold for issuing a warning message before the LSA limit is reached.
- An ignore state time during which the database must remain in the ignore state and after which normal operations can be resumed.
- An ignore state count that limits the number of times the database can enter the ignore state, after which it must enter the isolate state. The isolate state is very similar to the

ignore state, but has one important difference: once the database enters the isolate state, it must remain there until you issue a command to clear database protection before it can return to normal operations.

- A reset time during which the database must stay out of the ignore or isolate state before it is returned to a normal operating state.

Configuring OSPF Database Protection

By configuring OSPF database protection, you can help prevent your OSPF link-state database from being overrun with excessive LSAs that are not generated by the local router. You specify the maximum number of LSAs whose advertising router ID is not the same as the local router ID in an OSPF instance. This feature is particularly useful if your provider edge and customer edge routers are configured with VPN routing and forwarding using OSPF.

OSPF database protection is supported on:

- Logical systems
- All routing instances supported by OSPFv2 and OSPFv3
- OSPFv2 and OSPFv3 topologies
- OSPFv3 realms

To configure OSPF database protection:

1. Include the database-protection statement at one of the following hierarchy levels:
   - **[edit protocols ospf | ospf3]**
   - **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf |ospf3)]**
   - **[edit routing-instances *routing-instance-name* protocols (ospf |ospf3)]**
   - **[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-unicast | ipv6-multicast)]**
2. Include the **maximum-lsa *number*** statement.

   NOTE: The maximum-lsa statement is mandatory, and there is no default value for it. If you omit this statement, you cannot configure OSPF database protection.

3. (Optional) Include the following statements:
   - **ignore-count *number***—Specify the number of times the database can enter the ignore state before it goes into the isolate state.
   - **ignore-time *seconds***—Specify the time limit the database must remain in the ignore state before it resumes regular operations.

- **reset-time** ***seconds***—Specify the time during which the database must operate without being in either the ignore or isolate state before it is reset to a normal operating state.
- **warning-threshold** ***percent***—Specify the percent of the maximum LSA number that must be exceeded before a warning message is issued.

4. (Optional) Include the **warning-only** statement to prevent the database from entering the ignore state or isolate state when the maximum LSA count is exceeded.

   NOTE: If you include the warning-only statement, values for the other optional statements at the same hierarchy level are not used when the maximum LSA number is exceeded.

5. Verify your configuration by checking the database protection fields in the output of the **show ospf overview** command.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14

CHAPTER 15

OSPF Policy Configuration

Examples: Configuring OSPF Routing Policy

Understanding OSPF Routing Policy

Each routing policy is identified by a policy name. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks. Each routing policy name must be unique within a configuration. Once a policy is created and named, it must be applied before it is active.

In the **import** statement, you list the name of the routing policy used to filter OSPF external routes from being installed into the routing tables of OSPF neighbors. You can filter the routes, but not link-state address (LSA) flooding. An external route is a route that is outside the OSPF Autonomous System (AS). The import policy does not impact the OSPF database. This means that the import policy has no impact on the link-state advertisements.

In the **export** statement, you list the name of the routing policy to be evaluated when routes are being exported from the routing table into OSPF.

By default, if a routing device has multiple OSPF areas, learned routes from other areas are automatically installed into area 0 of the routing table.

To specify more than one policy and create a policy chain, you list the policies using a space as a separator. If multiple policies are specified, the policies are evaluated in the order in which they are specified. As soon as an accept or reject action is executed, the policy chain evaluation ends.

This topic describes the following information:

- Routing Policy Terms on page 282
- Routing Policy Match Conditions on page 282
- Routing Policy Actions on page 283

Routing Policy Terms

Routing policies are made up of one or more terms. A term is a named structure in which match conditions and actions are defined. You can define one or more terms. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks.

Each term contains a set of match conditions and a set of actions:

- Match conditions are criteria that a route must match before the actions can be applied. If a route matches all criteria, one or more actions are applied to the route.
- Actions specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

Routing Policy Match Conditions

A match condition defines the criteria that a route must match for an action to take place. You can define one or more match conditions for each term. If a route matches all of the match conditions for a particular term, the actions defined for that term are processed.

Each term can include two statements, **from** and **to**, that define the match conditions:

- In the **from** statement, you define the criteria that an incoming route must match. You can specify one or more match conditions. If you specify more than one, they all must match the route for a match to occur.

  The **from** statement is optional. If you omit the **from** and the **to** statements, all routes are considered to match.

  NOTE: In export policies, omitting the from statement from a routing policy term might lead to unexpected results. For more information, see the *Routing Policy Feature Guide for Routing Devices*.

- In the **to** statement, you define the criteria that an outgoing route must match. You can specify one or more match conditions. If you specify more than one, they all must match the route for a match to occur.

The order of the match conditions in a term is not important because a route must match all match conditions in a term for an action to be taken.

For a complete list of match conditions, see *Routing Policy Match Conditions* in the *Routing Policy Feature Guide for Routing Devices*.

Routing Policy Actions

An action defines what the routing device does with the route when the route matches all the match conditions in the **from** and **to** statements for a particular term. If a term does not have **from** and **to** statements, all routes are considered to match and the actions apply to all routes.

Each term can have one or more of the following types of actions. The actions are configured under the **then** statement.

- Flow control actions, which affect whether to accept or reject the route and whether to evaluate the next term or routing policy.
- Actions that manipulate route characteristics.
- Trace action, which logs route matches.

The **then** statement is optional. If you omit it, one of the following occurs:

- The next term in the routing policy, if one exists, is evaluated.
- If the routing policy has no more terms, the next routing policy, if one exists, is evaluated.
- If there are no more terms or routing policies, the **accept** or **reject** action specified by the default policy is executed.

For a complete list of routing policy actions, see *Actions in Routing Policy TermsRouting Policy Feature Guide for Routing Devices*

Example: Injecting OSPF Routes into the BGP Routing Table

This example shows how to create a policy that injects OSPF routes into the BGP routing table.

- Requirements on page 283
- Overview on page 284
- Configuration on page 284
- Verification on page 286
- Troubleshooting on page 286

Requirements

Before you begin:

- Configure network interfaces.
- Configure external peer sessions. See *Example: Configuring External BGP Point-to-Point Peer Sessions*.
- Configure interior gateway protocol (IGP) sessions between peers.

Overview

In this example, you create a routing policy called **injectpolicy1** and a routing term called **injectterm1**. The policy injects OSPF routes into the BGP routing table.

Configuration

Configuring the Routing Policy

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set policy-options policy-statement injectpolicy1 term injectterm1 from protocol ospf
set policy-options policy-statement injectpolicy1 term injectterm1 from area 0.0.0.1
set policy-options policy-statement injectpolicy1 term injectterm1 then accept
set protocols bgp export injectpolicy1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To inject OSPF routes into a BGP routing table:

1. Create the policy term.

   ```
   [edit policy-options policy-statement injectpolicy1]
   user@host# set term injectterm1
   ```

2. Specify OSPF as a match condition.

   ```
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set from protocol ospf
   ```

3. Specify the routes from an OSPF area as a match condition.

   ```
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set from area 0.0.0.1
   ```

4. Specify that the route is to be accepted if the previous conditions are matched.

   ```
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set then accept
   ```

5. Apply the routing policy to BGP.

   ```
   [edit]
   user@host# set protocols bgp export injectpolicy1
   ```

Results

Confirm your configuration by entering the **show policy-options** and **show protocols bgp** commands from configuration mode. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show policy-options
policy-statement injectpolicy1 {
    term injectterm1 {
        from {
            protocol ospf;
            area 0.0.0.1;
        }
        then accept;
    }
}
```

```
user@host# show protocols bgp
export injectpolicy1;
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Tracing for the Routing Policy

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set policy-options policy-statement injectpolicy1 term injectterm1 then trace
set routing-options traceoptions file ospf-bgp-policy-log
set routing-options traceoptions file size 5m
set routing-options traceoptions file files 5
set routing-options traceoptions flag policy
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Include a trace action in the policy.

   ```
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# then trace
   ```

2. Configure the tracing file for the output.

   ```
   [edit routing-options traceoptions]
   user@host# set file ospf-bgp-policy-log
   user@host# set file size 5m
   user@host# set file files 5
   user@host# set flag policy
   ```

Results

Confirm your configuration by entering the **show policy-options** and **show routing-options** commands from configuration mode. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show policy-options
policy-statement injectpolicy1 {
    term injectterm1 {
        then {
            trace;
        }
```

```
    }
  }
  user@host# show routing-options
  traceoptions {
    file ospf-bgp-policy-log size 5m files 5;
    flag policy;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying That the Expected BGP Routes Are Present

Purpose Verify the effect of the export policy.

Action From operational mode, enter the **show route** command.

Troubleshooting

Using the show log Command to Examine the Actions of the Routing Policy

Problem The routing table contains unexpected routes, or routes are missing from the routing table.

Solution If you configure policy tracing as shown in this example, you can run the **show log ospf-bgp-policy-log** command to diagnose problems with the routing policy. The **show log ospf-bgp-policy-log** command displays information about the routes that the **injectpolicy1** policy term analyzes and acts upon.

Example: Redistributing Static Routes into OSPF

This example shows how to create a policy that redistributes static routes into OSPF.

Requirements

Before you begin:

- Configure the device interfaces. See the *Junos OS Network Interfaces Library for Routing Devices*.
- Configure static routes. See *Examples: Configuring Static Routes* in the *Junos OS Routing Protocols Library for Routing Devices*.

Overview

In this example, you create a routing policy called exportstatic1 and a routing term called exportstatic1. The policy injects static routes into OSPF. This example includes the following settings:

- **policy-statement**—Defines the routing policy. You specify the name of the policy and further define the elements of the policy. The policy name must be unique and can contain letters, numbers, and hyphens (-) and be up to 255 characters long.
- **term**—Defines the match condition and applicable actions for the routing policy. The term name can contain letters, numbers, and hyphens (-) and be up to 255 characters long. You specify the name of the term and define the criteria that an incoming route must match by including the **from** statement and the action to take if the route matches the conditions by including the **then** statement. In this example you specify the static protocol match condition and the accept action.
- **export**—Applies the export policy you created to be evaluated when routes are being exported from the routing table into OSPF.

Configuration

CLI Quick Configuration

To quickly create a policy that injects static routes into OSPF, copy the following commands and paste them into the CLI.

```
[edit]
set policy-options policy-statement exportstatic1 term exportstatic1 from protocol static
set policy-options policy-statement exportstatic1 term exportstatic1 then accept
set protocols ospf export exportstatic1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To inject static routes into OSPF:

1. Create the routing policy.

   ```
   [edit]
   user@host# edit policy-options policy-statement exportstatic1
   ```

2. Create the policy term.

   ```
   [edit policy-options policy-statement exportstatic1]
   user@host# set term exportstatic1
   ```

3. Specify static as a match condition.

   ```
   [edit policy-options policy-statement exportstatic1 term exportstatic1]
   user@host# set from protocol static
   ```

4. Specify that the route is to be accepted if the previous condition is matched.

   ```
   [edit policy-options policy-statement exportstatic1 term exportstatic1]
   user@host# set then accept
   ```

5. Apply the routing policy to OSPF.

NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@host# set protocols ospf export exportstatic1
```

6. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Results Confirm your configuration by entering the **show policy-options** and **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show policy-options
policy-statement exportstatic1 {
  term exportstatic1 {
    from protocol static;
    then accept;
  }
}
```

```
user@host# show protocols ospf
export exportstatic1;
```

To confirm your OSPFv3 configuration, enter the **show policy-options** and the **show protocols ospf3** commands.

Verification

Confirm that the configuration is working properly.

- Verifying That the Expected Static Routes Are Present on page 288
- Verifying That AS External LSAs Are Added to the Routing Table on page 288

Verifying That the Expected Static Routes Are Present

Purpose Verify the effect of the export policy.

Action From operational mode, enter the **show route** command.

Verifying That AS External LSAs Are Added to the Routing Table

Purpose On the routing device where you configured the export policy, verify that the routing device originates an AS external LSA for the static routes that are added to the routing table.

Action From operational mode, enter the **show ospf database** command for OSPFv2, and enter the **show ospf3 database** command for OSPFv3.

Example: Configuring an OSPF Import Policy

This example shows how to create an OSPF import policy. OSPF import policies apply to external routes only. An external route is a route that is outside the OSPF autonomous system (AS).

Requirements

Before you begin:

- Configure static routes. See *Examples: Configuring Static Routes* in the *Junos OS Routing Protocols Library for Routing Devices*.
- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26.
- Configure a single-area OSPF network. See "Example: Configuring a Single-Area OSPF Network" on page 29 .

Overview

External routes are learned by AS boundary routers. External routes can be advertised throughout the OSPF domain if you configure the AS boundary router to redistribute the route into OSPF. An external route might be learned by the AS boundary router from a routing protocol other than OSPF, or the external route might be a static route that you configure on the AS boundary router.

For OSPFv3, the link-state advertisement (LSA) is referred to as the interarea prefix LSA and performs the same function as a network-summary LSA performs for OSPFv2. An area border router (ABR) originates an interarea prefix LSA for each IPv6 prefix that must be advertised into an area.

OSPF import policy allows you to prevent external routes from being added to the routing tables of OSPF neighbors. The import policy does not impact the OSPF database. This means that the import policy has no impact on the link-state advertisements. The filtering is done only on external routes in OSPF. The intra-area and interarea routes are not considered for filtering. The default action is to accept the route when the route does not match the policy.

This example includes the following OSPF policy settings:

- **policy-statement**—Defines the routing policy. You specify the name of the policy and further define the elements of the policy. The policy name must be unique and can contain letters, numbers, and hyphens (-) and be up to 255 characters long.

- **export**—Applies the export policy you created to be evaluated when network summary LSAs are flooded into an area. In this example, the export policy is named export_static.
- **import**—Applies the import policy you created to prevent external routes from being added to the routing table. In this example, the import policy is named filter_routes.

The devices you configure in this example represent the following functions:

- R1—Device R1 is in area 0.0.0.0 and has a direct connection to device R2. R1 has an OSPF export policy configured. The export policy redistributes static routes from R1's routing table into R1's OSPF database. Because the static route is in R1's OSPF database, the route is advertised in an LSA to R1's OSPF neighbor. R1's OSPF neighbor is device R2.
- R2—Device R2 is in area 0.0.0.0 and has a direct connection to device R1. R2 has an OSPF import policy configured that matches the static route to the 10.0.16.0/30 network and prevents the static route from being installed in R2's routing table. R2's OSPF neighbor is device R1.

Configuration

CLI Quick Configuration

To quickly configure an OSPF import policy, copy the following commands, removing any line breaks, and then paste the commands into the CLI.

Configuration on Device R1:

```
[edit]
set interfaces so-0/2/0 unit 0 family inet address 10.0.2.1/30
set protocols ospf export export_static
set protocols ospf area 0.0.0.0 interface so-0/2/0
set policy-options policy-statement export_static from protocol static
set policy-options policy-statement export_static then accept
```

Configuration on Device R2:

```
[edit]
set interfaces so-0/2/0 unit 0 family inet address 10.0.2.2/30
set protocols ospf import filter_routes
set protocols ospf area 0.0.0.0 interface so-0/2/0
set policy-options policy-statement filter_routes from route-filter 10.0.16.0/30 exact
set policy-options policy-statement filter_routes then reject
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure an OSPF import policy:

1. Configure the interfaces.

   ```
   [edit]
   user@R1# set interfaces so-0/2/0 unit 0 family inet address 10.0.2.1/30
   ```

   ```
   [edit]
   user@R2# set interfaces so-0/2/0 unit 0 family inet address 10.0.2.2/30
   ```

2. Enable OSPF on the interfaces.

NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@R1# set protocols ospf area 0.0.0.0 interface so-0/2/0
```

```
[edit]
user@R2# set protocols ospf area 0.0.0.0 interface so-0/2/0
```

3. On R1, redistribute the static route into OSPF.

```
[edit]
user@R1# set protocols ospf export export_static
user@R1# set policy-options policy-statement export_static from protocol static
user@R1# set policy-options policy-statement export_static then accept
```

4. On R2, configure the OSPF import policy.

```
[edit]
user@R2# set protocols ospf import filter_routes
user@R2# set policy-options policy-statement filter_routes from route-filter
  10.0.16.0/30 exact
user@R2# set policy-options policy-statement filter_routes then reject
```

5. If you are done configuring the devices, commit the configuration.

```
[edit]
user@host# commit
```

Results Confirm your configuration by entering the **show interfaces**, **show policy-options**, and **show protocols ospf** commands on the appropriate device. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Output for R1:

```
user@R1# show interfaces
so-0/2/0 {
  unit 0 {
    family inet {
      address 10.0.2.1/30;
    }
  }
}
```

```
user@R1# show policy-options
policy-statement export_static {
  from protocol static;
  then accept;
}
```

```
user@R1# show protocols ospf
export export_static;
area 0.0.0.0 {
```



```
    interface so-0/2/0.0;
}
```

Output for R2:

```
user@R2# show interfaces
so-0/2/0 {
    unit 0 {
        family inet {
            address 10.0.2.2/30;
        }
    }
}
```

```
user@R2# show policy-options
policy-statement filter_routes {
    from {
        route-filter 10.0.16.0/30 exact;
    }
    then reject;
}
```

```
user@R2# show protocols ospf
import filter_routes;
area 0.0.0.0 {
    interface so-0/2/0.0;
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces**, **show policy-options**, **show routing-options**, and **show protocols ospf3** commands on the appropriate device.

Verification

Confirm that the configuration is working properly.

- Verifying the OSPF Database on page 292
- Verifying the Routing Table on page 292

Verifying the OSPF Database

Purpose Verify that OSPF is advertising the static route in the OSPF database.

Action From operational mode, enter the **show ospf database** for OSPFv2, and enter the **show ospf3 database** command for OSPFv3.

Verifying the Routing Table

Purpose Verify the entries in the routing table.

Action From operational mode, enter the **show route** command.

Example: Configuring a Route Filter Policy to Specify Priority for Prefixes Learned Through OSPF

This example shows how to create an OSPF import policy that prioritizes specific prefixes learned through OSPF.

Requirements

Before you begin:

- Configure the device interfaces.
- Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring an OSPF Router Identifier” on page 24.
- Control OSPF designated router election. See “Example: Controlling OSPF Designated Router Election” on page 26.
- Configure a single-area OSPF network. See “Example: Configuring a Single-Area OSPF Network” on page 29.
- Configure a multiarea OSPF network. See “Example: Configuring a Multiarea OSPF Network” on page 31.

Overview

In a network with a large number of OSPF routes, it can be useful to control the order in which routes are updated in response to a network topology change. In Junos OS Release 9.3 and later, you can specify a priority of high, medium, or low for prefixes included in an OSPF import policy. In the event of an OSPF topology change, high priority prefixes are updated in the routing table first, followed by medium and then low priority prefixes.

OSPF import policy can only be used to set priority or to filter OSPF external routes. If an OSPF import policy is applied that results in a **reject** terminating action for a nonexternal route, then the **reject** action is ignored and the route is accepted anyway. By default, such a route is now installed in the routing table with a priority of low. This behavior prevents traffic black holes, that is, silently discarded traffic, by ensuring consistent routing within the OSPF domain.

In general, OSPF routes that are not explicitly assigned a priority are treated as priority medium, except for the following:

- Summary discard routes have a default priority of low.
- Local routes that are not added to the routing table are assigned a priority of low.

- External routes that are rejected by import policy and thus not added to the routing table are assigned a priority of low.

Any available match criteria applicable to OSPF routes can be used to determine the priority. Two of the most commonly used match criteria for OSPF are the **route-filter** and **tag** statements.

In this example, the routing device is in area 0.0.0.0, with interfaces fe-0/1/0 and fe-1/1/0 connecting to neighboring devices. You configure an import routing policy named ospf-import to specify a priority for prefixes learned through OSPF. Routes associated with these prefixes are installed in the routing table in the order of the prefixes' specified priority. Routes matching **200.3.0.0/16 orlonger** are installed first because they have a priority of **high**. Routes matching **200.2.0.0/16 orlonger** are installed next because they have a priority of **medium**. Routes matching **200.1.0.0/16 orlonger** are installed last because they have a priority of **low**. You then apply the import policy to OSPF.

NOTE: The priority value takes effect when a new route is installed, or when there is a change to an existing route.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces fe-0/1/0 unit 0 family inet address 192.168.8.4/30
set interfaces fe-0/2/0 unit 0 family inet address 192.168.8.5/30
set policy-options policy-statement ospf-import term t1 from route-filter 200.1.0.0/16
   orlonger
set policy-options policy-statement ospf-import term t1 then priority low
set policy-options policy-statement ospf-import term t1 then accept
set policy-options policy-statement ospf-import term t2 from route-filter 200.2.0.0/16
   orlonger
set policy-options policy-statement ospf-import term t2 then priority medium
set policy-options policy-statement ospf-import term t2 then accept
set policy-options policy-statement ospf-import term t3 from route-filter 200.3.0.0/16
   orlonger
set policy-options policy-statement ospf-import term t3 then priority high
set policy-options policy-statement ospf-import term t3 then accept
set protocols ospf import ospf-import
set protocols ospf area 0.0.0.0 interface fe-0/1/0.0
set protocols ospf area 0.0.0.0 interface fe-0/2/0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an OSPF import policy that prioritizes specific prefixes:

1. Configure the device interfaces.

[edit interfaces]
user@host# **set fe-0/1/0 unit 0 family inet address 192.168.8.4/30**

user@host# **set fe-0/2/0 unit 0 family inet address 192.168.8.5/30**

2. Enable OSPF on the interfaces.

NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

[edit protocols ospf area 0.0.0.0]
user@host# **set interface fe-0/1/0.0**
user@host# **set interface fe-0/2/0.0**

3. Configure the policy to specify the priority for prefixes learned through OSPF.

[edit policy-options policy-statement ospf-import]
user@host# **set term t1 from route-filter 200.1.0.0/16 orlonger**
user@host# **set term t1 then priority low**
user@host# **set term t1 then accept**

user@host# **set term t2 from route-filter 200.2.0.0/16 orlonger**
user@host# **set term t2 then priority medium**
user@host# **set term t2 then accept**

user@host# **set term t3 from route-filter 200.3.0.0/16 orlonger**
user@host# **set term t3 then priority high**
user@host# **set term t3 then accept**

4. Apply the policy to OSPF.

[edit protocols ospf]
user@host# **set import ospf-import**

5. If you are done configuring the device, commit the configuration.

[edit]
user@host# **commit**

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show policy-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show interfaces
fe-0/1/0 {
  unit 0 {
    family inet {
      address 192.168.8.4/30;
    }
  }
}
  fe-0/2/0 {
    unit 0 {
```

```
            family inet {
                address 192.168.8.5/30;
            }
        }
    }
```

```
user@host# show protocols ospf
import ospf-import;
area 0.0.0.0 {
    interface fe-0/1/0.0;
    interface fe-0/2/0.0;
}
```

```
user@host# show policy-options
policy-statement ospf-import {
    term t1 {
        from {
            route-filter 200.1.0.0/16 orlonger;
        }
        then {
            priority low;
            accept;
        }
    }
    term t2 {
        from {
            route-filter 200.2.0.0/16 orlonger;
        }
        then {
            priority medium;
            accept;
        }
    }
    term t3 {
        from {
            route-filter 200.3.0.0/16 orlonger;
        }
        then {
            priority high;
            accept;
        }
    }
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces**, **show protocols ospf3**, and **show policy-options** commands.

Verification

Confirm that the configuration is working properly.

Verifying the Prefix Priority in the OSPF Routing Table

Purpose Verify the priority assigned to the prefix in the OSPF routing table.

Action From operational mode, enter the **show ospf route detail** for OSPFv2, and enter the **show ospf3 route detail** command for OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14
- *Routing Policy Match Conditions* in the *Routing Policy Feature Guide for Routing Devices*
- *Actions in Routing Policy Terms* in the *Routing Policy Feature Guide for Routing Devices*

Examples: Configuring Routing Policy for Network Summaries

Import and Export Policies for Network Summaries Overview

By default, OSPF uses network-summary link-state advertisements (LSAs) to transmit route information across area boundaries. Each area border router (ABR) floods network-summary LSAs to other routing devices in the same area. The ABR also controls which routes from the area are used to generate network-summary LSAs into other areas. Each ABR maintains a separate topological database for each area to which they are connected. In Junos OS Release 9.1 and later, you can configure export and import policies for OSPFv2 and OSPFv3 that enable you to control how network-summary LSAs, which contain information about interarea OSPF prefixes, are distributed and generated. For OSPFv3, the LSA is referred to as the interarea prefix LSA and performs the same function as a network-summary LSA performs for OSPFv2. An ABR originates an interarea prefix LSA for each IPv6 prefix that must be advertised into an area.

The export policy enables you to specify which summary LSAs are flooded into an area. The import policy enables you to control which routes learned from an area are used to generate summary LSAs into other areas. You define a routing policy at the **[edit policy-options policy-statement *policy-name*]** hierarchy level. As with all OSPF export policies, the default for network-summary LSA export policies is to reject everything. Similarly, as with all OSPF import policies, the default for network-summary LSA import policies is to accept all OSPF routes.

Example: Configuring an OSPF Export Policy for Network Summaries

This example shows how to create an OSPF export policy to control the network-summary (Type 3) LSAs that the ABR floods into an OSPF area.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26

Overview

OSPF uses network-summary LSAs to transmit route information across area boundaries. Depending on your network environment, you might want to further filter the network-summary LSAs between OSPF areas. For example, if you create OSPF areas to define administrative boundaries, you might not want to advertise internal route information between those areas. To further improve the control of route distribution between multiple OSPF areas, you can configure network summary policies on the ABR for the area that you want to filter the advertisement of network-summary LSAs.

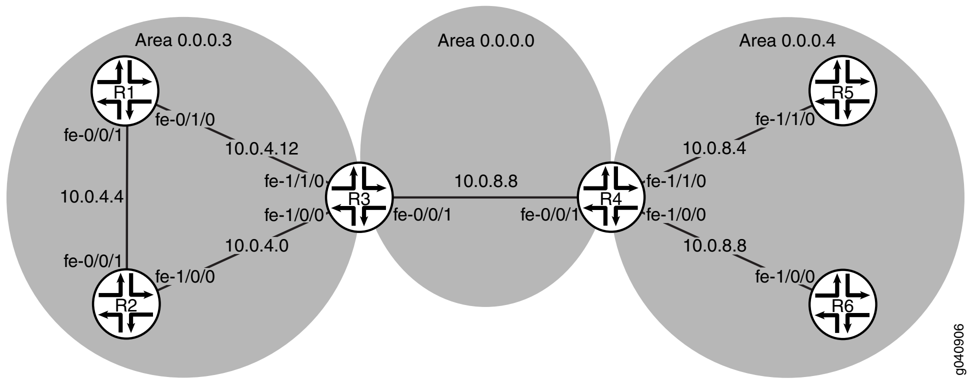
NOTE: For OSPFv3, the LSA is referred to as the interarea prefix LSA and performs the same function as a network-summary LSA performs for OSPFv2. An ABR originates an interarea prefix LSA for each IPv6 prefix that must be advertised into an area. In this topic, the terms network summary policy and network-summary policy are used to describe both OSPFv2 and OSPFv3 functionality.

The following guidelines apply to export network summary policies:

- You should have a thorough understanding of your network before configuring these policies. Incorrect network summary policy configuration might result in an unintended result such as suboptimal routing or dropped traffic.
- We recommend that you use the **route-filter** policy match condition for these types of policies.
- We recommend that you use the **accept** and **reject** routing policy terms for these types of policies.

Figure 22 on page 299 shows a sample topology with three OSPF areas. R4 generates network summaries for the routes in area 4 and sends them out of area 4 to area 0. R3 generates network summaries for the routes in area 3 and sends them out of area 3 to area 0.

Figure 22: Sample Topology Used for an OSPF Export Network Summary Policy



In this example, you configure R4 with an export network summary policy named export-policy that only allows routes that match the 10.0.4.4 prefix from area 3 into area 4. The export policy controls the network-summary LSAs that R4 floods into area 4. This results in only the allowed interarea route to enter area 4, and all other interarea routes to be purged from the OSPF database and the routing table of the devices in area 4. You first define the policy and then apply it to the ABR by including the **network-summary-export** statement for OSPFv2 or the **inter-area-prefix-export** statement for OSPFv3.

The devices operate as follows:

- R1—Device R1 is an internal router in area 3. Interface **fe-0/1/0** has an IP address of 10.0.4.13/30 and connects to R3. Interface **fe-0/0/1** has an IP address of 10.0.4.5/30 and connects to R2.
- R2—Device R2 is an internal router in area 3. Interface **fe-0/0/1** has an IP address of 10.0.4.6/30 and connects to R1. Interface **fe-1/0/0** has an IP address of 10.0.4.3 and connects to R3.
- R3—Device R3 participates in area 3 and area 0. R3 is the ABR between area 3 and area 0, and passes network-summary LSAs between the areas. Interface **fe-1/0/0** has an IP address of 10.0.4.2/30 and connects to R2. Interface **fe-1/1/0** has an IP address of 10.0.4.14/30 and connects to R1. Interface **fe-0/0/1** has an IP address of 10.0.2.3/30 and connects to R4.
- R4—Device R4 participates in area 0 and area 4. R4 is the ABR between area 0 and area 4, and passes network-summary LSAs between the areas. Interface **fe-0/0/1** has an IP address of 10.0.2.4/30 and connects to R3. Interface **fe-1/1/0** has an IP address of 10.0.8.3/30 and connects to R5. Interface **fe-1/0/0** has an IP address of 10.0.8.6/30 and connects to R6.
- R5—Device R5 is an internal router in area 4. Interface **fe-1/1/0** has an IP address of 10.0.8.5/30 and connects to R4.
- R6—Device R6 is an internal router in area 4. Interface **fe-1/0/0** has an IP address of 10.0.8.7/30 and connects to R4.

Configuration

CLI Quick Configuration

To quickly configure an OSPF export policy for network summaries, copy the following commands, removing any line breaks, and then paste the commands into the CLI.

Configuration on Device R1:

```
[edit]
set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.13/30
set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.5/30
set protocols ospf area 0.0.0.3 interface fe-0/1/0
set protocols ospf area 0.0.0.3 interface fe-0/0/1
```

Configuration on Device R2:

```
[edit]
set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.6/30
set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.3/30
set protocols ospf area 0.0.0.3 interface fe-0/1/0
set protocols ospf area 0.0.0.3 interface fe-1/0/0
```

Configuration on Device R3:

```
[edit]
set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.2/30
set interfaces fe-1/1/0 unit 0 family inet address 10.0.4.14/30
set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.3/30
set protocols ospf area 0.0.0.3 interface fe-1/0/0
set protocols ospf area 0.0.0.3 interface fe-1/1/0
set protocols ospf area 0.0.0.0 interface fe-0/0/1
```

Configuration on Device R4:

```
[edit]
set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.4/30
set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.3/30
set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.6/30
set policy-options policy-statement export-policy term term1 from route-filter 10.0.4.4/30
  prefix-length-range /30-/30
set policy-options policy-statement export-policy term term1 then accept
set protocols ospf area 0.0.0.0 interface fe-0/0/1
set protocols ospf area 0.0.0.4 interface fe-0/1/0
set protocols ospf area 0.0.0.4 interface fe-1/0/0
set protocols ospf area 0.0.0.4 network-summary-export export-policy
```

Configuration on Device R5:

```
[edit]
set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.5/30
set protocols ospf area 0.0.0.4 interface fe-0/1/0
```

Configuration on Device R6:

```
[edit]
set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.7/30
set protocols ospf area 0.0.0.4 interface fe-1/0/0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure an configure an OSPF export policy for network summaries:

1. Configure the interfaces.

   NOTE: For OSPFv3, use IPv6 addresses.

   ```
   [edit]
   user@R1# set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.13/30
   user@R1# set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.5/30

   [edit]
   user@R2# set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.6/30
   user@R2# set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.3/30

   [edit]
   user@R3# set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.2/30
   user@R3# set interfaces fe-1/1/0 unit 0 family inet address 10.0.4.14/30
   user@R3#set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.3/30

   [edit]
   user@R4# set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.4/30
   user@R4# set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.3/30
   user@R4# set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.6/30

   [edit]
   user@R5# set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.5/30

   [edit]
   user@R6# set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.7/30
   ```

2. Enable OSPF on the interfaces.

   NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@R1# set protocols ospf area 0.0.0.3 interface fe-0/1/0
   user@R1# set protocols ospf area 0.0.0.3 interface fe-0/0/1

   [edit]
   user@R2# set protocols ospf area 0.0.0.3 interface fe-0/1/0
   user@R2# set protocols ospf area 0.0.0.3 interface fe-1/0/0

   [edit]
   user@R3# set protocols ospf area 0.0.0.3 interface fe-1/0/0
   user@R3# set protocols ospf area 0.0.0.3 interface fe-1/1/0
   user@R3# set protocols ospf area 0.0.0.0 interface fe-0/0/1

   [edit]
   user@R4# set protocols ospf area 0.0.0.0 interface fe-0/0/1
   ```

user@R4# **set protocols ospf area 0.0.0.4 interface fe-1/1/0**
user@R4# **set protocols ospf area 0.0.0.4 interface fe-1/0/0**

[edit]
user@R5# **set protocols ospf area 0.0.0.4 interface fe-1/1/0**

[edit]
user@R6# **set protocols ospf area 0.0.0.4 interface fe-1/0/0**

3. On R4, configure the export network summary policy.

   [edit]
   user@R4# **set policy-options policy-statement export-policy term term1 from route-filter 10.0.4.4/30 prefix-length-range /30-/30**
   user@R4# **set policy-options policy-statement export-policy term term1 then accept**

4. On R4, apply the export network summary policy to OSPF.

   NOTE: For OSPFv3, include the **inter-area-prefix-export** statement at the **[edit protocols ospf3 area *area-id*]** hierarchy level.

   [edit]
   user@R4# **set protocols ospf area 0.0.0.4 network-summary-export export-policy**

5. If you are done configuring the devices, commit the configuration.

   [edit]
   user@host# **commit**

Results Confirm your configuration by entering the **show interfaces**, **show policy-options**, and **show protocols ospf** commands on the appropriate device. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Output for R1:

```
user@R1# show interfaces
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.4.5/30;
    }
  }
}
fe-1/1/0 {
  unit 0 {
    family inet {
      address 10.0.4.13/30;
    }
  }
}

user@R1# show protocols ospf
area 0.0.0.3 {
  interface fe-0/1/0.0;
```



```
  interface fe-0/0/1.0;
}
```

Output for R2:

```
user@R2# show interfaces
fe-0/1/0 {
  unit 0 {
    family inet {
      address 10.0.4.6/30;
    }
  }
}
fe-1/0/0 {
  unit 0 {
    family inet {
      address 10.0.4.3/30;
    }
  }
}

user@R2# show protocols ospf
area 0.0.0.3 {
  interface fe-0/1/0.0;
  interface fe-1/0/0.0;
}
```

Output for R3:

```
user@R3# show interfaces
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.2.3/30;
    }
  }
}
fe-1/0/0 {
  unit 0 {
    family inet {
      address 10.0.4.2/30;
    }
  }
}
fe-1/1/0 {
  unit 0 {
    family inet {
      address 10.0.4.14/30;
    }
  }
}

user@R3# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/1.0;
}
  area 0.0.0.3 {
    interface fe-1/0/0.0;
```

```
        interface fe-1/1/0.0;
    }
```

Output for R4:

```
user@R4# show interfaces
fe-0/0/1 {
    unit 0 {
        family inet {
            address 10.0.2.4/30;
        }
    }
}
fe-1/0/0 {
    unit 0 {
        family inet {
            address 10.0.8.6/30;
        }
    }
}
fe-1/1/0 {
    unit 0 {
        family inet {
            address 10.0.8.3/30;
        }
    }
}
```

```
user@R4# show protocols ospf
area 0.0.0.0 {
    interface fe-0/0/1.0;
}
area 0.0.0.4 {
    network-summary-export export-policy;
    interface fe-1/0/0.0;
    interface fe-1/1/0.0;
}
```

```
user@R4# show policy-options
policy-statement export-policy {
    term term1 {
        from {
            route-filter 10.0.4.4/30 prefix-length-range /30-/30;
        }
        then accept;
    }
}
```

Output for R5:

```
user@R5# show interfaces
fe-1/1/0 {
    unit 0 {
        family inet {
            address 10.0.8.5/30;
        }
    }
}
```

```
user@R5# show protocols ospf
area 0.0.0.4 {
  interface fe-1/1/0.0;
}
```

Output for R6:

```
user@R6# show interfaces
fe-1/0/0 {
  unit 0 {
    family inet {
      address 10.0.8.7/30;
    }
  }
}
```

```
user@R6# show protocols ospf
area 0.0.0.4 {
  interface fe-1/0/0.0;
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces**, **show policy-options**, and **show protocols ospf3** commands on the appropriate device.

Verification

Confirm that the configuration is working properly.

- Verifying the OSPF Database on page 305
- Verifying the Routing Table on page 305

Verifying the OSPF Database

Purpose Verify that the OSPF database for the devices in area 4 includes the interarea route that we permitted on the ABR R4. The other interarea routes that are not specified should age out or no longer be present in the OSPF database.

Action From operational mode, enter the **show ospf database netsummary area 0.0.0.4** command for OSPFv2, and enter the **show ospf3 database netsummary area 0.0.0.4** command for OSPFv3.

Verifying the Routing Table

Purpose Verify that the routes corresponding to the rejected network summaries are no longer present in R4's, R5's, or R6's routing table.

Action From operational mode, enter the **show route protocol ospf** command for both OSPFv2 and OSPFv3.

Example: Configuring an OSPF Import Policy for Network Summaries

This example shows how to create an OSPF import policy to control the network-summary (Type 3) LSAs that the ABR advertises out of an OSPF area.

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See "Example: Configuring an OSPF Router Identifier" on page 24.
- Control OSPF designated router election. See "Example: Controlling OSPF Designated Router Election" on page 26.

Overview

OSPF uses network-summary LSAs to transmit route information across area boundaries. Depending on your network environment, you might want to further filter the network-summary LSAs between OSPF areas. For example, if you create OSPF areas to define administrative boundaries, you might not want to advertise internal route information between those areas. To further improve the control of route distribution between multiple OSPF areas, you can configure network summary policies on the ABR for the area that you want to filter the advertisement of network-summary LSAs.

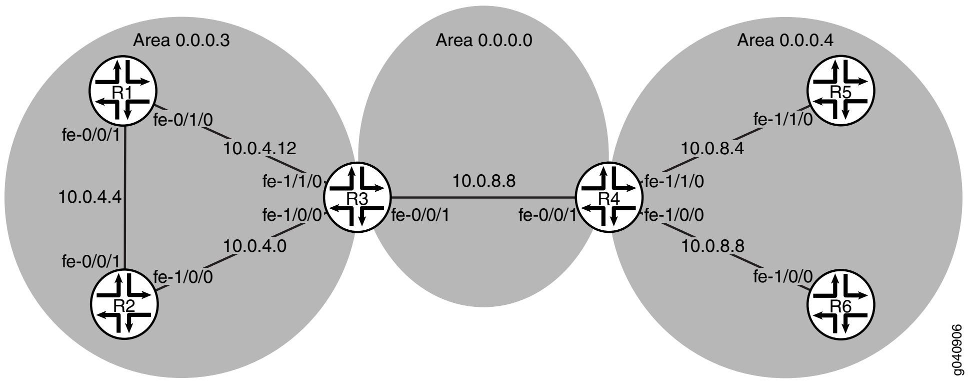
NOTE: For OSPFv3, the LSA is referred to as the interarea prefix LSA and performs the same function as a network-summary LSA performs for OSPFv2. An ABR originates an interarea prefix LSA for each IPv6 prefix that must be advertised into an area. In this topic, the terms network summary policy and network-summary policy are used to describe both OSPFv2 and OSPFv3 functionality.

The following guidelines apply to import network summary policies:

- You should have a thorough understanding of your network before configuring these policies. Incorrect network summary policy configuration might result in an unintended result such as suboptimal routing or dropped traffic.
- We recommend that you use the **route-filter** policy match condition for these types of policies.
- We recommend that you use the **accept** and **reject** routing policy terms for these types of policies.

Figure 23 on page 307 shows a sample topology with three OSPF areas. R4 generates network summaries for the routes in area 4 and sends them out of area 4 to area 0. R3 generates network summaries for the routes in area 3 and sends them out of area 3 to area 0.

Figure 23: Sample Topology Used for an OSPF Import Network Summary Policy



In this example, you configure R3 with an import network summary policy named import-policy so R3 only generates network summaries for the route 10.0.4.12/30. The import policy controls the routes and therefore the network summaries that R3 advertises out of area 3, so applying this policy means that R3 only advertises route 10.0.4.12/30 out of area 3. This results in existing network summaries from other interarea routes getting purged from the OSPF database in area 0 and area 4, as well as the routing tables of the devices in areas 0 and area 4. You first define the policy and then apply it to the ABR by including the **network-summary-import** statement for OSPFv2 or the **inter-area-prefix-import** statement for OSPFv3.

The devices operate as follows:

- R1—Device R1 is an internal router in area 3. Interface **fe-0/1/0** has an IP address of 10.0.4.13/30 and connects to R3. Interface **fe-0/0/1** has an IP address of 10.0.4.5/30 and connects to R2.
- R2—Device R2 is an internal router in area 3. Interface **fe-0/0/1** has an IP address of 10.0.4.6/30 and connects to R1. Interface **fe-1/0/0** has an IP address of 10.0.4.3 and connects to R3.
- R3—Device R3 participates in area 3 and area 0. R3 is the ABR between area 3 and area 0, and passes network-summary LSAs between the areas. Interface **fe-1/0/0** has an IP address of 10.0.4.2/30 and connects to R2. Interface **fe-1/1/0** has an IP address of 10.0.4.14/30 and connects to R1. Interface **fe-0/0/1** has an IP address of 10.0.2.3/30 and connects to R4.
- R4—Device R4 participates in area 0 and area 4. R4 is the ABR between area 0 and area 4, and passes network-summary LSAs between the areas. Interface **fe-0/0/1** has an IP address of 10.0.2.4/30 and connects to R3. Interface **fe-1/1/0** has an IP address of 10.0.8.3/30 and connects to R5. Interface **fe-1/0/0** has an IP address of 10.0.8.6/30 and connects to R6.

- R5—Device R5 is an internal router in area 4. Interface **fe-1/1/0** has an IP address of 10.0.8.5/30 and connects to R4.
- R6—Device R6 is an internal router in area 4. Interface **fe-1/0/0** has an IP address of 10.0.8.7/30 and connects to R4.

Configuration

CLI Quick Configuration

To quickly configure an OSPF import policy for network summaries, copy the following commands, removing any line breaks, and then paste the commands into CLI.

Configuration on Device R1:

```
[edit]
set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.13/30
set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.5/30
set protocols ospf area 0.0.0.3 interface fe-0/1/0
set protocols ospf area 0.0.0.3 interface fe-0/0/1
```

Configuration on Device R2:

```
[edit]
set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.6/30
set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.3/30
set protocols ospf area 0.0.0.3 interface fe-0/1/0
set protocols ospf area 0.0.0.3 interface fe-1/0/0
```

Configuration on Device R3:

```
[edit]
set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.2/30
set interfaces fe-1/1/0 unit 0 family inet address 10.0.4.14/30
set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.3/30
set policy-options policy-statement import-policy term term1 from route-filter 10.0.4.12/30
  prefix-length-range /30-/30
set policy-options policy-statement import-policy term term1 then accept
set protocols ospf area 0.0.0.3 interface fe-1/0/0
set protocols ospf area 0.0.0.3 interface fe-1/1/0
set protocols ospf area 0.0.0.0 interface fe-0/0/1
set protocols ospf area 0.0.0.3 network-summary-import import-policy
```

Configuration on Device R4:

```
[edit]
set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.4/30
set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.3/30
set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.6/30
set protocols ospf area 0.0.0.0 interface fe-0/0/1
set protocols ospf area 0.0.0.4 interface fe-1/1/0
set protocols ospf area 0.0.0.4 interface fe-1/0/0
```

Configuration on Device R5:

```
[edit]
set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.5/30
set protocols ospf area 0.0.0.4 interface fe-1/1/0
```

Configuration on Device R6:

```
[edit]
set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.7/30
set protocols ospf area 0.0.0.4 interface fe-1/0/0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure an configure an OSPF export policy for network summaries:

1. Configure the interfaces.

   NOTE: For OSPFv3, use IPv6 addresses.

   ```
   [edit]
   user@R1# set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.13/30
   user@R1# set interfaces fe-0/0/1 unit 0 family inet address 10.0.4.5/30

   [edit]
   user@R2# set interfaces fe-0/1/0 unit 0 family inet address 10.0.4.6/30
   user@R2# set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.3/30

   [edit]
   user@R3# set interfaces fe-1/0/0 unit 0 family inet address 10.0.4.2/30
   user@R3# set interfaces fe-1/1/0 unit 0 family inet address 10.0.4.14/30
   user@R3#set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.3/30

   [edit]
   user@R4# set interfaces fe-0/0/1 unit 0 family inet address 10.0.2.4/30
   user@R4# set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.3/30
   user@R4# set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.6/30

   [edit]
   user@R5# set interfaces fe-1/1/0 unit 0 family inet address 10.0.8.5/30

   [edit]
   user@R6# set interfaces fe-1/0/0 unit 0 family inet address 10.0.8.7/30
   ```

2. Enable OSPF on the interfaces.

   NOTE: For OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@R1# set protocols ospf area 0.0.0.3 interface fe-0/1/0
   user@R1# set protocols ospf area 0.0.0.3 interface fe-0/0/1

   [edit]
   user@R2# set protocols ospf area 0.0.0.3 interface fe-0/1/0
   user@R2# set protocols ospf area 0.0.0.3 interface fe-1/0/0

   [edit]
   user@R3# set protocols ospf area 0.0.0.3 interface fe-1/0/0
   ```

```
user@R3# set protocols ospf area 0.0.0.3 interface fe-1/1/0
user@R3# set protocols ospf area 0.0.0.0 interface fe-0/0/1

[edit]
user@R4# set protocols ospf area 0.0.0.0 interface fe-0/0/1
user@R4# set protocols ospf area 0.0.0.4 interface fe-1/1/0
user@R4# set protocols ospf area 0.0.0.4 interface fe-1/0/0

[edit]
user@R5# set protocols ospf area 0.0.0.4 interface fe-1/1/0

[edit]
user@R6# set protocols ospf area 0.0.0.4 interface fe-1/0/0
```

3. On R3, configure the import network summary policy.

```
[edit ]
user@R3# set policy-options policy-statement import-policy term term1 from
  route-filter 10.0.4.12/30 prefix-length-range /30-/30
user@R3# set policy-options policy-statement export-policy term term1 then accept
```

4. On R3, apply the import network summary policy to OSPF.

NOTE: For OSPFv3, include the **inter-area-prefix-export** statement at the **[edit protocols ospf3 area *area-id*]** hierarchy level.

```
[edit]
user@R3# set protocols ospf area 0.0.0.4 network-summary-import import-policy
```

5. If you are done configuring the devices, commit the configuration.

```
[edit]
user@host# commit
```

Results

Confirm your configuration by entering the **show interfaces**, **show policy-options**, and **show protocols ospf** commands on the appropriate device. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Output for R1:

```
user@R1# show interfaces
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.4.5/30;
    }
  }
}
fe-0/1/0 {
  unit 0 {
    family inet {
      address 10.0.4.13/30;
    }
  }
```

```
}
user@R1# show protocols ospf
area 0.0.0.3 {
   interface fe-0/1/0.0;
   interface fe-0/0/1.0;
}
```

Output for R2:

```
user@R2# show interfaces
fe-0/1/0 {
   unit 0 {
      family inet {
         address 10.0.4.6/30;
      }
   }
}
fe-1/0/0 {
   unit 0 {
      family inet {
         address 10.0.4.3/30;
      }
   }
}
user@R2# show protocols ospf
area 0.0.0.3 {
   interface fe-0/1/0.0;
   interface fe-1/0/0.0;
}
```

Output for R3:

```
user@R3# show interfaces
fe-0/0/1 {
   unit 0 {
      family inet {
         address 10.0.2.3/30;
      }
   }
}
fe-1/0/0 {
   unit 0 {
      family inet {
         address 10.0.4.2/30;
      }
   }
}
fe-1/1/0 {
   unit 0 {
      family inet {
         address 10.0.4.14/30;
      }
   }
}
user@R3# show protocols ospf
```



```
area 0.0.0.0 {
  interface fe-0/0/1.0;
}
  area 0.0.0.3 {
    network-summary-export export-policy;
    interface fe-1/0/0.0;
    interface fe-1/1/0.0;
  }
```

```
user@R3# show policy-options
policy-statement export-policy {
  term term1 {
    from {
      route-filter 10.0.4.12/30 prefix-length-range /30-/30;
    }
    then accept;
  }
}
```

Output for R4:

```
user@R4# show interfaces
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.0.2.4/30;
    }
  }
}
fe-1/0/0 {
  unit 0 {
    family inet {
      address 10.0.8.6/30;
    }
  }
}
fe-1/1/0 {
  unit 0 {
    family inet {
      address 10.0.8.3/30;
    }
  }
}
```

```
user@R4# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/1.0;
}
area 0.0.0.4 {
  interface fe-0/1/0.0;
  interface fe-1/0/0.0;
}
```

Output for R5:

```
user@R5# show interfaces
fe-1/1/0 {
  unit 0 {
```



```
        family inet {
            address 10.0.8.5/30;
        }
    }
}
```

```
user@R5# show protocols ospf
area 0.0.0.4 {
    interface fe-1/1/0.0;
}
```

Output for R6:

```
user@R6# show interfaces
fe-1/0/0 {
    unit 0 {
        family inet {
            address 10.0.8.7/30;
        }
    }
}
```

```
user@R6# show protocols ospf
area 0.0.0.4 {
    interface fe-1/0/0.0;
}
```

To confirm your OSPFv3 configuration, enter the **show interfaces**, **show policy-options**, and **show protocols ospf3** commands on the appropriate device.

Verification

Confirm that the configuration is working properly.

- Verifying the OSPF Database on page 313
- Verifying the Routing Table on page 313

Verifying the OSPF Database

Purpose Verify that the OSPF database for the devices in area 4 includes the interarea route that we are advertising from R3. Any other routes from area 3 should not be advertised into area 4, so those entries should age out or no longer be present in the OSPF database.

Action From operational mode, enter the **show ospf database netsummary area 0.0.0.4** command for OSPFv2, and enter the **show ospf3 database netsummary area 0.0.0.4** command for OSPFv3.

Verifying the Routing Table

Purpose Verify that the specified route is included in R4's, R5's, or R6's routing table. Any other routes from area 3 should not be advertised into area 4.

Action From operational mode, enter the **show route protocol ospf** command for both OSPFv2 and OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14
- *Routing Policy Match Conditions* in the *Routing Policy Feature Guide for Routing Devices*
- *Actions in Routing Policy Terms* in the *Routing Policy Feature Guide for Routing Devices*

Example: Redistributing OSPF Routes into IS-IS

Understanding Routing Policies

For some routing platform vendors, the flow of routes occurs between various protocols. If, for example, you want to configure redistribution from RIP to OSPF, the RIP process tells the OSPF process that it has routes that might be included for redistribution. In Junos OS, there is not much direct interaction between the routing protocols. Instead, there are central gathering points where all protocols install their routing information. These are the main unicast routing tables inet.0 and inet6.0.

From these tables, the routing protocols calculate the best route to each destination and place these routes in a forwarding table. These routes are then used to forward routing protocol traffic toward a destination, and they can be advertised to neighbors.

Importing and Exporting Routes

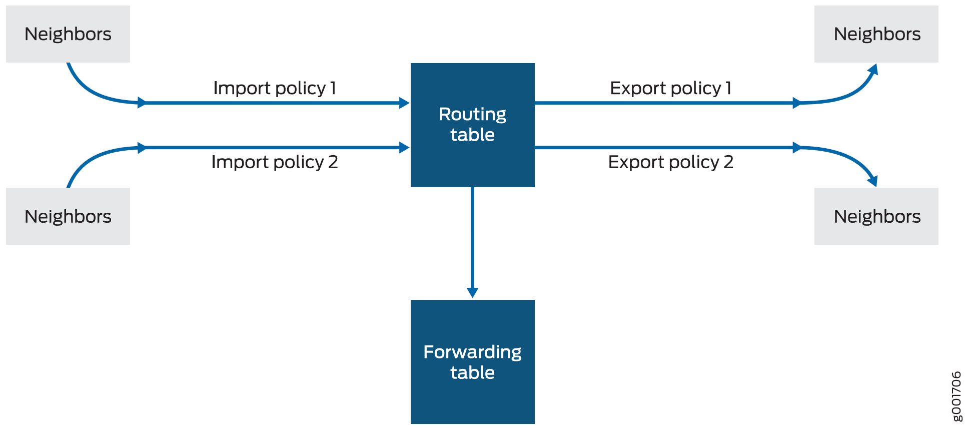
Two terms—*import* and *export*—explain how routes move between the routing protocols and the routing table.

- When the Routing Engine places the routes of a routing protocol into the routing table, it is *importing* routes into the routing table.
- When the Routing Engine uses active routes from the routing table to send a protocol advertisement, it is *exporting* routes from the routing table.

NOTE: The process of moving routes between a routing protocol and the routing table is described always *from the point of view of the routing table*. That is, routes are *imported into* a routing table from a routing protocol and they are *exported from* a routing table to a routing protocol. Remember this distinction when working with routing policies.

As shown in Figure 24 on page 315, you use import routing policies to control which routes are placed in the routing table, and export routing policies to control which routes are advertised from the routing table to neighbors.

Figure 24: Importing and Exporting Routes



In general, the routing protocols place all their routes in the routing table and advertise a limited set of routes from the routing table. The general rules for handling the routing information between the routing protocols and the routing table are known as the *routing policy framework*.

The routing policy framework is composed of default rules for each routing protocol that determine which routes the protocol places in the routing table and advertises from the routing table. The default rules for each routing protocol are known as *default routing policies*.

You can create routing policies to preempt the default policies, which are always present. A *routing policy* allows you to modify the routing policy framework to suit your needs. You can create and implement your own routing policies to do the following:

- Control which routes a routing protocol places in the routing table.
- Control which active routes a routing protocol advertises from the routing table. An *active route* is a route that is chosen from all routes in the routing table to reach a destination.
- Manipulate the route characteristics as a routing protocol places the route in the routing table or advertises the route from the routing table.

You can manipulate the route characteristics to control which route is selected as the active route to reach a destination. The active route is placed in the forwarding table and is used to forward traffic toward the route's destination. In general, the active route is also advertised to a router's neighbors.

Active and Inactive Routes

When multiple routes for a destination exist in the routing table, the protocol selects an active route and that route is placed in the appropriate routing table. For equal-cost routes, the Junos OS places multiple next hops in the appropriate routing table.

When a protocol is exporting routes from the routing table, it exports active routes only. This applies to actions specified by both default and user-defined export policies.

When evaluating routes for export, the Routing Engine uses only active routes from the routing table. For example, if a routing table contains multiple routes to the same destination and one route has a preferable metric, only that route is evaluated. In other words, an export policy does not evaluate all routes; it evaluates only those routes that a routing protocol is allowed to advertise to a neighbor.

NOTE: By default, BGP advertises active routes. However, you can configure BGP to advertise *inactive routes*, which go to the same destination as other routes but have less preferable metrics.

Explicitly Configured Routes

An *explicitly configured route* is a route that you have configured. *Direct routes* are not explicitly configured. They are created as a result of IP addresses being configured on an interface Explicitly configured routes include aggregate, generated, local, and static routes. (An *aggregate route* is a route that distills groups of routes with common addresses into one route. A *generated route* is a route used when the routing table has no information about how to reach a particular destination. A *local route* is an IP address assigned to a router interface. A *static route* is an unchanging route to a destination.)

The policy framework software treats direct and explicitly configured routes as if they are learned through routing protocols; therefore, they can be imported into the routing table. Routes cannot be exported from the routing table to the pseudoprotocol, because this protocol is not a real routing protocol. However, aggregate, direct, generated, and static routes can be exported from the routing table to routing protocols, whereas local routes cannot.

Dynamic Database

In Junos OS Release 9.5 and later, you can configure routing policies and certain routing policy objects in a dynamic database that is not subject to the same verification required by the standard configuration database. As a result, you can quickly commit these routing policies and policy objects, which can be referenced and applied in the standard configuration as needed. BGP is the only protocol to which you can apply routing policies that reference policies configured in the dynamic database. After a routing policy based on the dynamic database is configured and committed in the standard configuration, you can quickly make changes to existing routing policies by modifying policy objects in the dynamic database. Because Junos OS does not validate configuration changes to the dynamic database, when you use this feature, you should test and verify all configuration changes before committing them.

Example: Redistributing OSPF Routes into IS-IS

This example shows how to redistribute OSPF routes into an IS-IS network.

- Requirements on page 317
- Overview on page 317

- Configuration on page 318
- Verification on page 323

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

Export policy can be applied to IS-IS to facilitate route redistribution.

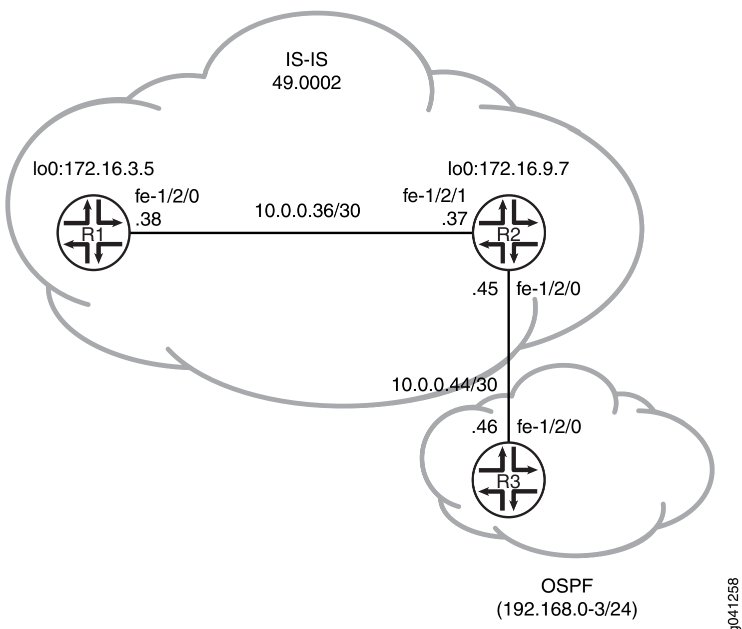
Junos OS does not support the application of import policy for link-state routing protocols like IS-IS because such policies can lead to inconsistent link-state database (LSDB) entries, which in turn can result in routing inconstancies.

In this example, OSPF routes 192.168.0/24 through 192.168.3/24 are redistributed into IS-IS area 49.0002 from Device R2.

In addition, policies are configured to ensure that Device R1 can reach destinations on the 10.0.0.44/30 network, and that Device R3 can reach destinations on the 10.0.0.36/30 network. This enables end-to-end reachability.

Figure 25 on page 317 shows the topology used in this example.

Figure 25: IS-IS Route Redistribution Topology



"CLI Quick Configuration" on page 318 shows the configuration for all of the devices in Figure 25 on page 317. The section "Step-by-Step Procedure" on page 319 describes the steps on Device R2. "Step-by-Step Procedure" on page 320 describes the steps on Device R3.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device R1

```
set interfaces fe-1/2/0 unit 0 description to-R7
set interfaces fe-1/2/0 unit 0 family inet address 10.0.0.38/30
set interfaces fe-1/2/0 unit 0 family iso
set interfaces lo0 unit 0 family inet address 172.16.3.5/32
set interfaces lo0 unit 0 family iso address 49.0002.0172.0016.0305.00
set protocols isis interface fe-1/2/0.38
set protocols isis interface lo0.0
```

Device R2

```
set interfaces fe-1/2/1 unit 0 description to-R5
set interfaces fe-1/2/1 unit 0 family inet address 10.0.0.37/30
set interfaces fe-1/2/1 unit 0 family iso
set interfaces fe-1/2/0 unit 0 description to-OSPF-network
set interfaces fe-1/2/0 unit 0 family inet address 10.0.0.45/30
set interfaces lo0 unit 0 family inet address 172.16.9.7/32
set interfaces lo0 unit 0 family iso address 49.0002.0172.0016.0907.00
set protocols isis export ospf-isis
set protocols isis export send-direct-to-isis-neighbors
set protocols isis interface fe-1/2/1.0
set protocols isis interface lo0.0
set protocols ospf export send-direct-to-ospf-neighbors
set protocols ospf area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf area 0.0.0.1 interface lo0.0 passive
set policy-options policy-statement ospf-isis term 1 from protocol ospf
set policy-options policy-statement ospf-isis term 1 from route-filter 192.168.0.0/22
  longer
set policy-options policy-statement ospf-isis term 1 then accept
set policy-options policy-statement send-direct-to-isis-neighbors from protocol direct
set policy-options policy-statement send-direct-to-isis-neighbors from route-filter
  10.0.0.44/30 exact
set policy-options policy-statement send-direct-to-isis-neighbors then accept
set policy-options policy-statement send-direct-to-ospf-neighbors from protocol direct
set policy-options policy-statement send-direct-to-ospf-neighbors from route-filter
  10.0.0.36/30 exact
set policy-options policy-statement send-direct-to-ospf-neighbors then accept
```

Device R3

```
set interfaces fe-1/2/0 unit 0 family inet address 10.0.0.46/30
set interfaces lo0 unit 0 family inet address 192.168.1.1/32
set interfaces lo0 unit 0 family inet address 192.168.2.1/32
set interfaces lo0 unit 0 family inet address 192.168.3.1/32
set interfaces lo0 unit 0 family inet address 192.168.0.1/32
set protocols ospf export ospf
set protocols ospf area 0.0.0.1 interface fe-1/2/0.0
set protocols ospf area 0.0.0.1 interface lo0.0 passive
set policy-options policy-statement ospf term 1 from protocol static
set policy-options policy-statement ospf term 1 then accept
set routing-options static route 192.168.0.0/24 discard
set routing-options static route 192.168.1.0/24 discard
set routing-options static route 192.168.3.0/24 discard
```


set routing-options static route 192.168.2.0/24 discard

Step-by-Step Procedure

To configure Device R2:

1. Configure the network interfaces.

   [edit interfaces]
   user@R2# **set fe-1/2/1 unit 0 description to-R5**
   user@R2# **set fe-1/2/1 unit 0 family inet address 10.0.0.37/30**
   user@R2# **set fe-1/2/1 unit 0 family iso**
   user@R2# **set fe-1/2/0 unit 0 description to-OSPF-network**
   user@R2# **set fe-1/2/0 unit 0 family inet address 10.0.0.45/30**
   user@R2# **set lo0 unit 0 family inet address 172.16.9.7/32**
   user@R2# **set lo0 unit 0 family iso address 49.0002.0172.0016.0907.00**

2. Configure IS-IS on the interface facing Device R1 and the loopback interface.

   [edit protocols isis]
   user@R2# **set interface fe-1/2/1.0**
   user@R2# **set interface lo0.0**

3. Configure the policy that enables Device R1 to reach the 10.0.0.44/30 network.

   [edit policy-options policy-statement send-direct-to-isis-neighbors]
   user@R2# **set from protocol direct**
   user@R2# **set from route-filter 10.0.0.44/30 exact**
   user@R2# **set then accept**

4. Apply the policy that enables Device R1 to reach the 10.0.0.44/30 network.

   [edit protocols isis]
   user@R2# **set export send-direct-to-isis-neighbors**

5. Configure OSPF on the interfaces.

   [edit protocols ospf]
   user@R2# **set area 0.0.0.1 interface fe-1/2/0.0**
   user@R2# **set area 0.0.0.1 interface lo0.0 passive**

6. Configure the OSPF route redistribution policy.

   [edit policy-options policy-statement ospf-isis term 1]
   user@R2# **set from protocol ospf**
   user@R2# **set from route-filter 192.168.0.0/22 longer**
   user@R2# **set then accept**

7. Apply the OSPF route redistribution policy to the IS-IS instance.

   [edit protocols isis]
   user@R2# **set export ospf-isis**

8. Configure the policy that enables Device R3 to reach the 10.0.0.36/30 network.

   [edit policy-options policy-statement send-direct-to-ospf-neighbors]
   user@R2# **set from protocol direct**
   user@R2# **set from route-filter 10.0.0.36/30 exact**
   user@R2# **set then accept**

9. Apply the policy that enables Device R3 to reach the 10.0.0.36/30 network.

   [edit protocols ospf]
   user@R2# **set export send-direct-to-ospf-neighbors**

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure multi-level IS-IS:

1. Configure the network interfaces.

   Multiple addresses are configured on the loopback interface to simulate multiple route destinations.

   ```
   [edit interfaces]
   user@R3# set fe-1/2/0 unit 0 family inet address 10.0.0.46/30
   user@R3# set lo0 unit 0 family inet address 192.168.1.1/32
   user@R3# set lo0 unit 0 family inet address 192.168.2.1/32
   user@R3# set lo0 unit 0 family inet address 192.168.3.1/32
   user@R3# set lo0 unit 0 family inet address 192.168.0.1/32
   ```

2. Configure static routes to the loopback interface addresses.

   These are the routes that are redistributed into IS-IS.

   ```
   [edit routing-options static]
   user@R3# set route 192.168.0.0/24 discard
   user@R3# set route 192.168.1.0/24 discard
   user@R3# set route 192.168.3.0/24 discard
   user@R3# set route 192.168.2.0/24 discard
   ```

3. Configure OSPF on the interfaces.

   ```
   [edit protocols ospf area 0.0.0.1]
   user@R3# set interface fe-1/2/0.0
   user@R3# set interface lo0.0 passive
   ```

4. Configure the OSPF policy to export the static routes.

   ```
   [edit policy-options policy-statement ospf term 1]
   user@R3# set from protocol static
   user@R3# set then accept
   ```

5. Apply the OSPF export policy.

   ```
   [edit protocols ospf]
   user@R3# set export ospf
   ```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device R2

```
user@R2# show interfaces
fe-1/2/1 {
  unit 0 {
    description to-R5;
    family inet {
      address 10.0.0.37/30;
    }
    family iso;
  }
```

```
}
fe-1/2/0 {
   unit 0 {
      description to-OSPF-network;
      family inet {
         address 10.0.0.45/30;
      }
   }
}
lo0 {
   unit 0 {
      family inet {
         address 172.16.9.7/32;
      }
      family iso {
         address 49.0002.0172.0016.0907.00;
      }
   }
}

user@R2# show protocols
isis {
   export [ ospf-isis send-direct-to-isis-neighbors ];
   interface fe-1/2/1.0;
   interface lo0.0;
}
ospf {
   export send-direct-to-ospf-neighbors;
   area 0.0.0.1 {
      interface fe-1/2/0.0;
      interface lo0.0 {
         passive;
      }
   }
}

user@R2# show policy-options
policy-statement ospf-isis {
   term 1 {
      from {
         protocol ospf;
         route-filter 192.168.0.0/22 longer;
      }
      then accept;
   }
}
policy-statement send-direct-to-isis-neighbors {
   from {
      protocol direct;
      route-filter 10.0.0.44/30 exact;
   }
   then accept;
}
policy-statement send-direct-to-ospf-neighbors {
   from {
      protocol direct;
```

```
        route-filter 10.0.0.36/30 exact;
    }
    then accept;
}
```

Device R3

```
user@R3# show interfaces
fe-1/2/0 {
    unit 0 {
        family inet {
            address 10.0.0.46/30;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.1.1/32;
            address 192.168.2.1/32;
            address 192.168.3.1/32;
            address 192.168.0.1/32;
        }
    }
}

user@R3# show protocols
ospf {
    export ospf;
    area 0.0.0.1 {
        interface fe-1/2/0.0;
        interface lo0.0 {
            passive;
        }
    }
}

user@R3# show policy-options
policy-statement ospf {
    term 1 {
        from protocol static;
        then accept;
    }
}

user@R3# show routing-options
static {
    route 192.168.0.0/24 discard;
    route 192.168.1.0/24 discard;
    route 192.168.3.0/24 discard;
    route 192.168.2.0/24 discard;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying OSPF Route Advertisement on page 323
- Verifying Route Redistribution on page 323
- Verifying Connectivity on page 324

Verifying OSPF Route Advertisement

Purpose Make sure that the expected routes are advertised by OSPF.

Action From operational mode on Device R2, enter the **show route protocol ospf** command.

```
user@R2> show route protocol ospf


inet.0: 15 destinations, 15 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/24     *[OSPF/150] 03:54:21, metric 0, tag 0
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.0.1/32     *[OSPF/10] 03:54:21, metric 1
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.1.0/24     *[OSPF/150] 03:54:21, metric 0, tag 0
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.1.1/32     *[OSPF/10] 03:54:21, metric 1
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.2.0/24     *[OSPF/150] 03:54:21, metric 0, tag 0
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.2.1/32     *[OSPF/10] 03:54:21, metric 1
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.3.0/24     *[OSPF/150] 03:54:21, metric 0, tag 0
                    > to 10.0.0.46 via fe-1/2/0.0
192.168.3.1/32     *[OSPF/10] 03:54:21, metric 1
                    > to 10.0.0.46 via fe-1/2/0.0
224.0.0.5/32       *[OSPF/10] 03:56:03, metric 1
                         MultiRecv

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

Meaning The 192.168/16 routes are advertised by OSPF.

Verifying Route Redistribution

Purpose Make sure that the expected routes are redistributed from OSPF into IS-IS.

Action From operational mode on Device R1, enter the **show route protocol isis** command.

```
user@R1> show route protocol isis


inet.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.44/30       *[IS-IS/160] 03:45:24, metric 20
                    > to 10.0.0.37 via fe-1/2/0.0
```



```
172.16.9.7/32      *[IS-IS/15] 03:49:46, metric 10
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.0.0/24     *[IS-IS/160] 03:49:46, metric 10
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.0.1/32     *[IS-IS/160] 03:49:46, metric 11, tag2 1
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.1.0/24     *[IS-IS/160] 03:49:46, metric 10
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.1.1/32     *[IS-IS/160] 03:49:46, metric 11, tag2 1
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.2.0/24     *[IS-IS/160] 03:49:46, metric 10
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.2.1/32     *[IS-IS/160] 03:49:46, metric 11, tag2 1
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.3.0/24     *[IS-IS/160] 03:49:46, metric 10
                    > to 10.0.0.37 via fe-1/2/0.0
192.168.3.1/32     *[IS-IS/160] 03:49:46, metric 11, tag2 1
                    > to 10.0.0.37 via fe-1/2/0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

Meaning The 192.168/16 routes are redistributed into IS-IS.

Verifying Connectivity

Purpose Check that Device R1 can reach the destinations on Device R3.

Action From operational mode, enter the **ping** command.

```
user@R1> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=63 time=2.089 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=1.270 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=2.135 ms
```

Meaning These results confirm that Device R1 can reach the destinations in the OSPF network.

Related Documentation

- *Example: Configuring IS-IS*

CHAPTER 16

OSPF and Logical Systems Configuration

Examples: Configuring OSPF and Logical Systems

OSPF Support for Logical Systems

This topic describes the following information:

Introduction to Logical Systems

With Junos OS, you can partition a single physical router into multiple logical devices that perform independent routing tasks. Because logical systems perform a subset of the tasks once handled by the main router, logical systems offer an effective way to maximize the use of a single routing or switching platform. Logical systems have their own unique routing tables, interfaces, policies, and routing instances.

OSPF and Logical Systems

You can configure both OSPF Version 2 (OSPFv2) and OSPF Version 3 (OSPFv3) for logical systems. In the case of OSPFv3, you can also configure OSPFv3 realms for logical systems, which allows OSPFv3 to advertise address families other than unicast IPv6.

You configure OSPF for logical systems at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* protocols (ospf | ospf3)]**
- **[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]**

- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]**

Example: Configuring OSPF on Logical Systems Within the Same Router

This example shows how to configure an OSPF network using multiple logical systems that are running on a single physical router. The logical systems are connected by logical tunnel interfaces.

Requirements

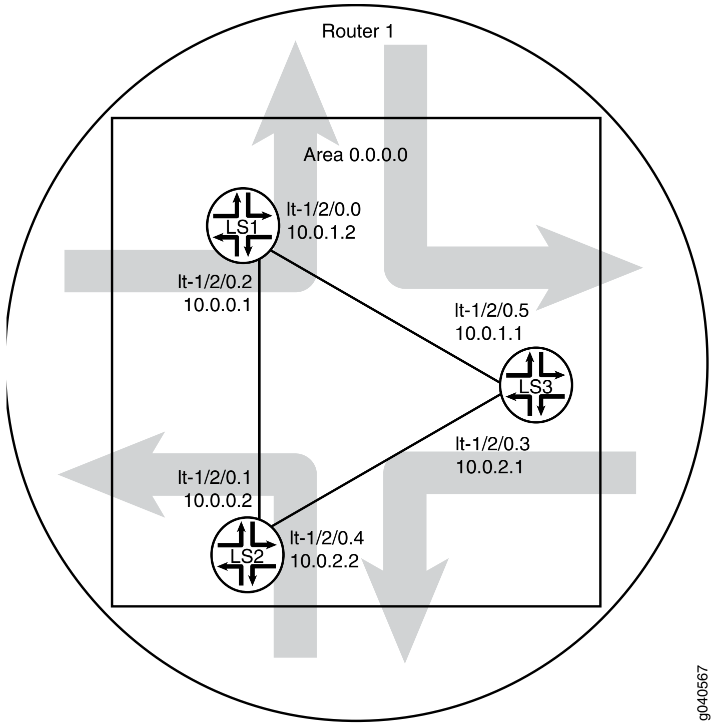
You must connect the logical systems by using logical tunnel (**lt**) interfaces. See *Example: Connecting Logical Systems Within the Same Router Using Logical Tunnel Interfaces*.

Overview

This example shows the configuration of a single OSPF area with three logical systems running on one physical router. Each logical system has its own routing table. The configuration enables the protocol on all logical system interfaces that participate in the OSPF domain and specifies the area that the interfaces are in.

Figure 26 on page 327 shows the sample network.

Figure 26: OSPF on Logical Systems



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set logical-systems LS1 interfaces lt-1/2/0 unit 0 description LS1->LS3
set logical-systems LS1 interfaces lt-1/2/0 unit 0 encapsulation ethernet
set logical-systems LS1 interfaces lt-1/2/0 unit 0 peer-unit 5
set logical-systems LS1 interfaces lt-1/2/0 unit 0 family inet address 10.0.1.2/30
set logical-systems LS1 interfaces lt-1/2/0 unit 2 description LS1->LS2
set logical-systems LS1 interfaces lt-1/2/0 unit 2 encapsulation ethernet
set logical-systems LS1 interfaces lt-1/2/0 unit 2 peer-unit 1
set logical-systems LS1 interfaces lt-1/2/0 unit 2 family inet address 10.0.0.1/30
set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.0
set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.2
set logical-systems LS2 interfaces lt-1/2/0 unit 1 description LS2->LS1
set logical-systems LS2 interfaces lt-1/2/0 unit 1 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 1 peer-unit 2
set logical-systems LS2 interfaces lt-1/2/0 unit 1 family inet address 10.0.0.2/30
set logical-systems LS2 interfaces lt-1/2/0 unit 4 description LS2->LS3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 4 peer-unit 3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 family inet address 10.0.2.2/30
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.1
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.4
set logical-systems LS3 interfaces lt-1/2/0 unit 3 description LS3->LS2
```


set logical-systems LS3 interfaces lt-1/2/0 unit 3 encapsulation ethernet
set logical-systems LS3 interfaces lt-1/2/0 unit 3 peer-unit 4
set logical-systems LS3 interfaces lt-1/2/0 unit 3 family inet address 10.0.2.1/30
set logical-systems LS3 interfaces lt-1/2/0 unit 5 description LS3->LS1
set logical-systems LS3 interfaces lt-1/2/0 unit 5 encapsulation ethernet
set logical-systems LS3 interfaces lt-1/2/0 unit 5 peer-unit 0
set logical-systems LS3 interfaces lt-1/2/0 unit 5 family inet address 10.0.1.1/30
set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.5
set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.3

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF on logical systems:

1. Configure the logical tunnel interface on Logical System LS1 connecting to Logical System LS2.

   [edit]
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 2 description LS1->LS2**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 2 encapsulation ethernet**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 2 peer-unit 1**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 2 family inet address 10.0.0.1/30**

2. Configure the logical tunnel interface on Logical System LS1 connecting to Logical System LS3.

   [edit]
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 0 description LS1->LS3**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 0 encapsulation ethernet**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 0 peer-unit 5**
   user@host# **set logical-systems LS1 interfaces lt-1/2/0 unit 0 family inet address 10.0.1.2/30**

3. Configure the logical tunnel interface on Logical System LS2 connecting to Logical System LS1.

   [edit]
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 1 description LS2->LS1**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 1 encapsulation ethernet**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 1 peer-unit 2**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 1 family inet address 10.0.0.2/30**

4. Configure the logical tunnel interface on Logical System LS2 connecting to Logical System LS3.

   [edit]
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 4 description LS2->LS3**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 4 encapsulation ethernet**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 4 peer-unit 3**
   user@host# **set logical-systems LS2 interfaces lt-1/2/0 unit 4 family inet address 10.0.2.2/30**

5. Configure the logical tunnel interface on Logical System LS3 connecting to Logical System LS2.

```
[edit]
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 3 description LS3->LS2
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 3 encapsulation ethernet
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 3 peer-unit 4
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 3 family inet address
  10.0.2.1/30
```

6. Configure the logical tunnel interface on Logical System LS3 connecting to Logical System LS1.

```
[edit]
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 5 description LS3->LS1
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 5 encapsulation ethernet
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 5 peer-unit 0
user@host# set logical-systems LS3 interfaces lt-1/2/0 unit 5 family inet address
  10.0.1.1/30
```

7. Configure OSPF on all the interfaces.

```
[edit]
user@host# set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.0
user@host# set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.2
user@host# set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.1
user@host# set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.4
user@host# set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.5
user@host# set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.3
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Results

Confirm your configuration by issuing the **show logical-systems** command.

```
show logical-systems
LS1 {
  interfaces {
    lt-1/2/0 {
      unit 0 {
        description LS1->LS3;
        encapsulation ethernet;
        peer-unit 5;
        family inet {
          address 10.0.1.2/30;
        }
      }
      unit 2 {
        description LS1->LS2;
        encapsulation ethernet;
        peer-unit 1;
        family inet {
          address 10.0.0.1/30;
```

```
            }
          }
        }
      }
      protocols {
        ospf {
          area 0.0.0.0 {
            interface lt-1/2/0.0;
            interface lt-1/2/0.2;
          }
        }
      }
    }
    LS2 {
      interfaces {
        lt-1/2/0 {
          unit 1 {
            description LS2->LS1;
            encapsulation ethernet;
            peer-unit 2;
            family inet {
              address 10.0.0.2/30;
            }
          }
          unit 4 {
            description LS2->LS3;
            encapsulation ethernet;
            peer-unit 3;
            family inet {
              address 10.0.2.2/30;
            }
          }
        }
      }
      protocols {
        ospf {
          area 0.0.0.0 {
            interface lt-1/2/0.1;
            interface lt-1/2/0.4;
          }
        }
      }
    }
    LS3 {
      interfaces {
        lt-1/2/0 {
          unit 3 {
            description LS3->LS2;
            encapsulation ethernet;
            peer-unit 4;
            family inet {
              address 10.0.2.1/30;
            }
          }
          unit 5 {
            description LS3->LS1;
```



```
                encapsulation ethernet;
                peer-unit 0;
                family inet {
                    address 10.0.1.1/30;
                }
            }
        }
    }
    protocols {
        ospf {
            area 0.0.0.0 {
                interface lt-1/2/0.5;
                interface lt-1/2/0.3;
            }
        }
    }
}
```

Verification

Confirm that the configuration is working properly.

- Verifying That the Logical Systems Are Up on page 331
- Verifying Connectivity Between the Logical Systems on page 331

Verifying That the Logical Systems Are Up

Purpose Make sure that the interfaces are properly configured.

Action

```
user@host> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
...
lt-1/2/0                up    up
lt-1/2/0.0              up    up   inet     10.0.1.2/30
lt-1/2/0.1              up    up   inet     10.0.0.2/30
lt-1/2/0.2              up    up   inet     10.0.0.1/30
lt-1/2/0.3              up    up   inet     10.0.2.1/30
lt-1/2/0.4              up    up   inet     10.0.2.2/30
lt-1/2/0.5              up    up   inet     10.0.1.1/30
...
```

Verifying Connectivity Between the Logical Systems

Purpose Make sure that the OSPF adjacencies are established by checking the OSPF neighbor tables, checking the routing tables, and pinging the logical systems.

Action

```
user@host> show ospf neighbor logical-system LS1
Address          Interface              State     ID               Pri  Dead
10.0.1.1         lt-1/2/0.0             Full      10.0.1.1         128    37
10.0.0.2         lt-1/2/0.2             Full      10.0.0.2         128    33

user@host> show ospf neighbor logical-system LS2
Address          Interface              State     ID               Pri  Dead
10.0.0.1         lt-1/2/0.1             Full      10.0.0.1         128    32
10.0.2.1         lt-1/2/0.4             Full      10.0.1.1         128    36

user@host> show ospf neighbor logical-system LS3
Address          Interface              State     ID               Pri  Dead
10.0.2.2         lt-1/2/0.3             Full      10.0.0.2         128    36
10.0.1.2         lt-1/2/0.5             Full      10.0.0.1         128    37

user@host> show route logical-system LS1
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[Direct/0] 00:28:00
                    > via lt-1/2/0.2
10.0.0.1/32        *[Local/0] 00:28:00
                      Local via lt-1/2/0.2
10.0.1.0/30        *[Direct/0] 00:28:00
                    > via lt-1/2/0.0
10.0.1.2/32        *[Local/0] 00:28:00
                      Local via lt-1/2/0.0
10.0.2.0/30        *[OSPF/10] 00:27:05, metric 2
                    > to 10.0.1.1 via lt-1/2/0.0
                      to 10.0.0.2 via lt-1/2/0.2
224.0.0.5/32       *[OSPF/10] 00:28:03, metric 1
                      MultiRecv

user@host> show route logical-system LS2
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[Direct/0] 00:28:31
                    > via lt-1/2/0.1
10.0.0.2/32        *[Local/0] 00:28:32
                      Local via lt-1/2/0.1
10.0.1.0/30        *[OSPF/10] 00:27:38, metric 2
                    > to 10.0.0.1 via lt-1/2/0.1
                      to 10.0.2.1 via lt-1/2/0.4
10.0.2.0/30        *[Direct/0] 00:28:32
                    > via lt-1/2/0.4
10.0.2.2/32        *[Local/0] 00:28:32
                      Local via lt-1/2/0.4
224.0.0.5/32       *[OSPF/10] 00:28:34, metric 1
                      MultiRecv

user@host> show route logical-system LS3
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[OSPF/10] 00:28:23, metric 2
                    > to 10.0.2.2 via lt-1/2/0.3
                      to 10.0.1.2 via lt-1/2/0.5
10.0.1.0/30        *[Direct/0] 00:29:13
                    > via lt-1/2/0.5
```



```
10.0.1.1/32        *[Local/0] 00:29:15
                      Local via lt-1/2/0.5
10.0.2.0/30        *[Direct/0] 00:29:14
                    > via lt-1/2/0.3
10.0.2.1/32        *[Local/0] 00:29:15
                      Local via lt-1/2/0.3
224.0.0.5/32       *[OSPF/10] 00:29:16, metric 1
                      MultiRecv
```

From LS1, Ping LS3

```
user@host> set cli logical-system LS1

user@host:LS1> ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1): 56 data bytes
64 bytes from 10.0.2.1: icmp_seq=0 ttl=64 time=1.215 ms
64 bytes from 10.0.2.1: icmp_seq=1 ttl=64 time=1.150 ms
64 bytes from 10.0.2.1: icmp_seq=2 ttl=64 time=1.134 ms
```

From LS3, Ping LS1

```
user@host> set cli logical-system LS3

user@host:LS3> ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=1.193 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.114 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.190 ms
```

Example: Configuring a Conditional OSPF Default Route Policy on Logical Systems

This example shows how to configure a conditional default route on one logical system and inject the default route into OSPF area 0.

Requirements

Before you begin:

- Connect the logical systems by using logical tunnel (**lt**) interfaces. See *Example: Connecting Logical Systems Within the Same Router Using Logical Tunnel Interfaces*.
- Enable OSPF on the interfaces. See "Example: Configuring OSPF on Logical Systems Within the Same Router" on page 326.

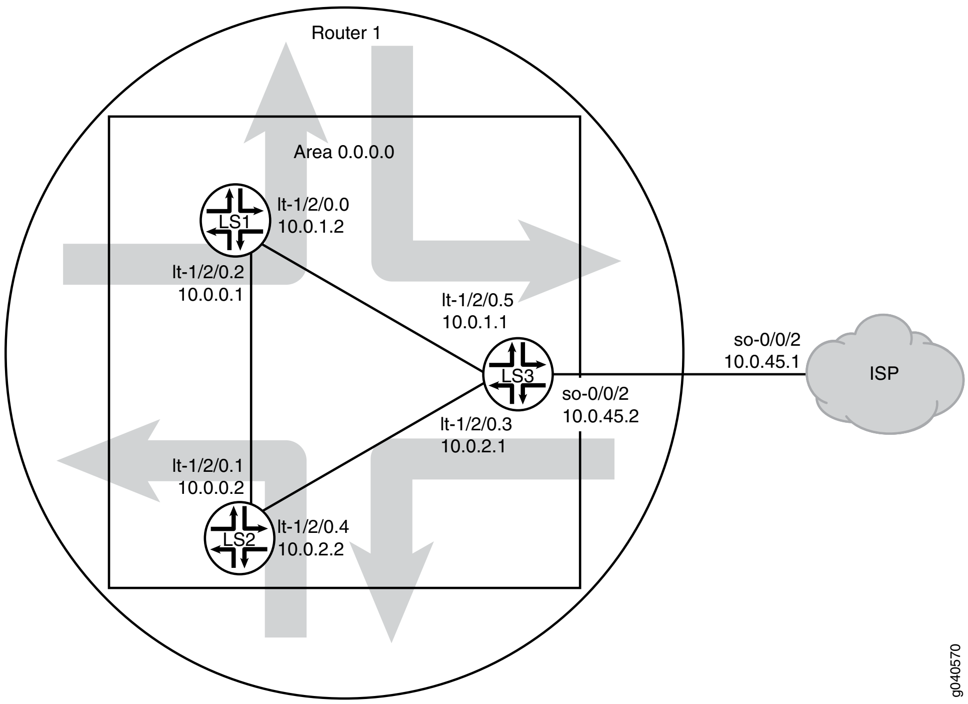
Overview

In this example, OSPF area 0 contains three logical systems that are configured on a single physical router. Logical System LS3 has a BGP session with an external peer, for example, an ISP.

The ISP injects a default static route into BGP, which provides the customer network with a default static route to reach external networks. Logical System LS3 exports the default route into OSPF. The route policy on Logical System LS3 is conditional such that if the connection to the external peer goes down, the default route is no longer active in the routing tables of the logical systems in area 0. This policy prevents blackholing of traffic. Blackholing occurs when packets are dropped without notification.

Figure 27 on page 334 shows the sample network.

Figure 27: OSPF with a Conditional Default Route to an ISP



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device LS1

```
set logical-systems LS1 interfaces lt-1/2/0 unit 0 description LS1->LS3
set logical-systems LS1 interfaces lt-1/2/0 unit 0 encapsulation ethernet
set logical-systems LS1 interfaces lt-1/2/0 unit 0 peer-unit 5
set logical-systems LS1 interfaces lt-1/2/0 unit 0 family inet address 10.0.1.2/30
set logical-systems LS1 interfaces lt-1/2/0 unit 2 description LS1->LS2
set logical-systems LS1 interfaces lt-1/2/0 unit 2 encapsulation ethernet
set logical-systems LS1 interfaces lt-1/2/0 unit 2 peer-unit 1
set logical-systems LS1 interfaces lt-1/2/0 unit 2 family inet address 10.0.0.1/30
set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.0
set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.2
```

Device LS2

```
set logical-systems LS2 interfaces lt-1/2/0 unit 1 description LS2->LS1
set logical-systems LS2 interfaces lt-1/2/0 unit 1 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 1 peer-unit 2
set logical-systems LS2 interfaces lt-1/2/0 unit 1 family inet address 10.0.0.2/30
```

```
set logical-systems LS2 interfaces lt-1/2/0 unit 4 description LS2->LS3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 4 peer-unit 3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 family inet address 10.0.2.2/30
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.1
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.4
```

Device LS3

```
set logical-systems LS3 interfaces lt-1/2/0 unit 3 description LS3->LS2
set logical-systems LS3 interfaces lt-1/2/0 unit 3 encapsulation ethernet
set logical-systems LS3 interfaces lt-1/2/0 unit 3 peer-unit 4
set logical-systems LS3 interfaces lt-1/2/0 unit 3 family inet address 10.0.2.1/30
set logical-systems LS3 interfaces lt-1/2/0 unit 5 description LS3->LS1
set logical-systems LS3 interfaces lt-1/2/0 unit 5 encapsulation ethernet
set logical-systems LS3 interfaces lt-1/2/0 unit 5 peer-unit 0
set logical-systems LS3 interfaces lt-1/2/0 unit 5 family inet address 10.0.1.1/30
set logical-systems LS3 interfaces so-0/0/2 unit 0 description LS3->ISP
set logical-systems LS3 interfaces so-0/0/2 unit 0 family inet address 10.0.45.2/30
set logical-systems LS3 protocols bgp group ext type external
set logical-systems LS3 protocols bgp group ext peer-as 65000
set logical-systems LS3 protocols bgp group ext neighbor 10.0.45.1
set logical-systems LS3 protocols ospf export gendefault
set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.5
set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.3
set logical-systems LS3 policy-options policy-statement gendefault term upstreamroutes
  from protocol bgp
set logical-systems LS3 policy-options policy-statement gendefault term upstreamroutes
  from as-path upstream
set logical-systems LS3 policy-options policy-statement gendefault term upstreamroutes
  from route-filter 0.0.0.0/0 upto /16
set logical-systems LS3 policy-options policy-statement gendefault term upstreamroutes
  then next-hop 10.0.45.1
set logical-systems LS3 policy-options policy-statement gendefault term upstreamroutes
  then accept
set logical-systems LS3 policy-options policy-statement gendefault term end then reject
set logical-systems LS3 policy-options as-path upstream "^65000 "
set logical-systems LS3 routing-options generate route 0.0.0.0/0 policy gendefault
set logical-systems LS3 routing-options autonomous-system 65001
```

Device ISP

```
set interfaces so-0/0/2 unit 0 family inet address 10.0.45.1/30
set protocols bgp group ext type external
set protocols bgp group ext export advertise-default
set protocols bgp group ext peer-as 65001
set protocols bgp group ext neighbor 10.0.45.2
set policy-options policy-statement advertise-default term 1 from route-filter 0.0.0.0/0
  exact
set policy-options policy-statement advertise-default term 1 then accept
set routing-options static route 0.0.0.0/0 discard
set routing-options autonomous-system 65000
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a conditional default route:

1. Configure the interfaces.

```
[edit logical-systems LS3 interfaces]
user@R3# set lt-1/2/0 unit 3 description LS3->LS2
user@R3# set lt-1/2/0 unit 3 encapsulation ethernet
user@R3# set lt-1/2/0 unit 3 peer-unit 4
user@R3# set lt-1/2/0 unit 3 family inet address 10.0.2.1/30
user@R3# set lt-1/2/0 unit 5 description LS3->LS1
user@R3# set lt-1/2/0 unit 5 encapsulation ethernet
user@R3# set lt-1/2/0 unit 5 peer-unit 0
user@R3# set lt-1/2/0 unit 5 family inet address 10.0.1.1/30
user@R3# set so-0/0/2 unit 0 description LS3->ISP
user@R3# set so-0/0/2 unit 0 encapsulation ethernet
user@R3# set so-0/0/2 unit 0 peer-unit 7
user@R3# set so-0/0/2 unit 0 family inet address 10.0.45.2/30
```

2. Configure the autonomous system (AS) number.

```
[edit logical-systems LS3 routing-options]
user@R3# set autonomous-system 65001
```

3. Configure the BGP session with the ISP device.

```
[edit logical-systems LS3 protocols bgp group ext]
user@R3# set type external
user@R3# set peer-as 65000
user@R3# set neighbor 10.0.45.1
```

4. Configure OSPF.

```
[edit logical-systems LS3 protocols ospf area 0.0.0.0]
user@R3# set interface lt-1/2/0.5
user@R3# set interface lt-1/2/0.3
```

5. Configure the routing policy.

```
[edit logical-systems LS3 policy-options policy-statement gendefault]
user@R3# set term upstreamroutes from protocol bgp
user@R3# set term upstreamroutes from as-path upstream
user@R3# set term upstreamroutes from route-filter 0.0.0.0/0 upto /16
user@R3# set term upstreamroutes then next-hop 10.0.45.1
user@R3# set term upstreamroutes then accept

user@R3# set term end then reject

[edit logical-systems LS3 policy-options]
user@R3# set as-path upstream "^65000 "
```

6. Configure the generated route.

```
[edit logical-systems LS3 routing-options]
user@R3# set generate route 0.0.0.0/0 policy gendefault
```


7. Apply the export policy to OSPF.

```
[edit logical-systems LS3 protocols ospf]
user@R3# set export gendefault
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@R3# commit
```

Results

Confirm your configuration by issuing the **show logical-systems LS3** command.

```
show logical-systems LS3
interfaces {
  lt-1/2/0 {
    unit 3 {
      description LS3->LS2;
      encapsulation ethernet;
      peer-unit 4;
      family inet {
        address 10.0.2.1/30;
      }
    }
    unit 5 {
      description LS3->LS1;
      encapsulation ethernet;
      peer-unit 0;
      family inet {
        address 10.0.1.1/30;
      }
    }
    unit 6 {
      description LS3->ISP;
      encapsulation ethernet;
      peer-unit 7;
      family inet {
        address 10.0.45.2/30;
      }
    }
  }
}
protocols {
  bgp {
    group ext {
      type external;
      peer-as 65000;
      neighbor 10.0.45.1;
    }
  }
  ospf {
    export gendefault;
    area 0.0.0.0 {
      interface lt-1/2/0.5;
      interface lt-1/2/0.3;
```

```
        }
      }
    }
    policy-options {
      policy-statement gendefault {
        term upstreamroutes {
          from {
            protocol bgp;
            as-path upstream;
            route-filter 0.0.0.0/0 upto /16;
          }
          then {
            next-hop 10.0.45.1;
            accept;
          }
        }
        term end {
          then reject;
        }
      }
      as-path upstream "^65000 ";
    }
    routing-options {
      generate {
        route 0.0.0.0/0 policy gendefault;
      }
      autonomous-system 65001;
    }
```

Verification

Confirm that the configuration is working properly.

- Verifying that the Route to the ISP Is Working on page 338
- Verifying That the Static Route Is Redistributed on page 339
- Testing the Policy Condition on page 339

Verifying that the Route to the ISP Is Working

Purpose Make sure connectivity is established between Logical System LS3 and the ISP's router.

Action

```
user@host>set cli logical-system LS3
Logical system: LS3

user@host:LS3>ping 10.0.45.1
PING 10.0.45.1 (10.0.45.1): 56 data bytes
64 bytes from 10.0.45.1: icmp_seq=0 ttl=64 time=1.185 ms
64 bytes from 10.0.45.1: icmp_seq=1 ttl=64 time=1.199 ms
64 bytes from 10.0.45.1: icmp_seq=2 ttl=64 time=1.186 ms
```

Meaning The **ping** command confirms reachability.

Verifying That the Static Route Is Redistributed

Purpose Make sure that the BGP policy is redistributing the static route into Logical System LS3's routing table. Also make sure that the OSPF policy is redistributing the static route into the routing tables of Logical System LS1 and Logical System LS2.

Action `user@host>` **show route logical-system LS3 protocol bgp**

```
inet.0: 9 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 00:00:25, localpref 100
                      AS path: 65000 I
                    > to 10.0.45.1 via so-0/0/2.0
```

`user@host>` **show route logical-system LS1 protocol ospf**

```
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 00:03:58, metric 0, tag 0
                    > to 10.0.1.1 via lt-1/2/0.0
10.0.2.0/30        *[OSPF/10] 03:37:45, metric 2
                      to 10.0.1.1 via lt-1/2/0.0
                    > to 10.0.0.2 via lt-1/2/0.2
224.0.0.5/32       *[OSPF/10] 03:38:41, metric 1
                      MultiRecv
```

`user@host>` **show route logical-system LS2 protocol ospf**

```
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 00:04:04, metric 0, tag 0
                    > to 10.0.2.1 via lt-1/2/0.4
10.0.1.0/30        *[OSPF/10] 03:37:46, metric 2
                      to 10.0.0.1 via lt-1/2/0.1
                    > to 10.0.2.1 via lt-1/2/0.4
224.0.0.5/32       *[OSPF/10] 03:38:47, metric 1
                      MultiRecv
```

Meaning The routing tables contain the default 0.0.0.0/0 route. If Logical System LS1 and Logical System LS2 receive packets destined for networks not specified in their routing tables, those packets will be sent to Logical System LS3 for further processing. If Logical System LS3 receives packets destined for networks not specified in its routing table, those packets will be sent to the ISP for further processing.

Testing the Policy Condition

Purpose Deactivate the interface to make sure that the route is removed from the routing tables if the external network becomes unreachable.

Action

user@host> **deactivate logical-systems LS3 interfaces so-0/0/2 unit 0 family inet address 10.0.45.2/30**

user@host> **commit**

user@host> **show route logical-system LS1 protocol ospf**

```
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.2.0/30        *[OSPF/10] 03:41:48, metric 2
                      to 10.0.1.1 via lt-1/2/0.0
                    > to 10.0.0.2 via lt-1/2/0.2
224.0.0.5/32       *[OSPF/10] 03:42:44, metric 1
                      MultiRecv
```

user@host> **show route logical-system LS2 protocol ospf**

```
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.1.0/30        *[OSPF/10] 03:42:10, metric 2
                      to 10.0.0.1 via lt-1/2/0.1
                    > to 10.0.2.1 via lt-1/2/0.4
224.0.0.5/32       *[OSPF/10] 03:43:11, metric 1
                      MultiRecv
```

Meaning

The routing tables on Logical System LS1 and Logical System LS2 do not contain the default 0.0.0.0/0. This verifies that the default route is no longer present in the OSPF domain. To reactivate the **so-0/0/2.0** interface, issue the **activate logical-systems LS3 interfaces so-0/0/2 unit 0 family inet address 10.0.45.2/30** configuration-mode command.

Example: Configuring an OSPF Default Route Policy on Logical Systems

This example shows how to configure a default route on one logical system and inject the default route into OSPF area 0. In this example, OSPF area 0 contains three logical systems that are configured on a single physical router.

Requirements

Before you begin:

- Connect the logical systems by using logical tunnel (**lt**) interfaces. See *Example: Connecting Logical Systems Within the Same Router Using Logical Tunnel Interfaces*.
- Enable OSPF on the interfaces. See “Example: Configuring OSPF on Logical Systems Within the Same Router” on page 326.

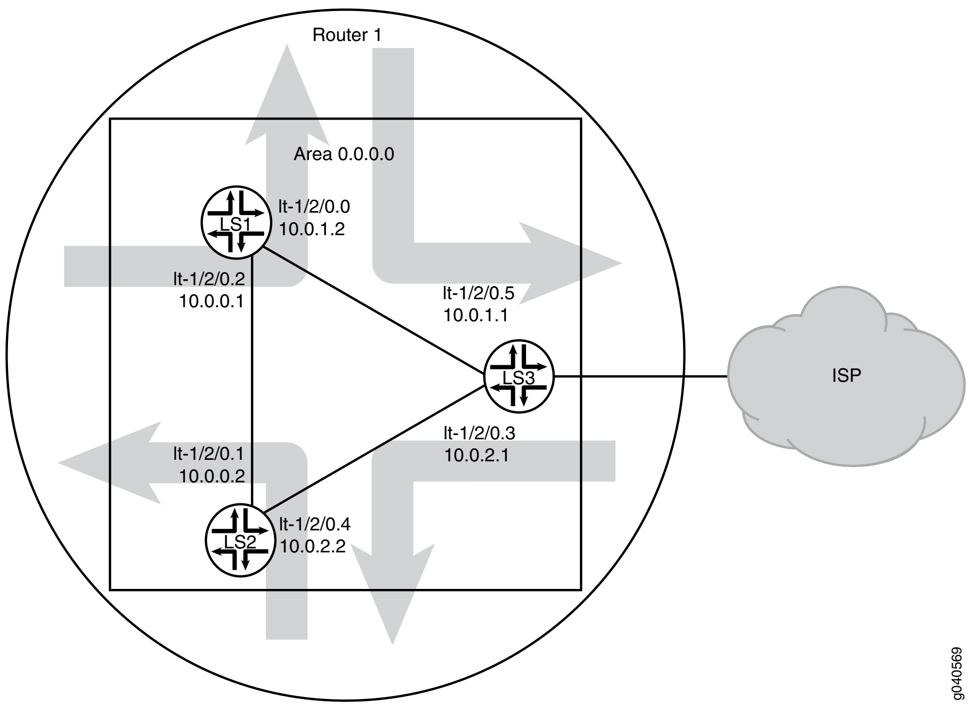
Overview

This example shows a logical system redistributing a default route to other logical systems. All logical systems are running OSPF. A common reason for a default route is to provide a path for sending traffic destined outside the OSPF domain.

In this example, the default route is not used for forwarding traffic. The **no-install** statement prevents the route from being installed in the forwarding table of Logical System LS3. If you configure a route so it is not installed in the forwarding table, the route is still eligible to be exported from the routing table to other protocols. The **discard** statement silently drops packets without notice.

Figure 28 on page 341 shows the sample network.

Figure 28: OSPF with a Default Route to an ISP



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set logical-systems LS3 routing-options static route 0.0.0.0/0 discard
set logical-systems LS3 routing-options static route 0.0.0.0/0 no-install
set logical-systems LS3 policy-options policy-statement ospf-default from protocol
   static
set logical-systems LS3 policy-options policy-statement ospf-default from route-filter
   0.0.0.0/0 exact
set logical-systems LS3 policy-options policy-statement ospf-default then accept
```


set logical-systems LS3 protocols ospf export ospf-default

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an OSPF default route policy on logical systems:

1. Change the context to Logical System LS3.

```
[edit]
user@host> set cli logical-system LS3
```

2. Configure the default route on Logical System LS3.

```
[edit]
user@host:LS3# set routing-options static route 0.0.0.0/0 discard
user@host:LS3# set routing-options static route 0.0.0.0/0 no-install
```

3. Configure the policy on Logical System LS3.

```
[edit]
user@host:LS3# set policy-options policy-statement ospf-default from protocol
  static
user@host:LS3# set policy-options policy-statement ospf-default from route-filter
  0.0.0.0/0 exact
user@host:LS3# set policy-options policy-statement ospf-default then accept
```

4. Apply the export policy to OSPF on Logical System LS3.

```
[edit]
user@host:LS3# set protocols ospf export ospf-default
```

5. If you are done configuring the device, commit the configuration.

```
[edit]
user@host:LS3# commit
```

Results

Confirm your configuration by issuing the **show logical-systems LS3** command.

```
show logical-systems LS3
interfaces {
  lt-1/2/0 {
    unit 3 {
      description LS3->LS2;
      encapsulation ethernet;
      peer-unit 4;
      family inet {
        address 10.0.2.1/30;
      }
    }
    unit 5 {
      description LS3->LS1;
      encapsulation ethernet;
      peer-unit 0;
      family inet {
```



```
            address 10.0.1.1/30;
          }
        }
      }
    }
    protocols {
      ospf {
        export ospf-default;
        area 0.0.0.0 {
          interface lt-1/2/0.5;
          interface lt-1/2/0.3;
        }
      }
    }
    policy-options {
      policy-statement ospf-default {
        from {
          protocol static;
          route-filter 0.0.0.0/0 exact;
        }
        then accept;
      }
    }
    routing-options {
      static {
        route 0.0.0.0/0 {
          discard;
          no-install;
        }
      }
    }
```

Verification

Confirm that the configuration is working properly.

Verifying That the Static Route Is Redistributed

Purpose Make sure that the OSPF policy is working by checking the routing tables.

Action

```
user@host> show route logical-system LS3
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 01:04:38
                      Discard
10.0.0.0/30        *[OSPF/10] 11:53:55, metric 2
                      to 10.0.2.2 via lt-1/2/0.3
                    > to 10.0.1.2 via lt-1/2/0.5
10.0.1.0/30        *[Direct/0] 11:54:50
                    > via lt-1/2/0.5
10.0.1.1/32        *[Local/0] 11:54:54
                      Local via lt-1/2/0.5
10.0.2.0/30        *[Direct/0] 11:54:50
                    > via lt-1/2/0.3
10.0.2.1/32        *[Local/0] 11:54:54
                      Local via lt-1/2/0.3
224.0.0.5/32       *[OSPF/10] 11:56:55, metric 1
                      MultiRecv

user@host> show route logical-system LS1
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 01:02:34, metric 0, tag 0
                    > to 10.0.1.1 via lt-1/2/0.0
10.0.0.0/30        *[Direct/0] 11:52:46
                    > via lt-1/2/0.2
10.0.0.1/32        *[Local/0] 11:52:50
                      Local via lt-1/2/0.2
10.0.1.0/30        *[Direct/0] 11:52:46
                    > via lt-1/2/0.0
10.0.1.2/32        *[Local/0] 11:52:50
                      Local via lt-1/2/0.0
10.0.2.0/30        *[OSPF/10] 11:51:56, metric 2
                    > to 10.0.1.1 via lt-1/2/0.0
                      to 10.0.0.2 via lt-1/2/0.2
224.0.0.5/32       *[OSPF/10] 11:54:50, metric 1
                      MultiRecv

user@host> show route logical-system LS2
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 01:05:20, metric 0, tag 0
                    > to 10.0.2.1 via lt-1/2/0.4
10.0.0.0/30        *[Direct/0] 11:55:32
                    > via lt-1/2/0.1
10.0.0.2/32        *[Local/0] 11:55:36
                      Local via lt-1/2/0.1
10.0.1.0/30        *[OSPF/10] 11:54:37, metric 2
                    > to 10.0.0.1 via lt-1/2/0.1
                      to 10.0.2.1 via lt-1/2/0.4
10.0.2.0/30        *[Direct/0] 11:55:32
                    > via lt-1/2/0.4
10.0.2.2/32        *[Local/0] 11:55:36
                      Local via lt-1/2/0.4
224.0.0.5/32       *[OSPF/10] 11:57:36, metric 1
                      MultiRecv
```


Meaning The routing table on Logical System LS3 contains the default 0.0.0.0/0 route from protocol **Static**. The routing tables on Logical System LS1 and Logical System LS2 contain the default 0.0.0.0/0 route from protocol **OSPF**. If Logical System LS1 and Logical System LS2 receive packets destined for networks not specified in their routing tables, those packets will be sent to Logical System LS3 for further processing. This configuration assumes that Logical System LS3 has a connection to an ISP or another external network.

Example: Configuring an OSPF Import Policy on Logical Systems

This example shows how to configure an OSPF import policy on logical systems. OSPF import policies apply to external routes only. An external route is a route that is outside the OSPF AS.

Requirements

This example shows logical systems that are configured within a single physical router. The logical systems connect to each other by using logical tunnel (**lt**) interfaces. See *Example: Connecting Logical Systems Within the Same Router Using Logical Tunnel Interfaces*. Alternatively, you can use multiple physical routers.

Overview

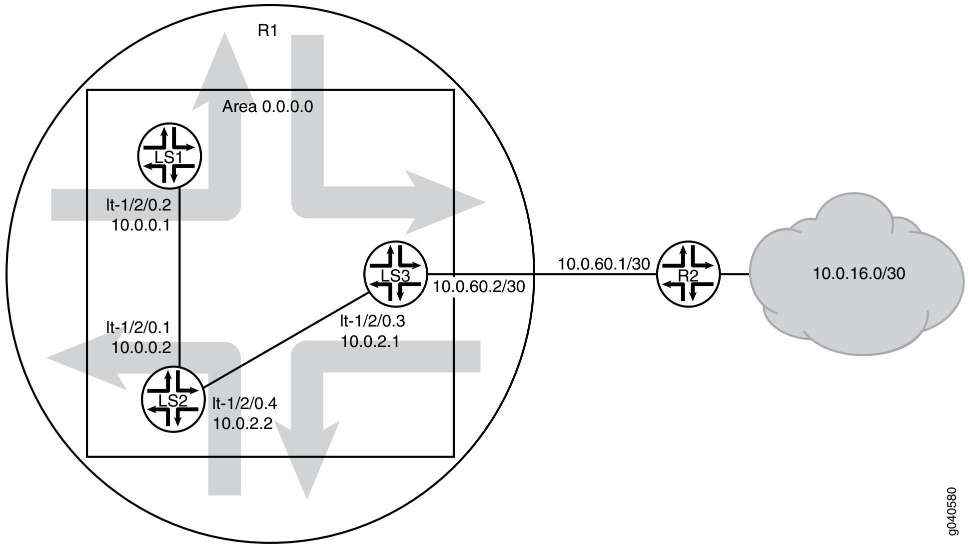
External routes are learned by Autonomous System Border Routers (ASBRs). External routes can be advertised throughout the OSPF domain if you configure the ASBR to redistribute the route into OSPF. An external route might be learned by the ASBR from a routing protocol other than OSPF, or the external route might be a static route that you configure on the ASBR.

OSPF import policy allows you to prevent external routes from being added to the routing tables of OSPF neighbors. The import policy does not impact the OSPF database. This means that the import policy has no impact on the link-state advertisements.

OSPF import policies have practical applications. Suppose, for example, that you are using OSPF to advertise a static route to the devices in your datacenter because you want some of the devices in the datacenter to use the static route. However, you want other devices in the datacenter to ignore the static route. So, you apply the OSPF import policy on the devices that you want to ignore the static route. The filtering is done only on external routes in OSPF. The intra-area and inter-area routes are not considered for filtering. The default action is to accept the route when the route does not match the policy.

Figure 29 on page 346 shows the sample network.

Figure 29: OSPF Import Policy on Logical Systems



In this example, the logical systems operate as follows:

1. LS3—Logical System LS3 has a static route to the 10.0.16.0/30 network. The next hop for the static route is 10.0.60.1. LS3 has an OSPF export policy configured. The export policy redistributes static routes from LS3's routing table into LS3's OSPF database. Because the static route is in LS3's OSPF database, the route is advertised in a link state advertisement (LSA) to LS3's OSPF neighbor. LS3's OSPF neighbor is Logical System LS2.
2. LS2—Logical System LS2 receives the route advertisement from LS3. LS2 then installs the route into LS2's OSPF database. LS2 has an OSPF import policy configured that matches the static route to the 10.0.16.0/30 network and prevents the static route from being installed in LS2's routing table. However, because the route is in LS2's OSPF database, LS2 advertises the route to its OSPF neighbor, Logical System LS1.
3. LS1—Logical System LS1 receives the route advertisement from LS2. LS1 then installs the route into LS1's OSPF database. LS1 does not have an OSPF import policy configured that matches the static route to the 10.0.16.0/30 network . Therefore, the route gets installed in LS1's routing table.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

LS3

```
set logical-systems LS3 interfaces so-0/0/0 unit 0 family inet address 10.0.60.2/30
set logical-systems LS3 interfaces lt-1/2/0 unit 3 description LS3->LS2
set logical-systems LS3 interfaces lt-1/2/0 unit 3 encapsulation ethernet
set logical-systems LS3 interfaces lt-1/2/0 unit 3 peer-unit 4
set logical-systems LS3 interfaces lt-1/2/0 unit 3 family inet address 10.0.2.1/30
set logical-systems LS3 protocols ospf export export_static
```

```
set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.3
set logical-systems LS3 policy-options policy-statement export_static from protocol
   static
set logical-systems LS3 policy-options policy-statement export_static then accept
set logical-systems LS3 routing-options static route 10.0.16.0/30 next-hop 10.0.60.1
```

LS2

```
set logical-systems LS2 interfaces lt-1/2/0 unit 1 description LS2->LS1
set logical-systems LS2 interfaces lt-1/2/0 unit 1 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 1 peer-unit 2
set logical-systems LS2 interfaces lt-1/2/0 unit 1 family inet address 10.0.0.2/30
set logical-systems LS2 interfaces lt-1/2/0 unit 4 description LS2->LS3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 encapsulation ethernet
set logical-systems LS2 interfaces lt-1/2/0 unit 4 peer-unit 3
set logical-systems LS2 interfaces lt-1/2/0 unit 4 family inet address 10.0.2.2/30
set logical-systems LS2 protocols ospf import filter_routes
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.1
set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.4
set logical-systems LS2 policy-options policy-statement filter_routes from route-filter
   10.0.16.0/30 exact
set logical-systems LS2 policy-options policy-statement filter_routes then reject
```

LS1

```
set logical-systems LS1 interfaces lt-1/2/0 unit 2 description LS1->LS2
set logical-systems LS1 interfaces lt-1/2/0 unit 2 encapsulation ethernet
set logical-systems LS1 interfaces lt-1/2/0 unit 2 peer-unit 1
set logical-systems LS1 interfaces lt-1/2/0 unit 2 family inet address 10.0.0.1/30
set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.2
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an OSPF import policy on logical systems:

1. Configure the interfaces.

```
[edit]
user@R1# set logical-systems LS3 interfaces so-0/0/0 unit 0 family inet address
   10.0.60.2/30
user@R1# set logical-systems LS3 interfaces lt-1/2/0 unit 3 description LS3->LS2
user@R1# set logical-systems LS3 interfaces lt-1/2/0 unit 3 encapsulation ethernet
user@R1# set logical-systems LS3 interfaces lt-1/2/0 unit 3 peer-unit 4
user@R1# set logical-systems LS3 interfaces lt-1/2/0 unit 3 family inet address
   10.0.2.1/30
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 1 description LS2->LS1
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 1 encapsulation ethernet
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 1 peer-unit 2
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 1 family inet address
   10.0.0.2/30
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 4 description LS2->LS3
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 4 encapsulation ethernet
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 4 peer-unit 3
user@R1# set logical-systems LS2 interfaces lt-1/2/0 unit 4 family inet address
   10.0.2.2/30
user@R1# set logical-systems LS1 interfaces lt-1/2/0 unit 2 description LS1->LS2
user@R1# set logical-systems LS1 interfaces lt-1/2/0 unit 2 encapsulation ethernet
```

```
user@R1# set logical-systems LS1 interfaces lt-1/2/0 unit 2 peer-unit 1
user@R1# set logical-systems LS1 interfaces lt-1/2/0 unit 2 family inet address
  10.0.0.1/30
```

2. Enable OSPF on the interfaces.

```
[edit]
user@R1# set logical-systems LS3 protocols ospf area 0.0.0.0 interface lt-1/2/0.3
user@R1# set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.1
user@R1# set logical-systems LS2 protocols ospf area 0.0.0.0 interface lt-1/2/0.4
user@R1# set logical-systems LS1 protocols ospf area 0.0.0.0 interface lt-1/2/0.2
```

3. Configure the static route on Logical System LS3.

```
[edit]
user@R1# set logical-systems LS3 routing-options static route 10.0.16.0/30 next-hop
  10.0.60.1
```

4. On Logical System LS3, redistribute the static route into OSPF.

```
[edit]
user@R1# set logical-systems LS3 protocols ospf export export_static
user@R1# set logical-systems LS3 policy-options policy-statement export_static
  from protocol static
user@R1# set logical-systems LS3 policy-options policy-statement export_static
  then accept
```

5. On Logical System LS2, configure the OSPF import policy.

```
[edit]
user@R1# set logical-systems LS2 protocols ospf import filter_routes
user@R1# set logical-systems LS2 policy-options policy-statement filter_routes
  from route-filter 10.0.16.0/30 exact
user@R1# set logical-systems LS2 policy-options policy-statement filter_routes
  then reject
```

6. If you are done configuring the device, commit the configuration.

```
[edit]
user@R1# commit
```

Results

Confirm your configuration by issuing the **show logical-systems** command.

```
user@R1# show logical-systems
LS1 {
  interfaces {
    lt-1/2/0 {
      unit 2 {
        description LS1->LS2;
        encapsulation ethernet;
        peer-unit 1;
        family inet {
          address 10.0.0.1/30;
        }
      }
    }
```



```
        }
        protocols {
            ospf {
                area 0.0.0.0 {
                    interface lt-1/2/0.2;
                }
            }
        }
    }
    LS2 {
        interfaces {
            lt-1/2/0 {
                unit 1 {
                    description LS2->LS1;
                    encapsulation ethernet;
                    peer-unit 2;
                    family inet {
                        address 10.0.0.2/30;
                    }
                }
                unit 4 {
                    description LS2->LS3;
                    encapsulation ethernet;
                    peer-unit 3;
                    family inet {
                        address 10.0.2.2/30;
                    }
                }
            }
        }
        protocols {
            ospf {
                import filter_routes;
                area 0.0.0.0 {
                    interface lt-1/2/0.1;
                    interface lt-1/2/0.4;
                }
            }
        }
        policy-options {
            policy-statement filter_routes {
                from {
                    route-filter 10.0.16.0/30 exact;
                }
                then reject;
            }
        }
    }
    LS3 {
        interfaces {
            so-0/0/0 {
                unit 0 {
                    family inet {
                        address 10.0.60.2/30;
                    }
                }
```



```
            }
            lt-1/2/0 {
                unit 3 {
                    description LS3->LS2;
                    encapsulation ethernet;
                    peer-unit 4;
                    family inet {
                        address 10.0.2.1/30;
                    }
                }
            }
        }
        protocols {
            ospf {
                export export_static;
                area 0.0.0.0 {
                    interface lt-1/2/0.3;
                }
            }
        }
        policy-options {
            policy-statement export_static {
                from protocol static;
                then accept;
            }
        }
        routing-options {
            static {
                route 10.0.16.0/30 next-hop 10.0.60.1;
            }
        }
    }
```

Verification

Confirm that the configuration is working properly.

- Viewing the OSPF Databases of the Logical Systems on page 350
- Viewing the Routing Tables of the Logical Systems on page 351

Viewing the OSPF Databases of the Logical Systems

Purpose Verify that OSPF is advertising the static route.

Action

```
user@R1> show ospf database logical-system all
logical-system: LS2

    OSPF database, Area 0.0.0.0
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.0.0.1         10.0.0.1         0x8000001f   107  0x22 0x8f59  36
Router  *10.0.0.2         10.0.0.2         0x80000025   101  0x22 0x4074  48
Router   10.0.2.1         10.0.2.1         0x80000018   107  0x22 0xab3a  36
Network  10.0.0.1         10.0.0.1         0x80000001   107  0x22 0x7b94  32
Network  10.0.2.1         10.0.2.1         0x8000000c   190  0x22 0x53ab  32
    OSPF AS SCOPE link state database
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Extern   10.0.16.0        10.0.2.1         0x80000007  1785  0x22 0x4147  36
-----

logical-system: LS1

    OSPF database, Area 0.0.0.0
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router  *10.0.0.1         10.0.0.1         0x8000001f   107  0x22 0x8f59  36
Router   10.0.0.2         10.0.0.2         0x80000025   103  0x22 0x4074  48
Router   10.0.2.1         10.0.2.1         0x80000018   109  0x22 0xab3a  36
Network *10.0.0.1         10.0.0.1         0x80000001   107  0x22 0x7b94  32
Network  10.0.2.1         10.0.2.1         0x8000000c   192  0x22 0x53ab  32

    OSPF AS SCOPE link state database
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Extern   10.0.16.0        10.0.2.1         0x80000007  1787  0x22 0x4147  36
-----

logical-system: LS3

    OSPF database, Area 0.0.0.0
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.0.0.1         10.0.0.1         0x8000001f   109  0x22 0x8f59  36
Router   10.0.0.2         10.0.0.2         0x80000025   103  0x22 0x4074  48
Router  *10.0.2.1         10.0.2.1         0x80000018   107  0x22 0xab3a  36
Network  10.0.0.1         10.0.0.1         0x80000001   109  0x22 0x7b94  32
Network *10.0.2.1         10.0.2.1         0x8000000c   190  0x22 0x53ab  32

    OSPF AS SCOPE link state database
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Extern  *10.0.16.0        10.0.2.1         0x80000007  1785  0x22 0x4147  36
...
```

Meaning The **Extern *10.0.16.0** output shows that OSPF is advertising the external route.

Viewing the Routing Tables of the Logical Systems

Purpose Make sure that Logical System LS3 and Logical System LS1 have the route to the 10.0.16.0/30 network installed in their respective routing tables. Make sure that Logical System LS2 does not have the route installed in its routing table.

Action

```
user@R1> show route logical-system all
logical-system: LS2

inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[Direct/0] 04:22:19
                    > via lt-1/2/0.1
10.0.0.2/32        *[Local/0] 04:22:19
                      Local via lt-1/2/0.1
10.0.2.0/30        *[Direct/0] 04:22:19
                    > via lt-1/2/0.4
10.0.2.2/32        *[Local/0] 04:22:19
                      Local via lt-1/2/0.4
224.0.0.5/32       *[OSPF/10] 04:22:23, metric 1
                      MultiRecv
-----

logical-system: LS1

inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[Direct/0] 04:22:19
                    > via lt-1/2/0.2
10.0.0.1/32        *[Local/0] 04:22:19
                      Local via lt-1/2/0.2
10.0.2.0/30        *[OSPF/10] 00:07:52, metric 2
                    > to 10.0.0.2 via lt-1/2/0.2
10.0.16.0/30       *[OSPF/150] 00:07:52, metric 0, tag 0
                    > to 10.0.0.2 via lt-1/2/0.2
224.0.0.5/32       *[OSPF/10] 04:22:23, metric 1
                      MultiRecv
-----

logical-system: LS3

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/30        *[OSPF/10] 00:07:57, metric 2
                    > to 10.0.2.2 via lt-1/2/0.3
10.0.2.0/30        *[Direct/0] 04:22:19
                    > via lt-1/2/0.3
10.0.2.1/32        *[Local/0] 04:22:19
                      Local via lt-1/2/0.3
10.0.16.0/30       *[Static/5] 03:51:18
                    > to 10.0.60.1 via so-0/0/0.0
10.0.60.0/30       *[Direct/0] 03:53:52
                    > via so-0/0/0.0
10.0.60.2/32       *[Local/0] 03:53:58
                      Local via so-0/0/0.0
224.0.0.5/32       *[OSPF/10] 04:22:23, metric 1
                      MultiRecv
```

Meaning

The route to 10.0.16.0/30 is not installed in Logical System LS2's routing table. The route to 10.0.16.0/30 is installed in Logical System LS1's routing table as a route learned from OSPF. Because it is an OSPF external route, it has a preference value of 150 (instead of 10). By default, routes resulting from OSPF external LSAs are installed with a preference value of 150. The route to 10.0.16.0/30 is installed in Logical System LS3's routing table as a static route.

Related Documentation

- OSPF Support for Logical Systems on page 325
- OSPF Overview on page 4
- *Introduction to Logical Systems* in the *Logical Systems Feature Guide for Routing Devices*.

CHAPTER 17

OSPF Monitoring Configuration

Example: Configuring OSPF Trace Options

Tracing OSPF Protocol Traffic

Tracing operations record detailed messages about the operation of OSPF. You can trace OSPF protocol traffic to help debug OSPF protocol issues. When you trace OSPF protocol traffic, you specify the name of the file and the type of information you want to trace.

You can specify the following OSPF protocol-specific trace options:

- **database-description**—All database description packets, which are used in synchronizing the OSPF topological database
- **error**—OSPF error packets
- **event**—OSPF state transitions
- **flooding**—Link-state flooding packets
- **graceful-restart**—Graceful-restart events
- **hello**—Hello packets, which are used to establish neighbor adjacencies and to determine whether neighbors are reachable
- **ldp-synchronization**—Synchronization events between OSPF and LDP
- **lsa-ack**—Link-state acknowledgment packets, which are used in synchronizing the OSPF topological database
- **lsa-analysis**—Link-state analysis. Specific to the Juniper Networks implementation of OSPF, Junos OS performs LSA analysis before running the shortest-path-first (SPF) algorithm. LSA analysis helps to speed the calculations performed by the SPF algorithm.
- **lsa-request**—Link-state request packets, which are used in synchronizing the OSPF topological database
- **lsa-update**—Link-state updates packets, which are used in synchronizing the OSPF topological database

- **nsr-synchronization**—Nonstop routing synchronization events
- **on-demand**—Trace demand circuit extensions
- **packet-dump**—Dump the contents of selected packet types
- **packets**—All OSPF packets
- **restart-signaling**—(OSPFv2 only) Restart-signaling graceful restart events
- **spf**—Shortest path first (SPF) calculations

You can optionally specify one or more of the following flag modifiers:

- **detail**—Detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

NOTE: Use the **detail** flag modifier with caution as it might cause the CPU to become very busy.

Global tracing options are inherited from the configuration set by the **traceoptions** statement at the **[edit routing-options]** hierarchy level. You can override the following global trace options for the OSPF protocol using the **traceoptions flag** statement included at the **[edit protocols ospf]** hierarchy level:

- **all**—All tracing operations
- **general**—All normal operations and routing table changes (a combination of the normal and route trace operations)
- **normal**—Normal events
- **policy**—Policy processing
- **route**—Routing information
- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing

NOTE: Use the trace flag **all** with caution as it might cause the CPU to become very busy.

Example: Tracing OSPF Protocol Traffic

This example shows how to trace OSPF protocol traffic.

- Requirements on page 357
- Overview on page 357

- Configuration on page 358
- Verification on page 361

Requirements

This example assumes that OSPF is properly configured and running in your network, and you want to trace OSPF protocol traffic for debugging purposes.

Overview

You can trace OSPF protocol traffic to help debug OSPF protocol issues. When you trace OSPF protocol traffic, you specify the name of the file and the type of information you want to trace. All files are placed in a directory on the routing device's hard disk. On M Series and T Series routers, trace files are stored in the */var/log* directory.

This example shows a few configurations that might be useful when debugging OSPF protocol issues. The verification output displayed is specific to each configuration.

TIP: To keep track of your log files, create a meaningful and descriptive name so it is easy to remember the content of the trace file. We recommend that you place global routing protocol tracing output in the file **routing-log**, and OSPF tracing output in the file **ospf-log**.

In the first example, you globally enable tracing operations for all routing protocols that are actively running on your routing device to the file routing-log. With this configuration, you keep the default settings for the trace file size and the number of trace files. After enabling global tracing operations, you enable tracing operations to provide detailed information about OSPF packets, including link-state advertisements, requests, and updates, database description packets, and hello packets to the file ospf-log, and you configure the following options:

- **size**—Specifies the maximum size of each trace file, in KB, MB, or GB. In this example, you configure 10 KB as the maximum size. When the file reaches its maximum size, it is renamed with a .0 extension. When the file again reaches its maximum size, it is renamed with a .1 extension, and the newly created file is renamed with a .0 extension. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option. You specify **k** for KB, **m** for MB, and **g** for GB. By default, the trace file size is 128 KB. The file size range is 10 KB through the maximum file size supported on your system.
- **files**—Specifies the maximum number of trace files. In this example, you configure a maximum of 5 trace files. When a trace file reaches its maximum size, it is renamed with a .0 extension, then a .1 extension, and so on until the maximum number of trace files is reached. When the maximum number of files is reached, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the **size** option. By default, there are 10 files. The range is 2 through 1000 files.

In the second example, you trace all SPF calculations to the file ospf-log by including the **spf** flag. You keep the default settings for the trace file size and the number of trace files.

In the third example, you trace the creation, receipt, and retransmission of all LSAs to the file ospf-log by including the **lsa-request**, **lsa-update**, and **lsa-ack** flags. You keep the default settings for the trace file size and the number of trace files.

Configuration

- Configuring Global Tracing Operations and Tracing OSPF Packet Information on page 358
- Tracing SPF Calculations on page 359
- Tracing Link-State Advertisements on page 360

Configuring Global Tracing Operations and Tracing OSPF Packet Information

CLI Quick Configuration

To quickly enable global tracing operations for all routing protocols actively running on your routing device and to trace detailed information about OSPF packets, copy the following commands and paste them into the CLI.

```
[edit]
set routing-options traceoptions file routing-log
set protocols ospf traceoptions file ospf-log
set protocols ospf traceoptions file files 5 size 10k
set protocols ospf traceoptions flag lsa-ack
set protocols ospf traceoptions flag database-description
set protocols ospf traceoptions flag hello
set protocols ospf traceoptions flag lsa-update
set protocols ospf traceoptions flag lsa-request
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Modifying the Junos OS Configuration* in *CLI User Guide*.

To configure global routing tracing operations and tracing operations for OSPF packets:

1. Configure tracing at the routing options level to collect information about the active routing protocols on your routing device.

   ```
   [edit]
   user@host# edit routing-options traceoptions
   ```

2. Configure the filename for the global trace file.

   ```
   [edit routing-options traceoptions]
   user@host# set file routing-log
   ```

3. Configure the filename for the OSPF trace file.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   ```



```
user@host# edit protocols ospf traceoptions
user@host# set file ospf-log
```

4. Configure the maximum number of trace files.

```
[edit protocols ospf traceoptions]
user@host# set file files 5
```

5. Configure the maximum size of each trace file.

```
[edit protocols ospf traceoptions]
user@host# set file size 10k
```

6. Configure tracing flags.

```
[edit protocols ospf traceoptions]
user@host# set flag lsa-ack
user@host# set flag database-description
user@host# set flag hello
user@host# set flag lsa-update
user@host# set flag lsa-request
```

7. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf traceoptions]
user@host# commit
```

Results Confirm your configuration by entering the **show routing-options** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show routing-options
traceoptions {
  file routing-log;
}
```

```
user@host# show protocols ospf
traceoptions {
  file ospf-log size 10k files 5;
  flag lsa-ack;
  flag database-description;
  flag hello;
  flag lsa-update;
  flag lsa-request;
}
```

To confirm your OSPFv3 configuration, enter the **show routing-options** and the **show protocols ospf3** commands.

Tracing SPF Calculations

CLI Quick Configuration To quickly trace SPF calculations, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf traceoptions file ospf-log
set protocols ospf traceoptions flag spf
```


Step-by-Step Procedure

To configure SPF tracing operations for OSPF:

1. Configure the filename for the OSPF trace file.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

   ```
   [edit]
   user@host# edit protocols ospf traceoptions
   user@host# set file ospf-log
   ```

2. Configure the SPF tracing flag.

   ```
   [edit protocols ospf traceoptions]
   user@host# set flag spf
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit protocols ospf traceoptions]
   user@host# commit
   ```

Results

Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
traceoptions {
  file ospf-log ;
  flag spf;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Tracing Link-State Advertisements

CLI Quick Configuration

To quickly trace the creation, receipt, and retransmission of all LSAs, copy the following commands and paste them into the CLI.

```
[edit]
set protocols ospf traceoptions file ospf-log
set protocols ospf traceoptions flag lsa-request
set protocols ospf traceoptions flag lsa-update
set protocols ospf traceoptions flag lsa-ack
```

Step-by-Step Procedure

To configure link-state advertisement tracing operations for OSPF:

1. Configure the filename for the OSPF trace file.

   NOTE: To specify OSPFv3, include the **ospf3** statement at the **[edit protocols]** hierarchy level.

```
[edit]
user@host# edit protocols ospf traceoptions
user@host# set file ospf-log
```

2. Configure the link-state advertisement tracing flags.

```
[edit protocols ospf traceoptions]
user@host# set flag lsa-request
user@host# set flag lsa-update
user@host# set flag lsa-ack
```

3. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf traceoptions]
user@host# commit
```

Results Confirm your configuration by entering the **show protocols ospf** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
traceoptions {
  file ospf-log;
  flag lsa-request;
  flag lsa-update;
  flag lsa-ack;
}
```

To confirm your OSPFv3 configuration, enter the **show protocols ospf3** command.

Verification

Confirm that the configuration is working properly.

Verifying Trace Operations

Purpose Verify that the Trace options field displays the configured trace operations, and verify that the Trace file field displays the location on the routing device where the file is saved, the name of the file to receive the output of the tracing operation, and the size of the file.

Action From operational mode, enter the **show ospf overview extensive** command for OSPFv2, and enter the **show ospf3 overview extensive** command for OSPFv3.

Related Documentation

- OSPF Overview on page 4
- OSPF Configuration Overview on page 14
- *Junos OS Tracing and Logging Operations* in the *Junos OS Administration Library for Routing Devices*
- *Example: Tracing Global Routing Protocol Operations* in the *Junos OS Routing Protocols Library for Routing Devices*

CHAPTER 18

OSPF Configuration Statements

[edit protocols ospf] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
  ospf {
    disable;
    area area-id {
      ... the area subhierarchy appears after the main [edit protocols ospf] hierarchy ...
    }
    backup-spf-options {
      disable;
      downstream-paths-only;
      no-install;
    }
    database-protection {
      ignore-count number;
      ignore-time seconds;
      maximum-lsa number;
      reset-time seconds;
      warning-only;
      warning-threshold percent;
    }
    export [ policy-names ];
    external-preference preference;
    graceful-restart {
      disable;
      helper-disable <both | restart-signaling | standard>;
      no-strict-lsa-checking;
      notify-duration seconds;
      restart-duration seconds;
    }
    import [ policy-names ];
    lsa-refresh-interval;
    no-nssa-abr;
    no-rfc-1583;
    overload <timeout seconds>;
```

```
    preference preference;
    prefix-export-limit number;
    reference-bandwidth reference-bandwidth;
    rib-group group-name;
    spf-options {
      delay milliseconds;
      holddown milliseconds;
      rapid-runs number;
    }
    topology (default | ipv4-multicast | name) {
      backup-spf-options {
        disable;
        downstream-paths-only;
        no-install;
      }
      overload;
      prefix-export-limit number;
      spf-options {
        delay milliseconds;
        holddown milliseconds;
        rapid-runs number;
      }
      topology-id number;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    traffic-engineering {
      advertise-unnumbered-interfaces;
      credibiliity-protocol-preference;
      ignore-lsp-metrics;
      multicast-rpf-routes;
      no-topology;
      shortcuts <lsp-metric-into-summary>;
    }
  }

  ospf {
    area area-id {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
      context-identifier identifier
      interface interface-name {
        ... the interface subhierarchy appears after the main [edit ospf area area-id] hierarchy
          level ...
      }
      label-switched-path name {
        disable;
        metric metric;
        topology (name | default | ipv4-multicast) {
          disable;
          metric metric;
        }
      }
      network-summary-export [ policy-names ];
```



```
    network-summary-import [ policy-names ];
    nssa {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
      default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
      }
      (summaries | no-summaries);
    }
    peer-interface interface-name {
      disable;
      authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
      }
      dead-interval seconds;
      demand-circuit;
      flood-reduction;
      hello-interval seconds;
      no-neighbor-down-notification;
      retransmit-interval seconds;
      transit-delay seconds;
    }
    stub <default-metric metric> <summaries | no-summaries>;
    virtual-link neighbor-id router-id transit-area area-id {
      disable;
      authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
      }
      dead-interval seconds;
      demand-circuit;
      flood-reduction;
      hello-interval seconds;
      ipsec-sa sa-name;
      no-neighbor-down-notification;
      retransmit-interval seconds;
      topology (name | default | ipv4-multicast) {
        disable;
        metric metric;
      }
      transit-delay seconds;
    }
  }

  area area-id {
    interface interface-name {
      disable;
      authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
      }
      bandwidth-based-metrics {
        bandwidth value metric number;
      }
```

```
bfd-liveness-detection {
  authentication {
    algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
      meticulous-keyed-sha-1 | simple-password);
    key-chain key-chain-name;
    loose-check;
  }
  detection-time {
    threshold milliseconds;
  }
  full-neighbors-only;
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  version (1 | automatic);
}
dead-interval seconds;
demand-circuit;
dynamic-neighbors;
flood-reduction;
hello-interval seconds;
interface-type (nbma | p2mp | p2p);
ipsec-sa sa-name;
ldp-synchronization {
  disable;
  hold-time seconds;
}
(link-protection | node-link-protection);
metric metric;
neighbor address <eligible>;
no-eligible-backup;
no-interface-state-traps;
no-neighbor-down-notification;
passive {
  traffic-engineering {
    remote-node-id address;
  }
}
poll-interval seconds;
priority number;
retransmit-interval seconds;
secondary;
te-metric metric;
topology (name | default | ipv4-multicast) {
  disable;
  bandwidth-based-metrics {
    bandwidth value;
    metric number;
  }
  metric metric;
}
```



```
            transit-delay seconds;
          }
        }
      }
    }
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

[edit protocols ospf3] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
  ospf3 {
    disable;
    area area-id {
      ... the area subhierarchy appears after the main [edit protocols ospf3] hierarchy ...
    }
    backup-spf-options {
      disable;
      downstream-paths-only;
      no-install;
    }
    database-protection {
      ignore-count number;
      ignore-time seconds;
      maximum-lsa number;
      reset-time seconds;
      warning-only;
      warning-threshold percent;
    }
    export [ policy-names ];
    external-preference preference;
    graceful-restart {
      disable;
      helper-disable;
      no-strict-lsa-checking;
      notify-duration seconds;
      restart-duration seconds;
    }
    import [ policy-names ];
    lsa-refresh-interval;
    no-nssa-abr;
    no-rfc-1583;
    overload <timeout seconds>;
    preference preference;
    prefix-export-limit number;
    realm (ipv4-multicast | ipv4-unicast | ipv6-multicast | ipv6-unicast) {
      ... the realm subhierarchies appear after the main [edit protocols ospf3] hierarchy ...
    }
    reference-bandwidth reference-bandwidth;
    rib-group group-name;
```

```
    spf-options {
      delay milliseconds;
      holddown milliseconds;
      no-ignore-our-externals;
      rapid-runs number;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    traffic-engineering {
      ignore-lsp-metrics;
      shortcuts <lsp-metric-into-summary>;
    }
  }

  ospf3 {
    area area-id {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
      inter-area-prefix-export [ policy-names ];
      inter-area-prefix-import [ policy-names ];
      interface interface-name {
        ... the interface subhierarchy appears after the main [edit ospf3 area area-id]
          hierarchy level ...
      }
      nssa {
        area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
        default-lsa {
          default-metric metric;
          metric-type type;
          type-7;
        }
        (summaries | no-summaries);
      }
      stub <default-metric metric> <summaries | no-summaries>;
      virtual-link neighbor-id router-id transit-area area-id {
        disable;
        dead-interval seconds;
        demand-circuit;
        flood-reduction;
        hello-interval seconds;
        ipsec-sa sa-name;
        retransmit-interval seconds;
        transit-delay seconds;
      }
    }

    area area-id {
      interface interface-name {
        disable;
        bandwidth-based-metrics {
          bandwidth value metric number;
        }
        bfd-liveness-detection {
          authentication {
```



```
            algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
              meticulous-keyed-sha-1 | simple-password);
            key-chain key-chain-name;
            loose-check;
          }
          detection-time {
            threshold milliseconds;
          }
          full-neighbors-only;
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          version (1 | automatic);
        }
        dead-interval seconds;
        demand-circuit;
        flood-reduction;
        hello-interval seconds;
        interface-type (p2mp-over-lan | p2p);
        ipsec-sa sa-name;
        (link-protection | node-link-protection);
        metric metric;
        no-eligible-backup;
        own-router-lsa;
        passive {
          traffic-engineering {
            remote-node-id address;
          }
        }
        priority number;
        retransmit-interval seconds;
        transit-delay seconds;
      }
    }
  }

  ospf3 {
    realm (ipv4-multicast| ipv6-multicast) {
      ... same statements as at the [edit protocols ospf3] hierarchy level, EXCEPT FOR ...
      area area-id {
        interface interface-name {
          no-eligible-backup;    # NOT valid at this level
        }
        virtual-link { ... }    # NOT valid at this level
      }
      backup-spf-options { ... }    # NOT valid at this level
      realm realm-identifier { ... }    # NOT valid at this level
      traffic-engineering { ... }    # NOT valid at this level
    }
  }
```

```
    ospf3 {
      realm ipv4-unicast {
        ... same statements as at the [edit protocols ospf3] hierarchy level, PLUS ...
          area area-id {
            interface interface-name {
              ldp-synchronization {
                disable;
                hold-time seconds;
              }
            }
          }

        ... BUT NOT ...
          area area-id {
            virtual-link { ... }    # NOT valid at this level
          }
          realm realm-identifier { ... }    # NOT valid at this level
          traffic-engineering { ... }    # NOT valid at this level

      }
    }

    ospf3 {
      realm ipv6-unicast {
        disable;
        backup-spf-options {
          disable;
          downstream-paths-only;
          no-install;
        }
      }
    }
  }
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

area

Syntax

```
area area-id {
  interface interface-name {
    passive;
    topology (ipv4-multicast | name) {
      disable;
    }
  }
  virtual-link neighbor-id router-id transit-area area-id {
    topology (ipv4-multicast | name) {
      disable;
    }
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify the area identifier for this routing device to use when participating in OSPF routing. All routing devices in an area must use the same area identifier to establish adjacencies.

Specify multiple **area** statements to configure the routing device as an area border router. An area border router does not automatically summarize routes between areas. Use the **area-range** statement to configure route summarization. By definition, an area border router must be connected to the backbone area either through a physical link or through a virtual link. To create a virtual link, include the **virtual-link** statement.

To specify that the routing device is directly connected to the OSPF backbone, include the **area 0.0.0.0** statement.

All routing devices on the backbone must be contiguous. If they are not, use the **virtual-link** statement to create the appearance of connectivity to the backbone.

You can also configure any interface that belongs to one or more topologies to advertise the direct interface addresses without actually running OSPF on that interface. By default, OSPF must be configured on an interface in order for direct interface addresses to be advertised as interior routes.

NOTE: If you configure an interface with the **passive** statement, it applies to all the topologies to which the interface belongs. You cannot configure an interface as passive for only one specific topology and have it remain active for any other topologies to which it belongs.

Options *area-id*—Area identifier. The identifier can be up to 32 bits. It is common to specify the area number as a simple integer or an IP address. Area number **0.0.0.0** is reserved for the OSPF backbone area.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Understanding Multiple Address Families for OSPFv3 on page 135
- **virtual-link on page 465**

area-range

Syntax

area-range *network/mask-length* <exact> <override-metric *metric*> <restrict>;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit protocols (ospf | ospf3) area *area-id*],
[edit protocols (ospf | ospf3) area *area-id* nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit routing-instances *routing-instance-name* realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

(Area border routers only) For an area, summarize a range of IP addresses when sending summary link advertisements (within an area). To summarize multiple ranges, include multiple **area-range** statements.

For a not-so-stubby area (NSSA), summarize a range of IP addresses when sending NSSA link-state advertisements. The specified prefixes are used to aggregate external routes learned within the area when the routes are advertised to other areas. To specify multiple prefixes, include multiple **area-range** statements. All external routes learned within the area that do not fall into one of the prefixes are advertised individually to other areas.

Default

By default, area border routers do not summarize routes being sent from one area to other areas, but rather send all routes explicitly.

Options

exact—(Optional) Summarization of a route is advertised only when an exact match is made with the configured summary range.

mask-length—Number of significant bits in the network mask.

network—IP address. You can specify one or more IP addresses.

override-metric *metric*—(Optional) Override the metric for the IP address range and configure a specific metric value.

restrict—(Optional) Do not advertise the configured summary. This hides all routes that are contained within the summary, effectively creating a route filter.

Range: 1 through 16,777,215

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Summarizing Ranges of Routes in OSPF Link-State Advertisements on page 142

authentication (Protocols OSPF)

Syntax

```
authentication {
  md5 key-identifier {
    key key-value;
    start-time YYYY-MM-DD.hh:mm;
  }
  simple-password key;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link],
[edit protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure an authentication key (password). Neighboring routers use the password to verify the authenticity of packets sent from this interface.

All routers that are connected to the same IP subnet must use the same authentication scheme and password.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPFv2 Authentication on page 173
- Example: Configuring MD5 Authentication for OSPFv2 Exchanges on page 178
- Example: Configuring a Transition of MD5 Keys on an OSPFv2 Interface on page 180
- Example: Configuring Simple Authentication for OSPFv2 Exchanges on page 176

backup-spf-options

Syntax

```
backup-spf options {
  disable;
  downstream-paths-only;
  no-install;
}
```

Hierarchy Level

[edit protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit protocols ospf topology (default | *name*)],
[edit logical-systems *logical-system-name* protocols ospf topology (default | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf topology (default | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf topology (default | *name*)];
[edit protocols ospf3 realm ipv4-unicast],
[edit logical-systems *logical-system-name* protocols ospf3 realm ipv4-unicast],
[edit routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure options for running the shortest-path-first (SPF) algorithm for backup next hops for protected OSPF interfaces. Use these options to override the default behavior of having Junos OS calculate backup paths for all the topologies in an OSPF instance when at least one OSPF interface is configured with link protection or node-link protection. These options also enable you to change the default behavior for a specific topology in an OSPF instance.

Options

disable—Do not calculate backup next hops for the specified OSPF instance or topology.

downstream-paths-only—Calculate and install only downstream paths as defined in RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates* for the specified OSPF instance or topology.

no-install—Do not install the backup next hops for the specified OSPF instance or topology.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control-level—To add this statement to the configuration.

Related Documentation

- Configuring Backup SPF Options for Protected OSPF Interfaces on page 238
- link-protection on page 412
- node-link-protection on page 426

bandwidth-based-metrics

Syntax

```
bandwidth-based-metrics {
  bandwidth value;
  metric number;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* topology *topology-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* topology *topology-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instances* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name* topology *topology-name*],
[edit protocols ospf3 realm (ivp4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology *topology-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description

Specify a set of bandwidth threshold values and associated metric values for an OSPF interface or for a topology on an OSPF interface. When the bandwidth of an interface changes, Junos OS automatically sets the interface metric to the value associated with the appropriate bandwidth threshold value.

Options

bandwidth *value*—Specify the bandwidth threshold in bits per second.

Range: 9600 through 1,000,000,000,000,000

metric *number*—Specify a metric value to associate with a specific bandwidth value.

Range: 1 through 65,535

NOTE: You must also configure a static metric value for the OSPF interface or topology with the **metric** statement. Junos OS uses this value to calculate the cost of a route from the OSPF interface or topology if the bandwidth for the interface is higher than of any bandwidth threshold values configured for bandwidth-based metrics.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth on page 156
- **metric on page 416**
- Example: Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth on page 156

bfd-liveness-detection (Protocols OSPF)

Syntax

```
bfd-liveness-detection {
  authentication {
    algorithm algorithm-name;
    key-chain key-chain-name;
    loose-check;
  }
  detection-time {
    threshold milliseconds;
  }
  full-neighbors-only
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  version (1 | automatic);
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
detection-time threshold and **transmit-interval threshold** options added in Junos OS Release 8.2.
Support for logical systems introduced in Junos OS Release 8.3.
no-adaptation option introduced in Junos OS Release 9.0.
no-adaptation option introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 introduced in Junos OS Release 9.3.
Support for OSPFv3 introduced in Junos OS Release 9.3 for EX Series switches.
full-neighbors-only option introduced in Junos OS Release 9.5.
full-neighbors-only option introduced in Junos OS Release 9.5 for EX Series switches.

authentication algorithm, **authentication key-chain**, and **authentication loose-check** options introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Configure bidirectional failure detection timers and authentication for OSPF.

The remaining statements are explained separately.

Options **authentication algorithm** ***algorithm-name*** —Configure the algorithm used to authenticate the specified BFD session: **simple-password**, **keyed-md5**, **keyed-sha-1**, **meticulous-keyed-md5**, or **meticulous-keyed-sha-1**.

authentication key-chain ***key-chain-name***—Associate a security key with the specified BFD session using the name of the security keychain. The name you specify must match one of the keychains configured in the **authentication-key-chains key-chain** statement at the **[edit security]** hierarchy level.

authentication loose-check—(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication may not be configured at both ends of the BFD session.

detection-time threshold ***milliseconds***—Configure a threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

full-neighbors-only—Establish BFD sessions only for OSPF neighbors in the full state. The default behavior is to establish BFD sessions for all OSPF neighbors.

minimum-interval ***milliseconds***—Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit and receive intervals separately using the **transmit-interval minimum-interval** and **minimum-receive-interval** statements.

Range: 1 through 255,000 milliseconds

minimum-receive-interval ***milliseconds***—Configure the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the **minimum-interval** statement.

Range: 1 through 255,000 milliseconds

multiplier ***number***—Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

Range: 1 through 255

Default: 3

no-adaptation—Specify that BFD sessions should not adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

transmit-interval threshold ***milliseconds***—Configure the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

Range: 0 through 4,294,967,295 (2^{32} – 1)

transmit-interval minimum-interval ***milliseconds***—Configure the minimum interval at which the routing device transmits hello packets to a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit interval using the **minimum-interval** statement.

Range: 1 through 255,000

version—Configure the BFD version to detect: **1** (BFD version 1) or **automatic** (autodetect the BFD version).

Default: **automatic**

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring BFD for OSPF on page 210
- Example: Configuring BFD Authentication for OSPF on page 213

context-identifier (Protocols OSPF)

Syntax

context-identifer *identifier*

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf |ospf3) area *area-id*],
[edit protocols (ospf | ospf3) area *area-id*]

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure OSPF context-identifier information.

Options

identifer—IPv4 address that defines a protection pair. The context identifier is manually configured on both the primary and protector provider edge (PE) devices.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *show ospf context-identifier*

database-protection

Syntax

```
database-protection {
  ignore-count number;
  ignore-time seconds;
  maximum-lsa number;
  reset-time seconds;
  warning-only;
  warning-threshold percent;
}
```

Hierarchy Level

[edit protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-unicast | ipv6-multicast)]

Release Information

Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure the maximum number of link-state advertisements (LSAs) that are not generated by the router or switch in a given OSPF instance.

Default

By default, OSPF database protection is not enabled.

Options

ignore-count *number*—Configure the number of times the database can enter the ignore state. When the ignore count is exceeded, the database enters the isolate state.

Range: 1 through 32

Default: 5

ignore-time *seconds*—Configure the time the database must remain in the ignore state before it resumes regular operations (enters retry state).

Range: 30 through 3,600 seconds

Default: 300 seconds

maximum-lsa *number*—Configure the maximum number of LSAs whose advertising router ID is different from the local router ID in a given OSPF instance. This includes external LSAs as well as LSAs with any scope, such as the link, area, and autonomous system (AS). This value is mandatory.

Range: 1 through 1,000,000

Default: None

reset-time *seconds*—Configure the time period during which the database must operate without being in the ignore or isolate state before it is reset to a normal operating state.

Range: 60 through 86,400 seconds

Default: 600 seconds

warning-only—Specify that only a warning should be issued when the maximum LSA number is exceeded. If configured, no other action is taken against the database.

warning-threshold ***percent***—Configure the percentage of the maximum number of LSAs to be exceeded before a warning message is logged.

Range: 30 through 100 percent

Default: 75 percent

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Database Protection Overview on page 277
- Configuring OSPF Database Protection on page 278

dead-interval

Syntax

dead-interval *seconds*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Specify how long OSPF waits before declaring that a neighboring routing device is unavailable. This is an interval during which the routing device receives no hello packets from the neighbor.

Options

seconds—Interval to wait.

Range: 1 through 65,535 seconds

Default: Four times the hello interval—40 seconds (broadcast and point-to-point networks); 120 seconds (nonbroadcast multiple access (NBMA) networks)

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Timers on page 202
- *Configuring RSVP and OSPF for LMP Peer Interfaces*

• hello-interval on page 398

default-lsa

Syntax

```
default-lsa {
  default-metric metric;
  metric-type type;
  type-7;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa],
[edit protocols (ospf | ospf3) area *area-id* nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

On area border routers only, for a not-so-stubby area (NSSA), inject a default link-state advertisement (LSA) with a specified metric value into the area. The default route matches any destination that is not explicitly reachable from within the area.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• OSPF Areas and Router Functionality Overview on page 9
• Example: Configuring OSPF Not-So-Stubby Areas on page 41
• nssa on page 427
• stub on page 453

default-metric

Syntax

default-metric *metric*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* stub],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* stub],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* stub],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* stub],
[edit protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit protocols (ospf | ospf3) area *area-id* stub],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* stub],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* stub],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* stub]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

On area border routers only, for a stub area, inject a default route with a specified metric value into the area. The default route matches any destination that is not explicitly reachable from within the area.

Options

metric—Metric value.

Range: 1 through 16,777,215

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- nssa on page 427

- stub on page 453

demand-circuit

Syntax demand-circuit;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Support for the **realm** statement introduced in Junos OS Release 9.2.

Description Configure an interface as a demand circuit.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Demand Circuits on page 129
- Example: Configuring OSPFv2 Sham Links on page 268

disable (Protocols OSPF)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 7.5.

Description Disable LDP synchronization for OSPF.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Synchronization Between LDP and OSPF on page 168

disable (OSPF)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface*interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instances* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) virtual-link],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit protocols ospf area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Disable OSPF, an OSPF interface, or an OSPF virtual link.

By default, control packets sent to the remote end of a virtual link must be forwarded using the default topology. In addition, the transit area path consists only of links that are in the default topology. You can disable a virtual link for a configured topology, but not for a default topology. Include the **disable** statement at the **[edit protocols ospf area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id* topology *name*]** hierarchy level.

NOTE: If you disable the virtual link by including the **disable** statement at the **[edit protocols ospf area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*]** hierarchy level, you disable the virtual link for all topologies, including the default topology. You cannot disable the virtual link only in the default topology.

Default The configured object is enabled (operational) unless explicitly disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Configuration Overview on page 14
- *Configuring RSVP and OSPF for LMP Peer Interfaces*

domain-id

Syntax domain-id *domain-id*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify a domain ID for a route. The domain ID identifies the OSPF domain from which the route originated.

Options *domain-id*—You can specify either an IP address or an IP address and a local identifier using the following format: ***ip-address:local-identifier***. If you do not specify a local identifier with the IP address, the identifier is assumed to have a value of 0.

Default: If the router ID is not configured in the routing instance, the router ID is derived from an interface address belonging to the routing instance.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Between PE and CE Routers in Layer 3 VPNs*

domain-vpn-tag

Syntax domain-vpn-tag *number*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Set a virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.

Options *number*—VPN tag.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Between PE and CE Routers in Layer 3 VPNs*

export (Protocols OSPF)

Syntax export [*policy-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Apply one or more policies to routes being exported from the routing table into OSPF.

Options ***policy-names***—Name of one or more policies.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPF Routing Policy on page 281
- Import and Export Policies for Network Summaries Overview on page 297
- import on page 401
- *Routing Policy Feature Guide for Routing Devices*

external-preference (Protocols OSPF)

Syntax

external-preference *preference*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast } ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Set the route preference for OSPF external routes.

Options

preference—Preference value.

Range: 0 through 4,294,967,295 (2^{32} – 1)

Default: 150

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Controlling OSPF Route Preferences on page 158
- preference on page 435

flood-reduction

Syntax

flood-reduction;

Hierarchy Level

[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interfaces *interface-name*],
[edit protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interfaces *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interfaces *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interfaces *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interfaces *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link neighbor-id *router-id* transit–area *transit-area* area-id],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote *address*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area area-id sham-link-remote *address*],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 10.4 for EX Series switches.

Description

Specify to send self-generated link-state advertisements (LSAs) with the DoNotAge bit set. As a result, self-originated LSAs are not reflooded every 30 minutes, as required by OSPF by default. An LSA is refreshed only when the content of the LSA changes, which reduces OSPF traffic overhead in stable topologies.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring OSPF Refresh and Flooding Reduction in Stable Topologies on page 149

graceful-restart (Protocols OSPF)

Syntax

```
graceful-restart {
  disable;
  helper-disable (standard | restart-signaling | both);
  no-strict-lsa-checking;
  notify-duration seconds;
  restart-duration seconds;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf]

Release Information

Statement introduced before Junos OS Release 7.4.
Support for the **no-strict-lsa-checking** statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the helper mode **standard**, **restart-signaling**, and **both** options introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure graceful restart for OSPF.

Graceful restart allows a routing device to restart with minimal effects to the network, and is enabled for all routing protocols at the **[edit routing-options]** hierarchy level.

Options

disable—Disable graceful restart for OSPF.

helper-disable (standard | restart-signaling| both)—Disable helper mode for graceful restart. When helper mode is disabled, a device cannot help a neighboring device that is attempting to restart. Beginning with Junos OS Release 11.4, you can configure restart signaling-based helper mode for OSPFv2 graceful restart configurations. The **standard**, **restart-signaling**, and **both** options are only supported for OSPFv2. Specify **standard** to disable helper mode for standard graceful restart (based on RFC 3623). Specify **restart-signaling** to disable helper mode for restart signaling-based graceful restart (based on RFC 4811, RFC 4812, and RFC 4813). Specify **both** to disable helper mode for both standard and restart signaling-based graceful restart. The last committed statement takes precedence over the previously configured statement.

Default: Helper mode is enabled by default. For OSPFv2, both standard and restart-signaling based helper modes are enabled by default.

no-strict-lsa-checking—Disable strict OSPF link-state advertisement (LSA) checking to prevent the termination of graceful restart by a helping router. LSA checking is enabled by default.

NOTE: The **helper-disable** statement and the **no-strict-lsa-checking** statement cannot be configured at the same time. If you attempt to configure both statements at the same time, the routing device displays a warning message when you enter the **show protocols (ospf | ospf3)** command.

notify-duration *seconds*—Estimated time needed to send out purged grace LSAs over all the interfaces.

Range: 1 through 3600 seconds

Default: 30 seconds

restart-duration *seconds*—Estimated time needed to reacquire a full OSPF neighbor from each area.

Range: 1 through 3600 seconds

Default: 180 seconds

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Graceful Restart for OSPF on page 221
- Example: Configuring the Helper Capability Mode for OSPFv2 Graceful Restart on page 225
- Example: Configuring the Helper Capability Mode for OSPFv3 Graceful Restart on page 228
- Example: Disabling Strict LSA Checking for OSPF Graceful Restart on page 232
- *Configuring Graceful Restart for QFabric Systems*
- *Junos OS High Availability Library for Routing Devices*

hello-interval (Protocols OSPF)

Syntax hello-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Specify how often the routing device sends hello packets out the interface. The hello interval must be the same for all routing devices on a shared logical IP network.

Options ***seconds***—Time between hello packets, in seconds.

Range: 1 through 255 seconds

Default: 10 seconds (broadcast and point-to-point networks); 30 seconds (nonbroadcast multiple access [NBMA] networks)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Timers on page 202
- *Configuring RSVP and OSPF for LMP Peer Interfaces*
- **dead-interval on page 385**

helper-disable (OSPF)

Syntax

helper-disable < both | restart-signaling | standard >;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf graceful-restart],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf graceful-restart],
[edit protocols ospf graceful-restart],
[edit routing-instances *routing-instance-name* protocols ospf graceful-restart]

Release Information

Statement introduced before Junos OS Release 7.4.
Options **both**, **restart-signaling**, and **standard** introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Disable helper mode for graceful restart. When helper mode is disabled, a router cannot help a neighboring router that is attempting to restart. The last committed statement takes precedence over the previously configured statement.

Default

Helper mode is enabled by default for OSPF.

Options

both—(Optional) Disable helper mode for both standard and restart signaling-based graceful restart.

restart-signaling—(Optional) Disable helper mode for restart signaling-based graceful restart (based on RFC 4811, RFC 4812, and RFC 4813).

NOTE: Restart signaling-based helper mode is not supported for OSPFv3 configurations.

standard—(Optional) Disable helper mode for standard graceful restart (based on RFC 3623).

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Protocols Graceful Restart*
- *Configuring Graceful Restart for MPLS-Related Protocols*
- *Configuring Graceful Restart for QFabric Systems*

hold-time (Protocols OSPF)

Syntax hold-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 7.5.

Description Configure the time period to advertise the maximum cost metric for a link that is not fully operational.

Options *seconds*—Hold-time value.

Range: 1 through 65,535 seconds

Default: Infinity

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Synchronization Between LDP and OSPF on page 168

ignore-lsp-metrics

Syntax ignore-lsp-metrics;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf traffic-engineering shortcuts],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf traffic-engineering shortcuts],
[edit protocols ospf traffic-engineering],
[edit routing-instances *routing-instance-name* protocols ospf traffic-engineering shortcuts]

Release Information Statement introduced in Junos OS Release 7.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for (OSPFv3) introduced in Junos OS Release 9.4.
Support for (OSPFv3) introduced in Junos OS Release 9.4 for EX Series switches.

Description Ignore RSVP LSP metrics in OSPF traffic engineering shortcut calculations.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Enabling OSPF Traffic Engineering Support on page 246

import (Protocols OSPF)

Syntax import [*policy-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Filter OSPF routes from being added to the routing table.

Options *policy-names*—Name of one or more policies.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPF Routing Policy on page 281
- Import and Export Policies for Network Summaries Overview on page 297
- export on page 393
- *Routing Policy Feature Guide for Routing Devices*

inter-area-prefix-export

Syntax inter-area-prefix-export [*policy-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf3 area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit protocols ospf3 area *area-id*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-muticast | ipv6-multicast) area *area-id*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Apply an export policy for OSPFv3 to specify which interarea prefix link-state advertisements (LSAs) are flooded into an area.

Options *policy-name*—Name of a policy configured at the **[edit policy-options policy-statement *policy-name* term *term-name*]** hierarchy level.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Import and Export Policies for Network Summaries Overview on page 297
- inter-area-prefix-import on page 403

- *Routing Policy Feature Guide for Routing Devices*

inter-area-prefix-import

Syntax inter-area-prefix-import [*policy-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf3 area *area-id*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit protocols ospf3 area *area-id*],
[edit protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)], area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Apply an import policy for OSPFv3 to specify which routes learned from an area are used to generate interarea prefixes into other areas.

Options *policy-name*—Name of a policy configured at the **[edit policy-options policy-statement *policy-name* term *term-name*]** hierarchy level.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Import and Export Policies for Network Summaries Overview on page 297
- **inter-area-prefix-export on page 402**

- *Routing Policy Feature Guide for Routing Devices*

interface (Protocols OSPF)

Syntax

```
interface interface-name {
  disable;
  authentication key <key-id identifier>;
  bfd-liveness-detection {
    authentication {
      algorithm algorithm-name;
      key-chain key-chain-name;
      loose-check;
    }
    detection-time {
      threshold milliseconds;
    }
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    transmit-interval {
      threshold milliseconds;
      minimum-interval milliseconds;
    }
    multiplier number;
  }
  dead-interval seconds;
  demand-circuit;
  hello-interval seconds;
  ipsec-sa name;
  interface-type type;
  ldp-synchronization {
    disable;
    hold-time seconds;
  }
  metric metric;
  neighbor address <eligible>;
  no-interface-state-traps;
  passive;
  poll-interval seconds;
  priority number;
  retransmit-interval seconds;
  te-metric metric;
  topology (ipv4-multicast | name) {
    metric metric;
  }
  transit-delay seconds;
  transmit-interval seconds;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit protocols (ospf | ospf3) area *area-id*],

[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast |
ipv4-multicast | ipv6-multicast) area *area-id*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **topology** statement introduced in Junos OS Release 9.0.
Support for the **topology** statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Support for the **no-interface-state-traps** statement introduced in Junos OS Release 10.3.
This statement is supported only for OSPFv2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable OSPF routing on a routing device interface.

You must include at least one **interface** statement in the configuration to enable OSPF on the routing device.

Options

interface-name—Name of the interface. Specify the interface by IP address or interface name for OSPFv2, or only the interface name for OSPFv3. Using both the interface name and IP address of the same interface produces an invalid configuration. To configure all interfaces, you can specify **all**. Specifying a particular interface and **all** produces an invalid configuration.

NOTE: For nonbroadcast interfaces, specify the IP address of the nonbroadcast interface as *interface-name*.

The remaining statements are explained separately.

NOTE: You cannot run both OSPF and ethernet-tcc encapsulation between two Juniper Networks routing devices.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Configuration Overview on page 14
- *Example: Configuring Multitopology Routing Based on Applications*
- *Example: Configuring Multitopology Routing Based on a Multicast Source*
- Example: Configuring Multiple Address Families for OSPFv3 on page 136
- **neighbor on page 419**

interface-type (Protocols OSPF)

Syntax

interface-type (nbma | p2mp | p2p);

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 for interface type **p2p** only introduced in Junos OS Release 9.4. You cannot configure other interface types for OSPFv3.
Support for OSPFv3 for interface type **p2p** only introduced in Junos OS Release 9.4 for EX Series switches.

Description

Specify the type of interface.

By default, the software chooses the correct interface type based on the type of physical interface. Therefore, you should never have to set the interface type. The exception to this is for NBMA interfaces, which default to an interface type of point-to-multipoint. To have these interfaces explicitly run in Nonbroadcast multiaccess (NBMA) mode, configure the **nbma** interface type, using the IP address of the local ATM interface.

In Junos OS Release 9.3 and later, a point-to-point interface can be an Ethernet interface without a subnet.

Default

The software chooses the correct interface type based on the type of physical interface.

Options

nbma (OSPFv2 only)—Nonbroadcast multiaccess (NBMA) interface.

p2mp (OSPFv2 only)—Point-to-multipoint interface.

p2p—Point-to-point interface.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- About OSPF Interfaces on page 121
- Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network on page 125

ipsec-sa (Protocols OSPF)

Syntax

ipsec-sa *name*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote *address*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote *address*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Support for OSPFv2 authentication added in Junos OS Release 8.3.
Support for the **realm** statement introduced in Junos OS Release 9.2.

Description

Apply IPsec authentication to an OSPF interface or virtual link or to an OSPFv2 remote sham link.

Options

name—Name of the IPsec authentication scheme.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPFv2 Authentication on page 173
- Understanding OSPFv3 Authentication on page 174
- Example: Configuring IPsec Authentication for an OSPF Interface on page 183

- *Junos OS Administration Library for Routing Devices*
- *Junos OS Services Interfaces Library for Routing Devices*

label-switched-path (Protocols OSPF)

Syntax label-switched-path *name* metric *metric*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id*],
[edit protocols ospf area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Advertise label-switched paths into OSPF as point-to-point links.

The label-switched path is advertised in the appropriate OSPF levels as a point-to-point link and contains a local address and a remote address.

Options *name*—Name of the label-switched path.

metric—Metric value.

Range: 1 through 65,535

Default: 1

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Advertising Label-Switched Paths into OSPFv2 on page 255

ldp-synchronization

Syntax

```
ldp-synchronization {
  disable;
  hold-time seconds;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 7.5.
Support for the **realm** statement introduced in Junos OS Release 9.2. Only the **ipv4-unicast** option is supported with this statement.

Description

Enable synchronization by advertising the maximum cost metric until LDP is operational on the link.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Synchronization Between LDP and OSPF on page 168

link-protection (Protocols OSPF)

Syntax link-protection;

Hierarchy Level [edit protocols (ospf | ospf3) area *area-name* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-name* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-name* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-name* interface *interface-name*],
[edit protocols ospf3 realm ipv4-unicast area *area-id*],
[edit logical-systems *logical-system-name* protocols ospf3 realm ipv4-unicast area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id*],
[edit protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology (default | *name*)]

Release Information Statement introduced in Junos OS Release 10.0.

Description Enable link protection on the specified OSPF interface. Junos OS creates a backup loop-free alternate path to the primary next hop for all destination routes that traverse the protected interface.

NOTE: This feature calculates alternate next hop paths for unicast routes only. Therefore, this statement is not supported with the OSPF IPv4 multicast topology or with the OSPFv3 IPv4 multicast and IPv6 multicast realms.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Link Protection for OSPF on page 236
- **node-link-protection on page 426**

lsa-refresh-interval

Syntax lsa-refresh-interval *minutes*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced in Junos OS Release 12.2.

Description Configure the refresh interval for all self-generated link-state advertisement (LSAs). The OSPF standard requires that every LSA be refreshed every 30 minutes. The Juniper Networks implementation refreshes LSAs every 50 minutes. By default, any LSA that is not refreshed expires after 60 minutes. By using this configuration, you can specify when self-originated LSAs are refreshed.

You can override the default behavior by globally configuring the OSPF LSA refresh interval at the **[edit protocols ospf | ospf3]** hierarchy level. However, if you also have OSPF flood reduction configured for a specific interface in an OSPF area at the **[edit protocols ospf | ospf3 area *area-id* interface *interface-name*]** hierarchy level, the flood reduction configuration takes precedence for that specific interface.

Options *minutes*—Time between an LSA refresh, in minutes.

Range: 25 through 50 minutes (1,500 through 3,000 seconds)

Default: 50 minutes

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring OSPF Refresh and Flooding Reduction in Stable Topologies on page 149

lsp-metric-into-summary

Syntax lsp-metric-into-summary;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) traffic-engineering shortcuts]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4 for EX Series switches.

Description Advertise the LSP metric in summary LSAs.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Support for Traffic Engineering on page 243
- Example: Enabling OSPF Traffic Engineering Support on page 246

md5

Syntax

```
md5 key-identifier {
  key key-values;
  start-time time;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* virtual-link authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link authentication],
[edit protocols ospf area *area-id* interface *interface-name* authentication],
[edit protocols ospf area *area-id* virtual-link authentication],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link authentication]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an MD5 authentication key (password).

Options

key-identifier—MD5 key identifier.

Range: 0 through 255

Default: 0

key *key-values*—One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list. Characters can include ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

start-time *time*—MD5 start time.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPFv2 Authentication on page 173
- Example: Configuring MD5 Authentication for OSPFv2 Exchanges on page 178
- Example: Configuring a Transition of MD5 Keys on an OSPFv2 Interface on page 180

metric (Protocols OSPF Interface)

Syntax metric *metric*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* topology (ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology (ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name* topology (ipv4-multicast | *name*)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* sham-link-remote],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology (ipv4-multicast | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Specify the cost of an OSPF interface. The cost is a routing metric that is used in the link-state calculation.

To set the cost of routes exported into OSPF, configure the appropriate routing policy.

Options *metric*—Cost of the route.

Range: 1 through 65,535

Default: By default, the cost of an OSPF route is calculated by dividing the reference-bandwidth value by the bandwidth of the physical interface. Any specific value you configure for the **metric** overrides the default behavior of using the reference-bandwidth value to calculate the cost of the route for that interface.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Controlling the Cost of Individual OSPF Network Segments on page 152
- Example: Configuring OSPFv2 Sham Links on page 268
- *Example: Configuring Multitopology Routing Based on Applications*
- *Example: Configuring Multitopology Routing Based on a Multicast Source*
- **bandwidth-based-metrics on page 377**
- **reference-bandwidth on page 441**

metric-type

Syntax metric-type *type*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* nssadefault-lsa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* nssa default-lsa],
[edit protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* nssa default-lsa],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit routing-instances *routing-instances* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* nssa default-lsa]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Specify the external metric type for the default LSA.

The configured metric determines the method used to compute the cost to a destination:

- The Type 1 external metric is equivalent to the link-state metric. The path cost uses the advertised external path cost and the path cost to the AS boundary router (the route is equal to the sum of all internal costs and the external cost).
- The Type 2 external metric uses the cost assigned by the AS boundary router (the route is equal to the external cost alone). By default, OSPF uses the Type 2 external metric.

Options *type*—Metric type: **1** or **2**

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Not-So-Stubby Areas on page 41

neighbor (Protocols OSPF)

Syntax

neighbor *address* <eligible>;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For nonbroadcast interfaces only, specify neighboring routers. On a nonbroadcast interface, you must specify neighbors explicitly because OSPF does not send broadcast packets to dynamically discover their neighbors. To specify multiple neighbors, include multiple **neighbor** statements.

Options

address—IP address of a neighboring router.

eligible—(Optional) Allow the neighbor to become a designated router.

Default: If you omit this option, the neighbor is not considered eligible to become a designated router.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- About OSPF Interfaces on page 121
- Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network on page 125

network-summary-export

Syntax network-summary-export *policy-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id*],
[edit protocols ospf area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]

Release Information Statement introduced in Junos OS Release 9.1.

Description Apply an export policy that specifies which network-summary link-state advertisements (LSAs) are flooded into an OSPFv2 area.

Options *policy-name*—Name of a policy configured at the **[edit policy-options policy-statement *policy-name* term *term-name*]** hierarchy level.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Import and Export Policies for Network Summaries Overview on page 297
- Example: Configuring an OSPF Export Policy for Network Summaries on page 297
- **network-summary-import on page 421**
- *Routing Policy Feature Guide for Routing Devices*

network-summary-import

Syntax network-summary-import *policy-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id*],
[edit protocols ospf area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]

Release Information Statement introduced in Junos OS Release 9.1.

Description Apply an import policy that specifies which routes learned from an OSPFv2 area are used to generate network-summary link-state advertisements to other areas.

Options *policy-name*—Name of a policy configured at the **[edit policy-options policy-statement *policy-name* term *term-name*]** hierarchy level.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Import and Export Policies for Network Summaries Overview on page 297
- Example: Configuring an OSPF Import Policy for Network Summaries on page 306
- network-summary-export on page 420
- *Routing Policy Feature Guide for Routing Devices*

no-domain-vpn-tag

Syntax no-domain-vpn-tag;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)]

Release Information Statement introduced in Junos OS Release 10.3.

Description Disable the virtual private network (VPN) tag for OSPFv2 and OSPFv3 external routes generated by the provider edge (PE) router when the VPN tag is no longer needed.

Options None.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Between PE and CE Routers in Layer 3 VPNs*

no-eligible-backup (Protocols OSPF)

Syntax no-eligbile-backup;

Hierarchy Level [edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* topology (default | *name*)],

Release Information Statement introduced in Junos OS Release 10.0.

Description Exclude the specified interface as a backup interface for OSPF interfaces on which link protection or node-link protection is enabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Excluding an OSPF Interface as a Backup for a Protected Interface on page 238
- link-protection on page 412
- node-link-protection on page 426

no-interface-state-traps

Syntax no-interface-state-traps;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],

Release Information Statement introduced in Junos OS Release 10.3.

Description Disable the OSPF traps for interface state changes. This statement is particularly useful for OSPF interfaces in passive mode.

NOTE: The **no-interface-state-traps** statement is supported only for OSPFv2.

Default This statement is disabled by default. You must include the **no-interface-state-traps** statement to disable OSPF traps for interface state changes.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring a Passive OSPF Interface on page 132
- passive on page 432

no-neighbor-down-notification

Syntax no-neighbor-down-notification;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.0.

Description Disable neighbor down notification for OSPF to allow for migration from OSPF to IS-IS without disruption of the RSVP neighbors and associated RSVP-signaled LSPs.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-nssa-abr

Syntax no-nssa-abr;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Disable exporting Type 7 link-state advertisements into not-so-stubby-areas (NSSAs) for an autonomous system boundary router (ASBR) or an area border router (ABR).

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring OSPF Not-So-Stubby Areas on page 41

no-rfc-1583

Syntax no-rfc-1583;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Disable compatibility with RFC 1583, *OSPF Version 2*. If the same external destination is advertised by AS boundary routers that belong to different OSPF areas, disabling compatibility with RFC 1583 can prevent routing loops.

Default Compatibility with RFC 1583 is enabled by default.

Required Privilege Level routing—To view this statement in the configuration.
routing-control-level—To add this statement to the configuration.

Related Documentation

- Example: Disabling OSPFv2 Compatibility with RFC 1583 on page 118

node-link-protection (Protocols OSPF)

Syntax node-link-protection;

Hierarchy Level [edit protocols (ospf | ospf3) protocols area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm ipv4-unicast area *area-id* interface *interface-name*],

Release Information Statement introduced in Junos OS Release 10.0.

Description Enable node-link protection on the specified OSPF interface. Junos OS creates an alternate loop-free path to the primary next hop for all destination routes that traverse a protected interface. This alternate path avoids the primary next-hop router altogether and establishes a path through a different router.

NOTE: This feature is not supported for the OSPF IPv4 multicast topology or for the OSPFv3 IPv4 multicast or IPv6 multicast topologies because node-link protection creates alternate next-hop paths only for unicast routes.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Node-Link Protection for OSPF on page 237
- link-protection on page 412

nssa

Syntax

```
nssa {
  area-range network/mask-length <restrict> <exact> <override-metric metric>;
  default-lsa {
    default-metric metric;
    metric-type type;
    type-7;
  }
  (no-summaries | summaries);
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3) area *area-id*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Configure a not-so-stubby area (NSSA). An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas.

You cannot configure an area as being both a stub area and an NSSA.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Not-So-Stubby Areas on page 41
- stub on page 453

ospf

Syntax ospf { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Enable OSPF routing on the routing device.

You must include the **ospf** statement to enable OSPF on the routing device.

Default OSPF is disabled on the routing device.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Configuration Overview on page 14
- [edit protocols ospf] Hierarchy Level on page 363

ospf3

Syntax

ospf3 { ... }

Hierarchy Level

[edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable OSPFv3 routing on the routing device.

You must include the **ospf3** statement to enable OSPFv3.

Default

OSPFv3 is disabled on the routing device.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Configuration Overview on page 14
- [edit protocols ospf3] Hierarchy Level on page 367

overload (Protocols OSPF)

Syntax

```
overload {
  timeout seconds;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (oospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf topology (default | ipv4-multicast | *name*)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure the local routing device so that it appears to be overloaded. You might do this when you want the routing device to participate in OSPF routing, but do not want it to be used for transit traffic.

NOTE: **Traffic destined to directly attached interfaces continues to reach the routing device.**

Options

timeout ***seconds***—(Optional) Number of seconds at which the overloading is reset. If no timeout interval is specified, the routing device remains in overload state until the **overload** statement is deleted or a timeout is set.

Range: 60 through 1800 seconds

Default: 0 seconds

NOTE: Multitopology Routing does not support the timeout option.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF to Make Routing Devices Appear Overloaded on page 161
- *Example: Configuring Multitopology Routing Based on Applications*
- *Example: Configuring Multitopology Routing Based on a Multicast Source*

passive (Protocols OSPF)

Syntax

```
passive {
  traffic-engineering {
    remote-node-id address;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
traffic-engineering and **remote-node-id *address*** statements introduced in Junos OS Release 8.0.
traffic-engineering and **remote-node-id *address*** statements introduced in Junos OS Release 8.0 for EX Series switches.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Advertise the direct interface addresses on an interface without actually running OSPF on that interface. A passive interface is one for which the address information is advertised as an internal route in OSPF, but on which the protocol does not run.

To configure an interface in OSPF passive traffic engineering mode, include the **traffic-engineering** statement. Configuring OSPF passive traffic engineering mode enables the dynamic discovery of OSPF AS boundary routers.

Enable OSPF on an interface by including the **interface** statement at the **[edit protocols (ospf | ospf3) area *area-id*]** or the **[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]** hierarchy levels. Disable it by including the **disable** statement, To prevent OSPF from running on an interface, include the **passive** statement. These three states are mutually exclusive.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring a Passive OSPF Interface on page 132
- Example: Configuring OSPF Passive Traffic Engineering Mode on page 252
- **disable on page 390**

peer-interface (Protocols OSPF)

Syntax

```
peer-interface interface-name {
  disable;
  dead-interval seconds;
  hello-interval seconds;
  retransmit-interval seconds;
  transit-delay seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id*], [edit protocols ospf area *area-id*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a peer interface.

Options *interface-name*—Name of the peer interface. To configure all interfaces, you can specify **all**.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPFv2 Peer interfaces on page 134
- *Configuring RSVP and OSPF for LMP Peer Interfaces*
- *Configuring a Hierarchy of RSVP LSPs*

poll-interval

Syntax poll-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For nonbroadcast interfaces only, specify how often the router sends hello packets out of the interface before it establishes adjacency with a neighbor.

Options *seconds*—Frequency at which to send hello packets.

Range: 1 through 255 seconds

Default: 120 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Timers Overview on page 201
- Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network on page 125

preference (Protocols OSPF)

Syntax
preference *preference*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Set the route preference for OSPF internal routes.

Options
preference—Preference value.

Range: 0 through 4,294,967,295 (2^{32} – 1)

Default: 10

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Example: Controlling OSPF Route Preferences on page 158
- **external-preference on page 394**

prefix-export-limit (Protocols OSPF)

Syntax

prefix-export-limit *number*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf topology (default | ipv4-multicast | *name*)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure a limit to the number of prefixes exported into OSPF.

Options

number—Prefix limit.

Range: 0 through 4,294,967,295 ($2^{32} – 1$)

Default: None

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Limiting the Number of Prefixes Exported to OSPF on page 147
- *Example: Configuring Multitopology Routing Based on Applications*
- *Example: Configuring Multitopology Routing Based on a Multicast Source*

priority (Protocols OSPF)

Syntax

priority *number*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Specify the routing device's priority for becoming the designated routing device. The routing device that has the highest priority value on the logical IP network or subnet becomes the network's designated router. You must configure at least one routing device on each logical IP network or subnet to be the designated router. You also should specify a routing device's priority for becoming the designated router on point-to-point interfaces.

Options

number—Routing device's priority for becoming the designated router. A priority value of 0 means that the routing device never becomes the designated router. A value of 1 means that the routing device has the least chance of becoming a designated router.

Range: 0 through 255

Default: 128

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Designated Router Overview on page 23
- Example: Controlling OSPF Designated Router Election on page 26

protocols

Syntax

```
protocols {
  bgp {
    ... bgp-configuration ...
  }
  isis {
    ... isis-configuration ...
  }
  ldp {
    ... ldp-configuration ...
  }
  msdp {
    ... msdp-configuration ...
  }
  mstp {
    ... mstp-configuration ...
  }
  ospf {
    domain-id domain-id;
    domain-vpn-tag number;
    route-type-community (iana | vendor);
    ... ospf-configuration ...
  }
  ospf3 {
    domain-id domain-id;
    domain-vpn-tag number;
    route-type-community (iana | vendor);
    ... ospf3-configuration ...
  }
  pim {
    ... pim-configuration ...
  }
  rip {
    ... rip-configuration ...
  }
  ripng {
    ... ripng-configuration ...
  }
  rstp {
    rstp-configuration;
  }
  vstp {
    vstp configuration;
  }
  vpls {
    vpls configuration;
  }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Support for RIPng introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Specify the protocol for a routing instance. You can configure multiple instances of many protocol types. Not all protocols are supported on the switches. See the switch CLI.

Options **bgp**—Specify BGP as the protocol for a routing instance.

isis—Specify IS-IS as the protocol for a routing instance.

ldp—Specify LDP as the protocol for a routing instance.

l2vpn—Specify Layer 2 VPN as the protocol for a routing instance.

msdp—Specify the Multicast Source Discovery Protocol (MSDP) for a routing instance.

mstp—Specify the Multiple Spanning Tree Protocol (MSTP) for a virtual switch routing instance.

ospf—Specify OSPF as the protocol for a routing instance.

ospf3—Specify OSPF version 3 (OSPFv3) as the protocol for a routing instance.

NOTE: **OSPFv3 supports the no-forwarding, virtual-router, and vrf routing instance types only.**

pim—Specify the Protocol Independent Multicast (PIM) protocol for a routing instance.

rip—Specify RIP as the protocol for a routing instance.

ripng—Specify RIP next generation (RIPng) as the protocol for a routing instance.

rstp—Specify the Rapid Spanning Tree Protocol (RSTP) for a virtual switch routing instance.

vstp—Specify the VLAN Spanning Tree Protocol (VSTP) for a virtual switch routing instance.

vpls—Specify VPLS as the protocol for a routing instance.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Multiple Routing Instances of OSPF on page 193

realm

Syntax

```
realm (ipv4-unicast | ipv4-multicast | ipv6-unicast) {
  area area-id {
    interface interface-name;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf3],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3],
[edit protocols ospf3],
[edit routing-instances *routing-instance-name* protocols ospf3]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Configure OSPFv3 to advertise address families other than unicast IPv6. Junos OS maps each address family you configure to a separate realm with its own set of neighbors and link-state database.

Options

ipv4-unicast—Configure a realm for IPv4 unicast routes.

ipv4-multicast—Configure a realm for IPv4 multicast routes.

ipv6-multicast—Configure a realm for IPv6 multicast routes.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Multiple Address Families for OSPFv3 on page 136

reference-bandwidth (Protocols OSPF)

Syntax reference-bandwidth *reference-bandwidth*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Set the reference bandwidth used in calculating the default interface cost. The cost is calculated using the following formula:

cost = ref-bandwidth/bandwidth

Options *reference-bandwidth*—Reference bandwidth, in bits per second.

Range: 9600 through 1,000,000,000,000 bits

Default: 100 Mbps (100,000,000 bits)

NOTE: The default behavior is to use the reference-bandwidth value to calculate the cost of OSPF interfaces. You can override this behavior for any OSPF interface by configuring a specific cost with the **metric** statement.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Controlling the Cost of Individual OSPF Network Segments on page 152
- metric on page 416

retransmit-interval (OSPF)

Syntax retransmit-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Specify how long the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements (LSAs) to an interface's neighbors.

Options ***seconds***—Interval to wait.

Range: 1 through 65,535 seconds

Default: 5 seconds

NOTE: You must configure LSA retransmit intervals to be equal to or greater than 3 seconds to avoid triggering a retransmit trap, because Junos OS delays LSA acknowledgments by up to 2 seconds.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Timers on page 202
- *Configuring RSVP and OSPF for LMP Peer Interfaces*

rib-group (Protocols OSPF)

Syntax

rib-group *group-name*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Install routes learned from OSPF routing instances into routing tables in the OSPF routing table group.

Options

group-name—Name of the routing table group.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Exporting Specific Routes from One Routing Table Into Another Routing Table*
- *Example: Importing Direct and Static Routes Into a Routing Instance*
- *Understanding Multiprotocol BGP*
- *interface-routes*
- *rib-group*

route-type-community

Syntax route-type-community (iana | vendor);

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description Specify an extended community value to encode the OSPF route type. Each extended community is coded as an eight-octet value. This statement sets the most significant bit to either an IANA or vendor-specific route type.

Options **iana**—Encode a route type with the value **0x0306**. This is the default value.

vendor—Encode the route type with the value **0x8000**.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Between PE and CE Routers in Layer 3 VPNs*

routing-instances (Multiple Routing Entities)

Syntax routing-instances *routing-instance-name* { ... }

Hierarchy Level [edit],
[edit logical-systems *logical-system-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an additional routing entity for a router. You can create multiple instances of BGP, IS-IS, OSPF, OSPFv3, and RIP for a router. You can also create multiple routing instances for separating routing tables, routing policies, and interfaces for individual wholesale subscribers (retailers) in a Layer 3 wholesale network.

Each routing instance consist of the following:

- A set of routing tables
- A set of interfaces that belong to these routing tables
- A set of routing option configurations

Each routing instance has a unique name and a corresponding IP unicast table. For example, if you configure a routing instance with the name **my-instance**, its corresponding IP unicast table is my-instance.inet.0. All routes for **my-instance** are installed into my-instance.inet.0.

Routes are installed into the default routing instance inet.0 by default, unless a routing instance is specified.

In Junos OS Release 9.0 and later, you can no longer specify a routing-instance name of *master*, *default*, or *bgp* or include special characters within the name of a routing instance.

In Junos OS Release 9.6 and later, you can include a slash (/) in a routing-instance name only if a logical system is not configured. That is, you cannot include the slash character in a routing-instance name if a logical system other than the default is explicitly configured. Routing-instance names, further, are restricted from having the form **__.*__** (beginning and ending with underscores). The colon **:** character cannot be used when multitopology routing (MTR) is enabled.

Default Routing instances are disabled for the router.

Options *routing-instance-name*—Name of the routing instance. This must be a non-reserved string of not more than 128 characters.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Interprovider Layer 3 VPN Option A*
- *Example: Configuring Interprovider Layer 3 VPN Option B*
- *Example: Configuring Interprovider Layer 3 VPN Option C*
- *Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers*

secondary (Protocols OSPF)

Syntax

secondary;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.2.

Description

Configure an interface to belong to another OSPF area. A logical interface can be configured as primary interface only for one area. For any other area for which you configure the interface, you must configure it as a secondary interface.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- interface on page 404
- Example: Configuring Multiarea Adjacency for OSPF on page 77
- interface on page 404

sham-link

Syntax

```
sham-link {
  local address;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf],
[edit routing-instances *routing-instance-name* protocols ospf]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the local endpoint of a sham link.

You can create an intra-area link or sham link between two provider edge (PE) routing devices so that the VPN backbone is preferred over the back-door link. A back-door link is a backup link that connects customer edge (CE) devices in case the VPN backbone is unavailable. When such a backup link is available and the CE devices are in the same OSPF area, the default behavior is to prefer this backup link over the VPN backbone. This is because the backup link is considered an intra-area link, while the VPN backbone is always considered an inter-area link. Intra-area links are always preferred over inter-area links.

The sham link is an unnumbered point-to-point intra-area link between PE devices. When the VPN backbone has a sham intra-area link, this sham link can be preferred over the backup link if the sham link has a lower OSPF metric than the backup link.

The sham link is advertised using Type 1 link-state advertisements (LSAs). Sham links are valid only for routing instances and OSPFv2.

Each sham link is identified by the combination of a local endpoint address and a remote endpoint address.

Options

local ***address***—The address for the local endpoint of the sham link.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration

Related Documentation

- Example: Configuring OSPFv2 Sham Links on page 268
- **sham-link-remote on page 448**

sham-link-remote

Syntax

```
sham-link-remote address {
  demand-circuit;
  ipsec-sa name;
  metric metric;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]

Release Information Statement introduced before Junos OS Release 7.4.
Support for **ipsec-sa** statement added in Junos OS Release 8.3.

Description Configure the remote endpoint of a sham link.

You can create an intra-area link or sham link between two provider edge (PE) routing devices so that the VPN backbone is preferred over the back-door link. A back-door link is a backup link that connects customer edge (CE) devices in case the VPN backbone is unavailable. When such a backup link is available and the CE devices are in the same OSPF area, the default behavior is to prefer this backup link over the VPN backbone. This is ecause the backup link is considered an intra-area link, while the VPN backbone is always considered an inter-area link. Intra-area links are always preferred over inter-area links.

The sham link is an unnumbered point-to-point intra-area link between PE devices. When the VPN backbone has a sham intra-area link, this sham link can be preferred over the backup link if the sham link has a lower OSPF metric than the backup link.

The sham link is advertised using Type 1 link-state advertisements (LSAs). Sham links are valid only for routing instances and OSPFv2.

Each sham link is identified by the combination of a local endpoint address and a remote endpoint address.

Options ***address***—Address for the remote end point of the sham link.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPFv2 Sham Links on page 268
- sham-link on page 447

shortcuts (Protocols OSPF)

Syntax

```
shortcuts {
  lsp-metric-into-summary;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) traffic-engineering],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) traffic-engineering],
[edit protocols (ospf | ospf3) traffic-engineering],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)traffic-engineering]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4 for EX Series switches.

Description

Configure OSPF to use MPLS label-switched paths (LSPs) as shortcut next hops. By default, shortcut routes calculated through OSPFv2 are installed in the **inet.3** routing table, and shortcut routes calculated through OSPFv3 are installed in the **inet6.3** routing table.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Enabling OSPF Traffic Engineering Support on page 246

simple-password

Syntax

simple-password *key*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit logical-systems *logical-system-name* protocols ospf area *area-id* virtual-link authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link authentication],
[edit protocols ospf area *area-id* interface *interface-name* authentication],
[edit protocols ospf area *area-id* virtual-link authentication],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name* authentication],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link authentication]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure a simple authentication key (password).

Options

key—Password string.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding OSPFv2 Authentication on page 173
- Example: Configuring Simple Authentication for OSPFv2 Exchanges on page 176

spf-options (Protocols OSPF)

Syntax

```
spf-options {
  delay milliseconds;
  holddown milliseconds;
  rapid-runs number;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf topology (default | ipv4-multicast | *name*)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | *name*)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure options for running the shortest-path-first (SPF) algorithm. You can configure the following:

- A delay for when to run the SPF algorithm after a network topology change is detected.
- The maximum number of times the SPF algorithm can run in succession.
- A hold-down interval after the SPF algorithm runs the maximum number of times.

Running the SPF algorithm is usually the beginning of a series of larger system-wide events. For example, the SPF algorithm can lead to interior gateway protocol (IGP) prefix changes, which then lead to BGP nexthop resolution changes. Consider what happens if there are rapid link changes in the network. The local routing device can become overwhelmed. This is why it sometimes makes sense to throttle the scheduling of the SPF algorithm.

Options

delay ***milliseconds***—Time interval between the detection of a topology change and when the SPF algorithm runs.

Range: 50 through 8000 milliseconds

Default: 200 milliseconds

holddown ***milliseconds***—Time interval to hold down, or to wait before a subsequent SPF algorithm runs after the SPF algorithm has run the configured maximum number of times in succession.

Range: 2000 through 20,000 milliseconds

Default: 5000 milliseconds

rapid-runs ***number***—Maximum number of times the SPF algorithm can run in succession. After the maximum is reached, the hold down interval begins.

Range: 1 through 10

Default: 3

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring SPF Algorithm Options for OSPF on page 165
- *Example: Configuring Multitopology Routing Based on Applications*
- *Example: Configuring Multitopology Routing Based on a Multicast Source*

stub

Syntax stub <default-metric *metric*> <(no-summaries | summaries)>;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3) area *area-id*],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Specify that this area not be flooded with AS external link-state advertisements (LSAs). You must include the **stub** statement when configuring all routing devices that are in the stub area.

The backbone cannot be configured as a stub area.

You cannot configure an area to be both a stub area and a not-so-stubby area (NSSA).

Options **no-summaries**—(Optional) Do not advertise routes into the stub area. If you include the **default-metric** option, only the default route is advertised.

summaries—(Optional) Flood summary LSAs into the stub area.

The remaining statement is explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Stub and Totally Stubby Areas on page 37
- **nssa on page 427**

summaries

Syntax

(summaries | no-summaries);

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa],
[edit protocols (ospf | ospf3) area *area-id* nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* nssa],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Configure whether or not area border routers advertise summary routes into an not-so-stubby area (NSSA):

- **summaries**—Flood summary link-state advertisements (LSAs) into the NSSA.
- **no-summaries**—Prevent area border routers from advertising summaries into an NSSA. If **default-metric** is configured for an NSSA, a Type 3 LSA is injected into the area by default.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Not-So-Stubby Areas on page 41
- nssa on page 427
- stub on page 453

te-metric (Protocols OSPF)

Syntax te-metric *metric*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Metric value used by traffic engineering for information injected into the traffic engineering database. The value of the traffic engineering metric does not affect normal OSPF forwarding.

Options *metric*—Metric value.

Range: 1 through 65,535

Default: Value of the IGP metric

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring the Traffic Engineering Metric for a Specific OSPF Interface on page 250

traceoptions (Protocols OSPF)

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure OSPF protocol-level tracing options.

To specify more than one tracing operation, include multiple **flag** statements.

NOTE: **The traceoptions statement is not supported on QFabric systems.**

Default

The default OSPF protocol-level tracing options are those inherited from the routing protocols **traceoptions** statement included at the **[edit routing-options]** hierarchy level.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place OSPF tracing output in the file **ospf-log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 10 files

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

OSPF Tracing Flags

- **database-description**—Database description packets, which are used in synchronizing the OSPF and OSPFv3 topological database.
- **error**—OSPF and OSPFv3 error packets.
- **event**—OSPF and OSPFv3 state transitions.
- **flooding**—Link-state flooding packets.
- **graceful-restart**—Graceful-restart events.
- **hello**—Hello packets, which are used to establish neighbor adjacencies and to determine whether neighbors are reachable.
- **ldp-synchronization**—Synchronization events between OSPF and LDP.
- **lsa-ack**—Link-state acknowledgment packets, which are used in synchronizing the OSPF topological database.
- **lsa-analysis**—Link-state analysis. Specific to the Juniper Networks implementation of OSPF, Junos OS performs LSA analysis before running the shortest-path-first (SPF) algorithm. LSA analysis helps to speed the calculations performed by the SPF algorithm.
- **lsa-request**—Link-state request packets, which are used in synchronizing the OSPF topological database.
- **lsa-update**—Link-state updates packets, which are used in synchronizing the OSPF topological database.
- **nsr-synchronization**—Nonstop routing synchronization events.
- **on-demand**—Trace demand circuit extensions.
- **packet-dump**—Content of selected packet types.
- **packets**—All OSPF packets.
- **restart-signaling**—(OSPFv2 only) Restart-signaling graceful restart events.
- **spf**—Shortest-path-first (SPF) calculations.

Global Tracing Flags

- **all**—All tracing operations.
- **general**—A combination of the **normal** and **route** trace operations.
- **normal**—All normal operations. If you do not specify this option, only unusual or abnormal operations are traced.
- **policy**—Policy operations and actions.
- **route**—Routing table changes.
- **state**—State transitions.
- **task**—Routing protocol task processing.
- **timer**—Routing protocol timer processing.

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Detailed trace information.
- **receive**—Packets being received.
- **send**—Packets being transmitted.

no-world-readable—(Optional) Prevent any user from reading the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.
If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 128 KB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- Example: Tracing OSPF Protocol Traffic on page 356

traffic-engineering (OSPF)

Syntax

```
traffic-engineering {
  <advertise-unnumbered-interfaces>;
  <credibility-protocol-preference>;
  ignore-lsp-metrics;
  multicast-rpf-routes;
  no-topology;
  shortcuts {
    lsp-metric-into-summary;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)]

Release Information

Statement introduced before Junos OS Release 7.4.
multicast-rpf-routes option introduced in Junos OS Release 7.5.
advertise-unnumbered-interfaces option introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4.
Support for OSPFv3 (**ospf3**) introduced in Junos OS Release 9.4 for EX Series switches.
credibility-protocol-preference statement introduced in Junos OS Release 9.4.
credibility-protocol-preference statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable the OSPF traffic engineering features.

Default

Traffic engineering support is disabled.

Options

advertise-unnumbered-interfaces—(Optional) (OSPFv2 only) Include the link-local identifier in the link-local traffic-engineering link-state advertisement. This statement must be included on both ends of an unnumbered link to allow an ingress LER to update the link in its traffic engineering database and use it for CSPF calculations. The link-local identifier is then used by RSVP to signal unnumbered interfaces as defined in RFC 3477.

credibility-protocol-preference—(Optional) (OSPFv2 only) Use the configured preference value for OSPF routes to calculate the traffic engineering database credibility value used to select IGP routes. Use this statement to override the default behavior, in which the traffic engineering database prefers IS-IS routes even if OSPF routes are configured with a lower, that is, preferred, preference value. For example, OSPF routes have a default preference value of 10, whereas IS-IS Level 1 routes have a default preference value of 15. When protocol preference is enabled, the credibility value is determined by deducting the protocol preference value from a base value of 512. Using default protocol preference values, OSPF has a credibility value of 502, whereas IS-IS has a credibility value of 497. Because the traffic engineering database prefers IGP routes with the highest credibility value, OSPF routes are now preferred.

multicast-rpf-routes—(Optional) (OSPFv2 only) Install routes for multicast RPF checks into the **inet.2** routing table. The **inet.2** routing table consists of unicast routes used for multicast RPF lookup. RPF is an antispoofing mechanism used to check whether the packet is coming in on an interface that is also sending data back to the packet source.

NOTE: You must enable OSPF traffic engineering shortcuts to use the **multicast-rpf-routes** statement. You must not allow LSP advertisements into OSPF when configuring the **multicast-rpf-routes** statement.

no-topology—(Optional) (OSPFv2 only) Disable the dissemination of the link-state topology information.

The remaining statements are explained separately.

CAUTION: When the OSPF traffic engineering configuration is considerably modified, the routing table entries are deleted and the routing table is recreated. Changes to configuration that can cause this behavior include enabling or disabling:

- Traffic engineering shortcuts
- IGP shortcuts
- LDP tunneling
- Multiprotocol LSP
- Advertise summary metrics
- Multicast RPF routes

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Enabling OSPF Traffic Engineering Support on page 246

traffic-engineering (Passive TE Mode)

Syntax

traffic-engineering {
  remote-node-id *address*;
}

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name* passive],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name* passive],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name* passive],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name* passive],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name* passive],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name* passive],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name* passive],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name* passive]

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Configure an interface in OSPF passive traffic engineering mode to enable dynamic discovery of OSPF AS boundary routers.

Default

OSPF passive traffic-engineering mode is disabled.

Options

remote-node-id ***address***—The IP address at the far end of the inter-AS link.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Passive Traffic Engineering Mode on page 252
- *Junos OS MPLS Applications Library for Routing Devices*

transit-delay (OSPF)

Syntax

transit-delay *seconds*;

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ospf area *area-id* peer-interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* virtual-link],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* peer-interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)] area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id* virtual-link],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* interface *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Set the estimated time required to transmit a link-state update on the interface. When calculating this time, make sure to account for transmission and propagation delays.

You should never have to modify the transit delay time.

Options

seconds—Estimated time, in seconds.

Range: 1 through 65,535 seconds

Default: 1 second

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Timers on page 202
- *Configuring RSVP and OSPF for LMP Peer Interfaces*

transmit-interval (Protocols OSPF)

Syntax transmit-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit protocols (ospf | ospf3) area *area-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set the interval at which OSPF packets are transmitted on an interface.

Options *milliseconds*—Transmission interval, in milliseconds.

Range: 1 through 4,294,967 milliseconds

Default: 30 milliseconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF Timers on page 202

type-7

Syntax type-7;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3) area *area-id* nssa default-lsa],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area *area-id* nssa default-lsa]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **realm** statement introduced in Junos OS Release 9.2.
Support for the **realm** statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Flood Type 7 default link-state advertisements (LSAs) if the **no-summaries** statement is configured.

By default, when the **no-summaries** statement is configured, a Type 3 LSA is injected into not-so-stubby areas (NSSAs) for Junos OS Release 5.0 and later. To support backward compatibility with earlier Junos OS releases, include the **type-7** statement. This statement enables NSSA ABRs to advertise a Type 7 default LSA into the NSSA if you have also included the **no-summaries** statement in the configuration.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Not-So-Stubby Areas on page 41
- no-summaries on page 454

virtual-link

Syntax

```
virtual-link neighbor-id router-id transit-area area-id {
  disable;
  authentication key <key-id identifier>;
  dead-interval seconds;
  hello-interval seconds;
  ipsec-sa name;
  retransmit-interval seconds;
  transit-delay seconds;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (ospf | ospf3) area *area-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf area *area-id*],
[edit protocols (ospf | ospf3) area *area-id*],
[edit routing-instances *routing-instance-name* protocols ospf area *area-id*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For backbone areas only, create a virtual link to use in place of an actual physical link. All area border routers and other routing devices on the backbone must be contiguous. If this is not possible and there is a break in OSPF connectivity, use virtual links to create connectivity to the OSPF backbone. When configuring virtual links, you must configure links on the two routing devices that form the end points of the link, and both of these routing devices must be area border routers. You cannot configure links through stub areas.

Options

neighbor-id ***router-id***—IP address of the routing device at the remote end of the virtual link.

transit-area ***area-id***—Area identifier of the area through which the virtual link transits. Virtual links are not allowed to transit the backbone area.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- OSPF Areas and Router Functionality Overview on page 9
- Example: Configuring OSPF Virtual Links on page 88

PART 3

Administration

CHAPTER 19

Verifiying OSPF Configuration

Verifying an OSPF Configuration

To verify an OSPF configuration, perform these tasks:

Verifying OSPF-Enabled Interfaces

Purpose Verify that OSPF is running on a particular interface and that the interface is in the desired area.

Action From the CLI, enter the **show ospf interface** command.

Sample Output

```
user@host> show ospf interface
Intf               State    Area            DR ID           BDR ID         Nbrs
at-5/1/0.0         PtToPt   0.0.0.0         0.0.0.0         0.0.0.0           1
ge-2/3/0.0         DR       0.0.0.0         192.168.4.16    192.168.4.15      1
lo0.0              DR       0.0.0.0         192.168.4.16    0.0.0.0           0
so-0/0/0.0         Down     0.0.0.0         0.0.0.0         0.0.0.0           0
so-6/0/1.0         PtToPt   0.0.0.0         0.0.0.0         0.0.0.0           1
so-6/0/2.0         Down     0.0.0.0         0.0.0.0         0.0.0.0           0
so-6/0/3.0         PtToPt   0.0.0.0         0.0.0.0         0.0.0.0           1
```

Meaning The output shows a list of the device interfaces that are configured for OSPF. Verify the following information:

- Each interface on which OSPF is enabled is listed.
- Under **Area**, each interface shows the area for which it was configured.
- Under **Intf** and **State**, the device loopback (**lo0.0**) interface and LAN interface that are linked to the OSPF network's designated router (DR) are identified.
- Under **DR ID**, the IP address of the OSPF network's designated router appears.

- Under **State**, each interface shows a state of **PtToPt** to indicate a point-to-point connection. If the state is **Waiting**, check the output again after several seconds. A state of **Down** indicates a problem.
- The designated router addresses always show a state of **DR**.

Verifying OSPF Neighbors

Purpose OSPF neighbors are interfaces that have an immediate adjacency. On a point-to-point connection between the device and another router running OSPF, verify that each router has a single OSPF neighbor.

Action From the CLI, enter the **show ospf neighbor** command.

Sample Output

```
user@host> show ospf neighbor
 Address          Intf              State      ID              Pri  Dead
192.168.254.225  fxp3.0             2Way      10.250.240.32    128   36
192.168.254.230  fxp3.0             Full      10.250.240.8     128   38
192.168.254.229  fxp3.0             Full      10.250.240.35    128   33
10.1.1.129       fxp2.0             Full      10.250.240.12    128   37
10.1.1.131       fxp2.0             Full      10.250.240.11    128   38
10.1.2.1         fxp1.0             Full      10.250.240.9     128   32
10.1.2.81        fxp0.0             Full      10.250.240.10    128   33
```

Meaning The output shows a list of the device's OSPF neighbors and their addresses, interfaces, states, router IDs, priorities, and number of seconds allowed for inactivity ("dead" time). Verify the following information:

- Each interface that is immediately adjacent to the device is listed.
- The device's own loopback address and the loopback addresses of any routers with which the device has an immediate adjacency are listed.
- Under **State**, each neighbor shows a state of **Full**. Because full OSPF connectivity is established over a series of packet exchanges between clients, the OSPF link might take several seconds to establish. During that time, the state might be displayed as **Attempt**, **Init**, or **2way**, depending on the stage of negotiation.

  If, after 30 seconds, the state is not **Full**, the OSPF configuration between the neighbors is not functioning correctly.

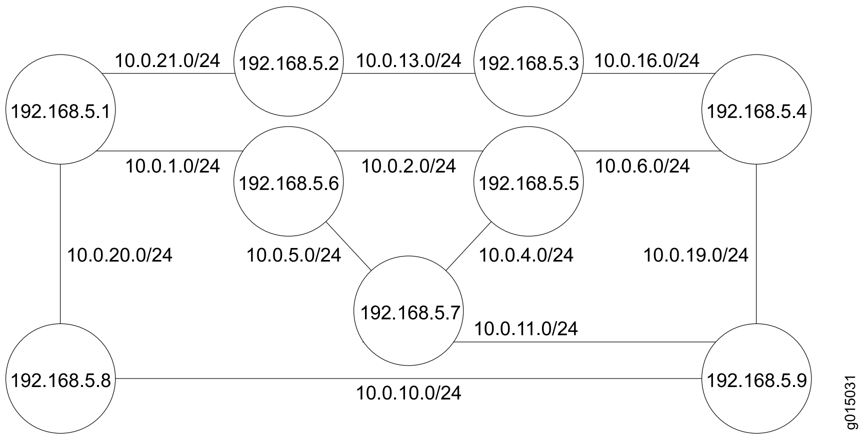
Verifying the Number of OSPF Routes

Purpose Verify that the OSPF routing table has entries for the following:

- Each subnetwork reachable through an OSPF link
- Each loopback address reachable on the network

For example, Figure 30 on page 471 shows a sample network with an OSPF topology.

Figure 30: Sample OSPF Network Topology



In this topology, OSPF is being run on all interfaces. Each segment in the network is identified by an address with a **/24** prefix, with interfaces on either end of the segment being identified by unique IP addresses.

Action From the CLI, enter the **show ospf route** command.

Sample Output

```
user@host> show ospf route
Prefix              Path   Route        NH    Metric   NextHop       Nexthop
                    Type   Type         Type           Interface     addr/label
10.10.10.1/24       Intra  Network      IP    1        ge-0/0/2.0    10.0.21.1
10.10.10.2/24       Intra  Network      IP    1        ge-0/0/2.0    10.0.21.1
10.10.10.4/24       Intra  Network      IP    1        ge-0/0/1.0    10.0.13.1
10.10.10.5/24       Intra  Network      IP    1        ge-0/0/2.0    10.0.21.1
10.10.10.6/24       Intra  Network      IP    1        ge-0/0/1.0    10.0.13.1
10.10.10.10/24      Intra  Network      IP    1        ge-0/0/2.0    10.0.21.1
10.10.10.11/24      Intra  Network      IP    1        ge-0/0/1.0    10.0.13.1
10.10.10.13/24      Intra  Network      IP    1        ge-0/0/1.0
10.10.10.16/24      Intra  Network      IP    1        ge-0/0/1.0    10.0.13.1
10.10.10.19/24      Intra  Network      IP    1        ge-0/0/1.0    10.0.13.1
10.10.10.20/24      Intra  Network      IP    1        ge-0/0/2.0    10.0.21.1
10.10.10.21/24      Intra  Network      IP    1        ge-0/0/2.0
192.168.5.1         Intra  Router       IP    1        ge-0/0/2.0    10.0.21.1
192.168.5.2         Intra  Router       IP    1        lo0
192.168.5.3         Intra  Router       IP    1        ge-0/0/1.0    10.0.13.1
192.168.5.4         Intra  Router       IP    1        ge-0/0/1.0    10.0.13.1
192.168.5.5         Intra  Router       IP    1        ge-0/0/1.0    10.0.13.1
192.168.5.6         Intra  Router       IP    1        ge-0/0/2.0    10.0.21.1
192.168.5.7         Intra  Router       IP    1        ge-0/0/2.0    10.0.21.1
192.168.5.8         Intra  Router       IP    1        ge-0/0/2.0    10.0.21.1
192.168.5.9         Intra  Router       IP    1        ge-0/0/1.0    10.0.13.1
```

Meaning The output lists each route, sorted by IP address. Routes are shown with a route type of **Network**, and loopback addresses are shown with a route type of **Router**.

For the example shown in Figure 30 on page 471, verify that the OSPF routing table has 21 entries, one for each network segment and one for each router's loopback address.

Verifying Reachability of All Hosts in an OSPF Network

Purpose

By using the traceroute tool on each loopback address in the network, verify that all hosts in the network are reachable from each device.

Action

For each device in the OSPF network:

1. In the J-Web interface, select **Troubleshoot>Traceroute**.
2. In the Host Name box, type the name of a host for which you want to verify reachability from the device.
3. Click **Start**. Output appears on a separate page.

Sample Output

```
1 172.17.40.254 (172.17.40.254) 0.362 ms 0.284 ms 0.251 ms
2 routera-fxp0.englab.mycompany.net (192.168.71.246) 0.251 ms 0.235 ms 0.200 ms
```

Meaning

Each numbered row in the output indicates a routing "hop" in the path to the host. The three-time increments indicate the round-trip time (RTT) between the device and the hop, for each traceroute packet. To ensure that the OSPF network is healthy, verify the following information:

- The final hop in the list is the host you want to reach.
- The number of expected hops to the host matches the number of hops in the traceroute output. The appearance of more hops than expected in the output indicates that a network segment is likely not reachable. In this case, verify the routes with the **show ospf route** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- OSPF Configuration Overview on page 14
- *traceroute* in the *Junos OS Operational Mode Commands*

CHAPTER 20

OSPF Operational Commands

clear (ospf | ospf3) database

Syntax

clear (ospf | ospf3) database
<advertising-router (*router-id* | self)>
<area *area-id*>
<asbrsummary>
<external>
<instance *instance-name*>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link-local>
<logical-system (all | *logical-system-name*)>
<lsa-id *lsa-id*>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>

Syntax (EX Series Switch and QFX Series)

clear (ospf | ospf3) database
<advertising-router (*router-id* | self)>
<area *area-id*>
<asbrsummary>
<external>
<instance *instance-name*>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link-local>
<lsa-id *lsa-id*>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<router>

Release Information

Command introduced before Junos OS Release 7.4.
advertising-router ***router-id***, **area** ***area-id***, **asbrsummary**, **external**, **inter-area-prefix**, **inter-area-router**, **intra-area-prefix**, **link-local**, **lsa-id** ***lsa-id***, **netsummary**, **network**, **nssa**, **opaque-area**, and **router** options added in Junos OS Release 8.3. You must use the **purge** command with these options.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option added in Junos OS Release 9.2.
advertising-router (***router-id*** | **self**) option added in Junos OS Release 9.5.
advertising-router (***router-id*** | **self**) option introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description With the master Routing Engine, delete entries in the Open Shortest Path First (OSPF) link-state advertisement (LSA) database. With the backup Routing Engine, delete the OSPF LSA database and sync the new database with the master Routing Engine. You can also use the **purge** command with any of the options to discard rather than delete the specified LSA entries.

> CAUTION: **This command is useful only for testing. Use it with care, because it causes significant network disruption.**

Options **none**—Delete all LSAs other than the system's own LSAs, which are regenerated. To resynchronize the database, the system destroys all adjacent neighbors that are in the state **EXSTART** or higher. The neighbors are then reacquired and the databases are synchronized.

advertising-router (*router-id* | self)—(Optional) Discard entries for the LSA entries advertised by the specified routing device or by this routing device.

area *area-id*—(Optional) Discard entries for the LSAs in the specified area.

asbrsummary—(Optional) Discard summary AS boundary router LSA entries.

external—(Optional) Discard external LSAs.

instance *instance-name*—(Optional) Delete or discard entries for the specified routing instance only.

inter-area-prefix—(OSPFv3 only) (Optional) Discard interarea prefix LSAs.

inter-area-router—(OSPFv3 only) (Optional) Discard interarea router LSAs.

intra-area-prefix—(OSPFv3 only) (Optional) Discard intra-area prefix LSAs.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

link-local—(Optional) Delete link-local LSAs.

lsa-id *lsa-id*—(Optional) Discard the LSA entries with the specified LSA identifier.

netsummary—(Optional) Discard summary network LSAs.

network—(Optional) Discard network LSAs.

nssa—(Optional) Discard not-so-stubby area (NSSA) LSAs.

opaque-area—(Optional) Discard opaque area-scope LSAs.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Delete the entries for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

router—(Optional) Discard router LSAs.

purge—(Optional) Discard all entries in the link-state advertisement database. All link-state advertisements are set to **MAXAGE** and are flooded. The database is repopulated when the originators of the link-state advertisements receive the **MAXAGE** link-state advertisements and reissue them.

Required Privilege Level clear

Related Documentation

- show ospf database on page 497
- show ospf3 database on page 506

List of Sample Output clear ospf database on page 476

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf database

```
user@host> clear ospf database
```


clear (ospf | ospf3) database-protection

Syntax

clear (ospf | ospf3) database-protection
<instance *instance-name*>

Release Information

Command introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear the Open Shortest Path First (OSPF) link-state database from its isolated state. Reset the ignore count, ignore timer, and reset timer, and resume normal operations.

Options

instance ***instance-name***—(Optional) Clear the OSPF link-state database for the specified routing instance only.

Required Privilege Level

clear

Output Fields

This command produces no output.

Sample Output

clear ospf database-protection

```
user@host> clear ospf database-protection
```


clear (ospf | ospf3) io-statistics

Syntax

clear (ospf | osfp3) io-statistics
<logical-system (all | *logical-system-name*)>

Syntax (EX Series Switch and QFX Series)

clear (ospf | osfp3) io-statistics

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear Open Shortest Path First (OSPF) input and output statistics.

Options

none—Clear OSPF input and output statistics.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

clear

List of Sample Output

clear ospf io-statistics on page 478

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf io-statistics

```
user@host> clear ospf io-statistics
```

clear (ospf | ospf3) neighbor

Syntax

clear (ospf | ospf3) neighbor
<area *area-id*>
<instance *instance-name*>
<interface *interface-name*>
<logical-system (all | *logical-system-name*)>
<neighbor>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switch and QFX Series)

clear (ospf | ospf3) neighbor
<area *area-id*>
<instance *instance-name*>
<interface *interface-name*>
<neighbor>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Tear down Open Shortest Path First (OSPF) neighbor connections.

Options

none—Tear down OSPF connections with all neighbors for all routing instances.

area *area-id*—(Optional) Tear down neighbor connections for the specified area only.

instance *instance-name*—(Optional) Tear down neighbor connections for the specified routing instance only.

interface *interface-name*—(Optional) Tear down neighbor connections for the specified interface only.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor—(Optional) Clear the state of the specified neighbor only.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Clear the state of the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

clear

Related Documentation

- show (ospf | ospf3) neighbor on page 529

List of Sample Output

clear ospf neighbor on page 480

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf neighbor

```
user@host> clear ospf neighbor
```

clear (ospf | ospf3) overload

Syntax

clear (ospf | ospf3) overload
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>

Syntax (EX Series Switches)

clear (ospf | ospf3) overload
<instance *instance-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear the Open Shortest Path First (OSPF) overload bit and rebuild link-state advertisements (LSAs).

Options

none—Clear the overload bit and rebuild LSAs for all routing instances.

instance ***instance-name***—(Optional) Clear the overload bit and rebuild LSAs for the specified routing instance only.

logical-system (all | ***logical-system-name*****)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

clear

List of Sample Output

clear ospf overload on page 481

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf overload

```
user@host> clear ospf overload
```

clear (ospf | ospf3) statistics

Syntax

clear (ospf | osfp3) statistics
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switch and QFX Series)

clear (ospf | osfp3) statistics
<instance *instance-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear Open Shortest Path First (OSPF) statistics.

Options

none—Clear OSPF statistics.

instance ***instance-name***—(Optional) Clear statistics for the specified routing instance only.

logical-system (all | ***logical-system-name*****)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Clear statistics for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

clear

Related Documentation

- show (ospf | ospf3) statistics on page 547

List of Sample Output

clear ospf statistics on page 483

Output Fields

See show (ospf | ospf3) statistics for an explanation of output fields.

Sample Output

clear ospf statistics

The following sample output displays OSPF statistics before and after the **clear ospf statistics** command is entered:

```
user@host> show ospf statistics

Packet type             Total                  Last 5 seconds
                   Sent        Received        Sent        Received
   Hello           3254            2268           3               1
     DbD             41              46           0               0
   LSReq              8               7           0               0
LSUpdate            212             154           0               0
   LSAck             65              98           0               0

DBDs retransmitted     :                  3, last 5 seconds :          0
LSAs flooded           :                 12, last 5 seconds :          0
LSAs flooded high-prio :                  0, last 5 seconds :          0
LSAs retransmitted     :                  0, last 5 seconds :          0
LSAs transmitted to nbr:                  3, last 5 seconds :          0
LSAs requested         :                  5, last 5 seconds :          0
LSAs acknowledged      :                 19, last 5 seconds :          0

Flood queue depth      :                0
Total rexmit entries   :                0
db summaries           :                0
lsreq entries          :                0

Receive errors:
  626 subnet mismatches
```

```
user@host> clear ospf statistics
```

```
user@host> show ospf statistics
Packet type             Total                  Last 5 seconds
                   Sent        Received        Sent        Received
   Hello              3               1           3               1
     DbD              0               0           0               0
   LSReq              0               0           0               0
LSUpdate              0               0           0               0
   LSAck              0               0           0               0

DBDs retransmitted     :                  0, last 5 seconds :          0
LSAs flooded           :                  0, last 5 seconds :          0
LSAs flooded high-prio :                  0, last 5 seconds :          0
LSAs retransmitted     :                  0, last 5 seconds :          0
LSAs transmitted to nbr:                  0, last 5 seconds :          0
LSAs requested         :                  0, last 5 seconds :          0
LSAs acknowledged      :                  0, last 5 seconds :          0

Flood queue depth      :                0
Total rexmit entries   :                0
db summaries           :                0
lsreq entries          :                0

Receive errors:
  None
```

show (ospf | ospf3) backup coverage

Syntax

show (ospf | ospf3) backup coverage
<instance *instance-name*>
< logical-system (all | *logical-system-name*)>
<realm (ipv4-unicast | ipv46-unicast>
<topology *topology-name*>

Syntax (QFX Series)

show (ospf | ospf3) backup coverage
<instance *instance-name*>
<topology *topology-name*>

Release Information

Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display information about the level of backup coverage available for all the nodes and prefixes in the network.

Options

none—Display information about the level backup coverage for all OSPF routing instances in all logical systems.

logical-system (all | *logical-system-name*)—(Optional) Display information about the level of backup coverage for all logical systems or for a specific logical system.

instance *instance-name*—(Optional) Display information about the level of backup coverage for a specific OSPF routing instance.

realm (ipv4-unicast | ipv6-unicast)—(Optional) (OSPFv3 only) Display information about the level of backup coverage for the specific OSPFv3 realm, or address family.

topology (default | *topology-name*)—(Optional) (OSPFv2 only) Display information about the level of backup coverage for the specific OSPF topology.

Required Privilege Level

view

Related Documentation

• show (ospf | ospf3) backup lsp on page 487

List of Sample Output

show ospf backup coverage on page 486
show ospf3 backup coverage on page 486

Output Fields

Table 4 on page 484 lists the output fields for the **show (ospf | ospf3) backup coverage** command. Output fields are listed in the approximate order in which they appear.

Table 4: show (ospf | ospf3) backup coverage Output Fields

Field Name	Field Description
Node Coverage	Information about backup coverage for each OSPF node.
Area	Area number. Area **0.0.0.0** is the backbone.

Table 4: show (ospf | ospf3) backup coverage Output Fields *(continued)*

Field Name	Field Description
Covered Nodes	Number of nodes for which backup coverage is available.
Total Nodes	Total number of OSPF nodes.
Route Coverage	Information about backup coverage for each type of OSPF route.
Path Type	Type of OSPF path: **Intra**, **Inter**, **Ext1**, **Ext2**, and **All**.
Covered Routes	For each path type, the number of routes for which backup coverage is available.
Total Routes	For each path type, the total number of configured routes.
Percent Covered	For all nodes and for each path type, the percentage for which backup coverage is available.

Sample Output

show ospf backup coverage

```
user@host> show ospf backup coverage
Topology default coverage:

Node Coverage:

Area              Covered  Total  Percent
                    Nodes  Nodes  Covered
0.0.0.0                 4      5   80.00%

Route Coverage:

Path Type  Covered   Total  Percent
            Routes  Routes  Covered
Intra            8      14   57.14%
Inter            0       0  100.00%
Ext1             0       0  100.00%
Ext2             1       1  100.00%
All              9      15   60.00%
```

show ospf3 backup coverage

```
user @host > show ospf3 backup coverage
show ospf3 backup coverage
Node Coverage:

Area              Covered  Total  Percent
                    Nodes  Nodes  Covered
0.0.0.0                 4      5   80.00%

Route Coverage:

Path Type  Covered   Total  Percent
            Routes  Routes  Covered
Intra            4       6   66.67%
Inter            0       0  100.00%
Ext1             0       0  100.00%
Ext2             1       1  100.00%
All              5       7   71.43%
```

show (ospf | ospf3) backup lsp

Syntax

show (ospf | ospf3) backup lsp
<logical-system (all | *logical-system-name*>
<realm (ipv4-unicast | ipv6-unicast)>

Release Information Command introduced in Junos OS Release 10.0.

Description Display information about MPLS label-switched-paths (LSPs) designated as backup routes for OSPF routes.

NOTE: MPLS LSPs can be used as backup routes only for routes in the default OSPFv2 topology and not for any configured topology. Additionally, MPLS LSPs cannot be used as backup routes for nondefault instances either for OSPFv2 or OSPFv3.

Options **none**—Display information all MPLS LSPs designated as backup routes.

logical-system (all | *logical-system-name*)—(Optional) Display information about MPLS LSPs designated as backup routes for all logical systems or a specific logical system.

realm (ipv4-unicast | ipv6-unicast)—(Optional) (OSPFv3 only) Display information about MPLS LSPs designated as backup routes for a specific realm, or address family.

Required Privilege Level view

Related Documentation

- show (ospf | ospf3) backup coverage on page 484

List of Sample Output

show ospf backup lsp on page 488
show ospf3 backup lsp on page 488

Output Fields Table 5 on page 487 lists the output fields for the **show (ospf | ospf3) backup lsp** command. Output fields are listed in the approximate order in which they appear.

Table 5: show (ospf | ospf3) backup lsp Output Fields

Field Name	Field Description
MPLS LSP name	Name of each MPLS LSP designated as a backup path.
Egress	IP address of the egress router for the LSP.

Table 5: show (ospf | ospf3) backup lsp Output Fields *(continued)*

Field Name	Field Description

Status	State of the LSP:
	• **Up**—The router can detect RSVP hello messages from the neighbor.
	• **Down**—The router has received one of the following indications:
	  ◦ Communication failure from the neighbor.
	  ◦ Communication from IGP that the neighbor is unavailable.
	  ◦ Change in the sequence numbers in the RSVP hello messages sent by the neighbor.
	• **Deleted**—The LSP is no longer available as a backup path.

Last change	Time elapsed since the neighbor state changed either from **up** or **down** or from **down** to **up**. The format is ***hh:mm:ss***.
TE-metric	Configured traffic engineering metric.
Metric	Configured metric.

Sample Output

show ospf backup lsp

```
user@host> show ospf backup lsp
tobanff
  Egress: 10.255.71.239, Status: up, Last change: 00:00:23
  TE-metric: 0, Metric: 0
```

Sample Output

show ospf3 backup lsp

```
user@host> show ospf3 backup lsp
tobanff
  Egress: 10.255.71.239, Status: up, Last change: 00:00:45
  TE-metric: 0, Metric: 0
```

show (ospf | ospf3) backup spf

Syntax

show (ospf | ospf3) backup spf
<brief | detail>
<area *area-id*>
<instance *instance-name*>
<logical-system (all | *logical-system-name*>
<no-coverage>
<*node-id*>
<realm (ipv4–unicast | ipv6–unicast)>
<topology (default | ipv4-multicast | *topology-name*)>

Syntax (QFX Series)

show (ospf | ospf3) backup spf
<brief | detail>
<area *area-id*>
<instance *instance-name*>
<no-coverage>
<*node-id*>
<topology (default | ipv4-multicast | *topology-name*)>

Release Information

Command introduced in JUNOS Release 10.0.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display information about OSPF shortest-path-first calculations for backup paths.

Options

none—Display information about OSPF shortest-path-first (SPF) calculations for all backup paths for all destination nodes.

brief | detail—(Optional) Display the specified level of output.

area *area-id*—(Optional) Display the area information.

instance *instance-name*—(Optional) Display information about the routing instance.

logical-system (all | *logical-system-name*)—(Optional) Display information about all logical systems or a specific logical system.

no-coverage—(Optional) Display information if there is no backup coverage.

node-id—(Optional) Display information about the node specified.

realm (ipv4–unicast | ipv6–unicast)—(Optional) Display information about the **ipv4** or **ipv6** realm.

topology (default | ipv4-multicast | *topology-name*)—(Optional) (OSPFv2 only) Display information about the default topology, IPv4 multicast topology, or a specifc topology.

Required Privilege Level

view

List of Sample Output

show ospf backup spf on page 491
show ospf backup spf detail on page 491
show ospf3 backup spf on page 493

Output Fields Table 6 on page 490 lists the output fields for the **show (ospf |ospf3) backup spf** command. Output fields are listed in the approximate order in which they appear.

Table 6: show (ospf |ospf3) backup spf Output Fields

Field Name	Field Description	Level of Output
Area *area-id* results	Area for which the results are displayed. Area 0.0.0.0 is the backbone area.	All levels
address	Address of the node for which the results are displayed.	All levels
Self to Destination Metric	Metric from the node to the destination.	All levels
Parent Node	Address of the parent node.	All levels
Primary next-hop	Address of the next hop.	All levels
Backup Neighbor	Address of the backup neighbor or LSP endpoint and the following information: • Neighbor to Destination Metric • Neighbor to Self Metric • Self to Neighbor Metric • Status (Eligible, Not Eligible, Not Evaluated) and the reason for the status. NOTE: If the backup neighbor is an LSP endpoint, it is indicated as such after the neighbor address.	All levels

Sample Output

show ospf backup spf

```
user@host> show ospf backup spf
Topology default results:

Area 0.0.0.0 results:

pro16-d-lo0.xxx.yyyy.net
  Self to Destination Metric: 1
  Parent Node: pro16-b-lo0.xxx.yyyy.net
  Primary next-hop: at-1/0/1.0
  Backup Neighbor: pro16-c-lo0.xxx.yyyy.net (LSP endpoint)
    Neighbor to Destination Metric: 4, Neighbor to Self Metric: 3
    Self to Neighbor Metric: 3
    Not eligible, Reason: Path loops
  Backup Neighbor: pro16-d-lo0.xxx.yyyy.net
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  ...
```

show ospf backup spf detail

```
user@host> show ospf backup spf detail
Topology default results:

Area 0.0.0.0 results:

11.14.10.2
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: ae0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.52
  Self to Destination Metric: 1
  Parent Node: 11.14.10.2
  Primary next-hop: ae0.0 via 11.14.10.2
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
```



```
    Not eligible, Reason: Path loops

10.255.71.242
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: as0.0
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.243
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: so-6/0/0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

12.15.0.1
  Self to Destination Metric: 2
  Parent Node: 10.255.71.243
  Primary next-hop: so-6/0/0.0
  Backup next-hop: ae0.0 via 11.14.10.2
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

10.255.71.238
  Self to Destination Metric: 2
  Parent Node: 10.255.71.243
  Primary next-hop: so-6/0/0.0
  Backup next-hop: as0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
```



```
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

10.255.71.239
  Self to Destination Metric: 2
  Parent Node: 12.15.0.1
  Primary next-hop: so-6/0/0.0
  Backup next-hop: ae0.0 via 11.14.10.2
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

14.15.0.2
  Self to Destination Metric: 3
  Parent Node: 10.255.71.239
  Primary next-hop: so-6/0/0.0
  Backup next-hop: ae0.0 via 11.14.10.2
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered
```

show ospf3 backup spf

```
user@host> show ospf3 backup spf
Area 0.0.0.0 results:

10.255.71.52;0.0.0.5
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: ae0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
```

```
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.52
  Self to Destination Metric: 1
  Parent Node: 10.255.71.52;0.0.0.5
  Primary next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.242
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: as0.0
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.243
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: so-6/0/0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.243;0.0.0.2
  Self to Destination Metric: 2
  Parent Node: 10.255.71.243
  Primary next-hop: so-6/0/0.0
```



```
  Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

10.255.71.238
  Self to Destination Metric: 2
  Parent Node: 10.255.71.243
  Primary next-hop: so-6/0/0.0
  Backup next-hop: as0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

10.255.71.239
  Self to Destination Metric: 2
  Parent Node: 10.255.71.243;0.0.0.2
  Primary next-hop: so-6/0/0.0
  Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Eligible, Reason: Contributes backup next-hop
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not evaluated, Reason: Interface is already covered

10.255.71.239;0.0.0.4
  Self to Destination Metric: 3
  Parent Node: 10.255.71.239
  Primary next-hop: so-6/0/0.0
  Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
```



```
  Self to Neighbor Metric: 1
  Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
  Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
  Self to Neighbor Metric: 1
  Not evaluated, Reason: Interface is already covered
```


show ospf database

Syntax

show ospf database
<brief | detail | extensive | summary>
<advertising-router (*address* | self)>
<area *area-id*>
<asbrsummary>
<external>
<instance *instance-name*>
<link-local>
<logical-system (all | *logical-system-name*)>
<lsa-id *lsa-id*>
<netsummary>
<network>
<nssa>
<opaque-area>
<router>

Syntax (EX Series Switches and QFX Series)

show ospf database
<brief | detail | extensive | summary>
<advertising-router (*address* | self)>
<area *area-id*>
<asbrsummary>
<external>
<instance *instance-name*>
<link-local>
<lsa-id *lsa-id*>
<netsummary>
<network>
<nssa>
<opaque-area>
<router>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
advertising-router self (***address*** | **self**) option introduced in Junos OS Release 9.5.
advertising-router self (***address*** | **self**) option introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the entries in the OSPF version 2 (OSPFv2) link-state database, which contains data about link-state advertisement (LSA) packets.

Options

none—Display standard information about entries in the OSPFv2 link-state database for all routing instances.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

advertising-router (*address* | self)—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.

area *area-id*—(Optional) Display the LSAs in a particular area.

asbrsummary—(Optional) Display summary AS boundary router LSA entries.

external—(Optional) Display external LSAs.

instance *instance-name*—(Optional) Display all OSPF database information under the named routing instance.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id *lsa-id*—(Optional) Display the LSA with the specified LSA identifier.

netsummary—(Optional) Display summary network LSAs.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

opaque-area—(Optional) Display opaque area-scope LSAs.

router—(Optional) Display information about router LSAs.

Required Privilege Level

view

Related Documentation

- clear (ospf | ospf3) database on page 474

List of Sample Output

show ospf database on page 501
show ospf database brief on page 501
show ospf database detail on page 501
show ospf database extensive on page 502
show ospf database summary on page 505

Output Fields

Table 7 on page 498 describes the output fields for the **show ospf database** command. Output fields are listed in the approximate order in which they appear.

Table 7: show ospf database Output Fields

Field Name	Field Description	Level of Output
area	Area number. Area **0.0.0.0** is the backbone area.	All levels
Type	Type of link advertisement: **ASBRSum**, **Extern**, **Network**, **NSSA**, **OpaqArea**, **Router**, or **Summary**.	All levels
ID	LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device.	All levels
Adv Rtr	Address of the routing device that sent the advertisement.	All levels
Seq	Link sequence number of the advertisement.	All levels

Table 7: show ospf database Output Fields *(continued)*

Field Name	Field Description	Level of Output
Age	Time elapsed since the LSA was originated, in seconds.	All levels
Opt	Optional OSPF capabilities associated with the LSA.	All levels
Cksum	Checksum value of the LSA.	All levels
Len	Length of the advertisement, in bytes.	All levels
Router	Router link-state advertisement information: • **bits**—Flags describing the routing device that generated the LSP. • **link count**—Number of links in the advertisement. • **id**—ID of a routing device or subnet on the link. • **data**—For stub networks, the subnet mask. Otherwise, the IP address of the routing device that generated the LSP. • **type**—Type of link. It can be **PointToPoint**, **Transit**, **Stub**, or **Virtual**. • **TOS count**—Number of type-of-service (ToS) entries in the advertisement. • **TOS 0 metric**—Metric for ToS 0. • **TOS**—Type-of-service (ToS) value. • **metric**—Metric for the ToS.	**detail extensive**
Network	Network link-state advertisement information: • **mask**—Network mask. • **attached router**—ID of the attached neighbor.	**detail extensive**
Summary	Summary link-state advertisement information: • **mask**—Network mask. • **TOS**—Type-of-service (ToS) value. • **metric**—Metric for the ToS.	**detail extensive**
Gen timer	How long until the LSA is regenerated.	**extensive**
Aging timer	How long until the LSA expires.	**extensive**
Installed *hh:mm:ss* ago	How long ago the route was installed.	**extensive**
expires in *hh:mm:ss*	How long until the route expires.	**extensive**
sent *hh:mm:ss* ago	How long ago the LSA was sent.	**extensive**
Last changed *hh:mm:ss* ago	How long ago the route was changed.	**extensive**
Change count	Number of times the route has changed.	**extensive**

Table 7: show ospf database Output Fields *(continued)*

Field Name	Field Description	Level of Output
Ours	Indicates that this is a local advertisement.	**extensive**
Router LSAs	Number of router link-state advertisements in the link-state database.	**summary**
Network LSAs	Number of network link-state advertisements in the link-state database.	**summary**
Summary LSAs	Number of summary link-state advertisements in the link-state database.	**summary**
NSSA LSAs	Number of not-so-stubby area link-state advertisements in the link-state database.	**summary**

Sample Output

show ospf database

```
user@host> show ospf database
OSPF link state database, Area 0.0.0.1
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.70.103    10.255.70.103    0x80000002  215  0x20 0x4112  48
Router  *10.255.71.242    10.255.71.242    0x80000002  214  0x20 0x11b1  48
Summary *23.1.1.0         10.255.71.242    0x80000002  172  0x20 0x6d72  28
Summary *24.1.1.0         10.255.71.242    0x80000002  177  0x20 0x607e  28
NSSA    *33.1.1.1         10.255.71.242    0x80000002  217  0x28 0x73bd  36

    OSPF link state database, Area 0.0.0.2
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.71.52     10.255.71.52     0x80000004  174  0x20 0xd021  36
Router  *10.255.71.242    10.255.71.242    0x80000003  173  0x20 0xe191  36
Network *23.1.1.1         10.255.71.242    0x80000002  173  0x20 0x9c76  32
Summary *12.1.1.0         10.255.71.242    0x80000001  217  0x20 0xfeec  28
Summary *24.1.1.0         10.255.71.242    0x80000002  177  0x20 0x607e  28
NSSA    *33.1.1.1         10.255.71.242    0x80000001  222  0x28 0xe047  36

    OSPF link state database, Area 0.0.0.3
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.71.238    10.255.71.238    0x80000003  179  0x20 0x3942  36
Router  *10.255.71.242    10.255.71.242    0x80000003  177  0x20 0xf37d  36
Network *24.1.1.1         10.255.71.242    0x80000002  177  0x20 0xc591  32
Summary *12.1.1.0         10.255.71.242    0x80000001  217  0x20 0xfeec  28
Summary *23.1.1.0         10.255.71.242    0x80000002  172  0x20 0x6d72  28
NSSA    *33.1.1.1         10.255.71.242    0x80000001  222  0x28 0xeb3b  36
```

show ospf database brief

The output for the **show ospf database brief** command is identical to that for the **show ospf database** command. For sample output, see show ospf database on page 501.

show ospf database detail

```
user@host> show ospf database detail
    OSPF link state database, Area 0.0.0.1
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.70.103    10.255.70.103    0x80000002  261  0x20 0x4112  48
  bits 0x0, link count 2
  id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)
  TOS count 0, TOS 0 metric 1
  id 12.1.1.0, data 255.255.255.0, Type Stub (3)
  TOS count 0, TOS 0 metric 1
Router  *10.255.71.242    10.255.71.242    0x80000002  260  0x20 0x11b1  48
  bits 0x3, link count 2
  id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
  TOS count 0, TOS 0 metric 1
  id 12.1.1.0, data 255.255.255.0, Type Stub (3)
  TOS count 0, TOS 0 metric 1
Summary *23.1.1.0         10.255.71.242    0x80000002  218  0x20 0x6d72  28
  mask 255.255.255.0
  TOS 0x0, metric 1
Summary *24.1.1.0         10.255.71.242    0x80000002  223  0x20 0x607e  28
  mask 255.255.255.0
  TOS 0x0, metric 1
NSSA    *33.1.1.1         10.255.71.242    0x80000002  263  0x28 0x73bd  36
  mask 255.255.255.255
  Type 2, TOS 0x0, metric 0, fwd addr 12.1.1.2, tag 0.0.0.0

    OSPF link state database, Area 0.0.0.2
```



```
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.71.52     10.255.71.52     0x80000004   220  0x20 0xd021  36
  bits 0x0, link count 1
  id 23.1.1.1, data 23.1.1.2, Type Transit (2)
  TOS count 0, TOS 0 metric 1
Router  *10.255.71.242    10.255.71.242    0x80000003   219  0x20 0xe191  36
  bits 0x3, link count 1
  id 23.1.1.1, data 23.1.1.1, Type Transit (2)
  TOS count 0, TOS 0 metric 1
Network *23.1.1.1         10.255.71.242    0x80000002   219  0x20 0x9c76  32
  mask 255.255.255.0
  attached router 10.255.71.242
  attached router 10.255.71.52
Summary *12.1.1.0         10.255.71.242    0x80000001   263  0x20 0xfeec  28
  mask 255.255.255.0
  TOS 0x0, metric 1
Summary *24.1.1.0         10.255.71.242    0x80000002   223  0x20 0x607e  28
  mask 255.255.255.0
  TOS 0x0, metric 1
NSSA    *33.1.1.1         10.255.71.242    0x80000001   268  0x28 0xe047  36
  mask 255.255.255.255
  Type 2, TOS 0x0, metric 0, fwd addr 23.1.1.1, tag 0.0.0.0

    OSPF link state database, Area 0.0.0.3
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.71.238    10.255.71.238    0x80000003   225  0x20 0x3942  36
  bits 0x0, link count 1
  id 24.1.1.1, data 24.1.1.2, Type Transit (2)
  TOS count 0, TOS 0 metric 1
Router  *10.255.71.242    10.255.71.242    0x80000003   223  0x20 0xf37d  36
  bits 0x3, link count 1
  id 24.1.1.1, data 24.1.1.1, Type Transit (2)
  TOS count 0, TOS 0 metric 1
Network *24.1.1.1         10.255.71.242    0x80000002   223  0x20 0xc591  32
  mask 255.255.255.0
  attached router 10.255.71.242
  attached router 10.255.71.238
Summary *12.1.1.0         10.255.71.242    0x80000001   263  0x20 0xfeec  28
  mask 255.255.255.0
  TOS 0x0, metric 1
Summary *23.1.1.0         10.255.71.242    0x80000002   218  0x20 0x6d72  28
  mask 255.255.255.0
  TOS 0x0, metric 1
NSSA    *33.1.1.1         10.255.71.242    0x80000001   268  0x28 0xeb3b  36
  mask 255.255.255.255
  Type 2, TOS 0x0, metric 0, fwd addr 24.1.1.1, tag 0.0.0.0
```

show ospf database extensive

```
user@host> show ospf database extensive
    OSPF link state database, Area 0.0.0.1
 Type       ID               Adv Rtr          Seq      Age  Opt  Cksum  Len
Router   10.255.70.103    10.255.70.103    0x80000002   286  0x20 0x4112  48
  bits 0x0, link count 2
  id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)
  TOS count 0, TOS 0 metric 1
  id 12.1.1.0, data 255.255.255.0, Type Stub (3)
  TOS count 0, TOS 0 metric 1
  Aging timer 00:55:14
  Installed 00:04:43 ago, expires in 00:55:14
  Last changed 00:04:43 ago, Change count: 2
Router  *10.255.71.242    10.255.71.242    0x80000002   285  0x20 0x11b1  48
  bits 0x3, link count 2
```



```
    id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
    Gen timer 00:45:15
    Aging timer 00:55:15
    Installed 00:04:45 ago, expires in 00:55:15, sent 00:04:43 ago
    Last changed 00:04:45 ago, Change count: 2, Ours
  Summary *23.1.1.0         10.255.71.242    0x80000002   243  0x20 0x6d72  28
    mask 255.255.255.0
    TOS 0x0, metric 1
    Gen timer 00:45:57
    Aging timer 00:55:57
    Installed 00:04:03 ago, expires in 00:55:57, sent 00:04:01 ago
    Last changed 00:04:48 ago, Change count: 1, Ours
  Summary *24.1.1.0         10.255.71.242    0x80000002   248  0x20 0x607e  28
    mask 255.255.255.0
    TOS 0x0, metric 1
    Gen timer 00:45:52
    Aging timer 00:55:52
    Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
    Last changed 00:04:48 ago, Change count: 1, Ours
  NSSA    *33.1.1.1         10.255.71.242    0x80000002   288  0x28 0x73bd  36
    mask 255.255.255.255
    Type 2, TOS 0x0, metric 0, fwd addr 12.1.1.2, tag 0.0.0.0
    Gen timer 00:45:12
    Aging timer 00:55:12
    Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:48 ago
    Last changed 00:04:48 ago, Change count: 2, Ours

      OSPF link state database, Area 0.0.0.2
   Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
  Router   10.255.71.52     10.255.71.52     0x80000004   245  0x20 0xd021  36
    bits 0x0, link count 1
    id 23.1.1.1, data 23.1.1.2, Type Transit (2)
    TOS count 0, TOS 0 metric 1
    Aging timer 00:55:55
    Installed 00:04:02 ago, expires in 00:55:55
    Last changed 00:04:02 ago, Change count: 2
  Router  *10.255.71.242    10.255.71.242    0x80000003   244  0x20 0xe191  36
    bits 0x3, link count 1
    id 23.1.1.1, data 23.1.1.1, Type Transit (2)
    TOS count 0, TOS 0 metric 1
    Gen timer 00:45:56
    Aging timer 00:55:56
    Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago
    Last changed 00:04:04 ago, Change count: 2, Ours
  Network *23.1.1.1         10.255.71.242    0x80000002   244  0x20 0x9c76  32
    mask 255.255.255.0
    attached router 10.255.71.242
    attached router 10.255.71.52
    Gen timer 00:45:56
    Aging timer 00:55:56
    Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago
    Last changed 00:04:04 ago, Change count: 1, Ours
  Summary *12.1.1.0         10.255.71.242    0x80000001   288  0x20 0xfeec  28
    mask 255.255.255.0
    TOS 0x0, metric 1
    Gen timer 00:45:12
    Aging timer 00:55:12
    Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:04 ago
```

```
  Last changed 00:04:48 ago, Change count: 1, Ours
Summary *24.1.1.0        10.255.71.242    0x80000002   248  0x20 0x607e  28
  mask 255.255.255.0
  TOS 0x0, metric 1
  Gen timer 00:45:52
  Aging timer 00:55:52
  Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:04 ago
  Last changed 00:04:48 ago, Change count: 1, Ours
NSSA    *33.1.1.1        10.255.71.242    0x80000001   293  0x28 0xe047  36
  mask 255.255.255.255
  Type 2, TOS 0x0, metric 0, fwd addr 23.1.1.1, tag 0.0.0.0
  Gen timer 00:45:07
  Aging timer 00:55:07
  Installed 00:04:53 ago, expires in 00:55:07, sent 00:04:04 ago
  Last changed 00:04:53 ago, Change count: 1, Ours

    OSPF link state database, Area 0.0.0.3
 Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.71.238    10.255.71.238    0x80000003   250  0x20 0x3942  36
  bits 0x0, link count 1
  id 24.1.1.1, data 24.1.1.2, Type Transit (2)
  TOS count 0, TOS 0 metric 1
  Aging timer 00:55:50
  Installed 00:04:07 ago, expires in 00:55:50
  Last changed 00:04:07 ago, Change count: 2
Router  *10.255.71.242    10.255.71.242    0x80000003   248  0x20 0xf37d  36
  bits 0x3, link count 1
  id 24.1.1.1, data 24.1.1.1, Type Transit (2)
  TOS count 0, TOS 0 metric 1
  Gen timer 00:45:52
  Aging timer 00:55:52
  Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
  Last changed 00:04:08 ago, Change count: 2, Ours
Network *24.1.1.1        10.255.71.242    0x80000002   248  0x20 0xc591  32
  mask 255.255.255.0
  attached router 10.255.71.242
  attached router 10.255.71.238
  Gen timer 00:45:52
  Aging timer 00:55:52
  Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
  Last changed 00:04:08 ago, Change count: 1, Ours
Summary *12.1.1.0        10.255.71.242    0x80000001   288  0x20 0xfeec  28
  mask 255.255.255.0
  TOS 0x0, metric 1
  Gen timer 00:45:12
  Aging timer 00:55:12
  Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:13 ago
  Last changed 00:04:48 ago, Change count: 1, Ours
Summary *23.1.1.0        10.255.71.242    0x80000002   243  0x20 0x6d72  28
  mask 255.255.255.0
  TOS 0x0, metric 1
  Gen timer 00:45:57
  Aging timer 00:55:57
  Installed 00:04:03 ago, expires in 00:55:57, sent 00:04:01 ago
  Last changed 00:04:48 ago, Change count: 1, Ours
NSSA    *33.1.1.1        10.255.71.242    0x80000001   293  0x28 0xeb3b  36
  mask 255.255.255.255
  Type 2, TOS 0x0, metric 0, fwd addr 24.1.1.1, tag 0.0.0.0
  Gen timer 00:45:07
  Aging timer 00:55:07
  Installed 00:04:53 ago, expires in 00:55:07, sent 00:04:13 ago
```



```
  Last changed 00:04:53 ago, Change count: 1, Ours
```

show ospf database summary

```
user@host> show ospf database summary
Area 0.0.0.1:
   2 Router LSAs
   2 Summary LSAs
   1 NSSA LSAs
Area 0.0.0.2:
   2 Router LSAs
   1 Network LSAs
   2 Summary LSAs
   1 NSSA LSAs
Area 0.0.0.3:
   2 Router LSAs
   1 Network LSAs
   2 Summary LSAs
   1 NSSA LSAs
Externals:
Interface fe-2/2/1.0:
Interface ge-0/3/2.0:
Interface so-0/1/2.0:
Interface so-0/1/2.0:
```


show ospf3 database

Syntax

show ospf3 database
<brief | detail | extensive | summary>
<advertising-router (*address* | self)>
<area *area-id*>
<external>
<instance *instance-name*>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link>
<link-local>
<logical-system (all | *logical-system-name*)>
<lsa-id *lsa-id*>
<network>
<nssa>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>

Syntax (EX Series Switches and QFX Series)

show ospf3 database
<brief | detail | extensive | summary>
<advertising-router (*address* | self)>
<area *area-id*>
<external>
<instance *instance-name*>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link>
<link-local>
<lsa-id *lsa-id*>
<network>
<nssa>
<router>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
advertising-router (***address*** | **self**) option introduced in Junos Relase 9.5.
advertising-router (***address*** | **self**) option introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the entries in the OSPF version 3 (OSPFv3) link-state database, which contains data about link-state advertisement (LSA) packets.

Options

none—Display standard information about all entries in the OSPFv3 link-state database.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

advertising-router (*address* | self)—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.

area *area-id*—(Optional) Display the LSAs in a particular area.

external—(Optional) Display external LSAs.

instance *instance-name*—(Optional) Display all OSPF database information under the named routing instance.

inter-area-prefix—(Optional) Display information about interarea-prefix LSAs.

inter-area-router—(Optional) Display information about interarea-router LSAs.

intra-area-prefix—(Optional) Display information about intra-area-prefix LSAs.

link—(Optional) Display information about link LSAs.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id *lsa-id*—(Optional) Display the LSA with the specified LSA identifier.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) Display information about the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family other than IPv6 unicast, which is the default.

router—(Optional) Display information about router LSAs.

Required Privilege Level view

Related Documentation

- clear (ospf | ospf3) database on page 474

List of Sample Output

show ospf3 database brief on page 513
show ospf3 database extensive on page 513
show ospf3 database summary on page 516

Output Fields Table 8 on page 507 lists the output fields for the **show ospf3 database** command. Output fields are listed in the approximate order in which they appear.

Table 8: show ospf3 database Output Fields

Field Name	Field Description	Level of Output
OSPF link state database, area *area-number*	Entries in the link-state database for this area.	**brief detail extensive**
OSPF AS SCOPE link state database	Entries in the AS scope link-state database.	**brief detail extensive**

Table 8: show ospf3 database Output Fields *(continued)*

Field Name	Field Description	Level of Output
OSPF Link-Local link state database, interface ***interface-name***	Entries in the link-local link-state database for this interface.	**brief detail extensive**
area	Area number. Area **0.0.0.0** is the backbone area.	All levels
Type	Type of link advertisement: **Extern**, **InterArPfx**, **InterArRtr**, **IntraArPrx** , **Link**, **Network**, **NSSA**, or **Router**.	**brief detail extensive**
ID	Link identifier included in the advertisement. An asterisk (*) preceding the identifier marks database entries that originated from the local routing device.	**brief detail extensive**
Adv Rtr	Address of the routing device that sent the advertisement.	**brief detail extensive**
Seq	Link sequence number of the advertisement.	**brief detail extensive**
Age	Time elapsed since the LSA was originated, in seconds.	**brief detail extensive**
Cksum	Checksum value of the LSA.	**brief detail extensive**
Len	Length of the advertisement, in bytes.	**brief detail extensive**
Router (Router Link-State Advertisements)		
bits	Flags describing the routing device that generated the LSP.	**detail extensive**
Options	Option bits carried in the router LSA.	**detail extensive**
For Each Router Link		
Type	Type of interface. The value of all other output fields describing a routing device interface depends on the interface's type: • **PointToPoint (1)**—Point-to-point connection to another routing device. • **Transit (2)**—Connection to a transit network. • **Virtual (4)**—Virtual link.	**detail extensive**
Loc-if-id	Local interface ID assigned to the interface that uniquely identifies the interface with the routing device.	**detail extensive**
Nbr-if-id	Interface ID of the neighbor's interface for this routing device link.	**detail extensive**
Nbr-rtr-id	Router ID of the neighbor routing device (for type 2 interfaces, the attached link's designated router).	**detail extensive**
Metric	Cost of the router link.	**detail extensive**
Gen timer	How long until the LSA is regenerated, in the format ***hours:minutes:seconds***.	**extensive**

Table 8: show ospf3 database Output Fields *(continued)*

Field Name	Field Description	Level of Output
Aging timer	How long until the LSA expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Installed *nn*:*nn*:*nn* ago	How long ago the route was installed, in the format ***hours*:*minutes*:*seconds***.	**extensive**
expires in *nn*:*nn*:*nn*	How long until the route expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
sent *nn*:*nn*:*nn* ago	Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Ours	Indicates that this is a local advertisement.	**extensive**
Network (Network Link-State Advertisements)		
Options	Option bits carried in the network LSA.	**detail extensive**
Attached Router	Router IDs of each of the routing devices attached to the link. Only routing devices that are fully adjacent to the designated router are listed. The designated router includes itself in this list.	**detail extensive**
InterArPfx (Interarea-Prefix Link-State Advertisements)		
Prefix	IPv6 address prefix.	**detail extensive**
Prefix-options	Option bit associated with the prefix.	**detail extensive**
Metric	Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.	**detail extensive**
Gen timer	How long until the LSA is regenerated, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Aging timer	How long until the LSA expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Installed *nn*:*nn*:*nn* ago	How long ago the route was installed, in the format ***hours*:*minutes*:*seconds***.	**extensive**
expires in *nn*:*nn*:*nn*	How long until the route expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
sent *nn*:*nn*:*nn* ago	Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Ours	Indicates that this is a local advertisement.	**extensive**
InterArRtr (Interarea-Router Link-State Advertisements)		
Dest-router-id	Router ID of the routing device described by the LSA.	**detail extensive**
options	Optional capabilities supported by the routing device.	**detail extensive**

Table 8: show ospf3 database Output Fields *(continued)*

Field Name	Field Description	Level of Output
Metric	Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.	**detail extensive**
Prefix	IPv6 address prefix.	**extensive**
Prefix-options	Option bit associated with the prefix.	**extensive**
Extern (External Link-State Advertisements)		
Prefix	IPv6 address prefix.	**detail extensive**
Prefix-options	Option bit associated with the prefix.	**detail extensive**
Metric	Cost of the route, which depends on the value of **Type**.	**detail extensive**
Type ***n***	Type of external metric: **Type 1** or **Type 2**.	**detail extensive**
Aging timer	How long until the LSA expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Installed ***nn:nn:nn*** **ago**	How long ago the route was installed, in the format ***hours*:*minutes*:*seconds***.	**extensive**
expires in ***nn:nn:nn***	How long until the route expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**
sent ***nn:nn:nn*** **ago**	Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Link (Link-State Advertisements)		
IPv6-Address	IPv6 link-local address on the link for which this link LSA originated.	**detail extensive**
Options	Option bits carried in the link LSA.	**detail extensive**
priority	Router priority of the interface attaching the originating routing device to the link.	**detail extensive**
Prefix-count	Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.	**detail extensive**
Prefix	IPv6 address prefix.	**detail extensive**
Prefix-options	Option bit associated with the prefix.	**detail extensive**
Gen timer	How long until the LSA is regenerated, in the format ***hours*:*minutes*:*seconds***.	**extensive**
Aging timer	How long until the LSA expires, in the format ***hours*:*minutes*:*seconds***.	**extensive**

Table 8: show ospf3 database Output Fields *(continued)*

Field Name	Field Description	Level of Output
Installed *nn:nn:nn* ago	How long ago the route was installed, in the format ***hours:minutes:seconds***.	**extensive**
expires in *nn:nn:nn*	How long until the route expires, in the format ***hours:minutes:seconds***.	**extensive**
sent *nn:nn:nn* ago	Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format ***hours:minutes:seconds***.	**extensive**
Ours	Indicates that this is a local advertisement.	**extensive**
IntraArPfx (Intra-Area-Prefix Link-State Advertisements)		
Ref-lsa-type	LSA type of the referenced LSA. • **Router**—Address prefixes are associated with a router LSA. • **Network**—Address prefixes are associated with a network LSA.	**detail extensive**
Ref-lsa-id	Link-state ID of the referenced LSA.	**detail extensive**
Ref-router-id	Advertising router ID of the referenced LSA.	**detail extensive**
Prefix-count	Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.	**detail extensive**
Prefix	IPv6 address prefix.	**detail extensive**
Prefix-options	Option bit associated with the prefix.	**detail extensive**
Metric	Cost of this prefix. Expressed in the same units as the interface costs in the router LSAs.	**detail extensive**
Gen timer	How long until the LSA is regenerated, in the format ***hours:minutes:seconds***.	**extensive**
Aging timer	How long until the LSA expires, in the format ***hours:minutes:seconds***.	**extensive**
Installed *hh:mm:ss* ago	How long ago the route was installed, in the format ***hours:minutes:seconds***.	**extensive**
expires in *hh:mm:ss*	How long until the route expires, in the format ***hours:minutes:seconds***.	**extensive**
sent *hh:mm:ss* ago	Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format ***hours:minutes:seconds***.	**extensive**
***n* Router LSAs**	Number of router LSAs in the link-state database.	**summary**
***n* Network LSAs**	Number of network LSAs in the link-state database.	**summary**
***n* InterArPfx LSAs**	Number of interarea-prefix LSAs in the link-state database.	**summary**

Table 8: show ospf3 database Output Fields *(continued)*

Field Name	Field Description	Level of Output
n **InterArRtr LSAs**	Number of interarea-router LSAs in the link-state database.	**summary**
n **IntraArPfx LSAs**	Number of intra-area-prefix LSAs in the link-state database.	**summary**
Externals	Display of the external LSA database.	**summary**
n **Extern LSAs**	Number of external LSAs in the link-state database.	**summary**
Interface *interface-name*	Name of the interface for which link-local LSA information is displayed.	**summary**
n **Link LSAs**	Number of link LSAs in the link-state database.	**summary**

Sample Output

show ospf3 database brief

```
user@host> show ospf3 database brief
    OSPF3 link state database, area 0.0.0.0
 Type        ID               Adv Rtr          Seq         Age  Cksum  Len
Router       0.0.0.1          10.255.4.85      0x80000003   885  0xa697  40
Router      *0.0.0.1          10.255.4.93      0x80000002   953  0xc677  40
InterArPfx *0.0.0.2          10.255.4.93      0x80000001   910  0xb96f  44
InterArRtr *0.0.0.1          10.255.4.93      0x80000001   910  0xe159  32
IntraArPfx *0.0.0.1          10.255.4.93      0x80000002   432  0x788f  72

    OSPF3 link state database, area 0.0.0.1
 Type        ID               Adv Rtr          Seq         Age  Cksum  Len
Router      *0.0.0.1          10.255.4.93      0x80000003   916  0xea40  40
Router       0.0.0.1          10.255.4.97      0x80000006   851  0xc95b  40
Network      0.0.0.2          10.255.4.97      0x80000002   916  0x4598  32
InterArPfx *0.0.0.1          10.255.4.93      0x80000002   117  0xa980  44
InterArPfx *0.0.0.2          10.255.4.93      0x80000002    62  0xd47e  44
NSSA         0.0.0.1          10.255.4.97      0x80000002   362  0x45ee  44
IntraArPfx  0.0.0.1          10.255.4.97      0x80000006   851  0x2f77  52

    OSPF3 AS SCOPE link state database
 Type        ID               Adv Rtr          Seq         Age  Cksum  Len
Extern       0.0.0.1          10.255.4.85      0x80000002    63  0x9b86  44
Extern      *0.0.0.1          10.255.4.93      0x80000001   910  0x59c9  44

    OSPF3 Link-Local link state database, interface ge-1/3/0.0
 Type        ID               Adv Rtr          Seq         Age  Cksum  Len
Link        *0.0.0.2          10.255.4.93      0x80000003   916  0x4dab  64
```

show ospf3 database extensive

```
user@host> show ospf3 database extensive
    OSPF3 link state database, area 0.0.0.0
 Type        ID               Adv Rtr          Seq         Age  Cksum  Len
Router       0.0.0.1          10.255.4.85      0x80000003  1028  0xa697  40
  bits 0x2, Options 0x13
  Type PointToPoint (1), Metric 10
      Loc-If-Id 2, Nbr-If-Id 3, Nbr-Rtr-Id 10.255.4.93
  Aging timer 00:42:51
  Installed 00:17:05 ago, expires in 00:42:52, sent 02:37:54 ago
Router      *0.0.0.1          10.255.4.93      0x80000002  1096  0xc677  40
  bits 0x3, Options 0x13
  Type PointToPoint (1), Metric 10
      Loc-If-Id 3, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.85
  Gen timer 00:00:40
  Aging timer 00:41:44
  Installed 00:18:16 ago, expires in 00:41:44, sent 00:18:14 ago
  Ours
InterArPfx *0.0.0.2          10.255.4.93      0x80000001  1053  0xb96f  44
  Prefix feee::10:10:2:0/126
  Prefix-options 0x0, Metric 10
  Gen timer 00:17:02
  Aging timer 00:42:26
  Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
  Ours
InterArPfx *0.0.0.3          10.255.4.93      0x80000001  1053  0x71d3  44
  Prefix feee::10:255:4:97/128
  Prefix-options 0x0, Metric 10
  Gen timer 00:21:07
  Aging timer 00:42:26
```

```
  Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
  Ours
InterArRtr *0.0.0.1          10.255.4.93      0x80000001  1053  0xe159  32
  Dest-router-id 10.255.4.97, Options 0x19, Metric 10
  Gen timer 00:29:18
  Aging timer 00:42:26
  Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
  Ours
IntraArPfx  0.0.0.1          10.255.4.85      0x80000002  1028  0x2403  72
  Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.85
  Prefix-count 2
  Prefix feee::10:255:4:85/128
    Prefix-options 0x2, Metric 0
  Prefix feee::10:10:1:0/126
    Prefix-options 0x0, Metric 10
  Aging timer 00:42:51
  Installed 00:17:05 ago, expires in 00:42:52, sent 02:37:54 ago
IntraArPfx *0.0.0.1          10.255.4.93      0x80000002   575  0x788f  72
  Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.93
  Prefix-count 2
  Prefix feee::10:255:4:93/128
    Prefix-options 0x2, Metric 0
  Prefix feee::10:10:1:0/126
    Prefix-options 0x0, Metric 10
  Gen timer 00:33:23
  Aging timer 00:50:24
  Installed 00:09:35 ago, expires in 00:50:25, sent 00:09:33 ago
    OSPF3 link state database, area 0.0.0.1
 Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Router     *0.0.0.1          10.255.4.93      0x80000003  1059  0xea40  40
  bits 0x3, Options 0x19
  Type Transit (2), Metric 10
      Loc-If-Id 2, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.97
  Gen timer 00:08:51
  Aging timer 00:42:20
  Installed 00:17:39 ago, expires in 00:42:21, sent 00:17:37 ago
Router      0.0.0.1          10.255.4.97      0x80000006   994  0xc95b  40
  bits 0x2, Options 0x19
  Type Transit (2), Metric 10
      Loc-If-Id 2, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.97
  Aging timer 00:43:25
  Installed 00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago
Network     0.0.0.2          10.255.4.97      0x80000002  1059  0x4598  32
  Options 0x11
  Attached router 10.255.4.97
  Attached router 10.255.4.93
  Aging timer 00:42:20
  Installed 00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago
InterArPfx *0.0.0.1          10.255.4.93      0x80000002   260  0xa980  44
  Prefix feee::10:10:1:0/126
  Prefix-options 0x0, Metric 10
  Gen timer 00:45:39
  Aging timer 00:55:39
  Installed 00:04:20 ago, expires in 00:55:40, sent 00:04:18 ago
  Ours
InterArPfx *0.0.0.2          10.255.4.93      0x80000002   205  0xd47e  44
  Prefix feee::10:255:4:93/128
  Prefix-options 0x0, Metric 0
  Gen timer 00:46:35
  Aging timer 00:56:35
  Installed 00:03:25 ago, expires in 00:56:35, sent 00:03:23 ago
```

```
  Ours
InterArPfx *0.0.0.3         10.255.4.93      0x80000001  1089  0x9bbb  44
  Prefix feee::10:255:4:85/128
  Prefix-options 0x0, Metric 10
  Gen timer 00:04:46
  Aging timer 00:41:51
  Installed 00:18:09 ago, expires in 00:41:51, sent 00:17:43 ago
  Ours
NSSA        0.0.0.1         10.255.4.97      0x80000002   505  0x45ee  44
  Prefix feee::200:200:1:0/124
  Prefix-options 0x8, Metric 10, Type 2,
  Aging timer 00:51:35
  Installed 00:08:22 ago, expires in 00:51:35, sent 02:37:54 ago
IntraArPfx  0.0.0.1         10.255.4.97      0x80000006   994  0x2f77  52
  Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.97
  Prefix-count 1
  Prefix feee::10:255:4:97/128
    Prefix-options 0x2, Metric 0
  Aging timer 00:43:25
  Installed 00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago
IntraArPfx  0.0.0.3         10.255.4.97      0x80000002  1059  0x4446  52
  Ref-lsa-type Network, Ref-lsa-id 0.0.0.2, Ref-router-id 10.255.4.97
  Prefix-count 1
  Prefix feee::10:10:2:0/126
    Prefix-options 0x0, Metric 0
  Aging timer 00:42:20
  Installed 00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago
    OSPF3 AS SCOPE link state database
 Type       ID              Adv Rtr          Seq         Age  Cksum  Len
Extern      0.0.0.1         10.255.4.85      0x80000002   206  0x9b86  44
  Prefix feee::100:100:1:0/124
  Prefix-options 0x0, Metric 20, Type 2,
  Aging timer 00:56:34
  Installed 00:03:23 ago, expires in 00:56:34, sent 02:37:54 ago
Extern     *0.0.0.1         10.255.4.93      0x80000001  1053  0x59c9  44
  Prefix feee::200:200:1:0/124
  Prefix-options 0x0, Metric 10, Type 2,
  Gen timer 00:25:12
  Aging timer 00:42:26
  Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago

    OSPF3 Link-Local link state database, interface ge-1/3/0.0
 Type       ID              Adv Rtr          Seq         Age  Cksum  Len
Link       *0.0.0.2         10.255.4.93      0x80000003  1059  0x4dab  64
  fe80::290:69ff:fe39:1cdb
  Options 0x11, priority 128
  Prefix-count 1
  Prefix feee::10:10:2:0/126 Prefix-options 0x0
  Gen timer 00:12:56
  Aging timer 00:42:20
  Installed 00:17:39 ago, expires in 00:42:21, sent 00:17:37 ago
Link        0.0.0.2         10.255.4.97      0x80000003   205  0xa87d  64
  fe80::290:69ff:fe38:883e
  Options 0x11, priority 128
  Prefix-count 1
  Prefix feee::10:10:2:0/126 Prefix-options 0x0
  Aging timer 00:56:35
  Installed 00:03:22 ago, expires in 00:56:35, sent 02:37:54 ago

    OSPF3 Link-Local link state database, interface so-2/2/0.0
 Type       ID              Adv Rtr          Seq         Age  Cksum  Len
```

```
Link        0.0.0.2         10.255.4.85      0x80000002   506  0x42bb  64
  fe80::280:42ff:fe10:f169
  Options 0x13, priority 128
  Prefix-count 1
  Prefix feee::10:10:1:0/126 Prefix-options 0x0
  Aging timer 00:51:34
  Installed 00:08:23 ago, expires in 00:51:34, sent 02:37:54 ago
Link       *0.0.0.3         10.255.4.93      0x80000002   505  0x6b7a  64
  fe80::280:42ff:fe10:f177
  Options 0x13, priority 128
  Prefix-count 1
  Prefix feee::10:10:1:0/126 Prefix-options 0x0
  Gen timer 00:37:28
  Aging timer 00:51:35
  Installed 00:08:25 ago, expires in 00:51:35, sent 00:08:23 ago
  Ours
```

show ospf3 database summary

```
user@host> show ospf3 database summary
Area 0.0.0.0:
   2 Router LSAs
   1 InterArPfx LSAs
   1 InterArRtr LSAs
   1 IntraArPfx LSAs
Area 0.0.0.1:
   2 Router LSAs
   1 Network LSAs
   2 InterArPfx LSAs
   1 NSSA LSAs
   1 IntraArPfx LSAs
Externals:
   2 Extern LSAs
Interface ge-1/3/0.0:
   1 Link LSAs
Interface lo0.0:
Interface so-2/2/0.0:
   1 Link LSAs
```

show (ospf | ospf3) interface

Syntax

show (ospf | ospf3) interface
<brief | detail | extensive>
<area *area-id*>
<*interface-name*>
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>
<realm (ip4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switches and QFX Series)

show (ospf | ospf3) interface
<brief | detail | extensive>
<area *area-id*>
<*interface-name*>
<instance *instance-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
area option introduced in Junos OS Release 9.2.
area option introduced in Junos OS Release 9.2 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the status of OSPF interfaces.

Options

none—Display standard information about the status of all OSPF interfaces for all routing instances

brief | detail | extensive—(Optional) Display the specified level of output.

area ***area-id***—(Optional) Display information about the interfaces that belong to the specified area.

interface-name—(Optional) Display information for the specified interface.

instance ***instance-name***—(Optional) Display all OSPF interfaces under the named routing instance.

logical-system (all | ***logical-system-name*****)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display information about the interfaces for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

view

List of Sample Output

show ospf interface brief on page 520
show ospf interface detail on page 520
show ospf3 interface detail on page 520

show ospf interface detail(When Multiarea Adjacency Is Configured) on page 520
show ospf interface area area-id on page 521
show ospf interface extensive (When Flooding Reduction Is Enabled) on page 521
show ospf interface extensive (When LDP Synchronization Is Configured) on page 522

Output Fields

Table 9 on page 518 lists the output fields for the **show (ospf | ospf3) interface** command. Output fields are listed in the approximate order in which they appear.

Table 9: show (ospf | ospf3) interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface running OSPF version 2 or OSPF version 3.	All levels
State	State of the interface: **BDR**, **Down**, **DR**, **DRother**, **Loop**, **PtToPt**, or **Waiting**.	All levels
Area	Number of the area that the interface is in.	All levels
DR ID	Address of the area's designated router.	All levels
BDR ID	Backup designated router for a particular subnet.	All levels
Nbrs	Number of neighbors on this interface.	All levels
Type	Type of interface: **LAN**, **NBMA**, **P2MP**, **P2P**, or **Virtual**.	**detail extensive**
Address	IP address of the neighbor.	**detail extensive**
Mask	Netmask of the neighbor.	**detail extensive**
Prefix-length	(OSPFv3) IPv6 prefix length, in bits.	**detail extensive**
OSPF3-Intf-Index	(OSPFv3) OSPF version 3 interface index.	**detail extensive**
MTU	Interface maximum transmission unit (MTU).	**detail extensive**
Cost	Interface cost (metric).	**detail extensive**
DR addr	Address of the designated router.	**detail extensive**
BDR addr	Address of the backup designated router.	**detail extensive**
Adj count	Number of adjacent neighbors.	**detail extensive**
Secondary	Indicates that this interface is configured as a secondary interface for this area. This interface can belong to more than one area, but can be designated as a primary interface for only one area.	**detail extensive**
Flood Reduction	Indicates that this interface is configured with flooding reduction. All self-originated LSAs from this interface are initially sent with the **DoNotAge** bit set. As a result, LSAs are refreshed only when a change occurs.	**extensive**

Table 9: show (ospf | ospf3) interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
Priority	Router priority used in designated router (DR) election on this interface.	**detail extensive**
Flood list	List of link-state advertisements (LSAs) that might be about to flood this interface.	**extensive**
Ack list	Acknowledgment list. List of pending acknowledgments on this interface.	**extensive**
Descriptor list	List of packet descriptors.	**extensive**
Hello	Configured value for the hello timer.	**detail extensive**
Dead	Configured value for the dead timer.	**detail extensive**
Auth type	(OSPFv2) Authentication mechanism for sending and receiving OSPF protocol packets: • **MD5**—The MD5 mechanism is configured in accordance with RFC 2328. • **None**—No authentication method is configured. • **Password**—A simple password (RFC 2328) is configured.	**detail extensive**
Topology	(Multiarea adjacency) Name of topology: **default** or ***name***.	
LDP sync state	(OSPFv2 and LDP synchronization) Current state of LDP synchronization: **in sync**, **in holddown**, and **not supported**.	**extensive**
reason	(OSPFv2 and LDP synchronization) Reason for the current state of LDP synchronization. The LDP session might be up or down, or adjacency might be up or down.	**extensive**
config holdtime	(OSPFv2 and LDP synchronization) Configured value of the hold timer. If the state is not synchronized, and the hold time is not infinity, the **remaining** field displays the number of seconds that remain until the configured hold timer expires.	**extensive**
IPSec SA name	(OSPFv2) Name of the IPSec security association name.	**detail extensive**
Active key ID	(OSPFv2 and MD5) Number from **0** to **255** that uniquely identifies an MD5 key.	**detail extensive**
Start time	(OSPFv2 and MD5) Time at which the routing device starts using an MD5 key to authenticate OSPF packets transmitted on the interface on which this key is configured. To authenticate received OSPF protocol packets, the key becomes effective immediately after the configuration is committed. If the start time option is not configured, the key is effective immediately for send and receive and is displayed as **Start time 1970 Jan 01 00:00:00 PST.**	**detail extensive**
ReXmit	Configured value for the Retransmit timer.	**detail extensive**
Stub, **Not Stub**, or **Stub NSSA**	Type of area.	**detail extensive**

Sample Output

show ospf interface brief

```
user@host> show ospf interface brief
Intf                State    Area            DR ID           BDR ID          Nbrs
at-5/1/0.0          PtToPt   0.0.0.0         0.0.0.0         0.0.0.0            1
ge-2/3/0.0          DR       0.0.0.0         192.168.4.16    192.168.4.15       1
lo0.0               DR       0.0.0.0         192.168.4.16    0.0.0.0            0
so-0/0/0.0          Down     0.0.0.0         0.0.0.0         0.0.0.0            0
so-6/0/1.0          PtToPt   0.0.0.0         0.0.0.0         0.0.0.0            1
so-6/0/2.0          Down     0.0.0.0         0.0.0.0         0.0.0.0            0
so-6/0/3.0          PtToPt   0.0.0.0         0.0.0.0         0.0.0.0            1
```

show ospf interface detail

```
user@host> show ospf interface detail
Interface              State     Area            DR ID           BDR ID Nbrs
fe-0/0/1.0             BDR      0.0.0.0         192.168.37.12   10.255.245.215 1
Type LAN, address 192.168.37.11, Mask 255.255.255.248, MTU 4460, Cost 40
DR addr 192.168.37.12, BDR addr 192.168.37.11, Adj count 1, Priority 128
Hello 10, Dead 40, ReXmit 5, Not Stub
t1-0/2/1.0             PtToPt   0.0.0.0         0.0.0.0         0.0.0.0 0
Type P2P, Address 0.0.0.0, Mask 0.0.0.0, MTU 1500, Cost 2604
  Adj count 0
Hello 10, Dead 40, ReXmit 5, Not Stub
Auth type: MD5, Active key ID 3, Start time 2002 Nov 19 10:00:00 PST
IPsec SA Name: sa
```

show ospf3 interface detail

```
user@host> show ospf3 interface so-0/0/3.0 detail
Interface              State     Area           DR-ID          BDR-ID      Nbrs
so-0/0/3.0             PtToPt   0.0.0.0        0.0.0.0        0.0.0.0        1
Address fe80::2a0:a5ff:fe28:1dfc, Prefix-length 64
OSPF3-Intf-index 1, Type P2P, MTU 4470, Cost 12, Adj-count 1
Hello 10, Dead 40, ReXmit 5, Not Stub
```

show ospf interface detail (When Multiarea Adjacency Is Configured)

```
user@host> show ospf interface detail
regress@router> show ospf interface detail
Interface           State   Area            DR ID           BDR ID          Nbrs
lo0.0               DR      0.0.0.0         10.255.245.2    0.0.0.0            0

  Type: LAN, Address: 127.0.0.1, Mask: 255.255.255.255, MTU: 65535, Cost: 0
  DR addr: 127.0.0.1, Adj count: 0, Priority: 128
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 0
lo0.0               DR      0.0.0.0         10.255.245.2    0.0.0.0            0

  Type: LAN, Address: 10.255.245.2, Mask: 255.255.255.255, MTU: 65535, Cost: 0
  DR addr: 10.255.245.2, Adj count: 0, Priority: 128
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 0
so-0/0/0.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
so-0/0/0.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            0
```



```
  Type: P2P, Address: 192.168.37.46, Mask: 255.255.255.254, MTU: 4470, Cost: 1
  Adj count: 0, , Passive
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Passive, Cost: 1
so-1/0/0.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
so-1/0/0.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            0

  Type: P2P, Address: 192.168.37.54, Mask: 255.255.255.254, MTU: 4470, Cost: 1
  Adj count: 0, , Passive
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Passive, Cost: 1
so-0/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1, Secondary
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
so-1/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1, Secondary
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
so-0/0/0.0          PtToPt  2.2.2.2         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1, Secondary
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
so-1/0/0.0          PtToPt  2.2.2.2         0.0.0.0         0.0.0.0            1

  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
  Adj count: 1, Secondary
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
```

show ospf interface area area-id

```
user@host> show ospf interface area 1.1.1.1
Interface           State   Area            DR ID           BDR ID          Nbrs
so-0/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1
so-1/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1
```

show ospf interface extensive (When Flooding Reduction Is Enabled)

```
user@host> show ospf interface extensive
Interface           State   Area            DR ID           BDR ID          Nbrs
fe-0/0/0.0          PtToPt  0.0.0.0         0.0.0.0         0.0.0.0            0

  Type: P2P, Address: 10.10.10.1, Mask: 255.255.255.0, MTU: 1500, Cost: 1
  Adj count: 0
```



```
  Secondary, Flood Reduction
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Topology default (ID 0) -> Cost: 1
```

show ospf interface extensive (When LDP Synchronization Is Configured)

```
user@host> show ospf interface extensive
Interface               State     Area            DR ID           BDR ID
Nbrs
so-1/0/3.0              Down     0.0.0.0         0.0.0.0         0.0.0.0
0
  Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 65535
  Adj count: 0
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  LDP sync state: in holddown, for: 00:00:08, reason: LDP down during config
           config holdtime: 10 seconds, remaining: 1
```


show (ospf | ospf3) io-statistics

Syntax

show (ospf | ospf3) io-statistics
<logical-system (all | *logical-system-name*)>

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) io-statistics

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display Open Shortest Path First (OSPF) input and output statistics.

Options

none—Display OSPF input and output statistics.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

Related Documentation

- clear (ospf | ospf3) statistics on page 482

List of Sample Output

show ospf io-statistics on page 524

Output Fields

Table 10 on page 523 lists the output fields for the **show ospf io-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 10: show (ospf | ospf3) io-statistics Output Fields

Field Name	Field Description
Packets read	Number of OSPF packets read since the last time the routing protocol was started.
average per run	Total number of packets divided by the total number of times the OSPF read operation is scheduled to run.
max run	Maximum number of packets for a given run among all scheduled runs.
Receive errors	Number of faulty packets received with errors.

Sample Output

show ospf io-statistics

user@host> **show ospf io-statistics**

```
Packets read: 7361, average per run: 1.00, max run: 1
Receive errors:
  None
```

show (ospf | ospf3) log

Syntax

show (ospf | osfp3) log
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<topology *topology-name*>

Syntax (EX Series Switch and QFX Series)

show (ospf | osfp3) log
<instance *instance-name*>
<topology *topology-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
topology option introduced in Junos OS Release 9.0.
topology option introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the entries in the Open Shortest Path First (OSPF) log of SPF calculations.

Options

none—Display entries in the OSPF log of SPF calculations for all routing instances.

instance ***instance-name***—(Optional) Display entries for the specified routing instance.

logical-system (all | ***logical-system-name*****)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

topology ***topology-name***—(Optional) (OSPFv2 only) Display entries for the specified topology.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display entries for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

view

List of Sample Output

show ospf log on page 527
show ospf log topology voice on page 527

Output Fields

Table 11 on page 525 lists the output fields for the **show (ospf | ospf3) log** command. Output fields are listed in the approximate order in which they appear.

Table 11: show (ospf | ospf3) log Output Fields

Field Name	Field Description
When	Time, in weeks (**w**) and days (**d**), since the SPF calculation was made.

Table 11: show (ospf | ospf3) log Output Fields *(continued)*

Field Name	Field Description
Type	Type of calculation: **Cleanup**, **External**, **Interarea**, **NSSA**, **Redist**, **SPF**, **Stub**, **Total**, or **Virtuallink**.
Elapsed	Amount of time, in seconds, that elapsed during the operation, or the time required to complete the SPF calculation. The start time is the time displayed in the **When** field.

Sample Output

show ospf log

```
user@host> show ospf log
When                Type            Elapsed

1w4d 17:25:58    Stub            0.000017
1w4d 17:25:58    SPF             0.000070
1w4d 17:25:58    Stub            0.000019
1w4d 17:25:58    Interarea       0.000054
1w4d 17:25:58    External        0.000005
1w4d 17:25:58    Cleanup         0.000203
1w4d 17:25:58      Total         0.000537
1w4d 17:24:48    SPF             0.000125
1w4d 17:24:48    Stub            0.000017
1w4d 17:24:48    SPF             0.000100
1w4d 17:24:48    Stub            0.000016
1w4d 17:24:48    Interarea       0.000056
1w4d 17:24:48    External        0.000005
1w4d 17:24:48    Cleanup         0.000238
1w4d 17:24:48      Total         0.000600
...
```

show ospf log topology voice

```
user@host> show ospf log topology voice
Topology voice SPF log:

   Last instance of each event type
When                Type            Elapsed
00:06:11        SPF             0.000116
00:06:11        Stub            0.000114
00:06:11        Interarea       0.000126
00:06:11        External        0.000067
00:06:11        NSSA            0.000037
00:06:11        Cleanup         0.000186

   Maximum length of each event type
When                Type            Elapsed
00:13:43        SPF             0.000140
00:13:33        Stub            0.000116
00:13:43        Interarea       0.000128
00:13:33        External        0.000075
00:13:38        NSSA            0.000039
00:13:53        Cleanup         0.000657

   Last 100 events
When                Type            Elapsed

00:13:53        SPF             0.000090
00:13:53        Stub            0.000041
00:13:53        Interarea       0.000123
00:13:53        External        0.000040
00:13:53        NSSA            0.000038
00:13:53        Cleanup         0.000657
00:13:53          Total         0.001252
.
.
00:06:11        SPF             0.000116
00:06:11        Stub            0.000114
00:06:11        Interarea       0.000126
00:06:11        External        0.000067
```

```
00:06:11        NSSA            0.000037
00:06:11        Cleanup         0.000186
00:06:11          Total         0.000818
```

show (ospf | ospf3) neighbor

Syntax

show (ospf | ospf3) neighbor
<brief | detail | extensive>
<area *area-id*>
<instance (all | *instance-name*)>
<interface *interface-name*>
<logical-system (all | *logical-system-name*)>
<*neighbor*>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switches and QFX Series)

show (ospf | ospf3) neighbor
<brief | detail | extensive>
<area *area-id*>
<instance (all | *instance-name*)>
<interface *interface-name*>
<*neighbor*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
instance all option introduced in Junos OS Release 9.1.
instance all option introduced in Junos OS Release 9.1 for EX Series switches.
area, **interface**, and **realm** options introduced in Junos OS Release 9.2.
area and **interface** options introduced in Junos OS Release 9.2 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display information about OSPF neighbors.

CPU utilization might increase while the device learns its OSPF neighbors. We recommend that you use the **show (ospf | ospf3) neighbor** command after the device learns and establishes OSPF neighbor adjacencies. Depending on the size of your network, this might take several minutes. If you receive a “timeout communicating with routing daemon” error when using the **show (ospf | ospf3) neighbor** command, wait several minutes before attempting to use the command again. This is not a critical system error, but you might experience a delay in using the CLI.

Options

none—Display standard information about all OSPF neighbors for all routing instances.

brief | detail | extensive—(Optional) Display the specified level of output.

area *area-id*—(Optional) Display information about the OSPF neighbors for the specified area.

instance (all | *instance-name*)—(Optional) Display all OSPF interfaces for all routing instances or under the named routing instance.

interface *interface-name*—(Optional) Display information about OSPF neighbors for the specified logical interface.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor—(Optional) Display information about the specified OSPF neighbor.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display information about the OSPF neighbors for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level view

Related Documentation

- clear (ospf | ospf3) neighbor on page 479

List of Sample Output

show ospf neighbor brief on page 533
show ospf neighbor detail on page 533
show ospf neighbor extensive on page 533
show ospf3 neighbor detail on page 534
show ospf neighbor area area-id on page 534
show ospf neighbor interface interface-name on page 534
show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled) on page 535

Output Fields Table 12 on page 530 lists the output fields for the **show (ospf | ospf3) neighbor** command. Output fields are listed in the approximate order in which they appear.

Table 12: show (ospf | ospf3) neighbor Output Fields

Field Name	Field Description	Level of Output
Address	Address of the neighbor.	All levels
Interface	Interface through which the neighbor is reachable.	All levels

Table 12: show (ospf | ospf3) neighbor Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	State of the neighbor: • **Attempt**—Valid only for neighbors attached to nonbroadcast networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort must be made to contact the neighbor. • **Down**—Initial state of a neighbor conversation. It indicates that no recent information has been received from the neighbor. Hello packets might continue to be sent to neighbors in the **Down** state, although at a reduced frequency. • **Exchange**—Routing device is describing its entire link-state database by sending database description packets to the neighbor. Each packet has a sequence number and is explicitly acknowledged. • **ExStart**—First step in creating an adjacency between the two neighboring routing devices. The goal of this step is to determine which routing device is the master, and to determine the initial sequence number. • **Full**—Neighboring routing devices are fully adjacent. These adjacencies appear in router link and network link advertisements. • **Init**—A hello packet has recently been sent by the neighbor. However, bidirectional communication has not yet been established with the neighbor. This state might occur, for example, because the routing device itself did not appear in the neighbor's hello packet. • **Loading**—Link-state request packets are sent to the neighbor to acquire more recent advertisements that have been discovered (but not yet received) in the **Exchange** state. • **2Way**—Communication between the two routing devices is bidirectional. This state has been ensured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (backup) designated router is selected from the set of neighbors in state **2Way** or greater.	All levels
ID	Router ID of the neighbor.	All levels
Pri	Priority of the neighbor to become the designated router.	All levels
Dead	Number of seconds until the neighbor becomes unreachable.	All levels
Link state acknowledgment list	Number of link-state acknowledgments received.	**extensive**
Link state retransmission list	Total number of link-state advertisements retransmitted. For **extensive** output only, the following information is also displayed: • **Type**—Type of link advertisement: **ASBR**, **Sum**, **Extern**, **Network**, **NSSA**, **OpaqArea**, **Router**, or **Summary**. • **LSA ID**—LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device. • **Adv rtr**—Address of the routing device that sent the advertisement. • **Seq**—Link sequence number of the advertisement.	**detail extensive**

Table 12: show (ospf | ospf3) neighbor Output Fields *(continued)*

Field Name	Field Description	Level of Output
Neighbor-address	(OSPFv3 only) If the neighbor uses virtual links, the **Neighbor-address** is the site-local, local, or global address. If the neighbor uses a physical interface, the **Neighbor-address** is an IPv6 link-local address.	**detail extensive**
area	Area that the neighbor is in.	**detail extensive**
OSPF3-Intf-Index	(OSPFv3 only) Displays the OSPFv3 interface index.	**detail extensive**
opt	Option bits received in the hello packets from the neighbor.	**detail extensive**
DR or **DR-ID**	Address of the designated router.	**detail extensive**
BDR or **BDR-ID**	Address of the backup designated router.	**detail extensive**
Up	Length of time since the neighbor came up.	**detail extensive**
adjacent	Length of time since the adjacency with the neighbor was established.	**detail extensive**

Sample Output

show ospf neighbor brief

```
user@host> show ospf neighbor brief
  Address          Intf              State     ID              Pri  Dead
192.168.254.225  fxp3.0            2Way      10.250.240.32   128   36
192.168.254.230  fxp3.0            Full      10.250.240.8    128   38
192.168.254.229  fxp3.0            Full      10.250.240.35   128   33
10.1.1.129       fxp2.0            Full      10.250.240.12   128   37
10.1.1.131       fxp2.0            Full      10.250.240.11   128   38
10.1.2.1         fxp1.0            Full      10.250.240.9    128   32
10.1.2.81        fxp0.0            Full      10.250.240.10   128   33
```

show ospf neighbor detail

```
user@host> show ospf neighbor detail
  Address          Interface             State     ID              Pri  Dead
10.5.1.2         ge-1/2/0.1            Full      10.5.1.2        128   37
  area 0.0.0.1, opt 0x42, DR 10.5.1.2, BDR 10.5.1.1
  Up 06:09:28, adjacent 05:17:36
    Link state acknowledgment list:  3 entries

    Link state retransmission list:  9 entries

10.5.10.2        ge-1/2/0.10           ExStart   10.5.1.38       128   34
  area 0.0.0.1, opt 0x42, DR 10.5.10.2, BDR 10.5.10.1
  Up 06:09:28
    master, seq 0xac1530f8, rexmit DBD in 3 sec
    rexmit LSREQ in 0 sec
10.5.11.2        ge-1/2/0.11           Full      10.5.1.42       128   38
  area 0.0.0.1, opt 0x42, DR 10.5.11.2, BDR 10.5.11.1
  Up 06:09:28, adjacent 05:26:46
    Link state retransmission list:  1 entries

10.5.12.2        ge-1/2/0.12           ExStart   10.5.1.46       128   33
  area 0.0.0.1, opt 0x42, DR 10.5.12.2, BDR 10.5.12.1
  Up 06:09:28
    master, seq 0xac188a68, rexmit DBD in 2 sec
    rexmit LSREQ in 0 sec
```

show ospf neighbor extensive

```
user@host> show ospf neighbor extensive
  Address          Interface             State     ID              Pri  Dead
10.5.1.2         ge-1/2/0.1            Full      10.5.1.2        128   33
  area 0.0.0.1, opt 0x42, DR 10.5.1.2, BDR 10.5.1.1
  Up 06:09:42, adjacent 05:17:50
    Link state retransmission list:

      Type       LSA ID           Adv rtr          Seq

     Summary   10.8.56.0        172.25.27.82     0x8000004d

     Router    10.5.1.94        10.5.1.94        0x8000005c

     Network   10.5.24.2        10.5.1.94        0x80000036

     Summary   10.8.57.0        172.25.27.82     0x80000024

     Extern    1.10.90.0        10.8.1.2         0x80000041

     Extern    1.4.109.0        10.6.1.2         0x80000041
```

```
     Router   10.5.1.190       10.5.1.190       0x8000005f

     Network  10.5.48.2        10.5.1.190       0x8000003d

     Summary  10.8.58.0        172.25.27.82     0x8000004d

     Extern   1.10.91.0        10.8.1.2         0x80000041

     Extern   1.4.110.0        10.6.1.2         0x80000041

     Router   10.5.1.18        10.5.1.18        0x8000005f

     Network  10.5.5.2         10.5.1.18        0x80000033

     Summary  10.8.59.0        172.25.27.82     0x8000003a

     Summary  10.8.62.0        172.25.27.82     0x80000025

10.5.10.2        ge-1/2/0.10           ExStart   10.5.1.38        128   38
  area 0.0.0.1, opt 0x42, DR 10.5.10.2, BDR 10.5.10.1
  Up 06:09:42
    master, seq 0xac1530f8, rexmit DBD in 2 sec
    rexmit LSREQ in 0 sec
10.5.11.2        ge-1/2/0.11           Full      10.5.1.42        128   33
  area 0.0.0.1, opt 0x42, DR 10.5.11.2, BDR 10.5.11.1
  Up 06:09:42, adjacent 05:27:00
    Link state retransmission list:

      Type      LSA ID           Adv rtr          Seq

     Summary  10.8.58.0        172.25.27.82     0x8000004d

     Extern   1.10.91.0        10.8.1.2         0x80000041

     Extern   1.1.247.0        10.5.1.2         0x8000003f

     Extern   1.4.110.0        10.6.1.2         0x80000041

     Router   10.5.1.18        10.5.1.18        0x8000005f

     Network  10.5.5.2         10.5.1.18        0x80000033

     Summary  10.8.59.0        172.25.27.82     0x8000003a
```

show ospf3 neighbor detail

```
user@host> show ospf3 neighbor detail
ID               Interface             State     Pri   Dead
10.255.71.13     fe-0/0/2.0            Full      128   30
  Neighbor-address fe80::290:69ff:fe9b:e002
  area 0.0.0.0, opt 0x13, OSPF3-Intf-Index 2
  DR-ID 10.255.71.13, BDR-ID 10.255.71.12
  Up 02:51:43, adjacent 02:51:43
```

show ospf neighbor area area-id

```
user@host >show ospf neighbor area 1.1.1.1
Address          Interface             State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0            Full      10.255.245.4     128    33
  Area 1.1.1.1
192.168.37.55    so-1/0/0.0            Full      10.255.245.5     128    37
  Area 1.1.1.1
```


show ospf neighbor interface interface-name

```
user@host >show ospf neighbor interface so-0/0/0.0
Address          Interface              State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    37
  Area 0.0.0.0
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    33
  Area 1.1.1.1
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    32
  Area 2.2.2.2
```

show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled)

```
user @host > show ospf3 neighbor instance all
Instance: ina
    Realm: ipv6-unicast
    ID               Interface              State     Pri   Dead
   100.1.1.1        fe-0/0/2.0             Full      128     37
       Neighbor-address fe80::217:cb00:c87c:8c03
   Instance: inb
   Realm: ipv4-unicast
   ID               Interface              State     Pri   Dead
  100.1.2.1        fe-0/0/2.1             Full      128     33
      Neighbor-address fe80::217:cb00:c97c:8c03
```

show (ospf | ospf3) overview

Syntax

show (ospf | ospf3) overview
<brief | extensive>
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) overview
<brief | extensive>
<instance *instance-name*>

Release Information

Command introduced in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Database protection introduced in Junos 10.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display Open Shortest Path First (OSPF) overview information.

Options

none—Display standard information about all OSPF neighbors for all routing instances.

brief | extensive—(Optional) Display the specified level of output.

instance *instance-name*—(Optional) Display all OSPF interfaces under the named routing instance.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Display information about the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

view

List of Sample Output

show ospf overview on page 539
show ospf overview (With Database Protection) on page 539
show ospf3 overview (With Database Protection) on page 539
show ospf overview extensive on page 540

Output Fields

Table 13 on page 536 lists the output fields for the **show ospf overview** command. Output fields are listed in the approximate order in which they appear.

Table 13: show ospf overview Output Fields

Field name	Field Description	Level of Output
Instance	OSPF routing instance.	All levels

Table 13: show ospf overview Output Fields *(continued)*

Field name	Field Description	Level of Output
Router ID	Router ID of the routing device.	All levels
Route table index	Route table index.	All levels
Configured overload	Overload capability is enabled. If the overload timer is also configured, display the time that remains before it is set to expire. This field is not displayed after the timer expires.	All levels
Toplogy	Topology identifier.	All levels
Prefix export count	Number of prefixes exported into OSPF.	All levels
Full SPF runs	Number of complete Shortest Path First calculations.	All levels
SPF delay	Delay before performing consecutive Shortest Path First calculations.	All levels
SPF holddown	Delay before performing additional Shortest Path First (SPF) calculations after the maximum number of consecutive SPF calculations is reached.	All levels
SPF rapid runs	Maximum number of Shortest Path First calculations that can be performed in succession before the hold-down timer begins.	All levels
LSA refresh time	Refresh period for link-state advertisement (in minutes).	All levels
Database protection state	Current state of database protection.	All levels
Warning threshold	Threshold at which a warning message is logged (percentage of maximum LSA count).	All levels
Non self-generated LSAs	Number of LSAs whose router ID is not equal to the local router ID: **Current**, **Warning** (threshold), and **Allowed**.	All levels
Ignore time	How long the database has been in the ignore state.	All levels
Reset time	How long the database must stay out of the ignore or isolated state before it returns to normal operations.	All levels
Ignore count	Number of times the database has been in the ignore state: **Current** and **Allowed**.	All levels
Restart	Graceful restart capability: **enabled** or **disabled**.	All levels
Restart duration	Time period for complete reacquisition of OSPF neighbors.	All levels
Restart grace period	Time period for which the neighbors should consider the restarting routing device as part of the topology.	All levels

Table 13: show ospf overview Output Fields *(continued)*

Field name	Field Description	Level of Output
Graceful restart helper mode	(OSPFv2) Standard graceful restart helper capability (based on RFC 3623): **enabled** or **disabled**.	All levels
Restart-signaling helper mode	(OSPFv2) Restart signaling-based graceful restart helper capability (based on RFC 4811, RFC 4812, and RFC 4813): **enabled** or **disabled**.	All levels
Helper mode	(OSPFv3) Graceful restart helper capability: **enabled** or **disabled**.	All levels
Trace options	OSPF-specific trace options.	**extensive**
Trace file	Name of the file to receive the output of the tracing operation.	**extensive**
Area	Area number. Area 0.0.0.0 is the backbone area.	All levels
Stub type	Stub type of area: **Normal Stub**, **Not Stub**, or **Not so Stubby Stub**.	All levels
Authentication Type	Type of authentication: **None**, **Password**, or **MD5**. NOTE: The **Authentication Type** field refers to the authentication configured at the **[edit protocols ospf area *area-id*]** level. Any authentication configured for an interface in this area will not affect the value of this field.	All levels
Area border routers	Number of area border routers.	All levels
Neighbors	Number of autonomous system boundary routers.	All levels

Sample Output

show ospf overview

```
user@host> show ospf overview
Instance: master
    Router ID: 10.255.245.6
    Route table index: 0
   Configured overload, expires in 118 seconds
    LSA refresh time: 50 minutes
  Restart: Enabled
     Restart duration: 20 sec
     Restart grace period: 40 sec
     Helper mode: enabled
  Area: 0.0.0.0
      Stub type: Not Stub
      Authentication Type: None
      Area border routers: 0, AS boundary routers: 0
      Neighbors
        Up (in full state): 0
    Topology: default (ID 0)
      Prefix export count: 0
      Full SPF runs: 1
      SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
```

show ospf overview (With Database Protection)

```
user@host> show ospf overview
Instance: master
  Router ID: 10.255.112.218
  Route table index: 0
  LSA refresh time: 50 minutes
  Traffic engineering
  Restart: Enabled
    Restart duration: 180 sec
    Restart grace period: 210 sec
    Graceful restart helper mode: Enabled
    Restart-signaling helper mode: Enabled
  Database protection state: Normal
    Warning threshold: 70 percent
    Non self-generated LSAs: Current 582, Warning 700, Allowed 1000
    Ignore time: 30, Reset time: 60
    Ignore count: Current 0, Allowed 1
  Area: 0.0.0.0
    Stub type: Not Stub
    Authentication Type: None
    Area border routers: 0, AS boundary routers: 0
    Neighbors
      Up (in full state): 160
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 70
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed
```

show ospf3 overview (With Database Protection)

```
user@host> show ospf3 overview
Instance: master
  Router ID: 10.255.112.128
  Route table index: 0
  LSA refresh time: 50 minutes
  Database protection state: Normal
```



```
    Warning threshold: 80 percent
    Non self-generated LSAs: Current 3, Warning 8, Allowed 10
    Ignore time: 30, Reset time: 60
    Ignore count: Current 0, Allowed 2
  Area: 0.0.0.0
    Stub type: Not Stub
    Area border routers: 0, AS boundary routers: 0
    Neighbors
      Up (in full state): 1
  Topology: default (ID 0)
    Prefix export count: 0
    Full SPF runs: 7
    SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
    Backup SPF: Not Needed
```

show ospf overview extensive

```
user@host> show ospf overview extensive
Instance: master
  Router ID: 1.1.1.103
  Route table index: 0
  Full SPF runs: 13, SPF delay: 0.200000 sec
  LSA refresh time: 50 minutes
  Restart: Disabled
  Trace options: lsa
  Trace file: /var/log/ospf size 131072 files 10
  Area: 0.0.0.0
    Stub type: Not Stub
    Authentication Type: None
    Area border routers: 0, AS boundary routers: 0
    Neighbors
      Up (in full state): 1
```

show (ospf | ospf3) route

Syntax

show (ospf | ospf3) route
<brief | detail | extensive>
<abr | asbr | extern | inter | intra>
<*destination*>
<instance (default | ipv4-multicast | *instance-name*)>
<logical-system (default | ipv4-multicast | *logical-system-name*)>
<network>
<no-backup-coverage>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>
<topology (default | ipv4-multicast | *topology-name*)>
<transit>

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) route
<brief | detail | extensive>
<abr | asbr | extern | inter | intra>
<*destination*>
<instance *instance-name*
<network>
<no-backup-coverage>
<router>
<topology (default | ipv4-multicast | *topology-name*)>
<transit>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
topology option introduced in Junos OS Release 9.0.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the entries in the Open Shortest Path First (OSPF) routing table.

Options

none—Display standard information about all entries in the OSPF routing table for all routing instances and all topologies.

destination—Display routes to the specified IP address (with optional destination prefix length).

brief | detail | extensive—(Optional) Display the specified level of output.

abr—(Optional) Display routes to area border routers.

asbr—(Optional) Display routes to autonomous system border routers.

extern—(Optional) Display external routes.

inter—(Optional) Display interarea routes.

intra—(Optional) Display intra-area routes.

instance (default | ipv4-multicast | ***instance-name*****)**—(Optional) Display entries for the default routing instance, the IPv4 multicast routing instance, or for the specified routing instance.

logical-system (default | ipv4-multicast | ***logical-system-name*****)**—(Optional) Perform this operation on the default logical system, the IPv4 multicast logical system, or on a particular logical system.

network—(Optional) Display routes to networks.

no-backup-coverage—(Optional) Display routes with no backup coverage.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display entries in the routing table for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

router—(Optional) Display routes to all routers.

topology (default | ipv4-multicast | ***topology-name*****)**—(OSPFv2 only) (Optional) Display routes for the default OSPF topology, IPv4 multicast topology, or for a particular topology.

transit—(Optional) (OSPFv3 only) Display OSPFv3 routes to pseudonodes.

Required Privilege Level view

List of Sample Output

show ospf route on page 545
show ospf route detail on page 545
show ospf3 route on page 545
show ospf3 route detail on page 545
show ospf route topology voice on page 546

Output Fields Table 14 on page 542 list the output fields for the **show (ospf | ospf3) route** command. Output fields are listed in the approximate order in which they appear.

Table 14: show (ospf | ospf3) route Output Fields

Field Name	Field Description	Output Level
Topology	Name of the topology.	All levels
Prefix	Destination of the route.	All levels
Path type	How the route was learned: • **Inter**—Interarea route • **Ext1**—External type 1 route • **Ext2**—External type 2 route • **Intra**—Intra-area route	All levels

Table 14: show (ospf | ospf3) route Output Fields *(continued)*

Field Name	Field Description	Output Level
Route type	The type of routing device from which the route was learned: • **AS BR**—Route to AS border router. • **Area BR**—Route to area border router. • **Area/AS BR**—Route to router that is both an **Area BR** and **AS BR**. • **Network**—Network router. • **Router**—Route to a router that is neither an **Area BR** nor an **AS BR**. • **Transit**—(OSPFv3 only) Route to a pseudonode representing a transit network, LAN, or nonbroadcast multiaccess (NBMA) link. • **Discard**—Route to a summary discard.	All levels
NH Type	Next-hop type: **LSP** or **IP**.	All levels
Metric	Route's metric value.	All levels
NH-interface	(OSPFv3 only) Interface through which the route's next hop is reachable.	All levels
NH-addr	(OSPFv3 only) IPv6 address of the next hop.	All levels
NextHop Interface	(OSPFv2 only) Interface through which the route's next hop is reachable.	All levels
Nexthop addr/label	(OSPFv2 only) If the **NH Type** is **IP**, then it is the address of the next hop. If the **NH Type** is **LSP**, then it is the name of the label-switched path.	All levels
Area	Area ID of the route.	**detail**
Origin	Router from which the route was learned.	**detail**
Type 7	Route was learned through a not-so-stubby area (NSSA) link-state advertisement (LSA).	**detail**
P-bit	Route was learned through NSSA LSA and the propagate bit was set.	**detail**
Fwd NZ	Forwarding address is nonzero. **Fwd NZ** is only displayed if the route is learned through an NSSA LSA.	**detail**
optional-capability	Optional capabilities propagated in the router LSA. This field is in the output for intra-area router routes only (when **Route Type** is **Area BR**, **AS BR**, **Area/AS BR**, or **Router**), not for interarea router routes or network routes. Three bits in this field are defined as follows: • **0x4 (V)**—Routing device is at the end of a virtual active link. • **0x2 (E)**—Routing device is an autonomous system boundary router. • **0x1 (B)**—Routing device is an area border router.	**detail**

Table 14: show (ospf | ospf3) route Output Fields *(continued)*

Field Name	Field Description	Output Level
priority	The priority assigned to the prefix: • **high** • **medium** • **low** NOTE: The **priority** field applies only to routes of type **Network**.	**detail**

Sample Output

show ospf route

```
user@host> show ospf route
Prefix               Path   Route      NH    Metric  NextHop       Nexthop
                     Type   Type       Type          Interface     addr/label
10.255.71.12         Intra  Router     IP    1       fe-0/0/2.0    192.16.22.86
10.255.71.13/32      Intra  Network    IP    0       lo0.0
192.168.222.84/30    Intra  Network    LSP   1       fe-0/0/2.0    lsp-ab
```

show ospf route detail

```
user@host> show ospf route detail
Topology default Route Table:

Prefix             Path   Route      NH    Metric  NextHop       Nexthop
                   Type   Type       Type          Interface     addr/label
10.255.14.174      Inter  AS BR      IP       210  t1-3/0/1.0
   area 0.0.0.2, origin 10.255.14.185
10.255.14.178      Intra  Router     IP       200  t3-3/1/3.0
   area 0.0.0.2, origin 10.255.14.178, optional-capability 0x0
10.210.1.0/30      Intra  Network    IP        10  t3-3/1/2.0
   area 0.0.0.2, origin 10.255.14.172, priority medium
100.1.1.1/32       Inter  Network    IP       210  t1-3/0/1.0
   area 0.0.0.2, origin 10.255.14.185, priority low
112.3.1.0/24       Ext2   Network    IP         0  t1-3/0/1.0
   area 0.0.0.0, origin 10.255.14.174, priority high
200.3.3.0/30       Inter  Network    IP       220  t1-3/0/1.0
   area 0.0.0.2, origin 10.255.14.185, priority high
```

show ospf3 route

```
user@host> show ospf3 route
Prefix               Path   Route      NH    Metric  NextHop       Nexthop

                     Type   Type       Type          Interface     addr/label
10.255.71.13         Intra  Router     IP         1
  NH-interface fe-0/0/2.0, NH-addr fe80::290:69ff:fe9b:e002
10.255.71.13;0.0.0.2
10.255.245.1         Intra  Router     IP        40  fxp1.1        192.168.36.17

  area 0.0.0.0, origin 10.255.245.1 optional-capability 0x0,
10.255.245.3         Intra  AS BR      IP         1  fxp2.3        192.168.36.34

  area 0.0.0.0, origin 10.255.245.3 optional-capability 0x0,
10.255.245.1/32      Intra  Network    IP        40  fxp1.1        192.168.36.17

  area 0.0.0.0, origin 10.255.245.1, priority high
10.255.245.2/32      Intra  Network    IP         0  lo0.0
  area 0.0.0.0, origin 10.255.245.2, priority medium
10.255.245.3/32      Intra  Network    IP         1  fxp2.3        192.168.36.34

  area 0.0.0.0, origin 10.255.245.3, priority low
                     Intra  Transit    IP         1
  NH-interface fe-0/0/2.0
192::168:222:84/126  Intra  Network    IP         1
  NH-interface fe-0/0/2.0
abcd::71:12/128      Intra  Network    IP         0
  NH-interface lo0.0
abcd::71:13/128      Intra  Network    LSP        1
  NH-interface fe-0/0/2.0, NH-addr lsp-cd
```

show ospf3 route detail

```
user@host> show ospf3 route detail
Prefix                                      Path   Route       NH    Metric
                                            type   type        type
10.255.14.174                               Intra  Area/AS BR  IP    110
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.174, Optional-capability 0x3
10.255.14.178                               Intra  Router      IP    200
   NH-interface t3-3/1/3.0
   Area 0.0.0.0, Origin 10.255.14.178, Optional-capability 0x0
10.255.14.185;0.0.0.2                       Intra  Transit     IP    200
   NH-interface t1-3/0/1.0
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.185
1000:1:1::1/128                             Inter  Network     IP    110
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.174, Priority low
1001:2:1::/48                               Ext1   Network     IP    110
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority medium
1002:1:7::/48                               Ext2   Network     IP    0
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority low
1002:3:4::/48                               Ext2   Network     IP    0
   NH-interface so-1/2/2.0
   Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority high
abcd::10:255:14:172/128                     Intra  Network     IP    0
   NH-interface lo0.0
   Area 0.0.0.0, Origin 10.255.14.172, Priority low
```

show ospf route topology voice

```
user@host show ospf route topology voice
Topology voice Route Table:
Prefix             Path   Route       NH    Metric  NextHop       Nexthop
                   Type   Type        Type          Interface     addr/label
10.255.8.2         Intra  Router      IP         1  so-0/2/0.0
10.255.8.3         Intra  Router      IP         2  so-0/2/0.0
10.255.8.1/32      Intra  Network     IP         0  lo0.0
10.255.8.2/32      Intra  Network     IP         1  so-0/2/0.0
10.255.8.3/32      Intra  Network     IP         2  so-0/2/0.0
192.168.8.0/29     Intra  Network     IP         2  so-0/2/0.0
192.168.8.44/30    Intra  Network     IP         2  so-0/2/0.0
192.168.8.46/32    Intra  Network     IP         1  so-0/2/0.0
192.168.8.48/30    Intra  Network     IP         1  so-0/2/1.0
192.168.8.52/30    Intra  Network     IP         2  so-0/2/0.0
192.168.9.44/30    Intra  Network     IP         1  so-0/2/0.0
192.168.9.45/32    Intra  Network     IP         2  so-0/2/0.0
```

show (ospf | ospf3) statistics

Syntax

show (ospf | ospf3) statistics
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) statistics
<instance *instance-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display OSPF statistics.

Options

none—Display OSPF statistics for all routing instances.

instance ***instance-name***—(Optional) Display all statistics for the specified routing instance.

logical-system (all | ***logical-system-name*****)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Display all statistics for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level

view

Related Documentation

- clear (ospf | ospf3) statistics on page 482

List of Sample Output

show ospf statistics on page 549
show ospf statistics logical-system all on page 549
show ospf3 statistics on page 550

Output Fields

Table 15 on page 547 lists the output fields for the **show (ospf | ospf3) statistics** command. Output fields are listed in the approximate order in which they appear.

Table 15: show (ospf | ospf3) statistics Output Fields

Field Name	Field Description
Packet type	Type of OSPF packet.
Total Sent/Total Received	Total number of packets sent and received.
Last 5 seconds Sent/Last 5 seconds Received	Total number of packets sent and received in the last 5 seconds.

Table 15: show (ospf | ospf3) statistics Output Fields *(continued)*

Field Name	Field Description
DBDs retransmitted	Total number of database description packets retransmitted, and number retransmitted in the last 5 seconds.
LSAs flooded	Total number of link-state advertisements flooded, and number flooded in the last 5 seconds.
LSAs flooded high-prio	Total number of high priority link-state advertisements flooded, and number flooded in the last 5 seconds. A link-state advertisement is deemed a high priority if it has changed since it was last sent.
LSAs retransmitted	Total number of link-state advertisements retransmitted, and number retransmitted in the last 5 seconds.
LSAs transmitted to nbr	Total number of link-state advertisements transmitted to a neighbor, and number transmitted in the last 5 seconds.
LSAs requested	Total number of link-state advertisements requested by neighboring devices, and number requested in the last 5 seconds.
LSAs acknowledged	Total number of link-state advertisements acknowledged, and number acknowledged in the last 5 seconds.
Flood queue depth	Total number of entries in the extended queue.
Total rexmit entries	Total number of retransmission entries waiting to be sent from the OSPF routing instance.
db summaries	Total number of database description summaries waiting to be sent from the OSPF routing instance.
lsreq entries	Total number of link-state request entries waiting to be sent from the OSPF routing instance.
Receive errors	Number and type of receive errors. Some sample receive errors include: • **mtu mismatches** • **no interface found** • **no virtual link found** • **nssa mismatches** • **stub area mismatches** • **subnet mismatches** If there are no receive errors, the output displays **none**.

Sample Output

show ospf statistics

```
user@host> show ospf statistics
Packet type             Total                  Last 5 seconds
                   Sent       Received        Sent       Received
   Hello             31             14           2              2
     DbD              9             10           0              0
   LSReq              2              2           0              0
LSUpdate              8             16           0              0
   LSAck              9              9           0              0

DBDs retransmitted     :                 3, last 5 seconds :          0
LSAs flooded           :                12, last 5 seconds :          0
LSAs flooded high-prio :                 0, last 5 seconds :          0
LSAs retransmitted     :                 0, last 5 seconds :          0
LSAs transmitted to nbr:                 3, last 5 seconds :          0
LSAs requested         :                 5, last 5 seconds :          0
LSAs acknowledged      :                19, last 5 seconds :          0

Flood queue depth      :                0
Total rexmit entries   :                0
db summaries           :                0
lsreq entries          :                0

Receive errors:
  862 no interface found
  115923 no virtual link found
```

show ospf statistics logical-system all

```
user@host> show ospf statistics logical-system all
logical-system: C
OSPF instance is not running
-----

logical-system: B

Packet type             Total                  Last 5 seconds
                   Sent       Received        Sent       Received
   Hello         313740         313653           1              0
     DbD              3              2           0              0
   LSReq              1              1           0              0
LSUpdate           2752           1825           0              0
   LSAck           1821           2747           0              0

DBDs retransmitted     :                 0, last 5 seconds :          0
LSAs flooded           :              2741, last 5 seconds :          0
LSAs flooded high-prio :                10, last 5 seconds :          0
LSAs retransmitted     :                 0, last 5 seconds :          0
LSAs transmitted to nbr:                 2, last 5 seconds :          0
LSAs requested         :                 1, last 5 seconds :          0
LSAs acknowledged      :              1831, last 5 seconds :          0

Flood queue depth      :                0
Total rexmit entries   :                0
db summaries           :                0
lsreq entries          :                0

Receive errors:
  None
-----
```



```
logical-system: A

Packet type             Total                   Last 5 seconds
                   Sent       Received         Sent       Received
   Hello         313698         313695            0              0
     DbD              2              3            0              0
   LSReq              1              1            0              0
LSUpdate           1825           2752            0              0
   LSAck           2747           1821            0              0

DBDs retransmitted     :                    0, last 5 seconds :          0
LSAs flooded           :                 1825, last 5 seconds :          0
LSAs flooded high-prio :                   10, last 5 seconds :          0
LSAs retransmitted     :                    0, last 5 seconds :          0
LSAs transmitted to nbr:                    1, last 5 seconds :          0
LSAs requested         :                    2, last 5 seconds :          0
LSAs acknowledged      :                 2748, last 5 seconds :          0

Flood queue depth      :               0
Total rexmit entries   :               0
db summaries           :               0
lsreq entries          :               0

Receive errors:
  None
-----
```

show ospf3 statistics

```
user@host> show ospf3 statistics
Packet type             Total                   Last 5 seconds
                   Sent       Received         Sent       Received
   Hello              0              0            0              0
     DbD              0              0            0              0
   LSReq              0              0            0              0
LSUpdate              0              0            0              0
   LSAck              0              0            0              0

DBDs retransmitted     :                    0, last 5 seconds :          0
LSAs flooded           :                    0, last 5 seconds :          0
LSAs flooded high-prio :                    0, last 5 seconds :          0
LSAs retransmitted     :                    0, last 5 seconds :          0
LSAs transmitted to nbr:                    0, last 5 seconds :          0
LSAs requested         :                    0, last 5 seconds :          0
LSAs acknowledged      :                    0, last 5 seconds :          0

Flood queue depth      :               0
Total rexmit entries   :               0
db summaries           :               0
lsreq entries          :               0

Receive errors:
  None
```


show policy

Syntax

show policy
<logical-system (all | *logical-system-name*)>
<*policy-name*>

Syntax (EX Series Switches)

show policy
<*policy-name*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display information about configured routing policies.

Options

none—List the names of all configured routing policies.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

policy-name—(Optional) Show the contents of the specified policy.

Required Privilege Level

view

Related Documentation

- *show policy damping*

List of Sample Output

show policy on page 552
show policy policy-name on page 552
show policy (Multicast Scoping) on page 552

Output Fields

Table 16 on page 551 lists the output fields for the **show policy** command. Output fields are listed in the approximate order in which they appear.

Table 16: show policy Output Fields

Field Name	Field Description
policy-name	Name of the policy listed.
term	Policy term listed.
from	Match condition for the policy.
then	Action for the policy.

Sample Output

show policy

```
user@host> show policy
Configured policies:
__vrf-export-red-internal__
__vrf-import-red-internal__
red-export
all_routes
```

show policy policy-name

```
user@host> show policy test-statics
Policy test-statics:
    from
         3.0.0.0/8  accept
         3.1.0.0/16  accept
    then reject
```

show policy (Multicast Scoping)

```
user@host> show policy test-statics
Policy test-statics:
    from
         multicast-scoping == 8
```


show route

Syntax

show route
<all>
<*destination-prefix*>
<logical-system (all | *logical-system-name*)>
<private>

Syntax (EX Series Switches)

show route
<all>
<*destination-prefix*>
<private>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **private** introduced in Junos OS Release 9.5.
Option **private** introduced in Junos OS Release 9.5 for EX Series switches.

Description

Display the active entries in the routing tables.

Options

none—Display brief information about all active entries in the routing tables.

all—(Optional) Display information about all routing tables, including private, or internal, routing tables.

destination-prefix—(Optional) Display active entries for the specified address or range of addresses.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

private—(Optional) Display information only about all private, or internal, routing tables.

Required Privilege Level

view

Related Documentation

- *Example: Configuring RIP*
- *Example: Configuring RIPng*
- *Example: Configuring IS-IS*
- *Examples: Configuring Internal BGP Peering*
- *Examples: Configuring External BGP Peering*
- Examples: Configuring OSPF Routing Policy on page 281

List of Sample Output

show route on page 557
show route on page 557
show route destination-prefix on page 557
show route extensive on page 557

Output Fields Table 17 on page 554 describes the output fields for the **show route** command. Output fields are listed in the approximate order in which they appear.

Table 17: show route Output Fields

Field Name	Field Description
routing-table-name	Name of the routing table (for example, inet.0).
number **destinations**	Number of destinations for which there are routes in the routing table.
number **routes**	Number of routes in the routing table and total number of routes in the following states: • **active** (routes that are active). • **holddown** (routes that are in the pending state before being declared inactive). A holddown route was once the active route and is no longer the active route. The route is in the holddown state because a protocol still has interest in the route, meaning that the interest bit is set. A protocol might have its interest bit set on the previously active route because the protocol is still advertising the route. The route will be deleted after all protocols withdraw their advertisement of the route and remove their interest bit. A persistent holddown state often means that the interested protocol is not releasing its interest bit properly. However, if you have configured advertisement of multiple routes (with the **add-path** or **advertise-inactive** statement), the holddown bit is most likely set because BGP is advertising the route as an active route. In this case, you can ignore the holddown state because nothing is wrong. • **hidden** (routes that are not used because of a routing policy).

destination-prefix	Route destination (for example:10.0.0.1/24). Sometimes the route information is presented in another format, such as:
	• *MPLS-label* (for example, 80001).
	• *interface-name* (for example, ge-1/0/2).
	• *neighbor-address*:*control-word-status*:*encapsulation type*:*vc-id* :*source* (Layer 2 circuit only. For example, 10.1.1.195:NoCtrlWord:1:1:Local/96):
	  ◦ *neighbor-address*—Address of the neighbor.
	  ◦ *control-word-status*—Whether the use of the control word has been negotiated for this virtual circuit: **NoCtrlWord** or **CtrlWord**.
	  ◦ *encapsulation type*—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.
	  ◦ *vc-id*—Virtual circuit identifier.
	  ◦ *source*—Source of the advertisement: **Local** or **Remote**.

[*protocol*, *preference*]	Protocol from which the route was learned and the preference value for the route. • **+**—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table. • **-** —A hyphen indicates the last active route. • *****—An asterisk indicates that the route is both the active and the last active route. An asterisk before a **to** line indicates the best subpath to the route. In every routing metric except for the BGP **LocalPref** attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the **LocalPref** value in the **Preference2** field. For example, if the **LocalPref** value for Route 1 is 100, the **Preference2** value is -101. If the **LocalPref** value for Route 2 is 155, the **Preference2** value is -156. Route 2 is preferred because it has a higher **LocalPref** value and a lower **Preference2** value.

Table 17: show route Output Fields *(continued)*

Field Name	Field Description
weeks:days hours:minutes:seconds	How long the route been known (for example, **2w4d 13:11:14**, or 2 weeks, 4 days, 13 hours, 11 minutes, and 14 seconds).
metric	Cost value of the indicated route. For routes within an AS, the cost is determined by the IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
localpref	Local preference value included in the route.
from	Interface from which the route was received.
AS path	AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated: • **I**—IGP. • **E**—EGP. • **?**—Incomplete; typically, the AS path was aggregated. When AS path numbers are included in the route, the format is as follows: • **[ ]**—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured. • **{ }**—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order. • **( )**—Parentheses enclose a confederation. • **([ ])**—Parentheses and brackets enclose a confederation set. NOTE: In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.
validation-state	(BGP-learned routes) Validation status of the route: • **Invalid**—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database. • **Unknown**—Indicates that the prefix is not among the prefixes or prefix ranges in the database. • **Valid**—Indicates that the prefix and autonomous system pair are found in the database.
to	Next hop to the destination. An angle bracket (>) indicates that the route is the selected route. If the destination is **Discard**, traffic is dropped.

Table 17: show route Output Fields *(continued)*

Field Name	Field Description
via	Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word **Selected**. This field can also contain the following information: • **Weight**—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible. • **Balance**—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing. • ***lsp-path-name***—Name of the LSP used to reach the next hop. • ***label-action***—MPLS label and operation occurring at the next hop. The operation can be **pop** (where a label is removed from the top of the stack), **push** (where another label is added to the label stack), or **swap** (where a label is replaced by another label). For VPNs, expect to see multiple **push** operations, corresponding to the inner and outer labels required for VPN routes (in the case of a direct PE-to-PE connection, the VPN route would have the inner label push only).

Sample Output

show route

```
user@host> show route
inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:65500:1:10.0.0.20/240
                   *[MVPN/70] 19:53:41, metric2 1
                      Indirect
1:65500:1:10.0.0.40/240
                   *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
                      AS path: I
                    > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD
                    [BGP/170] 19:53:26, localpref 100, from 10.0.0.33
                      AS path: I
                    > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD
1:65500:1:10.0.0.60/240
                   *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
                      AS path: I
                    > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF
                    [BGP/170] 19:53:25, localpref 100, from 10.0.0.33
                      AS path: I
                    > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF
```

show route

The following sample output shows a VPN route with composite next hops enabled. The first **Push** operation corresponds to the outer label. The second **Push** operation corresponds to the inner label.

```
user@host> show route 70.0.0.0

13979:665001.inet.0: 871 destinations, 3556 routes (871 active, 0 holddown, 0
hidden)
+ = Active Route, - = Last Active, * = Both

70.0.0.0/24        @[BGP/170] 00:28:32, localpref 100, from 10.9.9.160
                      AS path: 13980 ?
                    > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
                    [BGP/170] 00:28:28, localpref 100, from 10.9.9.169
                      AS path: 13980 ?
                    > to 10.100.0.42 via ae2.0, Push 126016, Push 300368(top)
                   #[Multipath/255] 00:28:28, metric2 102
                    > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
                      to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
```

show route destination-prefix

```
user@host> show route 172.16.0.0/12

inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.0.0/12      *[Static/5] 2w4d 12:54:27
                    > to 192.168.167.254 via fxp0.0
```

show route extensive

```
user@host> show route extensive
v1.mvpn.0: 5 destinations, 8 routes (5 active, 1 holddown, 0 hidden)
1:65500:1:10.0.0.40/240 (1 entry, 1 announced)
    *BGP    Preference: 170/-101
          PMSI: Flags 0x0: Label[0:0:0]: PIM-SM: Sender 10.0.0.40 Group 225.1.1.1
```

```
Next hop type: Indirect
Address: 0x92455b8
Next-hop reference count: 2
Source: 10.0.0.30
Protocol next hop: 10.0.0.40
Indirect next hop: 2 no-forward
State: <Active Int Ext>
          Local AS: 65500 Peer AS: 65500
Age: 3  Metric2: 1
Task: BGP_65500.10.0.0.30+179
Announcement bits (2): 0-PIM.v1 1-mvpn global task
AS path: I (Originator) Cluster list:  10.0.0.30
AS path:  Originator ID: 10.0.0.40
Communities: target:65520:100
Import Accepted
Localpref: 100
Router ID: 10.0.0.30
Primary Routing Table bgp.mvpn.0
Indirect next hops: 1
     Protocol next hop: 10.0.0.40 Metric: 1
     Indirect next hop: 2 no-forward
     Indirect path forwarding next hops: 1
           Next hop type: Router
           Next hop: 10.0.24.4 via lt-0/3/0.24 weight 0x1
     10.0.0.40/32 Originating RIB: inet.3
           Metric: 1                       Node path count: 1
           Forwarding nexthops: 1
              Nexthop: 10.0.24.4 via lt-0/3/0.24
```


show route instance

Syntax

show route instance
<brief | detail | summary>
<*instance-name*>
<logical-system (all | *logical-system-name*)>
<operational>

Syntax (EX Series Switches and QFX Series)

show route instance
<brief | detail | summary>
<*instance-name*>
<operational>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display routing instance information.

Options

none—(Same as **brief**) Display standard information about all routing instances.

brief | detail | summary—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**. (These options are not available with the **operational** keyword.)

instance-name—(Optional) Display information for all routing instances whose name begins with this string (for example, **cust1**, **cust11**, and **cust111** are all displayed when you run the **show route instance cust1** command).

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

operational—(Optional) Display operational routing instances.

Required Privilege Level

view

List of Sample Output

show route instance on page 561
show route instance detail (Graceful Restart Complete) on page 561
show route instance detail (Graceful Restart Incomplete) on page 563
show route instance detail (VPLS Routing Instance) on page 564
show route instance operational on page 565
show route instance summary on page 565

Output Fields

Table 18 on page 559 lists the output fields for the **show route instance** command. Output fields are listed in the approximate order in which they appear.

Table 18: show route instance Output Fields

Field Name	Field Description	Level of Output
Instance or *instance-name*	Name of the routing instance.	All levels

Table 18: show route instance Output Fields *(continued)*

Field Name	Field Description	Level of Output
Operational Routing Instances	(**operational** keyword only) Names of all operational routing instances.	—
Type	Type of routing instance: **forwarding**, **l2vpn**, **no-forwarding**, **vpls**, **virtual-router**, or **vrf**.	All levels
State	State of the routing instance: **active** or **inactive**.	**brief detail** none
Interfaces	Name of interfaces belonging to this routing instance.	**brief detail** none
Restart State	Status of graceful restart for this instance: **Pending** or **Complete**.	**detail**
Path selection timeout	Maximum amount of time, in seconds, remaining until graceful restart is declared complete. The default is **300**.	**detail**
Tables	Tables (and number of routes) associated with this routing instance.	**brief detail** none
Route-distinguisher	Unique route distinguisher associated with this routing instance.	**detail**
Vrf-import	VPN routing and forwarding instance import policy name.	**detail**
Vrf-export	VPN routing and forwarding instance export policy name.	**detail**
Vrf-import-target	VPN routing and forwarding instance import target community name.	**detail**
Vrf-export-target	VPN routing and forwarding instance export target community name.	**detail**
Fast-reroute-priority	Fast reroute priority setting for a VPLS routing instance: **high**, **medium**, or **low**. The default is **low**.	**detail**
Restart State	Restart state: • **Pending:***protocol-name*—List of protocols that have not yet completed graceful restart for this routing table. • **Complete**—All protocols have restarted for this routing table.	**detail**
Primary rib	Primary table for this routing instance.	**brief** none **summary**
Active/holddown/hidden	Number of active, hold-down, and hidden routes.	All levels

Sample Output

show route instance

```
user@host> show route instance
Instance             Type
         Primary RIB                                     Active/holddown/hidden
master               forwarding
         inet.0                                          16/0/1
         iso.0                                           1/0/0
         mpls.0                                          0/0/0
         inet6.0                                         2/0/0
         l2circuit.0                                     0/0/0
__juniper_private1__ forwarding
         __juniper_private1__.inet.0                     12/0/0
         __juniper_private1__.inet6.0                    1/0/0
```

show route instance detail (Graceful Restart Complete)

```
user@host> show route instance detail
master:
  Router ID: 10.255.14.176
  Type: forwarding        State: Active
  Restart State: Complete Path selection timeout: 300
  Tables:
    inet.0                 : 17 routes (15 active, 0 holddown, 1 hidden)
    Restart Complete
    inet.3                 : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Complete
    iso.0                  : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Complete
    mpls.0                 : 19 routes (19 active, 0 holddown, 0 hidden)
    Restart Complete
    bgp.l3vpn.0            : 10 routes (10 active, 0 holddown, 0 hidden)
    Restart Complete
    inet6.0                : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Complete
    bgp.l2vpn.0            : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Complete
BGP-INET:
  Router ID: 10.69.103.1
  Type: vrf               State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.103
  Route-distinguisher: 10.255.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
  Tables:
    BGP-INET.inet.0        : 4 routes (4 active, 0 holddown, 0 hidden)
    Restart Complete
BGP-L:
  Router ID: 10.69.104.1
  Type: vrf               State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.104
  Route-distinguisher: 10.255.14.176:104
  Vrf-import: [ BGP-L-import ]
  Vrf-export: [ BGP-L-export ]
  Tables:
    BGP-L.inet.0           : 4 routes (4 active, 0 holddown, 0 hidden)
    Restart Complete
```

```
    BGP-L.mpls.0           : 3 routes (3 active, 0 holddown, 0 hidden)
    Restart Complete
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn            State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.512
  Route-distinguisher: 10.255.14.176:512
  Vrf-import: [ L2VPN-import ]
  Vrf-export: [ L2VPN-export ]
  Tables:
    L2VPN.l2vpn.0          : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Complete
LDP:
  Router ID: 10.69.105.1
  Type: vrf              State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.105
  Route-distinguisher: 10.255.14.176:105
  Vrf-import: [ LDP-import ]
  Vrf-export: [ LDP-export ]
  Tables:
    LDP.inet.0             : 5 routes (4 active, 0 holddown, 0 hidden)
    Restart Complete
OSPF:
  Router ID: 10.69.101.1
  Type: vrf              State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.101
  Route-distinguisher: 10.255.14.176:101
  Vrf-import: [ OSPF-import ]
  Vrf-export: [ OSPF-export ]
  Vrf-import-target: [ target:11111
  Tables:
    OSPF.inet.0            : 8 routes (7 active, 0 holddown, 0 hidden)
    Restart Complete
RIP:
  Router ID: 10.69.102.1
  Type: vrf              State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.102
  Route-distinguisher: 10.255.14.176:102
  Vrf-import: [ RIP-import ]
  Vrf-export: [ RIP-export ]
  Tables:
    RIP.inet.0             : 6 routes (6 active, 0 holddown, 0 hidden)
    Restart Complete
STATIC:
  Router ID: 10.69.100.1
  Type: vrf              State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.100
  Route-distinguisher: 10.255.14.176:100
  Vrf-import: [ STATIC-import ]
  Vrf-export: [ STATIC-export ]
  Tables:
```



```
    STATIC.inet.0          : 4 routes (4 active, 0 holddown, 0 hidden)
    Restart Complete
```

show route instance detail (Graceful Restart Incomplete)

```
user@host> show route instance detail
master:
  Router ID: 10.255.14.176
  Type: forwarding        State: Active
  Restart State: Pending  Path selection timeout: 300
  Tables:
    inet.0                 : 17 routes (15 active, 1 holddown, 1 hidden)
    Restart Pending: OSPF LDP
    inet.3                 : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Pending: OSPF LDP
    iso.0                  : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Complete
    mpls.0                 : 23 routes (23 active, 0 holddown, 0 hidden)
    Restart Pending: LDP VPN
    bgp.l3vpn.0            : 10 routes (10 active, 0 holddown, 0 hidden)
    Restart Pending: BGP VPN
    inet6.0                : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Complete
    bgp.l2vpn.0            : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Pending: BGP VPN
BGP-INET:
  Router ID: 10.69.103.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.103
  Route-distinguisher: 10.255.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
  Tables:
    BGP-INET.inet.0        : 6 routes (5 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
BGP-L:
  Router ID: 10.69.104.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.104
  Route-distinguisher: 10.255.14.176:104
  Vrf-import: [ BGP-L-import ]
  Vrf-export: [ BGP-L-export ]
  Tables:
    BGP-L.inet.0           : 6 routes (5 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
    BGP-L.mpls.0           : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn             State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.512
  Route-distinguisher: 10.255.14.176:512
  Vrf-import: [ L2VPN-import ]
  Vrf-export: [ L2VPN-export ]
  Tables:
    L2VPN.l2vpn.0          : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Pending: VPN L2VPN
```

```
LDP:
  Router ID: 10.69.105.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.105
  Route-distinguisher: 10.255.14.176:105
  Vrf-import: [ LDP-import ]
  Vrf-export: [ LDP-export ]
  Tables:
    LDP.inet.0             : 5 routes (4 active, 1 holddown, 0 hidden)
    Restart Pending: OSPF LDP VPN
OSPF:
  Router ID: 10.69.101.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.101
  Route-distinguisher: 10.255.14.176:101
  Vrf-import: [ OSPF-import ]
  Vrf-export: [ OSPF-export ]
  Tables:
    OSPF.inet.0            : 8 routes (7 active, 1 holddown, 0 hidden)
    Restart Pending: OSPF VPN
RIP:
  Router ID: 10.69.102.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.102
  Route-distinguisher: 10.255.14.176:102
  Vrf-import: [ RIP-import ]
  Vrf-export: [ RIP-export ]
  Tables:
    RIP.inet.0             : 8 routes (6 active, 2 holddown, 0 hidden)
    Restart Pending: RIP VPN
STATIC:
  Router ID: 10.69.100.1
  Type: vrf               State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.100
  Route-distinguisher: 10.255.14.176:100
  Vrf-import: [ STATIC-import ]
  Vrf-export: [ STATIC-export ]
  Tables:
    STATIC.inet.0          : 4 routes (4 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
```

show route instance detail (VPLS Routing Instance)

```
user@host> show route instance detail test-vpls
test-vpls:
  Router ID: 0.0.0.0
  Type: vpls              State: Active
  Interfaces:
    lsi.1048833
    lsi.1048832
    fe-0/1/0.513
  Route-distinguisher: 10.255.37.65:1
  Vrf-import: [ __vrf-import-test-vpls-internal__ ]
  Vrf-export: [ __vrf-export-test-vpls-internal__ ]
  Vrf-import-target: [ target:300:1 ]
```

```
  Vrf-export-target: [ target:300:1 ]
  Fast-reroute-priority: high
  Tables:
    test-vpls.l2vpn.0          : 3 routes (3 active, 0 holddown, 0 hidden)
```

show route instance operational

```
user@host> show route instance operational
Operational Routing Instances:

master
default
```

show route instance summary

```
user@host> show route instance summary
Instance             Type                Primary rib              Active/holddown/hidden
master               forwarding
                                         inet.0                   15/0/1
                                         iso.0                    1/0/0
                                         mpls.0                   35/0/0
                                         l3vpn.0                  0/0/0
                                         inet6.0                  2/0/0
                                         l2vpn.0                  0/0/0
                                         l2circuit.0              0/0/0
BGP-INET             vrf
                                         BGP-INET.inet.0          5/0/0
                                         BGP-INET.iso.0           0/0/0
                                         BGP-INET.inet6.0         0/0/0
BGP-L                vrf
                                         BGP-L.inet.0             5/0/0
                                         BGP-L.iso.0              0/0/0
                                         BGP-L.mpls.0             4/0/0
                                         BGP-L.inet6.0            0/0/0
L2VPN                l2vpn
                                         L2VPN.inet.0             0/0/0
                                         L2VPN.iso.0              0/0/0
                                         L2VPN.inet6.0            0/0/0
                                         L2VPN.l2vpn.0            2/0/0
LDP                  vrf
                                         LDP.inet.0               4/0/0
                                         LDP.iso.0                0/0/0
                                         LDP.mpls.0               0/0/0
                                         LDP.inet6.0              0/0/0
                                         LDP.l2circuit.0          0/0/0
OSPF                 vrf
                                         OSPF.inet.0              7/0/0
                                         OSPF.iso.0               0/0/0
                                         OSPF.inet6.0             0/0/0
RIP                  vrf
                                         RIP.inet.0               6/0/0
                                         RIP.iso.0                0/0/0
                                         RIP.inet6.0              0/0/0
STATIC               vrf
                                         STATIC.inet.0            4/0/0
                                         STATIC.iso.0             0/0/0
                                         STATIC.inet6.0           0/0/0
```

show route protocol

Syntax

show route protocol *protocol*
<brief | detail | extensive | terse>
<logical-system (all | *logical-system-name*)>

Syntax (EX Series Switches)

show route protocol *protocol*
<brief | detail | extensive | terse>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
opsf2 and **ospf3** options introduced in Junos OS Release 9.2.
opsf2 and **ospf3** options introduced in Junos OS Release 9.2 for EX Series switches.
flow option introduced in Junos OS Release 10.0.
flow option introduced in Junos OS Release 10.0 for EX Series switches.

Description

Display the route entries in the routing table that were learned from a particular protocol.

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

protocol—Protocol from which the route was learned:

- **access**—Access route for use by DHCP application
- **access-internal**—Access-internal route for use by DHCP application
- **aggregate**—Locally generated aggregate route
- **arp**—Route learned through the Address Resolution Protocol
- **atmvpn**—Asynchronous Transfer Mode virtual private network
- **bgp**—Border Gateway Protocol
- **ccc**—Circuit cross-connect
- **direct**—Directly connected route
- **dvmrp**—Distance Vector Multicast Routing Protocol
- **esis**—End System-to-Intermediate System
- **flow**—Locally defined flow-specification route
- **frr**—Precomputed protection route or backup route used when a link goes down
- **isis**—Intermediate System-to-Intermediate System
- **ldp**—Label Distribution Protocol
- **l2circuit**—Layer 2 circuit
- **l2vpn**—Layer 2 virtual private network

- **local**—Local address
- **mpls**—Multiprotocol Label Switching
- **msdp**—Multicast Source Discovery Protocol
- **ospf**—Open Shortest Path First versions 2 and 3
- **ospf2**—Open Shortest Path First versions 2 only
- **ospf3**—Open Shortest Path First version 3 only
- **pim**—Protocol Independent Multicast
- **rip**—Routing Information Protocol
- **ripng**—Routing Information Protocol next generation
- **rsvp**—Resource Reservation Protocol
- **rtarget**—Local route target virtual private network
- **static**—Statically defined route
- **tunnel**—Dynamic tunnel
- **vpn**—Virtual private network

NOTE: EX Series switches run a subset of these protocols. See the switch CLI for details.

Required Privilege Level view

List of Sample Output

Output Fields For information about output fields, see the output field tables for the show route command, the *show route detail* command, the *show route extensive* command, or the *show route terse* command.

Sample Output

show route protocol access

```
user@host> show route protocol access
inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

13.160.0.3/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
13.160.0.5/32      *[Access/13] 00:00:09
                    > to 13.160.0.2 via fe-0/0/0.0
```

show route protocol access-internal extensive

```
user@host> show route protocol access-internal 13.160.0.19 extensive
inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
        *Access-internal Preference: 12
                Next-hop reference count: 200000
                Next hop: 13.160.0.2 via fe-0/0/0.0, selected
                State: <Active Int>
       Age: 36
                Task: RPD Unix Domain Server./var/run/rpd_serv.local
                Announcement bits (1): 0-KRT
                AS path: I
```

show route protocol arp

```
user@host> show route protocol arp
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.4/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.5/32        [ARP/4294967293] 00:04:32, from 20.20.1.1
                      Unusable
20.20.1.6/32        [ARP/4294967293] 00:04:34, from 20.20.1.1
                      Unusable
20.20.1.7/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.8/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.9/32        [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.10/32       [ARP/4294967293] 00:04:35, from 20.20.1.1
                      Unusable
20.20.1.11/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
20.20.1.12/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
20.20.1.13/32       [ARP/4294967293] 00:04:33, from 20.20.1.1
                      Unusable
...
```

show route protocol bgp

user@host> **show route protocol bgp 192.168.64.0/21**

```
inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.64.0/21      *[BGP/170] 6d 10:41:16, localpref 100, from 192.168.69.71
                      AS path: 10458 14203 2914 4788 4788 I
                    > to 192.168.167.254 via fxp0.0
```

show route protocol bgp detail

user@host> **show route protocol bgp 66.117.63.0/24 detail**

```
inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24  (1 entry, 1 announced)
        *BGP    Preference: 170/-101
                Next hop type: Indirect
                Next-hop reference count: 1006436
                Source: 192.168.69.71
                Next hop type: Router, Next hop index: 324
                Next hop: 192.168.167.254 via fxp0.0, selected
                Protocol next hop: 192.168.69.71
                Indirect next hop: 8e166c0 342
                State: <Active Ext>
                Local AS:    69 Peer AS: 10458
                Age: 6d 10:42:42        Metric2: 0
                Task: BGP_10458.192.168.69.71+179
                Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
1
                AS path: 10458 14203 2914 4788 4788 I
                Communities: 2914:410 2914:2403 2914:3400
                Accepted
                Localpref: 100
                Router ID: 207.17.136.192
```

show route protocol bgp extensive

user@host> **show route protocol bgp 192.168.64.0/21 extensive**

```
inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21 (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
    Nexthop: Self
    AS path: [69] 10458 14203 2914 4788 4788 I
    Communities: 2914:410 2914:2403 2914:3400
Path 1.9.0.0 from 192.168.69.71 Vector len 4.  Val: 1
        *BGP    Preference: 170/-101
                Next hop type: Indirect
                Next-hop reference count: 1006502
                Source: 192.168.69.71
                Next hop type: Router, Next hop index: 324
                Next hop: 192.168.167.254 via fxp0.0, selected
                Protocol next hop: 192.168.69.71
                Indirect next hop: 8e166c0 342
                State: <Active Ext>
                Local AS:    69 Peer AS: 10458
                Age: 6d 10:44:45        Metric2: 0
                Task: BGP_10458.192.168.69.71+179
                Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
1
                AS path: 10458 14203 2914 4788 4788 I
                Communities: 2914:410 2914:2403 2914:3400
```



```
                Accepted
                Localpref: 100
                Router ID: 207.17.136.192
                Indirect next hops: 1
                        Protocol next hop: 192.168.69.71
                        Indirect next hop: 8e166c0 342
                        Indirect path forwarding next hops: 1
                                Next hop type: Router
                                Next hop: 192.168.167.254 via fxp0.0
                        192.168.0.0/16 Originating RIB: inet.0
                          Node path count: 1
                          Forwarding nexthops: 1
                                Nexthop: 192.168.167.254 via fxp0.0
```

show route protocol bgp terse

user@host> **show route protocol bgp 192.168.64.0/21 terse**

```
inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
  192.168.64.0/21    B 170        100            >100.1.3.2       10023 21 I
```

show route protocol direct

user@host> **show route protocol direct**

```
inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

8.8.8.0/24          *[Direct/0] 17w0d 10:31:49
                     > via fe-1/3/1.0
10.255.165.1/32     *[Direct/0] 25w4d 04:13:18
                     > via lo0.0
30.30.30.0/24       *[Direct/0] 17w0d 23:06:26
                     > via fe-1/3/2.0
192.168.164.0/22    *[Direct/0] 25w4d 04:13:20
                     > via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152
                    *[Direct/0] 25w4d 04:13:21
                     > via lo0.0

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

abcd::10:255:165:1/128
                    *[Direct/0] 25w4d 04:13:21
                     > via lo0.0
fe80::2a0:a5ff:fe12:ad7/128
                    *[Direct/0] 25w4d 04:13:21
                     > via lo0.0
```

show route protocol frr

user@host> **show route protocol frr**

```
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
```



```
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.3 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.4/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.4 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.5/32       *[FRR/200] 00:05:35, from 20.20.1.1
                    > to 20.20.1.5 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.6/32       *[FRR/200] 00:05:37, from 20.20.1.1
                    > to 20.20.1.6 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.7/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.7 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.8/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.8 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.9/32       *[FRR/200] 00:05:38, from 20.20.1.1
                    > to 20.20.1.9 via ge-4/1/0.0
                      to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.10/32      *[FRR/200] 00:05:38, from 20.20.1.1
...
```

show route protocol l2circuit detail

```
user@host> show route protocol l2circuit detail

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
100000 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via ge-2/0/0.0, selected
                Label operation: Pop       Offset: 4
                State: <Active Int>
                Local AS:    99
                Age: 9:52
                Task: Common L2 VC
                Announcement bits (1): 0-KRT
                AS path: I

ge-2/0/0.0 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via so-1/1/2.0 weight 1, selected
                Label-switched-path my-lsp
                Label operation: Push 100000, Push 100000(top)[0] Offset: -4
                Protocol next hop: 10.245.255.63
                Push 100000 Offset: -4
                 Indirect next hop: 86af0c0 298
                State: <Active Int>
                Local AS:    99
                Age: 9:52
                Task: Common L2 VC
                Announcement bits (2): 0-KRT 1-Common L2 VC
                AS path: I

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
        *L2CKT  Preference: 7
                Next hop: via so-1/1/2.0 weight 1, selected
                Label-switched-path my-lsp
```

```
                Label operation: Push 100000[0]
                Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
                State: <Active Int>
                Local AS:    99
                Age: 10:21
                Task: l2 circuit
                Announcement bits (1): 0-LDP
                AS path: I
                VC Label 100000, MTU 1500, VLAN ID 512
```

show route protocol l2vpn extensive

```
user@host> show route protocol l2vpn extensive

inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
800001 (1 entry, 1 announced)
TSI:
KRT in-kernel 800001 /36 -> {so-0/0/0.0}
        *L2VPN  Preference: 7
                Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
                Label operation: Pop      Offset: 4
                State: <Active Int>
                Local AS:    69
                Age: 7:48
                Task: Common L2 VC
                Announcement bits (1): 0-KRT
                AS path: I

so-0/0/0.0 (1 entry, 1 announced)
TSI:
KRT in-kernel so-0/0/0.0.0     /16 -> {indirect(288)}
        *L2VPN  Preference: 7
                Next hop: via so-0/0/1.0, selected
                Label operation: Push 800000 Offset: -4
                Protocol next hop: 10.255.14.220
                Push 800000 Offset: -4
                 Indirect next hop: 85142a0 288
                State: <Active Int>
                Local AS:    69
                Age: 7:48
                Task: Common L2 VC
                Announcement bits (2): 0-KRT 1-Common L2 VC
                AS path: I
                Communities: target:69:1 Layer2-info: encaps:PPP,
                control flags:2, mtu: 0
```

show route protocol ldp

```
user@host> show route protocol ldp
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1/32    *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Push 100000
192.168.17.1/32    *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0
```

```
private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100064             *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Pop
100064(S=0)        *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Pop
100080             *[LDP/9] 1d 23:03:35, metric 1
                    > via t1-4/0/0.0, Swap 100000
```

show route protocol ldp extensive

```
user@host> show route protocol ldp extensive
192.168.16.1/32 (1 entry, 1 announced)
        State: <FlashAll>
        *LDP    Preference: 9
                Next-hop reference count: 3
                Next hop: via t1-4/0/0.0, selected
                Label operation: Push 100000
                State: <Active Int>
                Local AS: 65500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
                AS path: I

192.168.17.1/32 (1 entry, 1 announced)
        State: <FlashAll>
        *LDP    Preference: 9
                Next-hop reference count: 3
                Next hop: via t1-4/0/0.0, selected
                State: <Active Int>
                Local AS: 65500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
                AS path: I

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)

100064 (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /36 -> {t1-4/0/0.0}
        *LDP    Preference: 9
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                State: <Active Int>
                Local AS: 65500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I
                Prefixes bound to route: 192.168.17.1/32

100064(S=0) (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /40 -> {t1-4/0/0.0}
        *LDP    Preference: 9
```

```
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                Label operation: Pop
                State: <Active Int>
                Local AS: 65500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I

100080 (1 entry, 1 announced)
TSI:
KRT in-kernel 100080 /36 -> {t1-4/0/0.0}
        *LDP    Preference: 9
                Next-hop reference count: 2
                Next hop: via t1-4/0/0.0, selected
                Label operation: Swap 100000
                State: <Active Int>
                Local AS: 65500
                Age: 1d 23:03:58        Metric: 1
                Task: LDP
                Announcement bits (1): 0-KRT
                AS path: I
                Prefixes bound to route: 192.168.16.1/32
```

show route protocol ospf (Layer 3 VPN)

user@host> **show route protocol ospf**

```
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30       *[OSPF/10] 00:05:18, metric 4
                    > via t3-3/2/0.0
10.39.1.8/30        [OSPF/10] 00:05:18, metric 2
                    > via t3-3/2/0.0
10.255.14.171/32   *[OSPF/10] 00:05:18, metric 4
                    > via t3-3/2/0.0
10.255.14.179/32   *[OSPF/10] 00:05:18, metric 2
                    > via t3-3/2/0.0
224.0.0.5/32       *[OSPF/10] 20:25:55, metric 1

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30       [OSPF/10] 00:05:43, metric 1
                    > via so-0/2/2.0
10.255.14.173/32   *[OSPF/10] 00:05:43, metric 1
                    > via so-0/2/2.0
224.0.0.5/32       *[OSPF/10] 20:26:20, metric 1
```

show route protocol ospf detail

user@host> **show route protocol ospf detail**

```
VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
         OSPF   Preference:  10
                Nexthop: via so-0/2/2.0, selected
                State: <Int>
                Inactive reason: Route Preference
                Age: 6:25       Metric: 1
                Area: 0.0.0.0
                Task: VPN-AB-OSPF
```

```
                AS path: I
                Communities: Route-Type:0.0.0.0:1:0

...
```

show route protocol rip

```
user@host> show route protocol rip
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32   *[RIP/100] 20:24:34, metric 2
                    > to 10.39.1.22 via t3-0/2/2.0
224.0.0.9/32       *[RIP/100] 00:03:59, metric 1
```

show route protocol rip detail

```
user@host> show route protocol rip detail
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32 (1 entry, 1 announced)
        *RIP    Preference: 100
                Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
                State: <Active Int>
                Age: 20:25:02   Metric: 2
                Task: VPN-AB-RIPv2
                Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179
                AS path: I
                Route learned from 10.39.1.22 expires in 96 seconds
```

show route protocol ripng table inet6

```
user@host> show route protocol ripng table inet6
inet6.0: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::2/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::3/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::4/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::5/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::6/128        *[RIPng/100] 02:13:33, metric 2
                    > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
```

show route protocol static detail

```
user@host> show route protocol static detail
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
10.5.0.0/16 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
```

```
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I

10.10.0.0/16 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I

10.13.10.0/23 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Router, Next hop index: 324
                Address: 0x9274010
                Next-hop reference count: 27
                Next hop: 192.168.187.126 via fxp0.0, selected
                Session Id: 0x0
                State: <Active NoReadvrt Int Ext>
                Age: 7w3d 21:24:25
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: I
```

PART 4

Troubleshooting

CHAPTER 21

Routing Protocol Process Memory FAQs

Routing Protocol Process Memory FAQs Overview

Junos OS is based on the FreeBSD Unix operating system. The open source software is modified and hardened to operate in the device's specialized environment. For example, some executables have been deleted, while other utilities were de-emphasized. Additionally, certain software processes were added to enhance the routing functionality. The result of this transformation is the kernel, the heart of the Junos OS software.

The kernel is responsible for operating multiple processes that perform the actual functions of the device. Each process operates in its own protected memory space, while the communication among all the processes is still controlled by the kernel. This separation provides isolation between the processes, and resiliency in the event of a process failure. This is important in a core routing platform because a single process failure does not cause the entire device to cease functioning.

Some of the common software processes include the routing protocol process (rpd) that controls the device's protocols, the device control process (dcd) that controls the device's interfaces, the management process (mgd) that controls user access to the device, the chassis process (chassisd) that controls the device's properties itself, and the Packet Forwarding Engine process (pfed) that controls the communication between the device's Packet Forwarding Engine and the Routing Engine. The kernel also generates specialized processes as needed for additional functionality, such as SNMP, the Virtual Router Redundancy Protocol (VRRP), and Class of Service (CoS).

The routing protocol process is a software process within the Routing Engine software, which controls the routing protocols that run on the device. Its functionality includes all protocol messages, routing table updates, and implementation of routing policies.

The routing protocol process starts all configured routing protocols and handles all routing messages. It maintains one or more routing tables, which consolidate the routing information learned from all routing protocols. From this routing information, the routing protocol process determines the active routes to network destinations and installs these routes into the Routing Engine's forwarding table. Finally, it implements routing policy, which allows you to control the routing information that is transferred between the routing protocols and the routing table. Using routing policy, you can filter and limit the transfer of information as well as set properties associated with specific routes.

Related Documentation

- Routing Protocol Process Memory FAQs on page 582

Routing Protocol Process Memory FAQs

The following sections present the most frequently asked questions and answers related to the routing protocol process memory utilization, operation, interpretation of related command outputs, and troubleshooting the software process.

Frequently Asked Questions: Routing Protocol Process Memory

This section presents frequently asked questions and answers related to the memory usage of the routing protocol process.

Why does the routing protocol process use excessive memory?

The routing protocol process uses hundreds of megabytes of RAM in the Routing Engine to store information needed for the operation of routing and related protocols, such as BGP, OSPF, IS-IS, RSVP, LDP and MPLS. Such huge consumption of memory is common for the process, as the information it stores includes routes, next hops, interfaces, routing policies, labels, and label-switched paths (LSPs). Because access to the RAM memory is much faster than access to the hard disk, most of the routing protocol process information is stored in the RAM memory instead of using the hard disk space. This ensures that the performance of the routing protocol process is maximized.

How can I check the amount of memory the routing protocol process is using?

You can check routing protocol process memory usage by entering the **show system processes** and the **show task memory** Junos OS command-line interface (CLI) operational mode commands.

The **show system processes** command displays information about software processes that are running on the device and that have controlling terminals. The **show task memory** command displays memory utilization for routing protocol tasks on the Routing Engine.

You can check the routing protocol process memory usage by using the **show system processes** command with the **extensive** option. The **show task memory** command displays a report generated by the routing protocol process on its own memory usage. However, this report does not display all the memory used by the process. The value reported by the routing protocol process does not account for the memory used for the **TEXT** and **STACK** segments, or the memory used by the process's internal memory manager. Further, the Resident Set Size value includes shared library pages used by the routing protocol process.

For more information about checking the routing protocol process memory usage.

For more information, see the **show system processes** command and the **show task memory** command.

I just deleted a large number of routes from the routing protocol process. Why is it still using so much memory?

The **show system processes extensive** command displays a **RES** value measured in kilobytes. This value represents the amount of program memory resident in the physical memory. This is also known as RSS or Resident Set Size. The **RES** value includes shared library pages used by the process. Any amount of memory freed by the process might still be considered part of the **RES** value. Generally, the kernel delays the migrating of memory out of the **Inact** queue into the **Cache** or **Free** list unless there is a memory shortage. This can lead to large discrepancies between the values reported by the routing protocol process and the kernel, even after the routing protocol process has freed a large amount of memory.

Frequently Asked Questions: Interpreting Routing Protocol Process-Related Command Outputs

This section presents frequently asked questions and answers about the routing protocol process-related Junos OS command-line interface (CLI) command outputs that are used to display the memory usage of the routing protocol process.

How do I interpret memory numbers displayed in the show system processes extensive command output?

The **show system processes extensive** command displays exhaustive system process information about software processes that are running on the device and have controlling terminals. This command is equivalent to the UNIX **top** command. However, the UNIX **top** command shows real-time memory usage, with the memory values constantly changing, while the **show system processes extensive** command provides a snapshot of memory usage in a given moment.

To check overall CPU and memory usage, enter the **show system processes extensive** command. Refer to Table 19 on page 584 for information about the **show system processes extensive** commands output fields.

```
user@host> show system processes extensive
last pid:   544;  load averages:  0.00,  0.00,  0.00    18:30:33
37 processes:  1 running, 36 sleeping

Mem: 25M Active, 3968K Inact, 19M Wired, 184K Cache, 8346K Buf, 202M Free
Swap: 528M Total, 64K Used, 528M Free
  PID USERNAME PRI NICE SIZE    RES STATE    TIME   WCPU    CPU COMMAND
  544 root      30   0   604K   768K RUN      0:00  0.00%  0.00% top
    3 root      28   0     0K    12K psleep   0:00  0.00%  0.00% vmdaemon
    4 root      28   0     0K    12K update   0:03  0.00%  0.00% update
  528 aviva     18   0   660K   948K pause    0:00  0.00%  0.00% tcsh
  204 root      18   0   300K   544K pause    0:00  0.00%  0.00% csh
  131 root      18   0   332K   532K pause    0:00  0.00%  0.00% cron
  186 root      18   0   196K    68K pause    0:00  0.00%  0.00% watchdog
   27 root      10   0   512M 16288K mfsidl   0:00  0.00%  0.00% mount_mfs
    1 root      10   0   620K   344K wait     0:00  0.00%  0.00% init
  304 root       3   0   884K   900K ttyin    0:00  0.00%  0.00% bash
  200 root       3   0   180K   540K ttyin    0:00  0.00%  0.00% getty
  203 root       3   0   180K   540K ttyin    0:00  0.00%  0.00% getty
  202 root       3   0   180K   540K ttyin    0:00  0.00%  0.00% getty
  201 root       3   0   180K   540K ttyin    0:00  0.00%  0.00% getty
  194 root       2   0  2248K  1640K select   0:11  0.00%  0.00% rpd
  205 root       2   0   964K   800K select   0:12  0.00%  0.00% tnp.chassisd
```



```
189 root       2 -12   352K   740K select   0:03  0.00%  0.00% xntpd
114 root       2   0   296K   612K select   0:00  0.00%  0.00% amd
188 root       2   0   780K   600K select   0:00  0.00%  0.00% dcd
527 root       2   0   176K   580K select   0:00  0.00%  0.00% rlogind
195 root       2   0   212K   552K select   0:00  0.00%  0.00% inetd
187 root       2   0   192K   532K select   0:00  0.00%  0.00% tnetd
 83 root       2   0   188K   520K select   0:00  0.00%  0.00% syslogd
538 root       2   0  1324K   516K select   0:00  0.00%  0.00% mgd
 99 daemon     2   0   176K   492K select   0:00  0.00%  0.00% portmap
163 root       2   0   572K   420K select   0:00  0.00%  0.00% nsrexecd
192 root       2   0   560K   400K select   0:10  0.00%  0.00% snmpd
191 root       2   0  1284K   376K select   0:00  0.00%  0.00% mgd
537 aviva      2   0   636K   364K select   0:00  0.00%  0.00% cli
193 root       2   0   312K   204K select   0:07  0.00%  0.00% mib2d
  5 root       2   0     0K    12K pfesel   0:00  0.00%  0.00% if_pfe
  2 root     -18   0     0K    12K psleep   0:00  0.00%  0.00% pagedaemon
  0 root     -18   0     0K     0K sched    0:00  0.00%  0.00% swapper
```

Table 19 on page 584 describes the output fields that represent the memory values for the **show system processes extensive** command. Output fields are listed in the approximate order in which they appear.

Table 19: show system processes extensive Output Fields

Field Name	Field Description
Mem	Information about physical and virtual memory allocation.
Active	Memory allocated and actively used by the program.
Inact	Memory allocated but not recently used or memory freed by the programs. Inactive memory remains mapped in the address space of one or more processes and, therefore, counts toward the RSS value of those processes.
Wired	Memory that is not eligible to be swapped, usually used for in-kernel memory structures and/or memory physically locked by a process.
Cache	Memory that is not associated with any program and does not need to be swapped before being reused.
Buf	Size of memory buffer used to hold data recently called from the disk.
Free	Memory that is not associated with any programs. Memory freed by a process can become **Inactive**, **Cache**, or **Free**, depending on the method used by the process to free the memory.
Swap	Information about swap memory. • Total—Total memory available to be swapped to disk. • Used—Memory swapped to disk. • Free—Memory available for further swap.

The rest of the command output displays information about the memory usage of each process. The **SIZE** field indicates the size of the virtual address space, and the **RES** field indicates the amount of the program in physical memory, which is also known as RSS or Resident Set Size. For more information, see the **show system processes** command.

What is the difference between Active and Inact memory that is displayed by the show system processes extensive command?

When the system is under memory pressure, the pageout process reuses memory from the free, cache, inact and, if necessary, active pages. When the pageout process runs, it scans memory to see which pages are good candidates to be unmapped and freed up. Thus, the distinction between **Active** and **Inact** memory is only used by the pageout process to determine which pool of pages to free first at the time of a memory shortage.

The pageout process first scans the **Inact** list, and checks whether the pages on this list have been accessed since the time they have been listed here. The pages that have been accessed are moved from the **Inact** list to the **Active** list. On the other hand, pages that have not been accessed become prime candidates to be freed by the pageout process. If the pageout process cannot produce enough free pages from the **Inact** list, pages from the **Active** list get freed up.

Because the pageout process runs only when the system is under memory pressure, the pages on the **Inact** list remain untouched – even if they have not been accessed recently – when the amount of **Free** memory is adequate.

How do I interpret memory numbers displayed in the show task memory command output?

The **show task memory** command provides a comprehensive picture of the memory utilization for routing protocol tasks on the Routing Engine. The routing protocol process is the main task that uses Routing Engine memory.

To check routing process memory usage, enter the **show task memory** command. Refer to Table 20 on page 585 for information about the **show task memory** command output fields.

```
user@host> show task memory
Memory                 Size (kB)  %Available  When
  Currently In Use:        29417          3%  now
  Maximum Ever Used:       33882          4%  00/02/11 22:07:03
  Available:              756281        100%  now
```

Table 20 on page 585 describes the output fields for the **show task memory** command. Output fields are listed in the approximate order in which they appear.

Table 20: show task memory Output Fields

Field Name	Field Description
Memory Currently In Use	Memory currently in use. Dynamically allocated memory plus the **DATA** segment memory in kilobytes.
Memory Maximum Ever Used	Maximum memory ever used.
Memory Available	Memory currently available.

The **show task memory** command does not display all the memory used by the routing protocol process. This value does not account for the memory used for the **TEXT** and

STACK segments, or the memory used by the routing protocol process's internal memory manager.

Why is the Currently In Use value less than the RES value?

The **show task memory** command displays a **Currently In Use** value measured in kilobytes. This value represents the memory currently in use. It is the dynamically allocated memory plus the **DATA** segment memory. The **show system processes extensive** command displays a **RES** value measured in kilobytes. This value represents the amount of program memory resident in the physical memory. This is also known as RSS or Resident Set Size.

The **Currently In Use** value does not account for all of the memory that the routing protocol process uses. This value does not include the memory used for the **TEXT** and the **STACK** segments, and a small percentage of memory used by the routing protocol process's internal memory manager. Further, the **RES** value includes shared library pages used by the routing protocol process.

Any amount of memory freed by the routing protocol process might still be considered part of the **RES** value. Generally, the kernel delays the migrating of memory out of the **Inact** queue into the **Cache** or **Free** list unless there is a memory shortage. This can lead to large discrepancies between the **Currently In Use** value and the **RES** value.

Frequently Asked Questions: Routing Protocol Process Memory Swapping

This section presents frequently asked questions and answers related to the memory swapping of the routing protocol process from the Routing Engine memory to the hard disk memory.

How do I monitor swap activity?

When the system is under memory pressure, the pageout process reuses memory from the free, cache, inact and, if necessary, active pages. You can monitor the swap activity by viewing the syslog message reported by the kernel during periods of high pageout activity.

The syslog message appears as follows:

```
Mar  3 20:08:02 olympic /kernel: High pageout rate!! 277 pages/sec.
```

You can use the **vmstat -s** command to print the statistics for the swapout activity. The displayed statistics appear as follows:

```
0 swap pager pageouts
0 swap pager pages paged out
```

The **swap pager pageouts** is the number of pageout operations to the swap device, and the **swap pager pages paged out** is the number of pages paged out to the swap device.

Why does the system start swapping when I try to dump core using the request system core-dumps command?

The **request system core-dumps** command displays a list of system core files created when the device has failed. This command can be useful for diagnostic purposes. Each list item includes the file permissions, number of links, owner, group, size, modification date, path, and filename. You can use the **core-filename** option and the **core-file-info**, **brief**, and **detail** options to display more information about the specified core-dump files.

You can use the **request system core-dumps** command to perform a non-fatal core-dump without aborting the routing protocol process. To do this, the routing protocol process is forked, generating a second copy, and then aborted. This process can double the memory consumed by the two copies of the routing protocol processes, pushing the system into swap.

Why does the show system processes extensive command show that memory is swapped to disk although there is plenty of free memory?

Memory can remain swapped out indefinitely if it is not accessed again. Therefore, the **show system processes extensive** command shows that memory is swapped to disk even though there is plenty of free memory, and such a situation is not unusual.

Frequently Asked Questions: Troubleshooting the Routing Protocol Process

This section presents frequently asked questions and answers related to a shortage of memory and memory leakage by the routing protocol process.

What does the RPD_OS_MEMHIGH message mean?

The **RPD_OS_MEMHIGH** message is written into the system message file if the routing protocol process is running out of memory. This message alerts you that the routing protocol process is using the indicated amount and percentage of Routing Engine memory, which is considered excessive. This message is generated either because the routing protocol process is leaking memory or the use of system resources is excessive, perhaps because routing filters are misconfigured or the configured network topology is very complex.

When the memory utilization for the routing protocol process is using all available Routing Engine DRAM memory (Routing Engines with maximum 2 GB DRAM) or reaches the limit of 2 GB of memory (Routing Engines with 4 GB DRAM), a message of the following form is written every minute in the syslog message file:

```
RPD_OS_MEMHIGH: Using 188830 KB of memory, 100 percent of available
```

This message includes the amount, in kilobytes and/or the percentage, of the available memory in use.

This message should not appear under normal conditions, as any further memory allocations usually require a portion of existing memory to be written to swap. As a recommended solution, increase the amount of RAM in the Routing Engine. For more information, go to http://kb.juniper.net/InfoCenter/index?page=content&id=KB14186 .

What can I do when there is a memory shortage even after a swap?

It is not recommended for the system to operate in this state, notwithstanding the existence of swap. The protocols that run in the routing protocol process usually have a real-time requirement that cannot reliably withstand the latency of being swapped to hard disk. If the memory shortage has not resulted from a memory leak, then either a reduction in the memory usage or an upgrade to a higher memory-capacity Routing Engine is required.

How do I determine whether there is a memory leak in the routing protocol process?

Memory leaks are typically the result of a seemingly unbounded growth in the memory usage of a process as reported by the **show system processes extensive** command.

There are two classes of memory leaks that the routing protocol process can experience.

- The first class occurs when the allocated memory that is no longer in use is not freed. This class of leak can usually be fixed by taking several samples of the **show task memory detail** command over a period of time and comparing the deltas.
- The second class occurs when there is a late access to freed memory. If the access is not outside the mapped address space, the kernel backfills the accessed page with real memory. This backfill is done without the knowledge of the routing protocol process's internal memory allocator, which makes this class of leak much more difficult to resolve. If a memory leak of this class is suspected, writing the state of the system to a disk file (creating a core file) is suggested.

A large discrepancy between the **RES** value and the **Currently In Use** value might indicate a memory leak. However, large discrepancies can also occur for legitimate reasons. For example, the memory used for the **TEXT** and **STACK** segments or the memory used by the routing protocol process's internal memory manager might not be displayed. Further, the **RES** value includes shared library pages used by the process.

What is the task_timer?

The source of a routing protocol process memory leak can usually be identified by dumping the timers for each task. You can use the **show task *task-name*** command to display routing protocol tasks on the Routing Engine. Tasks can be baseline tasks performed regardless of the device's configuration, and other tasks that depend on the device configuration.

For more information, see the **show task** command.

Related Documentation

- Routing Protocol Process Memory FAQs Overview on page 581

PART 5

Index

Index

Symbols

V