



A Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter A.

address (VRRP)

To add a single, primary IP address to a virtual router, use the **address** command. To remove an IP address from a virtual router, use the **no** form of this command.

address *ip-address* [**secondary**]

no address

Syntax Description	<i>ip-address</i>	Virtual router address (IPv4). This address should be in the same subnet as the interface IP address.
	secondary	(Optional) Specifies a secondary virtual router address.

Defaults None

Command Modes VRRP configuration mode

Supported User Roles Superuser
VDC administrator

Command History	Release	Modified
	4.0(1)	This command was introduced.

Usage Guidelines You can configure one virtual router IP address for a virtual router. If the configured IP address is the same as the interface IP address, this switch automatically owns the IP address. You can configure an IPv4 address only.

Send document comments to nexus7k-docfeedback@cisco.com

The master VRRP router drops the packets addressed to the virtual router's IP address because the virtual router is only intended as a next-hop router to forward packets. In NX-OS devices, some applications require that packets addressed to the virtual router's IP address be accepted and delivered. By using the **secondary** option to the virtual router IPv4 address, the VRRP router will accept these packets when it is the master.

This command does not require a license.

Examples

This example shows how to configure a virtual router IP address:

```
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# address 10.0.0.10
```

This example shows how to remove all the IP addresses (primary and secondary) using a single command:

```
switch(config-if-vrrp)# show run interface ethernet 9/10
version 4.0(1)
```

```
interface Ethernet9/10
  vrrp 1
    address 10.10.10.10
    address 10.10.10.11 secondary
  ip address 10.10.10.1/24
  no shutdown
```

```
switch(config-if-vrrp)# no address
switch(config-if-vrrp)# sh run int e9/10
version 4.0(1)
```

```
interface Ethernet9/10
  vrrp 1
  ip address 10.10.10.1/24
  no shutdown
```

```
switch(config-if-vrrp)#
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

address-family (BGP)

To enter the address family mode or a VRF address-family mode and configure submode commands for the Border Gateway Protocol (BGP), use the **address-family** command. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

```
address-family {ipv4 | ipv6} {multicast | unicast}
```

```
no address-family {ipv4 | ipv6} {multicast | unicast}
```

Syntax Description

ipv4	Specifies the IPv4 address family.
ipv6	Specifies the IPv6 address family.
multicast	Specifies multicast address support.
unicast	Specifies unicast address support.

Command Default

This command has no default settings.

Command Modes

Router configuration
Neighbor configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **address-family** command to enter various address family configuration modes while configuring BGP routing. When you enter the **address-family** command from router configuration mode, you enable the address family and enter global address family configuration mode. The prompt changes to `switch(config-router-af)#`.

You must configure the address families if you are using route redistribution, address aggregation, load balancing, and other advanced features. IPv4 neighbor sessions support IPv4 unicast and multicast address families. IPv6 neighbor sessions support IPv6 unicast and multicast address families.

From the address family configuration mode, the following parameters are available:



Note

This applies to IPv4 multicast or unicast and IPv6 multicast or unicast.

- **suppress-inactive**—Advertise only active routes to peer. See the **suppress-inactive** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

- **aggregate-address**—Configures BGP aggregate prefixes. See the **aggregate-address** command for additional information.
- **client-to-client reflection**—Enables client-to-client route reflection. Route reflection allows a BGP speaker (route reflector) to advertise IBGP learned routes to certain IBGP peers. Use the **no** form of this command to disable client-to-client route reflection. Default: Enabled.
- **dampening** [*half-life* | **route-map** *name*]—Configures the route flap dampening. Optionally, you can set the time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The default half-life is 15 minutes. Range: 1 to 45. Default: Disabled.
- **default-metric** *metric*—Sets the default flap metric of redistributed routes. The **default-metric** command is used to set the metric value for routes redistributed into BGP with the **redistribute** command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur. This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value. Range: 0 to 4294967295.



Note

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

- **default-originate**—Originates a default toward this peer.
- **distance** *ebgp-route ibgp-route local-route*—Configures a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. BGP does not use discard routes for next-hop resolution. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP. Range: 1 to 255. Default: EBGp—20, IBGP—200.



Caution

Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

- **exit**—Exits from the current command mode.
- **maximum-paths** [**ibgp**] *parallel-paths*—Configures the number of parallel paths to forward packets. The **maximum-paths** **ibgp** command is used to configure equal-cost or unequal-cost multipath load sharing for iBGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to iBGP peers when iBGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path. To configure equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance. The optional **ibgp** keyword allows you to configure multipath for the IBGP paths. To return to the default, use the **no** form of this command. The range is from 1 to 16.

Send document comments to nexus7k-docfeedback@cisco.com

- **network**—Configures an IP prefix to advertise. See the **network** command for additional information.
- **no**—Negates a command or set its defaults
- **redistribute**—Enables the redistribution of routes learned by other protocols into BGP. Redistribution is supported for both IPv4 and IPv6 routes. To disable the redistribution of routes learned by other protocols into BGP, use the **no** form of this command.
 - **direct route-map name**—Specifies directly connected routes.
 - **eigrp AS-num route-map name**—Specifies Enhanced Interior Gateway Protocol routes. Range: 1 to 65535.
 - **isis src-protocol route-map name**—Specifies ISO IS-IS routes.
 - **ospf src-protocol route-map name**—Specifies Open Shortest Path First (OSPF) routes.
 - **rip src-protocol route-map name**—Specifies Routing Information Protocol (RIP) routes.
 - **static route-map name**—Specifies static routes.

This command requires the Enterprise Services license.

Examples

This example shows how to place the router in global address family configuration mode for the IPv4 unicast address family:

```
switch(config)# feature bgp
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)#
```

This example shows how to activate IPv4 multicast for neighbor 192.0.2.1 and place the device in neighbor address family configuration mode for the IPv4 multicast address family:

```
switch(config)# feature bgp
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# exit
switch(config-router)# neighbor 192.0.2.1
switch(config-router-neighbor)# remote-as 1
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)
```

Related Commands

Command	Description
aggregate-address	Configures BGP summary addresses.
client-to-client	Configures route reflection.
dampening	Configures route flap dampening.
default-metric (BGP)	Configures the default metric for routes redistributed into BGP.
distance (BGP)	Configures the administrative distance.
feature bgp	Enables BGP configuration.
maximum-paths (BGP)	Configures the maximum number of equal-cost paths.
redistribute (BGP)	Configures route redistribution for BGP.
timers (BGP)	Configures the BGP timers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

address-family (EIGRP)

To configure an address family for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **address-family** command in router configuration mode.

address-family {ipv4 | ipv6} unicast

Syntax Description

ipv4	Specifies the IPv4 address family.
ipv6	Specifies the IPv6 address family.
unicast	Specifies unicast address support.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise license.

Examples

The following example shows how to set the IPv4 unicast address family for an EIGRP instance:

```
switch(config)# router eigrp 201
switch(config-router)# address-family ipv4 unicast
```

Related Commands

Command	Description
default-information	Controls the distribution of a default route.
default-metric	Configures the default metric for routes redistributed into EIGRP.
distance	Configures the administrative distance.
maximum-paths	Configures the maximum number of equal-cost paths.
redistribute	Configures route redistribution for EIGRP.
router-id	Configures the router ID.
timers	Configures the EIGRP timers.

Send document comments to nexus7k-docfeedback@cisco.com

address-family (IS-IS)

To enter the address family mode or a VRF address-family mode and configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS), use the **address-family** command. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

address-family {ipv4 | ipv6} unicast

no address-family {ipv4 | ipv6} unicast

Syntax Description	Command	Description
	ipv4	Specifies the IPv4 address family.
	ipv6	Specifies the IPv6 address family.
	unicast	Specifies unicast address support.

Command Default None

Command Modes Router configuration
VRF configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **address-family** command to enter various address family configuration modes while configuring IS-IS routing. When you enter the **address-family** command from configuration mode, you enable the address family and enter global address family configuration mode. The prompt changes to `switch(config-router-af)#`.

You must configure the address families if you are using route redistribution, address aggregation, load balancing, and other advanced features. IPv4 neighbor sessions support IPv4 unicast address families. IPv6 neighbor sessions support IPv6 unicast address families.

From the address family configuration mode, the following configuration modes are available:



Note

This applies to IPv4 unicast and IPv6 unicast.

- **adjacency-check**—Allows Intermediate System-to-Intermediate System (IS-IS) IPv6 or IPv4 protocol-support consistency checks to be performed on hello packets. To disable consistency checks on hello packets, use the **no** form of this command. Default: Enabled. IS-IS performs

Send document comments to nexus7k-docfeedback@cisco.com

consistency checks on hello packets and will form an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 only.

Use the **no adjacency-check** command in address-family configuration mode to suppress the consistency checks for IPv6 IS-IS and allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS and IPv6. IS-IS will never form an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

Use the **no adjacency-check** configuration mode command to suppress the IPv4 subnet consistency check and allow IS-IS to form an adjacency with other routers regardless of whether or not they have an IPv4 subnet in common. By default, IS-IS makes checks in hello packets for IPv4 address subnet matching with a neighbor.



Tip

Use the **debug isis adjacency packets** command in privileged EXEC mode to check for adjacency errors. Error messages in the output may indicate where routers are failing to establish adjacencies.

- **default-information originate [always] [route-map name]**—Controls the origination of a default route.
 - **always**—(Optional) Always advertises the default route.
 - **route-map name**—(Optional) Specifies the name of the route-map to announce the default routes.
- **distance value**—Specifies the administrative distance. To return to the default distance, use the **no** form of this command. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Range: 1 to 255. Default: 115.
- **distribute {level-1 | level-2} into {level-1 | level-2} {all | route-map name}**—Configures domain-wide prefix distribution between levels.
 - **level-1**—Distributes the interarea routes into level-1 of this IS-IS instance.
 - **level-2**—Distributes the interarea routes into level-2 of this IS-IS instance.
 - **into**—Specifies from one level to another level.
 - **all**—Distributes all route levels.
 - **route-map name**—Prevents distribution of a specific route-map.
- **exit**—Exits from the current command mode.
- **no**—Negates a command or set its defaults.
- **redistribute protocol as-num[.as-num] [route-map map-tag]**—Redistributes information from another routing protocol into IS-IS. To remove the **redistribute** command from the configuration file and return to the default setting, use the **no** form of this command. Default: Software does not redistribute routes. See the **redistribute (IS-IS)** command for information.
- **summary-address {ip-addr | ip-prefix/length | ipv6-addr | ipv6-prefix/length} level**—Creates the IS-IS aggregate addresses. To remove the aggregate address, use the **no** form of this command. See the **summary-address** command for information.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv6 address family:

```
switch(config)# router isis 100
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)#
```

The following example redistributes directly connected routes into IS-IS. This example advertises only 10.1.0.0 into the IS-IS level-1 link-state PDU.

```
switch(config)# router isis 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute direct route-map core1
switch(config-router-af)# summary-address 10.1.0.0 255.255.0.0
```

The following example shows how to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, enter the **no adjacency-check** command.

```
switch(config)# router isis test2
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# no adjacency-check
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

address-family (OSPFv3)

To enter address family mode for the Open Shortest Path First version 3(OSPFv3) protocol, use the **address-family** command.

address-family ipv6 unicast

Syntax Description

ipv6	Specifies the IPv6 address family.
unicast	Specifies unicast address support.

Defaults

This command has no default settings.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to enter the IPv6 unicast address family for an OSPFv3v3 instance:

```
switch(config)# router ospfv3v3 Enterprise
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)#
```

Related Commands

Command	Description
default-information (OSPFv3)	Controls the distribution of a default route.
default-metric (OSPFv3)	Configures the default metric for routes redistributed into OSPFv3.
distance (OSPFv3)	Configures the administrative distance.
maximum-paths (OSPFv3)	Configures the maximum number of equal-cost paths.
redistribute (OSPFv3)	Configures route redistribution for OSPFv3.
timers (OSPFv3)	Configures the OSPFv3 timers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

address-family (RIP)

To configure an address family for the Routing Information Protocol (RIP), use the **address-family** command in router configuration mode.

address-family { ipv4 | ipv6 } unicast

Syntax Description

ipv4	Specifies the IPv4 address family.
ipv6	Specifies the IPv6 address family.
unicast	Specifies unicast address support.

Defaults

This command has no default settings.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to set the IPv4 unicast address family for a RIP instance:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
```

Related Commands

Command	Description
default-information	Controls the distribution of a default route.
default-metric	Configures the default metric for routes redistributed into RIP.
distance	Configures the administrative distance.
maximum-paths	Configures the maximum number of equal-cost paths.
redistribute	Configures route redistribution for RIP.
timers	Configures the RIP timers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

advertisement-interval (VRRP)

To specify the time interval between the advertisement packets that are being sent to other VRRP routers in the same group, use the **advertisement-interval** command. To return to the default interval value of 1 second, use the **no** form of this command.

advertisement-interval *seconds*

no advertisement-interval

Syntax	Description
<i>seconds</i>	Number of seconds between advertisement frames being sent. For IPv4, the range is from 1 to 255 seconds.

Defaults
1 second

Command Modes
VRRP configuration

Supported User Roles
Superuser VDC administrator

Command History	Release	Modified
	4.0(1)	This command was introduced.

Usage Guidelines

VRRP advertisements communicate the priority and state of the virtual router master. The advertisements are encapsulated in IP packets and are sent to the IPv4 multicast address that is assigned to the VRRP group.

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA-assigned VRRP IP protocol number is 112.

This command does not require a license.

Examples

This example shows how to specify an advertisement interval of 200 seconds for VRRP group 250:

```
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# advertisement-interval 200
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show vrrp	Displays VRRP configuration information.
	clear vrrp	Clears all the software counters for the specified virtual router.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aggregate-address

To create a summary address in a Border Gateway Protocol (BGP) routing table, use the **aggregate-address** command. To remove the summary address, use the **no** form of this command.

```
aggregate-address address/length [advertise-map map-name] [as-set] [attribute-map map-name]
[summary-only] [suppress-map map-name]
```

```
no aggregate-address address/mask-length [advertise-map map-name] [as-set] [attribute-map
map-name] [summary-only] [suppress-map map-name]
```

Syntax Description	
<i>address/length</i>	Aggregate IP address and mask length. Valid values for <i>length</i> are as follows: <ul style="list-style-type: none"> IPv4 addresses—1 to 32 IPv6 addresses—1 to 128
advertise-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select attribute information from specific routes.
as-set	(Optional) Generates the autonomous system set path information and community information from the contributing paths.
attribute-map <i>map-name</i>	(Optional) Specifies the name of the route map used to set the attribute information for specific routes. The map-name is an alphanumeric string up to 63 characters.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map <i>map-name</i>	(Optional) Specifies the name of the route map used to conditionally filter more specific routes. The map-name is an alphanumeric string up to 63 characters.

Defaults

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes

Address-family configuration
Neighbor address-family configuration
Router BGP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Usage Guidelines

You can implement aggregate routing in BGP and mBGP either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **summary-only** keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

This command requires the Enterprise Services license.

Examples

AS-Set Example

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
switch(config)# router bgp 50000
switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Summary-Only Example

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database (SAFI) under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
switch(config)# router bgp 50000
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Conditional Aggregation Example

In the following example, a route map called MAP-ONE is created to match on an as-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
switch(config)# ip as-path access-list 1 deny ^1234_
switch(config)# ip as-path access-list 1 permit .*
switch(config)# !
switch(config)# route-map MAP-ONE
switch(config-route-map)# match ip as-path 1
switch(config-route-map)# exit
switch(config)# router bgp 50000
switch(config-router)# address-family ipv4
switch(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
switch(config-router-af)# end
```

Related Commands

Command	Description
<code>route-map <i>map-name</i></code>	Creates a route map.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area authentication (OSPF)

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command. To remove authentication for an area, use the **no** form of this command.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication** [**message-digest**]

Syntax Description	
<i>area-id</i>	Identifier for the OSPF area where you want to enable authentication. Specify as either a positive integer value or an IP address.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the <i>area-id</i> argument.

Defaults No authentication

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Use the **area authentication** command to configure the authentication mode for the entire OSPF area. The authentication type and authentication password must be the same for all OSPF devices in an area. Use the **ip ospf authentication-key** command in interface configuration mode to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** command in interface configuration mode.

This command requires the Enterprise Services license.

Examples The following example shows how to configure authentication for area 0 of OSPF routing process 201:

```
switch(config)# router ospf 201
switch(config-router)# area 0 authentication message-digest
switch(config-router)# interface ethernet 1/1
switch(config-if)# ip ospf area 0
switch(config)-if# ip ospf message-digest-key 10 md5 0 adcdefgh
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ip ospf authentication-key	Assigns a password for simple password authentication for OSPF.
	ip ospf message-digest-key	Assigns a password for OSPF MD5 authentication.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area default-cost (OSPF)

To specify a cost for the default summary route sent into an Open Shortest Path First (OSPF) stub or not-so-stubby area (NSSA), use the **area default-cost** command. To remove the assigned default route cost, use the **no** form of this command.

```
area area-id default-cost cost
```

```
no area area-id default-cost cost
```

Syntax Description		
<i>area-id</i>		Identifier for the OSPF area where you want to configure the default cost. Specify as either a positive integer value or an IP address.
<i>cost</i>		Cost for the default summary route used for a stub or NSSA. The range is from 0 to 16777215.

Defaults The summary route cost is based on the area border router that generated the summary route.

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **area default-cost** command on an Area Border Router (ABR) attached to a stub or NSSA to configure the metric for the summary default route generated by the ABR into the stub area.

This command requires the Enterprise Services license.

Examples The following example shows how to a default cost of 20 to stub network 192.0.2.0:

```
switch(config)# router ospf 201
switch(config-router)# area 192.0.2.0 stub
switch(config-router)# area 192.0.2.0 default-cost 20
```

Related Commands	Command	Description
	area stub	Defines an area as a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area default-cost (OSPFv3)

To specify a cost for the default summary route sent into an Open Shortest Path First version 3 (OSPFv3) stub or not-so-stubby area (NSSA), use the **area default-cost** command. To remove the assigned default route cost, use the **no** form of this command.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost** *cost*

Syntax Description

<i>area-id</i>	Identifier for the OSPFv3 area where you want to configure the default cost. Specify as either an IP address or a number from 0 to 4294967295.
<i>cost</i>	Cost for the default summary route used for a stub or NSSA. The range is from 0 to 16777215.

Defaults

The summary route cost is based on the area border router that generated the summary route.

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **area default-cost** command on an Area Border Router (ABR) attached to a stub or NSSA to configure the metric for the summary default route generated by the ABR into the stub area.

This command requires the Enterprise Services license.

Examples

This example shows how to a default cost of 20 to stub network 33:

```
switch(config)# router ospfv3 201
switch(config-router)# area 33 stub
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 33 default-cost 20
```

Related Commands

Command	Description
area stub	Defines an area as a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area filter-list (OSPF)

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command. To change or cancel the filter, use the **no** form of this command.

```
area area-id filter-list route-map map-name {in | out}
```

```
no area area-id filter-list route-map map-name {in | out}
```

Syntax Description

<i>area-id</i>	Identifier for the OSPF area where you want to configure filtering. Specify as either a positive integer value or an IP address.
route-map <i>map-name</i>	Specifies the name of a route map used as the filter policy. The <i>map-name</i> argument can be any alphanumeric string of up to 63 characters.
in	Filters networks sent to this area.
out	Filters networks sent from this area.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **area filter-list** command to filter Type 3 LSAs. If you apply the route map with the **in** keyword, the route map filters all Type 3 LSAs originated by the ABR to this area, including Type 3 LSAs that originated as a result of the **area range** command in another area.

If you apply the route map with the **out** keyword, the route map filters all Type 3 LSAs that are advertised by the ABR to all other areas including Type 3 LSAs that originate locally as a result of the **area range** command configured in this area.

Cisco NX-OS implicitly denies any prefix that does not match an entry in the route map.

This command requires the Enterprise Services license.

Examples

The following example shows how to filter prefixes that are sent from all other areas to area 1:

```
switch(config)# router ospf 202
switch(config-router)# area 1 filter-list route-map FilterExternal in
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area filter-list (OSPFv3)

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First version 3 (OSPFv3) areas of an Area Border Router (ABR), use the **area filter-list** command. To change or cancel the filter, use the **no** form of this command.

```
area area-id filter-list route-map map-name {in | out}
```

```
no area area-id filter-list route-map map-name {in | out}
```

Syntax Description

<i>area-id</i>	Identifier for the OSPFv3 area where you want to configure filtering. Specify as either an IP address or a number from 0 to 4294967295.
route-map <i>map-name</i>	Specifies the name of a route map used as the filter policy. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
in	Filters networks sent to this area.
out	Filters networks sent from this area.

Defaults

None

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **area filter-list** command to filter Type 3 LSAs. If you apply the route map with the **in** keyword, the route map filters all Type 3 LSAs originated by the ABR to this area, including Type 3 LSAs that originated as a result of the **area range** command in another area.

If you apply the route map with the **out** keyword, the route map filters all Type 3 LSAs that are advertised by the ABR to all other areas including Type 3 LSAs that originate locally as a result of the **area range** command configured in this area.

Cisco NX-OS implicitly denies any prefix that does not match an entry in the route map.

This command requires the Enterprise Services license.

Examples

This example shows how to filter prefixes that are sent from all other areas to area 1:

```
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 1 filter-list route-map FilterExternal in
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area range (OSPFv3)	Consolidates and summarizes routes at an area boundary.
	route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area nssa (OSPF)

To configure an area as an Open Shortest Path First (OSPF) not-so-stubby area (NSSA), use the **area nssa** command. To remove the NSSA area, use the **no** form of this command.

```
area area-id nssa [default-information-originate [route-map map-name]] [no-redistribution]
[no-summary] [translate type7 [always | never] [suppress-fa]]
```

```
no area area-id nssa [default-information-originate [route-map map-name]]
[no-redistribution] [no-summary] [translate type7 [always | never] [suppress-fa]]
```

Syntax Description	
<i>area-id</i>	Identifier for the OSPF NSSA area. Specify as either a positive integer value or an IP address.
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on NSSA ABR or NSSA ASBR.
route-map <i>map-name</i>	(Optional) Filters the Type 7 default generation based on the route map. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
no-redistribution	(Optional) Blocks redistributed LSAs from entering this NSSA area. Use this keyword when the router is both an NSSA autonomous system border router (ASBR) and an NSSA area border router (ABR) and you want the redistribute command to import routes into the normal areas but not into the NSSA area.
no-summary	(Optional) Allows an area to be an NSSA area but not have summary routes injected into it.
translate type7	(Optional) Translates Type 7 LSAs to type 5 LSAs.
always	(Optional) Always translates LSAs.
never	(Optional) Never translates LSAs.
suppress-fa	(Optional) Suppresses the forwarding address in translated LSAs. The ABR uses 0.0.0.0 as the forwarding IPv4 address.

Defaults None

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **area nssa** command to create an NSSA area in an OSPF autonomous system. We recommend that you understand the network topology before configuring forwarding address suppression for translated LSAs. Suboptimal routing might result because there might be better paths to reach the destination's forwarding address.

This command requires the Enterprise Services license.

Examples

The following example shows how to configure area 1 as an NSSA area:

```
switch(config)# router ospf 10
switch(config-router)# area 1 nssa
```

The following example shows how to configure area 1 as an NSSA area and translate Type 7 LSAs from area 1 to Type 5 LSAs, but not place the Type 7 forwarding address into the Type 5 LSAs. (OSPF places 0.0.0.0 as the forwarding address in the Type 5 LSAs.):

```
switch(config)# router ospf 2
switch(config-router)# area 1 nssa translate type7 suppress-fa
```

Related Commands

Command	Description
redistribute	Redistributes routes learned from one routing protocol to another routing protocol domain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area nssa (OSPFv3)

To configure an area as an Open Shortest Path First version 3 (OSPFv3) not-so-stubby area (NSSA), use the **area nssa** command. To remove the NSSA area, use the **no** form of this command.

```
area area-id nssa [default-information-originate [route-map map-name]] [no-redistribution]
[no-summary] [translate type7 [always | never] [suppress-fa]]
```

```
no area area-id nssa [default-information-originate [route-map map-name]]
[no-redistribution] [no-summary] [translate type7 [always | never] [suppress-fa]]
```

Syntax Description	
<i>area-id</i>	Identifier for the OSPFv3 NSSA area. Specify as either an IP address or a number from 0 to 4294967295.
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on NSSA ABR or NSSA ASBR.
route-map <i>map-name</i>	(Optional) Filters the Type 7 default generation based on the route map. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
no-redistribution	(Optional) Blocks redistributed LSAs from entering this NSSA area. Use this keyword when the router is both an NSSA autonomous system border router (ASBR) and an NSSA area border router (ABR) and you want the redistribute command to import routes into the normal areas but not into the NSSA area.
no-summary	(Optional) Allows an area to be an NSSA area but not have summary routes injected into it.
translate type7	(Optional) Translates Type 7 LSAs to type 5 LSAs.
always	(Optional) Always translates LSAs.
never	(Optional) Never translates LSAs.
suppress-fa	(Optional) Suppresses the forwarding address in translated LSAs. The ABR uses 0.0.0.0 as the forwarding IPv4 address.

Defaults None

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **area nssa** command to create an NSSA area in an OSPFv3 autonomous system. We recommend that you understand the network topology before configuring forwarding address suppression for translated LSAs. Suboptimal routing might result because there might be better paths to reach the destination's forwarding address.

This command requires the Enterprise Services license.

Examples

This example shows how to configure area 1 as an NSSA area:

```
switch(config)# router ospfv3 10
switch(config-router)# area 1 nssa
```

This example shows how to configure area 1 as an NSSA area and translate Type 7 LSAs from area 1 to Type 5 LSAs, but not place the Type 7 forwarding address into the Type 5 LSAs. (OSPFv3 places 0.0.0.0 as the forwarding address in the Type 5 LSAs.):

```
switch(config)# router ospfv3 2
switch(config-router)# area 1 nssa translate type7 suppress-fa
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes routes learned from one routing protocol to another routing protocol domain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area range (OSPF)

To consolidate and summarize routes at an Open Shortest Path First (OSPF) area boundary, use the **area range** command. To disable this function, use the **no** form of this command.

```
area area-id range ip-prefix [not-advertise]
```

```
no area area-id range ip-prefix [not-advertise]
```

Syntax Description		
<i>area-id</i>	Identifier for the OSPF area where you want to summarize routes. Specify as either a positive integer value or an IP address.	
<i>ip-prefix</i>	IP prefix specified as IP address/subnet mask length (A.B.C.D/LEN).	
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.	

Defaults Disabled

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **area range** command only with Area Border Routers (ABRs) to consolidate or summarize routes for an area. The ABR advertises that a single summary route is advertised to other areas and condenses routing information at area boundaries.

You can configure OSPF to summarize addresses for many different sets of address ranges by configuring multiple **area range** commands.

This command requires the Enterprise Services license.

Examples The following example shows how to configure one summary route to be advertised by the ABR to other areas for all hosts on network 192.0.2.0:

```
switch(config-if)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.201 255.255.255.0
switch(config-if)# ip ospf area 201
switch(config-router)# area 0 range 192.0.2.0 255.255.0.0
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area range (OSPFv3)

To consolidate and summarize routes at an Open Shortest Path First version 3 (OSPFv3) area boundary, use the **area range** command. To disable this function, use the **no** form of this command.

```
area area-id range ipv6-prefix/length [not-advertise]
```

```
no area area-id range ipv6-prefix [not-advertise]
```

Syntax Description		
<i>area-id</i>	Identifier for the OSPF area where you want to summarize routes. Specify as either an IP address or a number from 0 to 4294967295.	
<i>ipv6-prefix/length</i>	IP prefix specified as IPv6 address/length (A:B::C:D/LEN). The <i>length</i> argument can be from 1 to 127.	
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.	

Defaults	
Disabled	

Command Modes	
Router configuration	

Supported User Roles	
network-admin vdc-admin	

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	
Use the area range command only with Area Border Routers (ABRs) to consolidate or summarize routes for an area. The ABR advertises that a single summary route is advertised to other areas and condenses routing information at area boundaries.	

You can configure OSPFv3 to summarize addresses for many different sets of address ranges by configuring multiple **area range** commands.

This command requires the Enterprise Services license.

Examples	
This example shows how to configure one summary route to be advertised by the ABR to other areas for all hosts on network 2001:0DB8::/32:	

```
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 0 range 2001:0DB8::/32
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area stub (OSPF)

To define an area as an Open Shortest Path First (OSPF) stub area, use the **area stub** command. To remove the area, use the **no** form of this command.

```
area area-id stub [no-summary]
```

```
no area area-id stub [no-summary]
```

Syntax Description		
<i>area-id</i>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	

Defaults	None
----------	------

Command Modes	Router configuration
---------------	----------------------

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the area stub command to configure all devices attached to the stub area. Use the area default-cost command on an area border router (ABR) attached to the stub area. The area default-cost command provides the metric for the summary default route generated by the ABR into the stub area.
------------------	---

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending Summary LSAs (Type 3 LSAs3) into the stub area.

This command requires the Enterprise Services license.

Examples	The following example shows how to create stub area 33 in OSPF 209:
----------	---

```
switch(config)# router ospf 201
switch(config-router)# area 33 stub
```

Related Commands	Command	Description
	area default-cost	Specifies a cost for the default summary route sent into a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area stub (OSPFv3)

To define an area as an Open Shortest Path First version 3 (OSPFv3) stub area, use the **area stub** command. To remove the area, use the **no** form of this command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Syntax Description		
	<i>area-id</i>	Identifier for the OSPFv3 stub area. Specify as either an IP address or a number from 0 to 4294967295.
	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Defaults	
	None

Command Modes	
	Router configuration

Supported User Roles	
	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Use the **area stub** command to configure all devices attached to the stub area. Use the **area default-cost** command on an area border router (ABR) attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending Summary LSAs (Type 3 LSAs3) into the stub area.

This command requires the Enterprise Services license.

Examples

This example shows how to create stub area 33 in OSPFv3 209:

```
switch(config)# router ospfv3 201
switch(config-router)# area 33 stub
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
area default-cost (OSPFv3)	Specifies a cost for the default summary route sent into a stub area.

Send document comments to nexus7k-docfeedback@cisco.com

area virtual-link (OSPF)

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id*

no area *area-id* **virtual-link** *router-id*

Syntax Description	Parameter	Description
	<i>area-id</i>	Identifier for the OSPF area assigned to the transit area for the virtual link. Specify as either a positive integer value or an IP address.
	<i>router-id</i>	Router ID associated with the virtual link neighbor. Specify as an IP address. The router ID appears in the show ip ospf neighbors display.

Defaults None

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **area virtual-link** command to establish a virtual link from a remote area to the backbone area. In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

Use the **area virtual-link** command to enter the virtual link configuration mode where you can use the following commands:

- **authentication** [**key-chain** | **message-digest** | **null**]
- **authentication-key** [**0** | **3**] *key*
- **dead-interval** *seconds*
- **hello-interval** *seconds*
- **message-digest-key** *key-id* **md5** *key*
- **retransmit-interval** *seconds*
- **transmit-delay** *seconds*

See each command for syntax and usage details.

Send document comments to nexus7k-docfeedback@cisco.com

You must configure both sides of a virtual link with the same area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf neighbors** command in any mode.

This command requires the Enterprise Services license.

Examples

The following example shows how to establish a virtual link between two devices, A, and B, with default values for all optional parameters:

```
Device A:
switch(config)# router ospf 1
switch(config-router)# router-id 192.0.2.2
switch(config-router)# area 1 virtual-link 192.0.2.1
```

```
Device B:
switch(config)# router ospf 209
switch(config-router)# router-id 192.0.2.1
switch(config-router)# area 1 virtual-link 192.0.2.2
```

Related Commands

Command	Description
authentication (OSPF virtual link)	Enables authentication for an OSPF virtual link.
authentication-key (OSPF virtual link)	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
dead-interval (OSPF virtual link)	Configures the dead interval for an OSPF virtual link.
hello-interval (OSPF virtual link)	Configures the hello interval for an OSPF virtual link.
message-digest-key (virtual link)	Enables OSPF MD5 authentication in an OSPF virtual link.
retransmit-interval (OSPF virtual link)	Configures the retransmit interval for an OSPF virtual link.
transmit-delay (OSPF virtual link)	Configures the transmit delay for an OSPF virtual link.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area virtual-link (OSPFv3)

To define an Open Shortest Path First version 3 (OSPFv3) virtual link, use the **area virtual-link** command. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id*

no area *area-id* **virtual-link** *router-id*

Syntax Description		
	<i>area-id</i>	Identifier for the OSPFv3 area assigned to the transit area for the virtual link. Specify as either an IP address or a number from 0 to 4294967295.
	<i>router-id</i>	Router ID associated with the virtual link neighbor. Specify as an IP address. The router ID appears in the show ospfv3 neighbors display.

Defaults	
	None

Command Modes	
	Router configuration

Supported User Roles	
	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Use the **area virtual-link** command to establish a virtual link from a remote area to the backbone area. In OSPFv3, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

Use the **area virtual-link** command to enter the virtual link configuration mode where you can use the following commands:

- **dead-interval** *seconds*
- **hello-interval** *seconds*
- **retransmit-interval** *seconds*
- **transmit-delay** *seconds*

See each command for syntax and usage details.

You must configure both sides of a virtual link with the same area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ospfv3 neighbors** command in any mode.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to establish a virtual link between two devices, A, and B, with default values for all optional parameters:

Device A:

```
switch(config)# router ospfv3 1
switch(config-router)# router-id 192.0.2.2
switch(config-router)# area 1 virtual-link 192.0.2.1
```

Device B:

```
switch(config)# router ospfv3 209
switch(config-router)# router-id 192.0.2.1
switch(config-router)# area 1 virtual-link 192.0.2.2
```

Related Commands

Command	Description
dead-interval (OSPFv3 virtual link)	Configures the dead interval for an OSPFv3 virtual link.
hello-interval (OSPFv3 virtual link)	Configures the hello interval for an OSPFv3 virtual link.
retransmit-interval (OSPFv3 virtual link)	Configures the retransmit interval for an OSPFv3 virtual link.
transmit-delay (OSPFv3 virtual link)	Configures the transmit delay for an OSPFv3 virtual link.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication (GLBP)

To configure an authentication for the Gateway Load Balancing Protocol (GLBP), use the **authentication** command. To disable authentication, use the **no** form of this command.

```
authentication {text string | md5 {key-string [encrypted] key | key-chain name-of-chain}}
```

```
no authentication {text string | md5 {key-string [0 | 7] key | key-chain name-of-chain}}
```

Syntax Description		
text <i>string</i>		Specifies an authentication string. The range is from 1 to 255 characters.
md5		Specifies the Message Digest 5 (MD5) authentication.
key-string <i>key</i>		Specifies the secret key for MD5 authentication. The range is from 1 to 255 characters. We recommend that you use at least 16 characters.
encrypted		(Optional) Specifies the encrypted key.
key-chain <i>name-of-chain</i>		Identifies a group of authentication keys.

Defaults No authentication of GLBP messages occurs.

Command Modes GLBP configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines To ensure interoperability, you must configure the same authentication method on all the gateways that are members of the same GLBP group. A gateway ignores all GLBP messages that contain the wrong authentication information.

This command does not require a license.

Examples The following example shows how to configure stringxyz as the authentication string for GLBP group 10:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# authentication text stringxyz
```

The following example shows how to configure GLBP to use the key chain "AuthenticateGLBP" to obtain the current live key and key ID for MD5 authentication:

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# interface ethernet1/1
switch(config-if)# glbp 2
switch(config-glbp)# authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp	Creates a GLBP group and enters GLBP configuration mode.
ip (GLBP)	Enables GLBP on an interface.
key chain	Creates a key chain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication (OSPF virtual link)

To specify the authentication type for an Open Shortest Path First (OSPF) virtual link, use the **authentication** command. To remove the authentication type for a virtual link, use the **no** form of this command.

authentication [**key-chain** *key-name* | **message-digest** | **null**]

no ip ospf authentication

Syntax Description

key-chain <i>key-name</i>	(Optional) Specifies the key-chain to use. The <i>key-name</i> argument can be any alphanumeric string up to 63 characters.
message-digest	(Optional) Specifies to use message-digest authentication.
null	(Optional) Specifies no authentication is used. Disables authentication if configured for an area.

Defaults

Defaults to password authentication if you configure authentication with none of the optional keywords.

Command Modes

OSPF virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **authentication** command in virtual link configuration mode to configure the authentication method used on the virtual link. Use the **message-digest** keyword to configure MD5 message digest authentication and use the **message-digest-key** command to complete this authentication configuration. Use the **key-chain** keyword to configure password authentication using key chains and use the **key chain** command to complete this authentication configuration. Use the **authentication** command with no keywords to configure a password for the virtual link, and use the **authentication-key** command to complete this authentication configuration.

This command requires the Enterprise Services license.

Examples

The following example shows how to enable message-digest authentication:

```
switch(config)# router ospf 22
switch(config-router)# area 99 virtual-link 192.0.2.12
switch(config-router-vlink)# authentication message-digest
switch(config-router-vlink)# message-digest key 4 md5 0 abcd
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area authentication	Enables authentication for an OSPF area.
	authentication-key (OSPF virtual link)	Assigns a password to be used by neighboring routers that are using the password authentication of OSPF.
	key chain	Creates a key chain for managing authentication keys.
	message-digest-key (OSPF virtual link)	Enables OSPF MD5 authentication.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication (VRRP)

To configure an authentication for the Virtual Router Redundancy Protocol (VRRP), use the **authentication** command. To disable authentication, use the **no** form of this command.

authentication text *password*

no authentication

Syntax Description	text <i>password</i>	Selects to use simple text password of up to 8 alphanumeric characters.
--------------------	-----------------------------	---

Defaults	No authentication
----------	-------------------

Command Modes	VRRP configuration mode
---------------	-------------------------

SupportedUserRoles	Superuser VDC administrator
--------------------	--------------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to configure md5 authentication for VRRP:
----------	--

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# authentication text mypasswd
```

Related Commands	Command	Description
	show vrrp	Displays VRRP configuration information.
	clear vrrp	Clears all the software counters for the specified virtual router.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication (HSRP)

To configure authentication for the Hot Standby Router Protocol (HSRP), use the **authentication** command. To disable authentication, use the **no** form of this command.

```
authentication {text string | md5 {key-chain key-chain | key-string {0 | 7} text [timeout
seconds]}}
```

```
no authentication {text string | md5 {key-chain key-chain | key-string {0 | 7} text [timeout
seconds]}}
```

Syntax Description		
text <i>string</i>		Specifies an authentication string. The range is from 1 to 255 characters. The default string is "cisco".
md5		Specifies the Message Digest 5 (MD5) authentication.
key-chain <i>key-chain</i>		Identifies a group of authentication keys.
key-string		Specifies the secret key for MD5 authentication.
0		Specifies a clear text string.
7		Specifies an encrypted string.
<i>text</i>		The secret key for MD5 authentication. The range is from 1 to 255 characters. We recommend that you use at least 16 characters.
timeout <i>seconds</i>		(Optional) Specifies the authentication timeout value. The range is from 0 to 32767.

Defaults Disabled

Command Modes HSRP configuration or HSRP template mode

SupportedUserRoles Superuser
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **authentication text** command to prevent misconfigured routers from participating in HSRP groups that they are not intended to participate in. The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers in the same group to ensure interoperability. HSRP protocol packets that do not authenticate are ignored.



Caution

If two routers are configured with identical HSRP IP addresses, but with different authentication strings, then neither router will be aware of the duplication.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

The following example shows how to configure an authentication string for HSRP group 2:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# priority 110
switch(config-if-hsrp)# preempt
switch(config-if-hsrp)# authentication text sanjose
switch(config-if-hsrp)# ip 10.0.0.3
switch(config-if-hsrp)# end
```

Related Commands

Command	Description
feature hsrp	Enable HSRP and enters HSRP configuration mode.
hsrp group	Creates an HSRP group.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication key-chain (EIGRP)

To enable authentication for the Enhanced Interior Gateway Routing Protocol (EIGRP) packets and to specify the set of keys that can be used on an interface, use the **authentication key-chain** command. To prevent authentication, use the **no** form of this command.

authentication key-chain *name-of-chain*

no authentication key-chain *name-of-chain*

Syntax Description

<i>name-of-chain</i>	Group of keys that are valid.
----------------------	-------------------------------

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

Set the authentication mode using the **authentication mode** command in VRF configuration mode. You must separately configure a key chain using the **key-chain** command to complete the authentication configuration for an interface.

This command requires the Enterprise Services license.

Examples

The following example shows how to configure the interface to accept and send any key that belongs to the key-chain trees:

```
switch(config)# router eigrp 209
switch(config-router)# vrf red
switch(config-router-vrf)# authentication key-chain trees
```

Related Commands

Command	Description
authentication mode (EIGRP)	Sets the authentication mode for EIGRP in a VRF.
ip authentication key-chain eigrp	Enables authentication for EIGRP and specifies the set of keys that can be used on an interface.
key-chain	Creates a set of keys that can be used by an authentication method.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication key-chain (IS-IS)

To enable authentication for Intermediate System-to-Intermediate System (IS-IS), use the **authentication key-chain** configuration mode command. To disable such authentication, use the **no** form of this command.

authentication key-chain *auth-key* {**level-1** | **level-2**}

no authentication key-chain *auth-key* {**level-1** | **level-2**}

Syntax Description	<i>auth-key</i>	Authentication key chain.
	level-1	Specifies the authentication key for level-1 link state packets (LSP), complete sequence number packets (CSNP), and partial sequence number packets (PSNP) only.
	level-2	Specifies the authentication key for level-2 LSP, CSNP and PSNP packets only.

Command Default No key chain authentication is provided for IS-IS packets at the router level.

Command Modes Router configuration
VRF configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines If no key chain is configured with the **authentication key-chain** command, no key chain authentication is performed.

Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the authentication mode command.

Only one authentication key chain is applied to IS-IS at one time. For example, if you configure a second **authentication key-chain** command, the first authentication key chain is overridden.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key-chain** command.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
switch(config)# router isis real_secure_network  
switch(config-router)# authentication key-chain site1 level-1
```

Related Commands

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
isis authentication key-chain	Enables authentication for an individual IS-IS interface.
no	Negates a command or sets its defaults.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

authentication mode (EIGRP)

To specify the type of authentication used in the Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **authentication mode** command. To remove authentication, use the **no** form of this command.

authentication mode md5

no authentication mode md5

Syntax Description	md5	Specifies Message Digest 5 (MD5) authentication.
Defaults	None	
Command Modes	Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to configure the interface to use MD5 authentication:	
	<pre>switch(config)# router eigrp 209 switch(config-router)# vrf red switch(config-router-vrf)# authentication mode md5</pre>	
Related Commands	Command	Description
	authentication key-chain eigrp	Enables authentication for EIGRP and specifies the set of keys that can be used on an interface.
	ip authentication mode eigrp	Configures the authentication mode for EIGRP on an interface.
	key chain	Creates a set of keys that can be used by an authentication method.

Send document comments to nexus7k-docfeedback@cisco.com

authentication-check

To specify for the Intermediate System-to-Intermediate System (IS-IS) instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication-check** configuration mode command. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

authentication-check {level-1 | level-2}

no authentication-check

Syntax Description

level-1	Specifies that authentication is performed only on level-1 packets that are being sent (not received)
level-2	Specifies that authentication is performed only on level-2 packets that are being sent (not received).

Command Default

If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes

Router configuration
VRF configuration

Usage Guidelines

Enter the **authentication-check** command before configuring the authentication mode and authentication key chain. Entering the **authentication-check** command allows the routers to have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After you enter the authentication-check command on all communicating routers, enable the authentication mode and key chain on each router. Then enter the **no authentication-check** command to disable the command.

This command could apply to clear text authentication or Message Digest 5 (MD5) authentication. The mode is determined by the authentication mode command.

You can specify authentication for an individual IS-IS interface by using the **isis authentication-check {level-1 | level-2}** interface configuration mode command.

This command requires the Enterprise Services license.

Examples

The following example configures IS-IS level-1 packets to use clear text authentication on packets being sent (not received):

```
switch(config)# router isis test1
switch(config-router)# authentication-check level-1
switch(config-router)# authentication key-chain site1 level-1
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	isis authentication-check	Enables authentication on IS-IS packets being sent (not received) from a specific interface.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication-key (OSPF virtual link)

To assign a password to be used by an Open Shortest Path First (OSPF) virtual link, use the **authentication-key** command. To remove a previously assigned OSPF password, use the **no** form of this command.

authentication-key [**0** | **3**] *password*

no authentication-key

Syntax Description		
	0	(Optional) Specifies an unencrypted authentication key.
	3	(Optional) Specifies a 3DES encrypted authentication key.
	<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Defaults Unencrypted password

Command Modes OSPF virtual link configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **authentication-key** command to configure the password for password authentication on an OSPF virtual link. All devices on the same virtual link must have the same password to be able to exchange OSPF information.

This command requires the Enterprise Services license.

Examples The following example shows how to enable the authentication key with the string yourpass:

```
switch(config)# router ospf 22
switch(config-router)# area 99 virtual-link 192.0.2.12
switch(config-router-vlink)# authentication
switch(config-router-vlink)# authentication-key yourpass
```

Related Commands	Command	Description
	authentication (virtual link)	Enables authentication for an OSPF virtual link.

Send document comments to nexus7k-docfeedback@cisco.com

authentication-type

To specify the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets for the IS-IS instance, use the **authentication-type** configuration mode command. To restore clear text authentication, use the **no** form of this command.

authentication-type { **cleartext** | **md5** } [**level-1** | **level-2**]

no authentication-type

Syntax Description

cleartext	Specifies clear text authentication.
md5	Specifies Message Digest 5 (MD5) authentication.
level-1	Enables the specified authentication for level-1 link state packet (LSP), complete sequence number packet (CSNP) and partial sequence number packet (PSNP) packets only.
level-2	Enables the specified authentication for level-2 LSP, CSNP and PSNP packets only.

Command Default

No authentication is provided for IS-IS packets at the router level by use of this command.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you do not enter the **level-1** or **level-2** keywords, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **authentication-type** command.

You can specify authentication type for an individual IS-IS interface by using the **isis authentication-type** { **cleartext** | **md5** } [**level-1** | **level-2**] interface configuration mode command.

Examples

The following example configures for the IS-IS instance that Message Digest 5 (MD5) authentication is performed on level-1 packets:

```
switch(config)# router isis TEST1
switch(config-router)# authentication-type md5 level-1
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	exit	Exits the current configuration mode.
	feature isis	Enables IS-IS on the router.
	isis authentication-type	Specifies the authentication type for an individual IS-IS interface.
	no	Negates a command or sets its defaults.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

auto-cost (OSPF)

To control how Open Shortest Path First (OSPF) calculates default metrics for an interface, use the **auto-cost** command. To assign the default reference bandwidth of 40Gb/s, use the **no** form of this command.

auto-cost reference-bandwidth *bandwidth* [**Gbps** | **Mbps**]

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth <i>bandwidth</i>	Sets the reference bandwidth used to calculate the default metrics for an interface. The range depends on whether you use the Gbps or MBps keywords.
Gbps	(Optional) Specifies the rate in Gbps (bandwidth). The range is from 1 to 4000; the default is 40.
Mbps	(Optional) Specifies the rate in Mbps (bandwidth). The range is from 1 to 4000000; the default is 40000.

Defaults

40 Gb/s. The bandwidth defaults to Gb/s if you do not specify the **Gbps** or **Mbps** keyword.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **auto-cost** command to set the reference bandwidth used by the OSPF cost-metric calculation. The value set by the **ip ospf cost** command overrides the cost that results from the **auto-cost** command. This command requires the Enterprise Services license.

Examples

The following example shows how to set the reference bandwidth for all local interfaces in an OSPF instance:

```
switch(config)# router ospf 201
switch(config-router)# auto-cost reference-bandwidth 10
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
<code>ip ospf cost</code>	Explicitly specifies the cost of sending a packet on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

auto-cost (OSPFv3)

To control how Open Shortest Path First version 3 (OSPFv3) calculates default metrics for an interface, use the **auto-cost** command. To assign the default reference bandwidth of 40Gb/s, use the **no** form of this command.

auto-cost reference-bandwidth *bandwidth* [**Gbps** | **Mbps**]

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth <i>bandwidth</i>	Sets the reference bandwidth used to calculate the default metrics for an interface. The range depends on whether you use the Gbps or MBps keywords.
Gbps	(Optional) Specifies the rate in Gbps (bandwidth). The range is from 1 to 4000; the default is 40.
Mbps	(Optional) Specifies the rate in Mbps (bandwidth). The range is from 1 to 4000000; the default is 40000.

Defaults

40 Gb/s. The bandwidth defaults to Gb/s if you do not specify the **Gbps** or **Mbps** keyword.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **auto-cost** command to set the reference bandwidth used by the OSPFv3 cost-metric calculation. The value set by the **ipv6 ospfv3 cost** command overrides the cost that results from the **auto-cost** command.

This command requires the Enterprise Services license.

Examples

This example shows how to set the reference bandwidth for all local interfaces in an OSPFv3 instance:

```
switch(config)# router ospfv3 201
switch(config-router)# auto-cost reference-bandwidth 10
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ipv6 ospfv3 cost	Explicitly specifies the cost of sending a packet on an interface.

Send document comments to nexus7k-docfeedback@cisco.com