



Configuring OSPFv3

This chapter describes how to configure Open Shortest Path First version 3 (OSPFv3) for IPv6 networks on the Cisco NX-OS device.

This chapter includes the following sections:

- [Information About OSPFv3, on page 1](#)
- [Prerequisites for OSPFv3, on page 13](#)
- [Guidelines and Limitations for OSPFv3, on page 13](#)
- [Default Settings, on page 13](#)
- [Configuring Basic OSPFv3, on page 14](#)
- [Configuring Advanced OSPFv3, on page 24](#)
- [Configuring Encryption and Authentication, on page 45](#)
- [Verifying the OSPFv3 Configuration, on page 57](#)
- [Monitoring OSPFv3, on page 58](#)
- [Configuration Examples for OSPFv3, on page 58](#)
- [Related Topics, on page 59](#)
- [Additional References, on page 59](#)

Information About OSPFv3

OSPFv3 is an IETF link-state protocol (see [Overview](#)). An OSPFv3 router sends a special message, called a hello packet, out each OSPF-enabled interface to discover other OSPFv3 neighbor routers. Once a neighbor is discovered, the two routers compare information in the Hello packet to determine if the routers have compatible configurations. The neighbor routers attempt to establish adjacency, which means that the routers synchronize their link-state databases to ensure that they have identical OSPFv3 routing information. Adjacent routers share link-state advertisements (LSAs) that include information about the operational state of each link, the cost of the link, and any other neighbor information. The routers then flood these received LSAs out every OSPF-enabled interface so that all OSPFv3 routers eventually have identical link-state databases. When all OSPFv3 routers have identical link-state databases, the network is converged (see the [Convergence](#) section). Each router then uses Dijkstra's Shortest Path First (SPF) algorithm to build its route table.

You can divide OSPFv3 networks into areas. Routers send most LSAs only within one area, which reduces the CPU and memory requirements for an OSPF-enabled router.

OSPFv3 supports IPv6. For information about OSPF for IPv4, see [Configuring OSPFv2](#).

Comparison of OSPFv3 and OSPFv2

Much of the OSPFv3 protocol is the same as in OSPFv2. OSPFv3 is described in RFC 2740.

The key differences between the OSPFv3 and OSPFv2 protocols are as follows:

- OSPFv3 expands on OSPFv2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses.
- LSAs in OSPFv3 are expressed as prefix and prefix length instead of address and mask.
- The router ID and area ID are 32-bit numbers with no relationship to IPv6 addresses.
- OSPFv3 uses link-local IPv6 addresses for neighbor discovery and other features.
- OSPFv3 can use the IPv6 authentication trailer (RFC 6506) or IPSec (RFC 4552) for authentication. However, Cisco NX-OS does not support RFC 6506 and provides only partial support for RFC 4552, beginning with Cisco NX-OS release 7.0(3)I3(1).
- OSPFv3 redefines LSA types.

Hello Packet

OSPFv3 routers periodically send Hello packets on every OSPF-enabled interface. The hello interval determines how frequently the router sends these Hello packets and is configured per interface. OSPFv3 uses Hello packets for the following tasks:

- Neighbor discovery
- Keepalives
- Bidirectional communications
- Designated router election (see the [Designated Routers](#) section)

The Hello packet contains information about the originating OSPFv3 interface and router, including the assigned OSPFv3 cost of the link, the hello interval, and optional capabilities of the originating router. An OSPFv3 interface that receives these Hello packets determines if the settings are compatible with the receiving interface settings. Compatible interfaces are considered neighbors and are added to the neighbor table (see the [Neighbors](#) section).

Hello packets also include a list of router IDs for the routers that the originating interface has communicated with. If the receiving interface sees its own router ID in this list, then bidirectional communication has been established between the two interfaces.

OSPFv3 uses Hello packets as a keepalive message to determine if a neighbor is still communicating. If a router does not receive a Hello packet by the configured dead interval (usually a multiple of the hello interval), then the neighbor is removed from the local neighbor table.

Neighbors

An OSPFv3 interface must have a compatible configuration with a remote interface before the two can be considered neighbors. The two OSPFv3 interfaces must match the following criteria:

- Hello interval

- Dead interval
- Area ID (see the [Areas](#) section)
- Authentication
- Optional capabilities

If there is a match, the information is entered into the neighbor table:

- Neighbor ID—The router ID of the neighbor router.
- Priority—Priority of the neighbor router. The priority is used for designated router election (see the [Designated Routers](#) section).
- State—Indication of whether the neighbor has just been heard from, is in the process of setting up bidirectional communications, is sharing the link-state information, or has achieved full adjacency.
- Dead time—Indication of how long since the last Hello packet was received from this neighbor.
- Link-local IPv6 Address—The link-local IPv6 address of the neighbor.
- Designated Router—Indication of whether the neighbor has been declared the designated router or backup designated router (see the [Designated Routers](#) section).
- Local interface—The local interface that received the Hello packet for this neighbor.

When the first Hello packet is received from a new neighbor, the neighbor is entered into the neighbor table in the initialization state. Once bidirectional communication is established, the neighbor state becomes two-way. ExStart and exchange states come next, as the two interfaces exchange their link-state database. Once this is all complete, the neighbor moves into the full state, which signifies full adjacency. If the neighbor fails to send any Hello packets in the dead interval, then the neighbor is moved to the down state and is no longer considered adjacent.

Adjacency

Not all neighbors establish adjacency. Depending on the network type and designated router establishment, some neighbors become fully adjacent and share LSAs with all their neighbors, while other neighbors do not. For more information, see the [Designated Routers](#) section.

Adjacency is established using Database Description packets, Link State Request packets, and Link State Update packets in OSPFv3. The Database Description packet includes the LSA headers from the link-state database of the neighbor (see the [Link-State Database](#) section). The local router compares these headers with its own link-state database and determines which LSAs are new or updated. The local router sends a Link State Request packet for each LSA that it needs new or updated information on. The neighbor responds with a Link State Update packet. This exchange continues until both routers have the same link-state information.

Designated Routers

Networks with multiple routers present a unique situation for OSPFv3. If every router floods the network with LSAs, the same link-state information is sent from multiple sources. Depending on the type of network, OSPFv3 might use a single router, the designated router (DR), to control the LSA floods and represent the network to the rest of the OSPFv3 area (see the [Areas](#) section). If the DR fails, OSPFv3 selects a backup designated router (BDR). If the DR fails, OSPFv3 uses the BDR.

Network types are as follows:

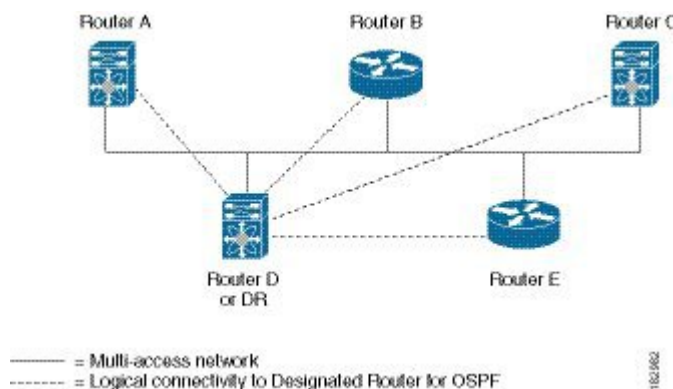
- Point-to-point—A network that exists only between two routers. All neighbors on a point-to-point network establish adjacency and there is no DR.
- Broadcast—A network with multiple routers that can communicate over a shared medium that allows broadcast traffic, such as Ethernet. OSPFv3 routers establish a DR and BDR that controls LSA flooding on the network. OSPFv3 uses the well-known IPv6 multicast addresses, FF02::5, and a MAC address of 0100.5300.0005 to communicate with neighbors.

The DR and BDR are selected based on the information in the Hello packet. When an interface sends a Hello packet, it sets the priority field and the DR and BDR field if it knows who the DR and BDR are. The routers follow an election procedure based on which routers declare themselves in the DR and BDR fields and the priority field in the Hello packet. As a final determinant, OSPFv3 chooses the highest router IDs as the DR and BDR.

All other routers establish adjacency with the DR and the BDR and use the IPv6 multicast address FF02::6 to send LSA updates to the DR and BDR. The following figure shows this adjacency relationship between all routers and the DR.

DRs are based on a router interface. A router might be the DR for one network and not for another network on a different interface

Figure 1: DR in Multi-Access Network



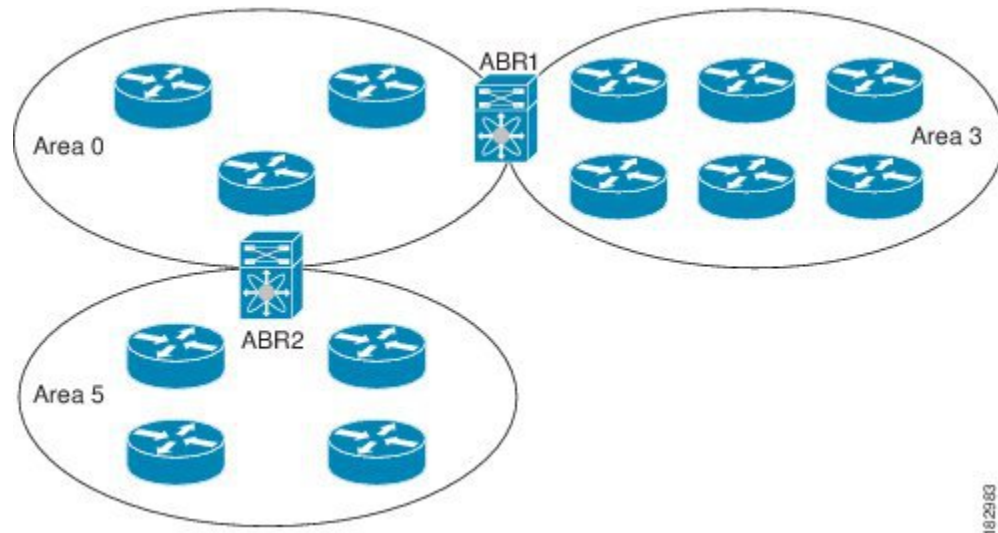
Areas

You can limit the CPU and memory requirements that OSPFv3 puts on the routers by dividing an OSPFv3 network into areas. An area is a logical division of routers and links within an OSPFv3 domain that creates separate subdomains. LSA flooding is contained within an area, and the link-state database is limited to links within the area. You can assign an area ID to the interfaces within the defined area. The Area ID is a 32-bit value that can be expressed as a number or in dotted decimal notation, such as 10.2.3.1.

Cisco NX-OS always displays the area in dotted decimal notation.

If you define more than one area in an OSPFv3 network, you must also define the backbone area, which has the reserved area ID of 0. If you have more than one area, then one or more routers become area border routers (ABRs). An ABR connects to both the backbone area and at least one other defined area (see the following figure).

Figure 2: OSPFv3 Areas



The ABR has a separate link-state database for each area which it connects to. The ABR sends Inter-Area Prefix (type 3) LSAs (see the [Route Summarization](#) section) from one connected area to the backbone area. The backbone area sends summarized information about one area to another area. In Figure **OSPFv3 Areas**, Area 0 sends summarized information about Area 5 to Area 3.

OSPFv3 defines one other router type: the autonomous system boundary router (ASBR). This router connects an OSPFv3 area to another autonomous system. An autonomous system is a network controlled by a single technical administration entity. OSPFv3 can redistribute its routing information into another autonomous system or receive redistributed routes from another autonomous system. For more information, see the [Advanced Features](#) section.

Link-State Advertisement

OSPFv3 uses link-state advertisements (LSAs) to build its routing table.

LSA Types

Following table shows the LSA types supported by Cisco NX-OS.

Table 1: LSA Types

Name	Name	Description
1	Router LSA	LSA sent by every router. This LSA includes the state and cost of all links but does not include prefix information. Router LSAs trigger an SPF recalculation. Router LSAs are Designated Routers flooded to the local OSPFv3 area.

Name	Name	Description
2	Network LSA	LSA sent by the DR. This LSA lists all routers in the multi-access network but does not include prefix information. Network LSAs trigger an SPF recalculation. See the Designated Routers section.
3	Inter-Area Prefix LSA	LSA sent by the area border router to an external area for each destination in local area. This LSA includes the link cost from the border router to the local destination. See the Areas section.
4	Inter-Area Router LSA	LSA sent by the area border router to an external area. This LSA advertises the link cost to the ASBR only. See the Areas section.
5	AS External LSA	LSA generated by the ASBR. This LSA includes the link cost to an external autonomous system destination. AS External LSAs are flooded throughout the autonomous system. See the Areas section.
7	Type-7 LSA	LSA generated by the ASBR within an NSSA. This LSA includes the link cost to an external autonomous system destination. Type-7 LSAs are flooded only within the local NSSA. See the Areas section.
8	Link LSA	LSA sent by every router, using a link-local flooding scope (see the Flooding and LSA Group Pacing section). This LSA includes the link-local address and IPv6 prefixes for this link.
9	Intra-Area Prefix LSA	LSA sent by every router. This LSA includes any prefix or link state changes. Intra-Area Prefix LSAs are flooded to the local OSPFv3 area. This LSA does not trigger an SPF recalculation.

Name	Name	Description
11	Grace LSAs	LSA sent by a restarting router, using a link-local flooding scope. This LSA is used for a graceful restart of OSPFv3. See the High Availability and Graceful Restart section.

Link Cost

Each OSPFv3 interface is assigned a link cost. The cost is an arbitrary number. By default, Cisco NX-OS assigns a cost that is the configured reference bandwidth divided by the interface bandwidth. By default, the reference bandwidth is 40 Gb/s. The link cost is carried in the LSA updates for each link.

Flooding and LSA Group Pacing

OSPFv3 floods LSA updates to different sections of the network, depending on the LSA type. OSPFv3 uses the following flooding scopes:

- Link-local—LSA is flooded only on the local link. Used for Link LSAs and Grace LSAs.
- Area-local—LSA is flooded throughout a single OSPF area only. Used for Router LSAs, Network LSAs, Inter-Area-Prefix LSAs, Inter-Area-Router LSAs, and Intra-Area-Prefix LSAs.
- AS scope—LSA is flooded throughout the routing domain. An AS scope is used for AS External LSAs.

LSA flooding guarantees that all routers in the network have identical routing information. LSA flooding depends on the OSPFv3 area configuration (see the [Areas](#) section). The LSAs are flooded based on the link-state refresh time (every 30 minutes by default). Each LSA has its own link-state refresh time.

You can control the flooding rate of LSA updates in your network by using the LSA group pacing feature. LSA group pacing can reduce high CPU or buffer utilization. This feature groups LSAs with similar link-state refresh times to allow OSPFv3 to pack multiple LSAs into an OSPFv3 Update message.

By default, LSAs with link-state refresh times within 10 seconds of each other are grouped together. You should lower this value for large link-state databases or raise it for smaller databases to optimize the OSPFv3 load on your network.

Link-State Database

Each router maintains a link-state database for the OSPFv3 network. This database contains all the collected LSAs and includes information on all the routes through the network. OSPFv3 uses this information to calculate the best path to each destination and populates the routing table with these best paths.

LSAs are removed from the link-state database if no LSA update has been received within a set interval, called the MaxAge. Routers flood a repeat of the LSA every 30 minutes to prevent accurate link-state information from being aged out. Cisco NX-OS supports the LSA grouping feature to prevent all LSAs from refreshing at the same time. For more information, see the [Flooding and LSA Group Pacing](#) section.

Multi-Area Adjacency

OSPFv3 multi-area adjacency allows you to configure a link on the primary interface that is in more than one area. This link becomes the preferred intra-area link in those areas. Multi-area adjacency establishes a point-to-point unnumbered link in an OSPFv3 area that provides a topological path for that area. The primary adjacency uses the link to advertise an unnumbered point-to-point link in the Router LSA for the corresponding area when the neighbor state is full.

The multi-area interface exists as a logical construct over an existing primary interface for OSPF; however, the neighbor state on the primary interface is independent of the multi-area interface. The multi-area interface establishes a neighbor relationship with the corresponding multi-area interface on the neighboring router. See the [Configuring Multi-Area Adjacency, on page 30](#) section for more information.

OSPFv3 and the IPv6 Unicast RIB

OSPFv3 runs the Dijkstra shortest path first algorithm on the link-state database. This algorithm selects the best path to each destination based on the sum of all the link costs for each link in the path. The shortest path for each destination is then put in the OSPFv3 route table. When the OSPFv3 network is converged, this route table feeds into the IPv6 unicast RIB. OSPFv3 communicates with the IPv6 unicast RIB to do the following:

- Add or remove routes
- Handle route redistribution from other protocols
- Provide convergence updates to remove stale OSPFv3 routes and for stub router advertisements (see the [Multiple OSPFv3 Instances](#) section.)

OSPFv3 also runs a modified Dijkstra algorithm for fast recalculation for Inter-Area Prefix, Inter-Area Router, AS-External, type-7, and Intra-Area Prefix (type 3, 4, 5, 7, 8) LSA changes

Address Family Support

Cisco NX-OS supports multiple address families, such as unicast IPv6 and multicast IPv6. OSPFv3 features that are specific to an address family are as follows:

- Default routes
- Route summarization
- Route redistribution
- Filter lists for border routers
- SPF optimization

Use the **address-family ipv6 unicast** command to enter the IPv6 unicast address family configuration mode when configuring these features.

Authentication and Encryption

You can configure authentication on OSPFv3 messages to prevent unauthorized or invalid routing updates in your network.

RFC 4552 provides authentication to OSPFv3 using an IPv6 Authentication Header (AH) or Encapsulating Security Payload (ESP) extension header. Beginning with Cisco NX-OS 7.0(3)I3(1), Cisco NX-OS supports RFC 4552 by using the IPv6 AH header to authenticate OSPFv3 packets.

Cisco NX-OS supports the IP Security (IPSec) authentication method and the Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1) algorithm to authenticate OSPFv3 packets. OSPFv3 IPSec authentication supports static keys using commands.

Cisco NX-OS also supports the IPSec ESP method for both encryption and authentication of OSPFv3 messages. Encryption supports AES or 3DES algorithm for ESP encryption and SHA-1 or NULL for ESP authentication.

Beginning with Cisco NX-OS Release 10.4(1)F, Cisco NX-OS supports configuring encryption or authentication algorithms and keys using the keychain option.

You can configure IPSec encryption or authentication for an OSPFv3 process, an area, and/or an interface. The authentication configuration is inherited from process to area to interface level. If authentication is configured at all three levels, the interface configuration takes precedence over an area configurations, and an area configuration takes precedence over the process level.

Advanced Features

Cisco NX-OS supports advanced OSPFv3 features that enhance the usability and scalability of OSPFv3 in the network.

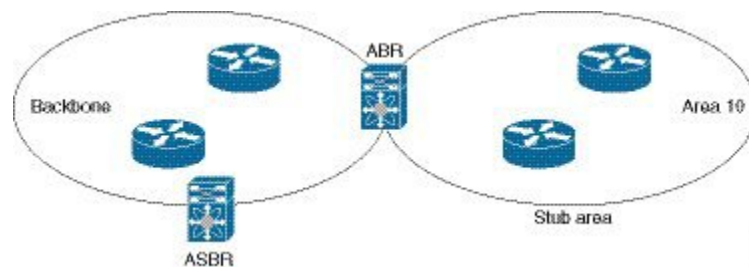
Stub Area

You can limit the amount of external routing information that floods an area by making it a stub area. A stub area is an area that does not allow AS External (type 5) LSAs (see the [Link-State Advertisement](#) section). These LSAs are usually flooded throughout the local autonomous system to propagate external route information. Stub areas have the following requirements:

- All routers in the stub area are stub routers. See the [Stub Routing](#) section.
- No ASBR routers exist in the stub area.
- You cannot configure virtual links in the stub area.

Following figure shows an example an OSPFv3 autonomous system where all routers in area 0.0.0.10 have to go through the ABR to reach external autonomous systems. Area 0.0.0.10 can be configured as a stub area.

Figure 3: Stub Area



Stub areas use a default route for all traffic that needs to go through the backbone area to the external autonomous system. The default route is an Inter-Area-Prefix LSA with the prefix length set to 0 for IPv6.

Not-So-Stubby Area

A Not-So-Stubby Area (NSSA) is similar to the stub area, except that an NSSA allows you to import autonomous system external routes within an NSSA using redistribution. The NSSA ASBR redistributes these routes and generates type-7 LSAs that it floods throughout the NSSA. You can optionally configure the ABR that connects the NSSA to other areas to translate this type-7 LSA to AS External (type 5) LSAs. The ABR then floods these AS External LSAs throughout the OSPFv3 autonomous system. Summarization and filtering are supported during the translation. See the [Link-State Advertisement](#) section for details on type-7 LSAs.

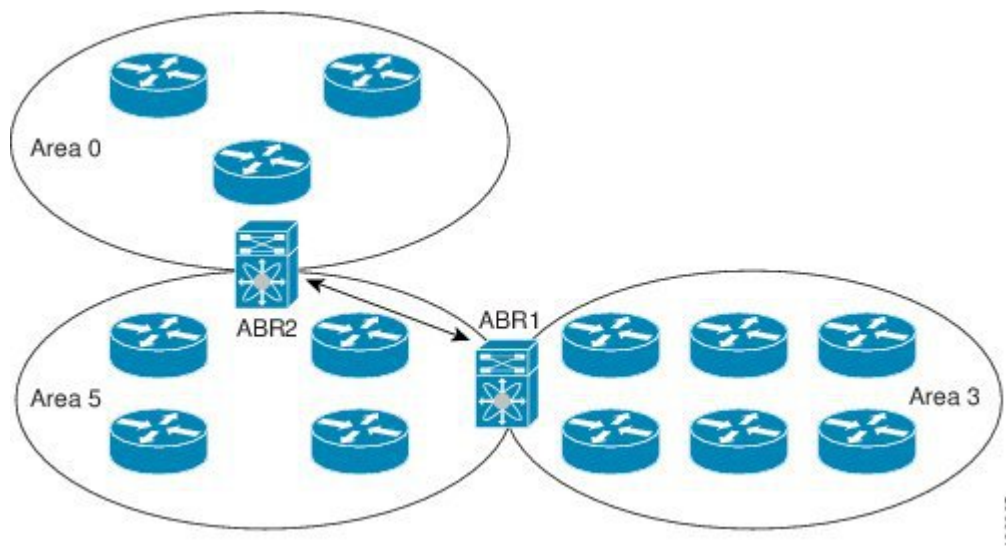
You can, for example, use NSSA to simplify administration if you are connecting a central site using OSPFv3 to a remote site that is using a different routing protocol. Before NSSA, the connection between the corporate site border router and a remote router could not be run as an OSPFv3 stub area because routes for the remote site could not be redistributed into a stub area. With NSSA, you can extend OSPFv3 to cover the remote connection by defining the area between the corporate router and remote router as an NSSA (see the [Configuring NSSA, on page 27](#) section).

The backbone Area 0 cannot be an NSSA.

Virtual Links

Virtual links allow you to connect an OSPFv3 area ABR to a backbone area ABR when a direct physical connection is not available. Following figure shows a virtual link that connects Area 3 to the backbone area through Area 5.

Figure 4: Virtual Links



You can also use virtual links to temporarily recover from a partitioned area, which occurs when a link within the area fails, isolating part of the area from reaching the designated ABR to the backbone area.

Route Redistribution

OSPFv3 can learn routes from other routing protocols by using route redistribution. See the [Route Redistribution](#) section. You configure OSPFv3 to assign a link cost for these redistributed routes or a default link cost for all redistributed routes.

Route redistribution uses route maps to control which external routes are redistributed. You must configure a route map with the redistribution to control which routes are passed into OSPFv2. A route map allows you to filter routes based on attributes such as the destination, origination protocol, route type, route tag, and so on. You can use route maps to modify parameters in the AS External (type 5) and NSSA External (type 7) LSAs before these external routes are advertised in the local OSPFv3 autonomous system. For more information, see [Configuring Route Policy Manager](#).

Route Summarization

Because OSPFv3 shares all learned routes with every OSPF-enabled router, you might want to use route summarization to reduce the number of unique routes that are flooded to every OSPF-enabled router. Route summarization simplifies route tables by replacing more-specific addresses with an address that represents all the specific addresses. For example, you can replace 2010:11:22:0:1000::1 and 2010:11:22:0:2000:679:1 with one summary address, 2010:11:22::/32.

Typically, you would summarize at the boundaries of area border routers (ABRs). Although you could configure summarization between any two areas, it is better to summarize in the direction of the backbone so that the backbone receives all the aggregate addresses and injects them, already summarized, into other areas. The two types of summarization are as follows:

- Inter-area route summarization
- External route summarization

You configure inter-area route summarization on ABRs, summarizing routes between areas in the autonomous system. To take advantage of summarization, assign network numbers in areas in a contiguous way to be able to lump these addresses into one range.

External route summarization is specific to external routes that are injected into OSPFv3 using route redistribution. You should make sure that external ranges that are being summarized are contiguous. Summarizing overlapping ranges from two different routers could cause packets to be sent to the wrong destination. Configure external route summarization on ASBRs that are redistributing routes into OSPF.

When you configure a summary address, Cisco NX-OS automatically configures a discard route for the summary address to prevent routing black holes and route loops.

High Availability and Graceful Restart

Cisco NX-OS supports high-availability. If a Cisco NX-OS system experiences a cold reboot, the network stops forwarding traffic to the system and removes the system from the network topology. In this scenario, OSPFv3 experiences a stateless restart, and removes all neighbor adjacencies on the local system. Cisco NX-OS applies the startup configuration and OSPFv3 rediscovers the neighbors and establishes the adjacencies again.

OSPFv3 automatically restarts if the process experiences problems. After the restart, OSPFv3 initiates a graceful restart so that the platform is not taken out of the network topology. If you manually restart OSPF, it performs a graceful restart, which is similar to a stateful switchover. The running configuration is applied in both cases.

A graceful restart, or nonstop forwarding (NSF), allows OSPFv3 to remain in the data forwarding path through a process restart. When OSPFv3 needs to restart, it first sends a link-local Grace (type 11) LSA. This restarting OSPFv3 platform is called NSF capable.

The Grace LSA includes a grace period, which is a specified time that the neighbor OSPFv3 interfaces hold onto the LSAs from the restarting OSPFv3 interface. (Typically, OSPFv3 tears down the adjacency and discards all LSAs from a down or restarting OSPFv3 interface.) The participating neighbors, which are called

NSF helpers, keep all LSAs that originate from the restarting OSPFv3 interface as if the interface were still adjacent.

When the restarting OSPFv3 interface is operational again, it rediscovers its neighbors, establishes adjacency, and starts sending its LSA updates again. At this point, the NSF helpers recognize that graceful restart has finished.



Note If the restarting OSPFv3 interface does not come back up before the end of the grace period, or if the network experiences a topology change, the OSPFv3 neighbors tear down adjacency with the restarting OSPFv3 and treat it as a normal OSPFv3 restart.



Note You must enable graceful restart to support an in-service software upgrade (ISSU) for OSPFv3. If you disable graceful restart, Cisco NX-OS issues a warning that ISSU cannot be supported with this configuration.

Multiple OSPFv3 Instances

Cisco NX-OS supports multiple instances of the OSPFv3 protocol. By default, every instance uses the same system router ID. You must manually configure the router ID for each instance if the instances are in the same OSPFv3 autonomous system.

The OSPFv3 header includes an instance ID field to identify that OSPFv3 packet for a particular OSPFv3 instance. You can assign the OSPFv3 instance. The interface drops all OSPFv3 packets that do not have a matching OSPFv3 instance ID in the packet header.

Cisco NX-OS allows only one OSPFv3 instance on an interface.

SPF Optimization

Cisco NX-OS optimizes the SPF algorithm in the following ways:

- Partial SPF for Network (type 2) LSAs, Inter-Area Prefix (type 3) LSAs, and AS External (type 5) LSAs—When there is a change on any of these LSAs, Cisco NX-OS performs a faster partial calculation rather than running the whole SPF calculation.
- SPF timers—You can configure different timers for controlling SPF calculations. These timers include exponential backoff for subsequent SPF calculations. The exponential backoff limits the CPU load of multiple SPF calculations.

BFD

This feature supports bidirectional forwarding detection (BFD). BFD is a detection protocol designed to provide fast forwarding-path failure detection times. BFD provides subsecond failure detection between two adjacent devices and can be less CPU-intensive than protocol hello messages because some of the BFD load can be distributed onto the data plane on supported modules.

Virtualization Support

OSPFv3 supports virtual routing and forwarding (VRF) instances.

Prerequisites for OSPFv3

OSPFv3 has the following prerequisites:

- You must be familiar with routing fundamentals to configure OSPFv3.
- You must be logged on to the switch.
- You have configured at least one interface for IPv6 that is capable of communicating with a remote OSPFv3 neighbor.
- You have installed the Enterprise Services license.
- You have completed the OSPFv3 network strategy and planning for your network. For example, you must decide whether multiple areas are required.
- You have enabled OSPF (see the [Enabling OSPFv3, on page 14](#) section).
- You have installed the Advanced Services license.
- You are familiar with IPv6 addressing and basic configuration. See [Configuring IPv6](#) for information on IPv6 routing and addressing.

Guidelines and Limitations for OSPFv3

OSPFv3 has the following configuration guidelines and limitations:

- Cisco NX-OS displays areas in dotted decimal notation regardless of whether you enter the area in decimal or dotted decimal notation.
- If you configure OSPFv3 in a virtual port channel (vPC) environment, use the following timer commands in router configuration mode on the core switch to ensure fast OSPF convergence when a vPC peer link is shut down:

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```
- Beginning with Cisco NX-OS Release 10.4(1)F, the keychain support is provided for OSPFv3 encryption and authentication commands on the Cisco NX-OS switches.

Default Settings

Following table lists the default settings for OSPFv3 parameters:

Table 2: Default OSPFv3 Parameters

Parameters	Default
Hello interval	10 seconds
Dead interval	40 seconds

Parameters	Default
Graceful restart grace period	60 seconds
Graceful restart notify period	15 seconds
OSPFv3 feature	Disabled
Stub router advertisement announce time	600 seconds
Reference bandwidth for link cost calculation	40 Gb/s
LSA minimal arrival time	1000 milliseconds
LSA group pacing	10 seconds
SPF calculation initial delay time	0 milliseconds
SPF calculation hold time	5000 milliseconds
SPF calculation initial delay time	0 milliseconds

Configuring Basic OSPFv3

Configure OSPFv3 after you have designed your OSPFv3 network.

Enabling OSPFv3

You must enable OSPFv3 before you can configure OSPFv3.

SUMMARY STEPS

1. **configure terminal**
2. **feature ospfv3**
3. (Optional) **show feature**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	feature ospfv3 Example: <code>switch(config)# feature ospfv3</code>	Enables OSPFv3.
Step 3	(Optional) show feature Example: <code>switch(config)# show feature</code>	Displays enabled and disabled features.
Step 4	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	Saves this configuration change.

Example

To disable the OSPFv3 feature and remove all associated configuration, use the following command in configuration mode.

Command	Purpose
no feature ospfv3 Example: <code>switch(config)# no feature ospfv3</code>	Disables the OSPFv3 feature and removes all associated configuration.

Creating an OSPFv3 Instance

The first step in configuring OSPFv3 is to create an instance or OSPFv3 instance. You assign a unique instance tag for this OSPFv3 instance. The instance tag can be any string. For each OSPFv3 instance, you can also configure the following optional parameters:

- Router ID—Configures the router ID for this OSPFv3 instance. If you do not use this parameter, the router ID selection algorithm is used. For more information, see the [Router IDs](#) section.
- Administrative distance—Rates the trustworthiness of a routing information source. For more information, see the [Administrative Distance](#) section.
- Log adjacency changes—Creates a system message whenever an OSPFv3 neighbor changes its state.
- Maximum paths—Sets the maximum number of equal paths that OSPFv3 installs in the route table for a particular destination. Use this parameter for load balancing between multiple paths.
- Reference bandwidth—Controls the calculated OSPFv3 cost metric for a network. The calculated cost is the reference bandwidth divided by the interface bandwidth. You can override the calculated cost by assigning a link cost when a network is added to the OSPFv3 instance. For more information, see the [Configuring Networks in OSPFv3, on page 18](#) section.

For more information about OSPFv3 instance parameters, see the [Configuring Advanced OSPFv3](#) section.

Before you begin

You must enable OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

Ensure that the OSPFv3 instance tag that you plan on using is not already in use on this router.

Use the show **ospfv3 instance-tag** command to verify that the instance tag is not in use.

OSPFv3 must be able to obtain a router identifier (for example, a configured loopback address) or you must configure the router ID option.

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. (Optional) **router-id ip-address**
4. (Optional) **show ipv6 ospfv3 instance-tag**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS**Procedure**

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	(Optional) router-id ip-address Example: <pre>switch(config-router)# router-id 192.0.2.1</pre>	Configures the OSPFv3 router ID. This ID uses the dotted decimal notation and identifies this OSPFv3 instance and must exist on a configured interface in the system.
Step 4	(Optional) show ipv6 ospfv3 instance-tag Example: <pre>switch(config-router)# show ipv6 ospfv3 201</pre>	Displays OSPFv3 information.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Saves this configuration change.

Example

To remove the OSPFv3 instance and all associated configuration, use the following command in configuration mode:

Command	Purpose
no router ospfv3 instance-tag Example: switch(config)# no router ospfv3 201	Deletes the OSPFv3 instance and all associated configuration.



Note This command does not remove OSPF configuration in interface mode. You must manually remove any OSPFv3 commands configured in interface mode.

You can configure the following optional parameters for OSPFv3 in router configuration mode:

Command	Purpose
log-adjacency-changes [detail] Example: switch(config-router)# log-adjacency-changes	Generates a system message whenever a neighbor changes state.
passive-interface default Example: switch(config-router)# passive-interface default	Suppresses routing updates on all interfaces. This command is overridden by the VRF or interface command mode configuration.

You can configure the following optional parameters for OSPFv3 in address family configuration mode:

Command	Purpose
distance number Example: switch(config-router-af)# distance 25	Configures the administrative distance for this OSPFv3 instance. The range is from 1 to 255. The default is 110.
maximum-paths paths Example: switch(config-router-af)# maximum-paths 4	Suppresses routing updates on all interfaces. This command is overridden by the VRF or interface command mode configuration.

This example shows how to create an OSPFv3 instance:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# copy running-config startup-config
```

Configuring Networks in OSPFv3

You can configure a network to OSPFv3 by associating it through the interface that the router uses to connect to that network (see the [Neighbors](#) section). You can add all networks to the default backbone area (Area 0), or you can create new areas using any decimal number or an IP address.



Note All areas must connect to the backbone area either directly or through a virtual link.



Note OSPFv3 is not enabled on an interface until you configure a valid IPv6 address for that interface.

Before you begin

You must enable OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **ipv6 address** *ipv6-prefix/length*
4. **ipv6 router ospfv3** *instance-tag area area-id* [**secondaries none**]
5. (Optional) **show ipv6 ospfv3** *instance-tag interface interface-type slot/port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode
Step 2	interface <i>interface-type slot/port</i> Example: <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	Enters interface configuration mode.
Step 3	ipv6 address <i>ipv6-prefix/length</i> Example: <pre>switch(config-if)# ipv6 address 2001:0DB8::1/48</pre>	Assigns an IPv6 address to this interface.
Step 4	ipv6 router ospfv3 <i>instance-tag area area-id</i> [secondaries none]	Adds the interface to the OSPFv3 instance and area.

	Command or Action	Purpose
	Example: <pre>switch(config-if)# ipv6 router ospfv3 201 area 0</pre>	
Step 5	(Optional) show ipv6 ospfv3 instance-tag interface interface-type slot/port Example: <pre>switch(config-if)# show ipv6 ospfv3 201 interface ethernet 1/2</pre>	Displays OSPFv3 information.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Saves this configuration change.

Example

You can configure the following optional parameters for OSPFv3 in interface configuration mode:

Command	Purpose
ospfv3 cost number Example: <pre>switch(config-if)# ospfv3 cost 25</pre>	Configures the OSPFv3 cost metric for this interface. The default is to calculate a cost metric, based on the reference bandwidth and interface bandwidth. The range is from 1 to 65535.
ospfv3 dead-interval seconds Example: <pre>switch(config-if)# ospfv3 dead-interval 50</pre>	Configures the OSPFv3 dead interval, in seconds. The range is from 1 to 65535. The default is four times the hello interval, in seconds.
ospfv3 hello-interval seconds Example: <pre>switch(config-if)# ospfv3 hello-interval 25</pre>	Configures the OSPFv3 hello interval, in seconds. The range is from 1 to 65535. The default is 10 seconds.
ospfv3 instance instance Example: <pre>switch(config-if)# ospfv3 instance 25</pre>	Configures the OSPFv3 instance ID. The range is from 0 to 255. The default is 0. The instance ID is link-local in scope.
ospfv3 mtu-ignore Example: <pre>switch(config-if)# ospfv3 mtu-ignore</pre>	Configures OSPFv3 to ignore any IP maximum transmission unit (MTU) mismatch with a neighbor. The default is to not establish adjacency if the neighbor MTU does not match the local interface MTU.
ospfv3 network{ broadcast point-point } Example: <pre>switch(config-if)# ospfv3 network broadcast</pre>	Sets the OSPFv3 network type.

Command	Purpose
[default no] ospfv3 passive-interface Example: <pre>switch(config-if)# ospfv3 passive-interface</pre>	Suppresses routing updates on the interface. This command overrides the router or VRF command mode configuration. The default option removes this interface mode command and reverts to the router or VRF configuration, if present.
ospfv3 priority number Example: <pre>switch(config-if)# ospfv3 priority 25</pre>	Configures the OSPFv3 priority, used to determine the DR for an area. The range is from 0 to 255. The default is 1. See the Designated Routers section.
ospfv3 shutdown Example: <pre>switch(config-if)# ospfv3 shutdown</pre>	Shuts down the OSPFv3 instance on this interface.

This example shows how to add a network area 0.0.0.10 in OSPFv3 instance 201:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/48
switch(config-if)# ipv6 ospfv3 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

Configuring OSPFv3 IPsec Authentication

You can configure OSPFv3 IP security (IPsec) authentication for a process, an area, and/or an interface.

The authentication configuration is inherited from process to area to interface level. If authentication is configured at all three levels, the interface configuration takes precedence over the process and area configurations.

Before you begin

Ensure that you have enabled OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature imp**
3. **router ospfv3 instance-tag**
4. **exit**
5. **authentication ipsec spi spi auth [0 | 3 | 7] key**
- 6.
7. (Optional) **show ospfv3 process**
8. (Optional) **show ospfv3 interface interface-type slot/port**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action		Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#		Enters global configuration mode.
Step 2	[no] feature imp Example: switch(config)# feature imp		Enables the Internet messaging program (IMP), which is required for OSPFv3 authentication.
Step 3	router ospfv3 instance-tag Example: switch(config)# router ospfv3 100 switch(config-router)#		Creates a new OSPFv3 instance with the configured instance tag.
Step 4	exit Example: switch(config-router)# exit switch(config)#		Exits OSPFv3 router configuration mode.
Step 5	authentication ipsec spi spi auth [0 3 7] key Example: switch(config)# authentication ipsec spi 475 md5 111111111111111111112222222222222222		Configures OSPFv3 IPsec authentication at the process (or VRF) level. The spi argument specifies the security parameter index (SPI). The range is from 256 to 4294967295. The auth argument specifies the type of authentication. The supported values are md5 or sha1. 0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco type 7 encrypted. If the cleartext option (0) is used, the key argument must be 32 characters long for md5 or 40 characters long for sha1.
Step 6	Option	Description	
	Command	Purpose	
	area area authentication ipsec spi spi auth [0 3 7] key Example: switch(config)# area 0 authenticationipsec spi 475 md5 111111111111111111112222222222222222	Configures OSPFv3 IPsec authentication at the area level. The spi argument specifies the	

Command or Action		Purpose
Option	Description	
	security parameter index (SPI). The range is from 256 to 4294967295. The auth argument specifies the type of authentication. The supported values are md5 or sha1. 0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco type 7 encrypted. If the cleartext option (0) is used, the key argument must be 32 characters long for md5 or 40 characters long for sha1. Note Use the area authentication disable command to disable OSPFv3 IPsec authentication at the area level.	
interface <i>interface-type slot/port</i> ospfv3 authentication ipsec spi spi auth [0 3 7] key Example: <pre>switch(config)# interface ethernet 1/1 switch(config-if)# ospfv3 authentication ipsec spi 475 md5 11111111111111112222222222222222</pre>	Configures OSPFv3 IPsec authentication for the specified interface. The spi argument specifies the security parameter index (SPI). The	

	Command or Action		Purpose
	Option	Description	
		range is from 256 to 4294967295. The auth argument specifies the type of authentication. The supported values are md5 or sha1. 0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco type 7 encrypted. If the cleartext option (0) is used, the key argument must be 32 characters long for md5 or 40 characters long for sha1. Note Use the ospfv3 authentication disable command to disable OSPFv3 IPsec authentication for the specified interface.	
Step 7	(Optional) show ospfv3 process Example: <pre>switch(config)# show ospfv3 100</pre>		Displays the OSPFv3 authentication configuration at the process level.
Step 8	(Optional) show ospfv3 interface interface-type slot/port Example: <pre>switch(config)# show ospfv3 interface ethernet 1/1</pre>		Displays the OSPFv3 authentication configuration at the interface level.

	Command or Action	Purpose
Step 9	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Saves this configuration change.

Configuring Advanced OSPFv3

Configure OSPFv3 after you have designed your OSPFv3 network.

Configuring Filter Lists for Border Routers

You can separate your OSPFv3 domain into a series of areas that contain related networks. All areas must connect to the backbone area through an area border router (ABR). OSPFv3 domains can connect to external domains as well through an autonomous system border router (ASBR). See the [Areas](#) section.

ABRs have the following optional configuration parameters:

- **Area range**—Configures route summarization between areas. For more information, see the [Configuring Route Summarization, on page 37](#) section.
- **Filter list**—Filters the Inter-Area Prefix (type 3) LSAs on an ABR that are allowed in from an external area.

ASBRs also support filter lists.

Before you begin

Create the route map that the filter list uses to filter IP prefixes in incoming or outgoing Inter-Area Prefix (type 3) LSAs. See [Configuring Route Policy Manager](#).

You must enable OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 *instance-tag***
3. **address-family ipv6 unicast**
4. **area *area-id* filter-list route-map *map-name* { in | out }**
5. (Optional) **show ipv6 ospfv3 policy statistics area *id* filter-list { in | out }**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: switch(config)# router ospfv3 201 switch(config-router)#	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	address-family ipv6 unicast Example: switch(config-router)# address-family ipv6 unicast switch(config-router-af)#	Enters IPv6 unicast address family mode.
Step 4	area area-id filter-list route-map map-name { in out } Example: switch(config-router-af)# area 0.0.0.10 filter-list route-map FilterLSAs in	Filters incoming or outgoing Inter-Area Prefix (type 3) LSAs on an ABR.
Step 5	(Optional) show ipv6 ospfv3 policy statistics area id filter-list { in out } Example: switch(config-if)# show ipv6 ospfv3 policy statistics area 0.0.0.10 filter-list in	Displays OSPFv3 policy information.
Step 6	(Optional) copy running-config startup-config Example: switch(config-router)# copy running-config startup-config	Saves this configuration change.

Example

This example shows how to enable graceful restart if it has been disabled:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router-af)# copy running-config startup-config
```

Configuring Stub Areas

You can configure a stub area for part of an OSPFv3 domain where external traffic is not necessary. Stub areas block AS External (type 5) LSAs, limiting unnecessary routing to and from selected networks. See the [Stub Area](#) section. You can optionally block all summary routes from going into the stub area.

Before you begin

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

Ensure that there are no virtual links or ASBRs in the proposed stub area.

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **area area-id stub**
4. (Optional) **address-family ipv6 unicast**
5. (Optional) **area area-id default-cost cost**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: switch(config)# router ospfv3 201 switch(config-router)#	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	area area-id stub Example: switch(config-router)# area 0.0.0.10 stub	Creates this area as a stub area.
Step 4	(Optional) address-family ipv6 unicast Example: switch(config-router)# address-family ipv6 unicast switch(config-router-af)#	Enters IPv6 unicast address family mode.
Step 5	(Optional) area area-id default-cost cost Example:	Sets the cost metric for the default summary route sent into this stub area. The range is from 0 to 16777215.

	Command or Action	Purpose
	<code>switch(config-router-af)# area 0.0.0.10 default-cost 25</code>	
Step 6	(Optional) copy running-config startup-config Example: <code>switch(config-router)# copy running-config startup-config</code>	Saves this configuration change.

Example

This example shows how to create a stub area that blocks all summary route updates:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 stub no-summary
switch(config-router)# copy running-config startup-config
```

Configuring a Totally Stubby Area

You can create a totally stubby area and prevent all summary route updates from going into the stub area.

To create a totally stubby area, use the following command in router configuration mode:

SUMMARY STEPS

1. **area area-id stub no-summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	area area-id stub no-summary Example: <code>switch(config-router)# area 20 stub no-summary</code>	Creates this area as a totally stubby area.

Configuring NSSA

You can configure an NSSA for part of an OSPFv3 domain where limited external traffic is required. You can optionally translate this external traffic to an AS External (type 5) LSA and flood the OSPFv3 domain with this routing information. An NSSA can be configured with the following optional parameters:

- No redistribution—Redistributes routes that bypass the NSSA to other areas in the OSPFv3 autonomous system. Use this option when the NSSA ASBR is also an ABR.
- Default information originate—Generates a Type-7 LSA for a default route to the external autonomous system. Use this option on an NSSA ASBR if the ASBR contains the default route in the routing table.

This option can be used on an NSSA ABR whether or not the ABR contains the default route in the routing table.

- **Route map**—Filters the external routes so that only those routes you want are flooded throughout the NSSA and other areas.
- **Translate**—Translates Type-7 LSAs to AS External (type 5) LSAs for areas outside the NSSA. Use this command on an NSSA ABR to flood the redistributed routes throughout the OSPFv3 autonomous system. You can optionally suppress the forwarding address in these AS External LSAs.
- **No summary**—Blocks all summary routes from flooding the NSSA. Use this option on the NSSA ABR.

Before you begin

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

Ensure that there are no virtual links in the proposed NSSA and that it is not the backbone area.

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **area area-id nssa [no-redistribution] [default-information-originate] [route-map map-name] [no-summary] [translate type7 { always | never } [suppress-fa]]**
4. (Optional) **address-family ipv6 unicast**
5. (Optional) **area area-id default-cost cost**
6. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	area area-id nssa [no-redistribution] [default-information-originate] [route-map map-name] [no-summary] [translate type7 { always never } [suppress-fa]] Example: <pre>switch(config-router)# area 0.0.0.10 nssa</pre>	Creates this area as an NSSA.

	Command or Action	Purpose
Step 4	(Optional) address-family ipv6 unicast Example: <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	Enters IPv6 unicast address family mode.
Step 5	(Optional) area area-id default-cost cost Example: <pre>switch(config-router-af)# area 0.0.0.10 default-cost 25</pre>	Sets the cost metric for the default summary route sent into this NSSA. The range is from 0 to 16777215.
Step 6	copy running-config startup-config Example: <pre>switch(config-router)# copy running-config startup-config</pre>	Saves this configuration change.

Example

This example shows how to create an NSSA that blocks all summary route updates:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

This example shows how to create an NSSA that generates a default route:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

This example shows how to create an NSSA that filters external routes and blocks all summary route updates:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

This example shows how to create an NSSA that always translates Type-7 LSAs to AS External (type 5) LSAs:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

This example shows how to create an NSSA that blocks all summary route updates:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

Configuring Multi-Area Adjacency

You can add more than one area to an existing OSPFv3 interface. The additional logical interfaces support multi-area adjacency.

Before you begin

You must enable OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

Ensure that you have configured a primary area for the interface (see the [Configuring Networks in OSPFv3, on page 18](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **ipv6 router ospfv3 instance-tag multi-area area-id**
4. (Optional) **show ipv6 ospfv3 instance-tag interface** *interface-type slot/port*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	Enters interface configuration mode.
Step 3	ipv6 router ospfv3 instance-tag multi-area area-id Example: <pre>switch(config-if)# ipv6 router ospfv3 201 multi-area 3</pre>	Adds the interface to another area. Note Beginning with Cisco NX-OS Release 7.0(3)I5(1), the instance tag argument is optional. If you do not specify an instance the multi-area configuration is applied to the same instance that is configured for the primary area on the interface.
Step 4	(Optional) show ipv6 ospfv3 instance-tag interface <i>interface-type slot/port</i> Example: <pre>switch(config-if)# show ipv6 ospfv3 201 interface ethernet 1/2</pre>	Displays OSPFv3 information.

	Command or Action	Purpose
Step 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Saves this configuration change.

Example

This example shows how to add a second area to an OSPFv3 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/48
switch(config-if)# ipv6 ospfv3 201 area 0.0.0.10
switch(config-if)# ipv6 ospfv3 201 multi-area 20
switch(config-if)# copy running-config startup-config
```

Configuring Virtual Links

A virtual link connects an isolated area to the backbone area through an intermediate area. See the [Virtual Links](#) section. You can configure the following optional parameters for a virtual link:

- Dead interval—Sets the time that a neighbor waits for a Hello packet before declaring the local router as dead and tearing down adjacencies.
- Hello interval—Sets the time between successive Hello packets.
- Retransmit interval—Sets the estimated time between successive LSAs.
- Transmit delay—Sets the estimated time to transmit an LSA to a neighbor.



Note You must configure the virtual link on both routers involved before the link becomes active.

Before you begin

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **area area-id virtual-link router-id**
4. (Optional) **show ipv6 ospfv3 virtual-link [brief]**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: switch(config)# router ospfv3 201 switch(config-router)#	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	area area-id virtual-link router-id Example: switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1 switch(config-router-vlink)#	Creates one end of a virtual link to a remote router. You must create the virtual link on that remote router to complete the link.
Step 4	(Optional) show ipv6 ospfv3 virtual-link [brief] Example: switch(config-if)# show ipv6 ospfv3 virtual-link	Displays OSPFv3 virtual link information.
Step 5	(Optional) copy running-config startup-config Example: switch(config-router)# copy running-config startup-config	Saves this configuration change.

Example

You can configure the following optional commands in virtual link configuration mode:

Command	Purpose
dead-interval seconds Example: switch(config-router-vlink)# dead-interval 50	Configures the OSPFv3 dead interval, in seconds. The range is from 1 to 65535. The default is four times the hello interval, in seconds.
hello-interval seconds Example: switch(config-router-vlink)# hello-interval 25	Configures the OSPFv3 hello interval, in seconds. The range is from 1 to 65535. The default is 10 seconds.

Command	Purpose
retransmit-interval <i>seconds</i> Example: <pre>switch(config-router-vlink)# retransmit-interval 50</pre>	Configures the OSPFv3 retransmit interval, in seconds. The range is from 1 to 65535. The default is 5.
transmit-delay <i>seconds</i> Example: <pre>switch(config-router-vlink)# transmit-delay 2</pre>	Configures the OSPFv3 transmit-delay, in seconds. The range is from 1 to 450. The default is 1.

These examples show how to create a simple virtual link between two ABRs:

Configuration for ABR 1 (router ID 2001:0DB8::1) is as follows:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::10
switch(config-router)# copy running-config startup-config
```

Configuration for ABR 2 (router ID 2001:0DB8::10) is as follows:

```
switch# configure terminal
switch(config)# router ospf 101
switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1
switch(config-router)# copy running-config startup-config
```

Configuring Redistribution

You can redistribute routes learned from other routing protocols into an OSPFv3 autonomous system through the ASBR.

You can configure the following optional parameters for route redistribution in OSPF:

- **Default information originate**—Generates an AS External (type 5) LSA for a default route to the external autonomous system.



Note Default information originate ignores **match** statements in the optional route map.

- **Default metric**—Sets all redistributed routes to the same cost metric.



Note If you redistribute static routes, Cisco NX-OS also redistributes the default static route.

Before you begin

Create the necessary route maps used for redistribution.

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **redistribute { bgp id | direct | isis id | rip id | static } route-map map-name**
5. **default-information originate [always] [route-map map-name]**
6. **default-metric cost**
7. **copy running-config startup-config**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: <pre>switch(config) # router ospfv3 201 switch(config-router) #</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	address-family ipv6 unicast Example: <pre>switch(config-router) # address-family ipv6 unicast switch(config-router-af) #</pre>	Enters IPv6 unicast address family mode.
Step 4	redistribute { bgp id direct isis id rip id static } route-map map-name Example: <pre>switch(config-router-af) # redistribute bgp route-map FilterExternalBGP</pre>	Redistributes the selected protocol into OSPFv3 through the configured route map. Note If you redistribute static routes, Cisco NX-OS also redistributes the default static route.
Step 5	default-information originate [always] [route-map map-name] Example: <pre>switch(config-router-af) # default-information-originate route-map DefaultRouteFilter</pre>	Creates a default route into this OSPFv3 domain if the default route exists in the RIB. Use the following optional keywords: • always —Always generates the default route of 0.0.0.0 even if the route does not exist in the RIB. • route-map —Generates the default route if the route map returns true. Note This command ignores match statements in the route map

	Command or Action	Purpose
Step 6	default-metric <i>cost</i> Example: <pre>switch(config-router-af)# default-metric 25</pre>	Sets the cost metric for the redistributed routes. The range is from 1 to 16777214. This command does not apply to directly connected routes. Use a route map to set the default metric for directly connected routes.
Step 7	copy running-config startup-config Example: <pre>switch(config-router)# copy running-config startup-config</pre>	Saves this configuration change.

Example

This example shows how to redistribute the Border Gateway Protocol (BGP) into OSPFv3:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# copy running-config startup-config
```

Limiting the Number of Redistributed Routes

Route redistribution can add many routes to the OSPFv3 route table. You can configure a maximum limit to the number of routes accepted from external protocols. OSPFv3 provides the following options to configure redistributed route limits:

- **Fixed limit**—Logs a message when OSPFv3 reaches the configured maximum. OSPFv3 does not accept any more redistributed routes. You can optionally configure a threshold percentage of the maximum where OSPFv3 logs a warning when that threshold is passed.
- **Warning only**—Logs a warning only when OSPFv3 reaches the maximum. OSPFv3 continues to accept redistributed routes.
- **Withdraw**—Starts the configured timeout period when OSPFv3 reaches the maximum. After the timeout period, OSPFv3 requests all redistributed routes if the current number of redistributed routes is less than the maximum limit. If the current number of redistributed routes is at the maximum limit, OSPFv3 withdraws all redistributed routes. You must clear this condition before OSPFv3 accepts more redistributed routes. You can optionally configure the timeout period.

Before you begin

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3** *instance-tag*
3. **address-family** *ipv6 unicast*
4. **redistribute** { **bgp** *id* | **direct** | **isis** *id* | **rip** *id* | **static** } **route-map** *map-name*

5. **redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries* *timemout*]]
6. (Optional) **show running-config ospfv3**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	address-family ipv6 unicast Example: <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	Enters IPv6 unicast address family mode.
Step 4	redistribute { bgp id direct isis id rip id static } route-map map-name Example: <pre>switch(config-router-af)# redistribute bgp route-map FilterExternalBGP</pre>	Redistributes the selected protocol into OSPFv3 through the configured route map.
Step 5	redistribute maximum-prefix max [threshold] [warning-only withdraw [num-retries timemout]] Example: <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	Specifies a maximum number of prefixes that OSPFv2 distributes. The range is from 0 to 65536. Optionally, specifies the following: • threshold —Percent of maximum prefixes that triggers a warning message. • warning-only —Logs an warning message when the maximum number of prefixes is exceeded. • withdraw —Withdraws all redistributed routes and optionally tries to retrieve the redistributed routes. The <i>num-retries</i> range is from 1 to 12. The <i>timeout</i> range is from 60 to 600 seconds. The default is 300 seconds.
Step 6	(Optional) show running-config ospfv3 Example: <pre>switch(config-router)# show running-config ospf</pre>	Displays the OSPFv3 configuration.

	Command or Action	Purpose
Step 7	(Optional) copy running-config startup-config Example: <pre>switch(config-router)# copy running-config startup-config</pre>	Saves this configuration change.

Example

This example shows how to limit the number of redistributed routes into OSPF:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
```

Configuring Route Summarization

You can configure route summarization for inter-area routes by configuring an address range that is summarized. You can also configure route summarization for external, redistributed routes by configuring a summary address for those routes on an ASBR. For more information, see the [Route Summarization](#) section.

Before you begin

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **area area-id range ipv6-prefix/length [no-advertise] [cost cost]**
5. **summary-address ipv6-prefix/length [no-advertise] [tag tag]**
6. (Optional) **show ipv6 ospfv3 summary-address**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	router ospfv3 instance-tag Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	address-family ipv6 unicast Example: <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	Enters IPv6 unicast address family mode.
Step 4	area area-id range ipv6-prefix/length [no-advertise] [cost cost] Example: <pre>switch(config-router-af)# area 0.0.0.10 range 2001:0DB8::/48 advertise</pre>	Creates a summary address on an ABR for a range of addresses and optionally advertises this summary address in a Inter-Area Prefix (type 3) LSA. The <i>cost</i> range is from 0 to 16777215.
Step 5	summary-address ipv6-prefix/length [no-advertise] [tag tag] Example: <pre>switch(config-router-af)# summary-address 2001:0DB8::/48 tag 2</pre>	Creates a summary address on an ASBR for a range of addresses and optionally assigns a tag for this summary address that can be used for redistribution with route maps.
Step 6	(Optional) show ipv6 ospfv3 summary-address Example: <pre>switch(config-router)# show ipv6 ospfv3 summary-address</pre>	Displays information about OSPFv3 summary addresses
Step 7	(Optional) copy running-config startup-config Example: <pre>switch(config-router)# copy running-config startup-config</pre>	Saves this configuration change.

Example

This example shows how to create summary addresses between areas on an ABR:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router)# area 0.0.0.10 range 2001:0DB8::/48
switch(config-router)# copy running-config startup-config
```

This example shows how to create summary addresses on an ASBR:

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# address-family ipv6 unicast
switch(config-router)# summary-address 2001:0DB8::/48
switch(config-router)# copy running-config startup-config
```

Modifying the Default Timers

OSPFv3 includes a number of timers that control the behavior of protocol messages and shortest path first (SPF) calculations. OSPFv3 includes the following optional timer parameters:

- LSA arrival time—Sets the minimum interval allowed between LSAs arriving from a neighbor. LSAs that arrive faster than this time are dropped.
- Pacing LSAs—Sets the interval at which LSAs are collected into a group and refreshed, checksummed, or aged. This timer controls how frequently LSA updates occur and optimizes how many are sent in an LSA update message (see the [Flooding and LSA Group Pacing](#) section).
- Throttle LSAs—Sets rate limits for generating LSAs. This timer controls how frequently LSAs are generated after a topology change occurs.
- Throttle SPF calculation—Controls how frequently the SPF calculation is run.

At the interface level, you can also control the following timers:

- Retransmit interval—Sets the estimated time between successive LSAs.
- Transmit delay—Sets the estimated time to transmit an LSA to a neighbor.

See the [Configuring Networks in OSPFv3, on page 18](#) section for information on the hello interval and dead timer.

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **timers lsa-arrival**
4. **timers lsa-group-pacing seconds**
5. **timers throttle lsa start-time hold-interval max-time**
6. **address-family ipv6 unicast**
7. **timers throttle spf delay-time hold-time**
8. **interface interface type slot/port**
9. **ospfv3 retransmit-interval seconds**
10. **ospfv3 transmit-delay seconds**
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	router ospfv3 instance-tag Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	timers lsa-arrival Example: <pre>switch(config-router)# timers lsa-arrival 2000</pre>	Sets the LSA arrival time in milliseconds. The range is from 10 to 600000. The default is 1000 milliseconds.
Step 4	timers lsa-group-pacing seconds Example: <pre>switch(config-router)# timers lsa-group-pacing 200</pre>	Sets the interval in seconds for grouping LSAs. The range is from 1 to 1800. The default is 10 seconds.
Step 5	timers throttle lsa start-time hold-interval max-time Example: <pre>switch(config-router)# timers throttle lsa network 350 5000 6000</pre>	Sets the rate limit in milliseconds for generating LSAs. You can configure the following timers: start-time —The range is from 50 to 5000 milliseconds. The default value is 50 milliseconds. hold-interval —The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds. max-time —The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.
Step 6	address-family ipv6 unicast Example: <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	Enters IPv6 unicast address family mode.
Step 7	timers throttle spf delay-time hold-time Example: <pre>switch(config-router)# timers throttle spf 3000 2000</pre>	Sets the SPF best-path schedule initial delay time and the minimum hold time in seconds between SPF best-path calculations. The range is from 1 to 600000. The default is no delay time and 5000 millisecond hold time.
Step 8	interface interface type slot/port Example: <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	Enters interface configuration mode.
Step 9	ospfv3 retransmit-interval seconds Example: <pre>switch(config-if)# ospfv3 retransmit-interval 30</pre>	Sets the estimated time in seconds between LSAs transmitted from this interface. The range is from 1 to 65535. The default is 5.
Step 10	ospfv3 transmit-delay seconds Example: <pre>switch(config-if)# ospfv3 transmit-delay 600 switch(config-if)#</pre>	Sets the estimated time in seconds to transmit an LSA to a neighbor. The range is from 1 to 450. The default is 1.

	Command or Action	Purpose
Step 11	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Saves this configuration change.

Example

This example shows how to control LSA flooding with the `lsa-group-pacing` option:

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

Configuring Graceful Restart

Graceful restart is enabled by default. You can configure the following optional parameters for graceful restart in an OSPFv3 instance:

- **Grace period**—Configures how long neighbors should wait after a graceful restart has started before tearing down adjacencies.
- **Helper mode disabled**—Disables helper mode on the local OSPFv3 instance. OSPFv3 does not participate in the graceful restart of a neighbor.
- **Planned graceful restart only**—Configures OSPFv3 to support graceful restart only in the event of a planned restart.

Before you begin

You must enable OSPFv3 (see the [Enabling OSPFv3, on page 14](#) section).

Ensure that all neighbors are configured for graceful restart with matching optional parameters set.

SUMMARY STEPS

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **graceful-restart**
4. **graceful-restart grace-period** *seconds*
5. **graceful-restart helper-disable**
6. **graceful-restart planned-only**
7. (Optional) **show ipv6 ospfv3 instance-tag**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	router ospfv3 instance-tag Example: switch(config)# router ospfv3 201 switch(config-router)#	Creates a new OSPFv3 instance with the configured instance tag.
Step 3	graceful-restart Example: switch(config-router)# graceful-restart	Enables graceful restart. A graceful restart is enabled by default.
Step 4	graceful-restart grace-period seconds Example: switch(config-router)# graceful-restart grace-period 120	Sets the grace period, in seconds. The range is from 5 to 1800. The default is 60 seconds.
Step 5	graceful-restart helper-disable Example: switch(config-router)# graceful-restart helper-disable	Disables helper mode. Enabled by default.
Step 6	graceful-restart planned-only Example: switch(config-router)# graceful-restart planned-only	Configures graceful restart for planned restarts only.
Step 7	(Optional) show ipv6 ospfv3 instance-tag Example: switch(config-if)# show ipv6 ospfv3 201	Displays OSPFv3 information.
Step 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Saves this configuration change.

Example

This example shows how to enable graceful restart if it has been disabled and set the grace period to 120 seconds:

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart grace-period 120
switch(config-router)# copy running-config startup-config
```

Restarting an OSPFv3 Instance

You can restart an OSPv3 instance. This action clears all neighbors for the instance.

To restart an OSPFv3 instance and remove all associated neighbors, use the following command:

SUMMARY STEPS

1. **restart ospfv3** *instance-tag*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	restart ospfv3 <i>instance-tag</i> Example: switch(config)# restart ospfv3 201	Restarts the OSPFv3 instance and removes all neighbors.

Configuring OSPFv3 with Virtualization

You can configure multiple OSPFv3 instances in each VDC. You can also create multiple VRFs within each VDC and use the same or multiple OSPFv3 instances in each VRF. You assign an OSPFv3 interface to a VRF.



Note Configure all other parameters for an interface after you configure the VRF for an interface. Configuring a VRF for an interface deletes all the configuration for that interface.

Before you begin

Create the VDCs.

You must enable OSPF (see the [Enabling OSPFv3, on page 14](#) section).

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **router ospfv3** *instance-tag*
4. **vrf** *vrf-name*
5. (Optional) **maximum-paths** *paths*

6. **interface** *interface type slot/port*
7. **vrf member** *vrf-name*
8. **ipv6 address** *ipv6-prefix/length*
9. **ipv6 ospfv3** *instance-tag area area-id*
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	vrf context <i>vrf-name</i> Example: <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	Creates a new VRF and enters VRF configuration mode.
Step 3	router ospfv3 <i>instance-tag</i> Example: <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	Creates a new OSPFv3 instance with the configured instance tag.
Step 4	vrf <i>vrf-name</i> Example: <pre>switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#</pre>	Enters VRF configuration mode.
Step 5	(Optional) maximum-paths <i>paths</i> Example: <pre>switch(config-router-vrf)# maximum-paths 4</pre>	Configures the maximum number of equal OSPFv3 paths to a destination in the route table for this VRF. Use this command for load balancing.
Step 6	interface <i>interface type slot/port</i> Example: <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	Enters interface configuration mode.
Step 7	vrf member <i>vrf-name</i> Example: <pre>switch(config-if)# vrf member RemoteOfficeVR</pre>	Adds this interface to a VRF.
Step 8	ipv6 address <i>ipv6-prefix/length</i> Example: <pre>switch(config-if)# ipv6 address 2001:0DB8::1/48</pre>	Configures an IP address for this interface. You must do this step after you assign this interface to a VRF.

	Command or Action	Purpose
Step 9	ipv6 ospfv3 instance-tag area area-id Example: switch(config-if)# ipv6 ospfv3 201 area 0	Assigns this interface to the OSPFv3 instance and area configured.
Step 10	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Saves this configuration change.

Example

This example shows how to create a VRF and add an interface to the VRF:

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router ospfv3 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# vrf member NewVRF
switch(config-if)# ipv6 address 2001:0DB8::1/48
switch(config-if)# ipv6 ospfv3 201 area 0
switch(config-if)# copy running-config startup-config
```

Configuring Encryption and Authentication

Beginning with Cisco Nexus Release 10.2(1), you can encrypt and authenticate OSPFv3 messages using ESP encapsulation. OSPFv3 depends on IPSec for secure connection. IPSec supports two encapsulation types:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- RFC4552 'Authentication/Confidentiality for OSPFv3' covers both the above aspects

ESP configuration provides both encryption and authentication for OSPFv3 messages.

Beginning with Cisco Nexus Release 10.4(1)F, the encryption and authentication algorithms and keys can be configured using the keychain option.

The following are the limitations:

1. Only IPSec transport mode is supported and tunnel mode is not supported.

2. AH and ESP configurations together are not allowed on an interface. Though two different interfaces can have AH and ESP.
3. Non-disruptive rekeying as defined in section 10 of RFC 4552 is not supported.
4. The following Encryption Algorithms will be supported under ESP:
 - AES-CBC (128 bit)
 - AES 192 bit and AES 256 bit will not be supported in this release.
 - 3DES-CBC
 - NULL
5. The following Authentications will be supported under ESP:
 - SHA-1
 - NULL
6. Both Encryption and Authentication algorithms cannot be configured NULL in one ESP CLI.
7. An interface which is part of multiple areas use the same ESP parameters as the parent.
8. On SPI conflict during configuration, error will be thrown to user and configuration will not be saved. So, while changing the ESP configuration the user must use different SPI for a new configuration.
9. Max 128 SA/SPI values can be configured per OSPFv3 process.

You can configure ESP at the following levels:

- Router
- Area
- Interface
- Virtual Links

Configuring OSPFv3 Encryption at Router Level

You can configure OSPFv3 ESP to encrypt and authenticate OSPFv3 packets at the router level using the following commands.

Before you begin

Enable OSPFv3 feature.

Enable authentication package.

Procedure

Step 1 Enter the global configuration mode:

```
switch# configure terminal
```

Step 2 Enable OSPFv3:

```
switch(config)# feature ospfv3
```

Step 3 Enable authentication package:

```
switch(config)# feature imp
```

Step 4 Create a new OSPFv3 instance with the configured instance tag:

```
switch(config)# router ospfv3 instance-tag
```

Step 5 Enable IPsec ESP encryption:

```
switch(config-router)# encryption ipsec spi spi_id esp [encrypt_algorithm [ 0 | 3 | 7] key | key-chain enc_keychain_name  
| null] authentication [auth_algorithm [ 0 | 3 | 7] key | key-chain auth_keychain_name | null]
```

You can specify the security policy index through *spi_id* and define the encryption algorithm through *encrypt_algorithm* which can be 3DES, AES 128 or null. Numbers 0, 3, and 7 specify the format of the *key*. You can define the authentication algorithm through *auth_algorithm* which can be SHA-1 or NULL.

You can also configure keys and algorithms using the **key-chain** option.

Step 6 (Optional) Display OSPFv3 information:

```
switch(config)# show running-config ospfv3
```

Configuring OSPFv3 Encryption at Area Level

You can configure OSPFv3 ESP to encrypt and authenticate OSPFv3 packets at the area level using the following commands.

Before you begin

Enable OSPFv3 feature.

Enable authentication package.

Procedure

Step 1 Enter the global configuration mode:

```
switch# configure terminal
```

Step 2 Enable OSPFv3:

```
switch(config)# feature ospfv3
```

Step 3 Enable the authentication package:

```
switch(config)# feature imp
```

Step 4 Create a new OSPFv3 instance with the configured instance tag:

```
switch(config)# router ospfv3 instance-tag
```

Step 5 Enable IPsec ESP Encryption:

```
switch(config-router)#area area-num encryption ipsec spi spi_val esp encrypt_algorithm [ 0 | 3 | 7]key | key-chain  
enc_keychain_name | null] authentication auth_algorithm [ 0 | 3 | 7] key | key-chain auth_keychain_name | null]
```

You can specify the security policy index through *spi_id* and define the encryption algorithm through *encrypt_algorithm* which can be 3DES, AES 128 or null. Numbers 0, 3, 6 and 7 specify the format of the *key*. You can define the authentication algorithm through *auth_algorithm* which can be SHA-1 or NULL or key-chain.

You can also configure keys and algorithms using the **key-chain** option.

Step 6 (Optional) Display OSPFv3 information:

```
switch(config)# show running-config ospfv3
```

Configuring OSPFv3 Encryption at Interface Level

You can configure OSPFv3 ESP to encrypt and authenticate OSPFv3 packets at the interface level using the following commands.

Before you begin

You must enable OSPFv3.

Enable authentication package.

Procedure

Step 1 Enter the global configuration mode:

```
switch# configure terminal
```

Step 2 Enable OSPFv3:

```
switch(config)# feature ospfv3
```

Step 3 Enables the authentication mode:

```
switch(config)# feature imp
```

Step 4 Enters the interface configuration mode:

```
switch(config)# interface ethernet interface
```

Step 5 Specify the OSPFv3 instance and area for the interface:

```
switch(config-if)# ipv6 router ospfv3 instance-tag area area-id
```

Step 6 Enable IPsec ESP Encryption:


```
switch(config-if)# ospfv3 encryption ipsec spi spi_id esp encrypt_algorithm [ 0 | 3 | 7 ] key | key-chain enc_keychain_name  
| null authentication auth_algorithm [ 0 | 3 | 7 ] key | key-chain auth_keychain_name | null
```

You can specify the security policy index through *spi_id* and define the encryption algorithm through *encrypt_algorithm* which can be 3DES, AES 128 or null. Numbers 0, 3 and 7 specify the format of the *key*. You can define the authentication algorithm through *auth_algorithm* which can be SHA-1 or NULL.

You can also configure keys and algorithms using the key-chain option.

Step 7 (Optional) Display the running configuration on the interface:

```
switch(config-if)#show run interface interface
```

Configuration Example

The following example shows how to enable security for Ethernet interface 3/2:

```
switch# configure terminal  
switch(config)# feature ospfv3  
switch(config)# feature imp  
switch(config)# interface ethernet 3/2  
switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0  
switch(config-if)# ospfv3 encryption ipsec spi 444  
    esp Specify encryption parameters  
switch(config-if)# ospfv3 encryption ipsec spi 444 esp  
    3des Use the triple DES algorithm  
    aes Use the AES algorithm  
    key-chain Encryption password key-chain  
    null Use NULL authentication  
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes  
    128 Use the 128-bit AES algorithm  
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128  
    0 Specifies an UNENCRYPTED encryption key will follow  
    3 Specifies an 3DES ENCRYPTED encryption key will follow  
    7 Specifies a Cisco type 7 ENCRYPTED encryption key will follow  
    WORD The UNENCRYPTED (cleartext) encryption key  
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128  
12345678123456781234567812345678 authentication null  
switch(config-if)# sh ospfv3 interface  
Ethernet3/2 is up, line protocol is up  
IPv6 address 1::1::1::2/64  
Process ID 1 VRF default, Instance ID 0, area 0.0.0.0  
Enabled by interface configuration  
State DOWN, Network type BROADCAST, cost 40  
ESP Encryption AES, Authentication NULL, SPI 444, ConnId 444  
switch(config-if)#
```

Configuring OSPFv3 Encryption for Virtual Links

You can configure OSPFv3 ESP to encrypt and authenticate OSPFv3 packets for virtual links using the following commands.

Before you begin

Enable OSPFv3 feature.

Enable authentication package.

Procedure

-
- Step 1** Enter the global configuration mode:
- ```
switch# configure terminal
```
- Step 2** Enable OSPFv3:
- ```
switch(config)# feature ospfv3
```
- Step 3** Enable the authentication package:
- ```
switch(config)# feature imp
```
- Step 4** Create a new OSPFv3 instance with the configured instance tag:
- ```
switch(config)#router ospfv3 instance-tag
```
- Step 5** Creates one end of a virtual link to a remote router. You must create the virtual link on that remote router to complete the link.
- ```
switch(config-router)# area area-id virtual-link router-id
```
- Step 6** Enable IPsec ESP Encryption:
- ```
switch(config-router-vlink)# encryption ipsec spi spi_id esp encrypt_algorithm [ 0 | 3 | 7] key | key-chain  
enc_keychain_name | null] authentication auth_algorithm [ 0 | 3 | 7] key | key-chain auth_keychain_name | null]
```
- You can specify the security policy index through *spi_id* and define the encryption algorithm through *encrypt_algorithm* which can be 3DES, AES 128 or null. Numbers 0, 3 and 7 specify the format of the *key*. You can define the authentication algorithm through *auth_algorithm* which can be SHA-1 or NULL.
- You can also configure keys and algorithms using the **key-chain** option.
- Step 7** (Optional) Display OSPFv3 information:
- ```
switch(config)# show running-config ospfv3
```
- 

## Configuration Example

The following example shows how to encrypt Virtual links:

```
switch(config)# feature ospfv3
switch(config)# feature imp
switch(config-if)# router ospfv3 1
switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3
switch(config-router-vlink)# encryption ipsec spi ?
<256-4294967295> SPI Value
switch(config-router-vlink)# encryption ipsec spi 256 esp ?
3des Use the triple DES algorithm
aes Use the AES algorithm
key-chain Encryption password key-chain
null Use NULL authentication
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication ?
null Use NULL authentication
```

```

sh1 Use the SHA1 algorithm
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication null

```



**Note** To permit multiple OSPFv3 neighbors to have IPsec ESP, the following policy-map has to be applied for a control-plane:

```

ipv6 access-list copp-acl-ipsec
10 permit ahp any any
20 permit esp any any

class-map type control-plane match-any copp-class-critical-customized-copp
match access-group name copp-acl-ipsec
policy-map type control-plane customized-copp
class copp-class-critical-customized-copp
police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
control-plane
service-policy input customized-copp

```

## Configuring OSPFv3 Authentication at Router Level

You can configure OSPFv3 ESP to authenticate OSPFv3 packets at the router level using the following commands.

### Before you begin

Ensure that you have enabled OSPFv3, for more information see [Enabling OSPFv3](#) section.

### SUMMARY STEPS

1. configure terminal
2. **feature ospfv3**
3. **feature imp**
4. **router ospfv3 instance-tag**
5. **[no] authentication {ipsec spi spi\_id [auth\_algorithm [ 0 | 3 | 7] key | key-chain auth\_keychain\_name | null]**
6. (Optional) **show running-config ospfv3**
7. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                        | Purpose                           |
|--------|--------------------------------------------------------------------------|-----------------------------------|
| Step 1 | configure terminal                                                       | Enters global configuration mode. |
|        | <b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> |                                   |

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>feature ospfv3</b><br><br><b>Example:</b><br>switch(config)# feature ospfv3                                                                                                                                                                                                                                                                                                                      | Enables OSPFv3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>feature imp</b><br><br><b>Example:</b><br>switch(config)# feature imp                                                                                                                                                                                                                                                                                                                            | Enables authentication mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 4</b> | <b>router ospfv3 instance-tag</b><br><br><b>Example:</b><br>switch(config)# router ospfv3 100<br>switch(config-router)#                                                                                                                                                                                                                                                                             | Creates a new OSPFv3 instance with the configured instance tag.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 5</b> | <b>[no] authentication {ipsec spi spi_id [auth_algorithm [ 0   3   7] key   key-chain auth_keychain_name   null]}</b><br><br><b>Example:</b><br>For authentication algorithm and key option:<br><br>switch(config-router)# authentication ipsec spi 475 md5 11111111111111112222222222222222<br><br>For keychain option:<br><br>switch(config-router)# authentication ipsec spi 333 key-chain test1 | Configures OSPFv3 IPsec authentication at the process (or VRF) level.<br><br>The spi argument specifies the security parameter index (SPI). The range is from 256 to 4294967295.<br><br>The auth argument specifies the type of authentication. The supported values are md5 or sha1.<br><br>0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco type 7 encrypted.<br><br>If the cleartext option (0) is used, the key argument must be 32 characters long for md5 or 40 characters long for sha1.<br><br>Beginning with Cisco NX-OS Release 10.4(1)F, the <b>key-chain</b> option is provided to configure key and algorithm.<br><br>Use the <b>no</b> form of this command to disable the OSPFv3 IPsec authentication. |
| <b>Step 6</b> | (Optional) <b>show running-config ospfv3</b><br><br><b>Example:</b><br>switch(config)# show running-config ospfv3                                                                                                                                                                                                                                                                                   | Displays the OSPFv3 authentication configuration information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 7</b> | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config                                                                                                                                                                                                                                                                   | Saves this configuration change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Configuring OSPFv3 Authentication at Area Level

You can configure OSPFv3 ESP to authenticate OSPFv3 packets at the area level using the following commands.

For information on how to configure a keychain, see **Configuring Keychain Management** of *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

### Before you begin

Ensure that you have enabled OSPFv3, for more information see [Enabling OSPFv3](#) section.

## SUMMARY STEPS

1. **configure terminal**
2. **feature ospfv3**
3. **feature imp**
4. **router ospfv3 instance-tag**
5. **[no] area area-id-ip authentication {ipsec spi spi\_id[auth\_algorithm [ 0 | 3 | 7] key | key-chain auth\_keychain\_name | null]**
6. (Optional) **show running-config ospfv3**
7. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|               | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                          |
| <b>Step 2</b> | <b>feature ospfv3</b><br><br><b>Example:</b><br><pre>switch(config)# feature ospfv3</pre>                                                                                                                  | Enables OSPFv3.                                                                                                                                                                                                                                                            |
| <b>Step 3</b> | <b>feature imp</b><br><br><b>Example:</b><br><pre>switch(config)# feature imp</pre>                                                                                                                        | Enables authentication mode.                                                                                                                                                                                                                                               |
| <b>Step 4</b> | <b>router ospfv3 instance-tag</b><br><br><b>Example:</b><br><pre>switch(config)# router ospfv3 100 switch(config-router)#</pre>                                                                            | Creates a new OSPFv3 instance with the configured instance tag.                                                                                                                                                                                                            |
| <b>Step 5</b> | <b>[no] area area-id-ip authentication {ipsec spi spi_id[auth_algorithm [ 0   3   7] key   key-chain auth_keychain_name   null]</b><br><br><b>Example:</b><br>For authentication algorithm and key option: | Configures OSPFv3 IPsec authentication at the area level.<br><br>The spi argument specifies the security parameter index (SPI). The range is from 256 to 4294967295.<br><br>The auth argument specifies the type of authentication. The supported values are MD5 or SHA-1. |

|               | Command or Action                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <pre>switch(config-router)# area 0 authentication ipsec spi 475 md5 111111111111111111112222222222222222</pre> <p>For keychain option:</p> <pre>switch(config-router)# area 0 authentication ipsec spi 333 key-chain test1</pre> | <p>0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco Type-7 encrypted.</p> <p>If the cleartext option (0) is used, the key argument must be 32 characters long for MD5 or 40 characters long for SHA-1.</p> <p>Beginning with Cisco NX-OS Release 10.4(1)F, the <b>key-chain</b> option is provided to configure key and algorithm.</p> <p>Use the <b>no</b> form of this command to disable the OSPFv3 IPsec authentication.</p> |
| <b>Step 6</b> | <p>(Optional) <b>show running-config ospfv3</b></p> <p><b>Example:</b></p> <pre>switch(config)# show running-config ospfv3</pre>                                                                                                 | Displays the OSPFv3 authentication configuration information.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 7</b> | <p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>                                                                                 | Saves this configuration change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Configuring OSPFv3 Authentication at Interface Level

You can configure OSPFv3 ESP to authenticate OSPFv3 packets at interface level using the following commands.

For information on how to configure a keychain, see **Configuring Keychain Management** of *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

### Before you begin

Ensure that you have enabled OSPFv3, for more information see [Enabling OSPFv3](#) section.

### SUMMARY STEPS

1. configure terminal
2. **interface** *interface-type slot/port*
3. **[no] ospfv3 authentication {disable | ipsec spi *spi\_id* {md5 *akey* | sha1 *akey* | key-chain *keychain\_ah*}}**
4. (Optional) **show running-config ospfv3**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | configure terminal<br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)#                                                                                                                                                                                                                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 2</b> | <b>interface</b> <i>interface-type slot/port</i><br><br><b>Example:</b><br>switch(config)# interface ethernet 1/1<br>switch(config-if)#                                                                                                                                                                                                                                                           | Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>[no] ospfv3 authentication {disable   ipsec spi spi_id {md5 akey   sha1 akey   key-chain keychain_ah}}</b><br><br><b>Example:</b><br>For authentication algorithm and key option:<br><br>switch(config-if)# ospfv3 authentication ipsec spi 475 md5 11111111111111111222222222222222<br><br>For keychain option:<br><br>switch(config-if)# ospfv3 authentication ipsec spi 333 key-chain test1 | Configures OSPFv3 IPsec authentication for the specified interface.<br><br>The spi argument specifies the security parameter index (SPI). The range is from 256 to 4294967295.<br><br>The auth argument specifies the type of authentication. The supported values are MD5 or SHA-1.<br><br>0 configures the password in cleartext. 3 configures the password as 3DES encrypted. 7 configures the key as Cisco Type-7 encrypted.<br><br>If the cleartext option (0) is used, the key argument must be 32 characters long for MD5 or 40 characters long for SHA-1.<br><br>Beginning with Cisco NX-OS Release 10.4(1)F, the <b>key-chain</b> option is provided to configure key and algorithm.<br><br>Use the <b>no</b> form of this command to disable the OSPFv3 IPsec authentication. |
| <b>Step 4</b> | (Optional) <b>show running-config ospfv3</b><br><br><b>Example:</b><br>switch(config)# show running-config ospfv3                                                                                                                                                                                                                                                                                 | Displays the OSPFv3 authentication configuration information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 5</b> | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config                                                                                                                                                                                                                                                                 | Saves this configuration change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Configuring OSPFv3 Authentication at Virtual Links Level

You can configure OSPFv3 ESP to authenticate OSPFv3 packets at the virtual link level using the following commands.

For information on how to configure a keychain, see **Configuring Keychain Management** of *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

### Before you begin

Ensure that you have enabled OSPFv3, for more information see [Enabling OSPFv3](#) section.

## SUMMARY STEPS

1. `configure terminal`
2. `feature ospfv3`
3. `feature imp`
4. `router ospfv3 instance-tag`
5. `area area-id virtual-link router-id`
6. `[no] authentication {ipsec spi spi_id [auth_algorithm [ 0 | 3 | 7] key | key-chain auth_keychain_name | null]`
7. (Optional) `show running-config ospfv3`
8. (Optional) `copy running-config startup-config`

## DETAILED STEPS

### Procedure

|               | Command or Action                                                                                                                                                                 | Purpose                                                                                                                            |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>configure terminal</code><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                   | Enters global configuration mode.                                                                                                  |
| <b>Step 2</b> | <code>feature ospfv3</code><br><br><b>Example:</b><br><pre>switch(config)# feature ospfv3</pre>                                                                                   | Enables OSPFv3.                                                                                                                    |
| <b>Step 3</b> | <code>feature imp</code><br><br><b>Example:</b><br><pre>switch(config)# feature imp</pre>                                                                                         | Enables authentication mode.                                                                                                       |
| <b>Step 4</b> | <code>router ospfv3 instance-tag</code><br><br><b>Example:</b><br><pre>switch(config)# router ospfv3 100 switch(config-router)#</pre>                                             | Creates a new OSPFv3 instance with the configured instance tag.                                                                    |
| <b>Step 5</b> | <code>area area-id virtual-link router-id</code><br><br><b>Example:</b><br><pre>switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1 switch(config-router-vlink)#</pre> | Creates one end of a virtual link to a remote router. You must create the virtual link on that remote router to complete the link. |



|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b> | <p><b>[no] authentication {ipsec spi spi_id [auth_algorithm [ 0   3   7] key   key-chain auth_keychain_name   null]}</b></p> <p><b>Example:</b></p> <p>For authentication algorithm and key option:</p> <pre>switch(config-router-vlink)# authentication ipsec spi 475 md5 11111111111111111222222222222222</pre> <p>For keychain option:</p> <pre>switch(config-router-vlink)# authentication ipsec spi 333 key-chain test1</pre> | <p>Configures OSPFv3 IPsec authentication at the virtual link level.</p> <p>The spi argument specifies the security parameter index (SPI). The range is from 256 to 4294967295.</p> <p>The auth argument specifies the type of authentication. The supported values are MD5 or SHA-1.</p> <p>0 configures the password in cleartext. 3 configures the pass key as 3DES encrypted. 7 configures the key as Cisco Type-7 encrypted.</p> <p>If the cleartext option (0) is used, the key argument must be 32 characters long for MD5 or 40 characters long for SHA-1.</p> <p>Beginning with Cisco NX-OS Release 10.4(1)F, the <b>key-chain</b> option is provided to configure key and algorithm.</p> <p>Use the <b>no</b> form of this command to disable the OSPFv3 IPsec authentication.</p> |
| <b>Step 7</b> | <p>(Optional) <b>show running-config ospfv3</b></p> <p><b>Example:</b></p> <pre>switch(config)# show running-config ospfv3</pre>                                                                                                                                                                                                                                                                                                   | Displays the OSPFv3 authentication configuration information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 8</b> | <p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                   | Saves this configuration change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Verifying the OSPFv3 Configuration

To display the OSPFv3 configuration, perform one of the following tasks:

| Command                                                                                         | Purpose                                                                             |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>show ipv6 ospfv3</b>                                                                         | Displays the OSPFv3 configuration.                                                  |
| <b>show ipv6 ospfv3 border-routers</b>                                                          | Displays the internal OSPF routing table entries to an ABR and ASBR                 |
| <b>show ipv6 ospfv3 database</b>                                                                | Displays lists of information related to the OSPFv3 database for a specific router. |
| <b>show ipv6 ospfv3 interface type number [ vrf { vrf-name   all   default   management } ]</b> | Displays the OSPFv3 interface configuration.                                        |

| Command                                                      | Purpose                                                                                                                  |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>show ipv6 ospfv3 neighbors</b>                            | Displays the neighbor information. Use the <b>clear ospfv3 neighbors</b> command to remove adjacency with all neighbors. |
| <b>show ipv6 ospfv3 request-list</b>                         | Displays a list of LSAs requested by a router.                                                                           |
| <b>show ipv6 ospfv3 retransmission-list</b>                  | Displays a list of LSAs waiting to be retransmitted.                                                                     |
| <b>show ipv6 ospfv3 summary-address</b>                      | Displays a list of all summary address redistribution information configured under an OSPFv3 instance.                   |
| <b>show ospfv3 process</b>                                   | Displays the OSPFv3 authentication configuration at the process level.                                                   |
| <b>show ospfv3 interface</b> <i>interface-type slot/port</i> | Displays the OSPFv3 authentication configuration at the interface level.                                                 |
| <b>show running-configuration ospfv3</b>                     | Displays the current running OSPFv3 configuration.                                                                       |

## Monitoring OSPFv3

To display OSPFv3 statistics, use the following commands:

| Command                                                                                                                                                 | Purpose                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>show ipv6 ospfv3 memory</b>                                                                                                                          | Displays the OSPFv3 memory usage statistics.             |
| <b>show ipv6 ospfv3 policy statistics area</b> <i>area-id filter-list {in   out} [ vrf {vrf-name   all   default   management}]</i>                     | Displays the OSPFv3 route policy statistics for an area. |
| <b>show ipv6 ospfv3 policy statistics redistribute</b> <i>{bgp id   direct   isis id   rip id   static} vrf {vrf-name   all   default   management}</i> | Displays the OSPFv3 route policy statistics.             |
| <b>show ipv6 ospfv3 statistics</b> <i>[vrf {vrf-name   all   default   management}]</i>                                                                 | Displays the OSPFv3 event counters                       |
| <b>show ipv6 ospfv3 traffic</b> <i>[interface-type number] [vrf {vrf-name   all   default   management}]</i>                                            | Displays the OSPFv3 packet counters.                     |

## Configuration Examples for OSPFv3

This example shows how to configure OSPFv3:

```
feature ospfv3
router ospfv3 201
router-id 290.0.2.1
```

```
interface ethernet 1/2
ipv6 address 2001:0DB8::1/48

ipv6 ospfv3 201 area 0.0.0.10
```

This example shows how to configure OSPFv3 encryption using **key-chain** option:

```
switch(config-if)# ospfv3 encryption ipsec spi 333 esp ?
 3des Use the triple DES algorithm
 aes Use the AES algorithm
 key-chain Encryption password key-chain
 null Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain ?
 WORD Encryption key-chain name (Max Size 63)
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 ?
 authentication Specify authentication parameters
 key-chain Authentication password key-chain
 null Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 authentication
key-chain ?
 WORD Authentication key-chain name (Max Size 63)
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 authentication
key-chain test2 ?
 <CR>
switch(config-router)# sh ospfv3
Routing Process 2 with ID 20.20.10.2 VRF default
Routing Process Instance Number 1
Install discard route for summarized internal routes.
ESP Encryption 3DES, Authentication SHA1, SPI 334, ConnId 334
ESP keychains: Encr test_key_chain_01(ready), Auth test1(ready)
Number of new LSAs originated : 3
Number of new LSAs received : 0
```

# Related Topics

The following topics can give more information on OSPF:

- [Configuring OSPFv2](#)
- [Configuring Route Policy Manager](#)

# Additional References

For additional information related to implementing OSPF, see the following sections:

## MIBs

| MIBs                                                                                  | MIBs Link                                                                       |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• OSPF-MIB</li> <li>• OSPF-TRAP-MIB</li> </ul> | To locate and download MIBs, go to the following: <a href="#">MIB Locator</a> . |

