I Commands

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

inject-map

To specify the inject-map and exist-map routes for conditional route injection, use the **inject-map** command.

inject-map *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**]

Syntax Description

inject-map-name	Inject map route map. An inject map defines the prefixes that are created and installed into the local Border Gateway Protocol (BGP) table.
exist-map	Specifies the prefixes that BGP tracks.
exist-map-name	Exist map route name
copy-attributes	(Optional) Specifies that the injected route inherits the attributes of the aggregate route.

Defaults

None

Command Modes

config-router-neighbor-af mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

The BGP conditional route injection option is available only for IPv4 and IPv6 unicast address families in all VRF instances.

This command requires the Enterprise Services license.

Examples

This example shows how to specify the inject-map and exist-map routes for conditional route injection:

```
switch# configure terminal
switch(config)# router bgp 40000
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# inject-map ORIGINATE exist-map AGGREGATEcopy-attributes
switch(config-router-af)# exit
switch(config-router)# exit
switch(config)#
```

Related Commands

Command	Description
ip prefix-list	Configures a prefix list.
router-map	Configures a route map and enters route-map configuration mode.

ip (GLBP)

To activate the Gateway Load Balancing Protocol (GLBP) for a group, use the **ip** command. To disable GLBP in the group, use the **no** form of this command.

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

no ip [*ip-address* [**secondary**]]

Syntax Description

ip-address	(Optional) Virtual IP address for the GLBP group. The IP address must be in the same subnet as the interface IP address.
secondary	(Optional) Indicates that the IP address is a secondary GLBP virtual address.

Defaults

Disabled

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip** command to activate GLBP on the configured interface. If you configure a virtual IP address, that address is the designated virtual IP address for the entire GLBP group. If you do not configure a virtual IP address, the gateway learns the virtual IP address from another gateway in the same GLBP group. To allow GLBP to elect an active virtual gateway (AVG), you must configure at least one gateway on the LAN with a virtual IP address.

Configuring the virtual IP address on the AVG always overrides a virtual IP address that is in use.

When you configure the **ip** command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Note You must configure all GLBP options before you use the **ip** command to assign a virtual IP address and activate the GLBP group.

This command does not require a license.

Examples

This example shows how to activate GLBP for group 10 on Ethernet interface 1/1. The virtual IP address used by the GLBP group is set to 192.0.2.10.

```
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# glbp 10
switch(config-glbp)# ip 192.0.2.10
```

This example shows how to activate GLBP for group 10 on Ethernet interface 2/1. The virtual IP address used by the GLBP group will be learned from another gateway configured to be in the same GLBP group.

```
switch(config)# interface ethernet 2/1
switch(config-if)# glbp 10
switch(config-glbp)# ip
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
show glbp	Displays GLBP information.

ip (HSRP)

To assign a virtual address to an HSRP group, use the **ip** command. To disable HSRP in the group, use the **no** form of this command.

ip [**autoconfig** | *ip-address* [**secondary**]]

no ip [**autoconfig |** *ip-address* [**secondary**]]

Syntax Description

autoconfig	(Optional) Generates a link-local address from the link-local prefix and a modified EUI-64 format Interface Identifier, where the EUI-64 Interface Identifier is created from the relevant HSRP virtual MAC address. You cannot configure this option if there are global unicast virtual IPv6 addresses configured.
ip-address	(Optional) Virtual IP address for the virtual router (HSRP group). The IP address must be in the same subnet as the interface IP address. You must configure the virtual IP address for at least one of the routers in the HSRP group. Other routers in the group will pick up this address. The IP address can be an IPv4 or an IPv6 address.
secondary	(Optional) Indicates that the IPv4 address is a secondary HSRP virtual address. HSRP IPv6 groups do no have secondary addresses.

Defaults

Disabled

Command Modes

HSRP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	Added IPv6 support and the **autoconfig** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip** command to activate HSRP on the configured interface. If you configure a virtual IP address, that address is the designated virtual IP address for the entire HSRP group. For IPv4 groups, if you do not configure a virtual IP address, the gateway learns the virtual IP address from another gateway in the same HSRP group. To allow HSRP to elect an active group, you must configure at least one gateway on the LAN with a virtual IP address. For IPv6 groups, you can generate the virtual IP address using the **autoconfig** keyword.

If a configured IPv6 address as a link-local address, there are no HSRP ipv6 secondary addresses.

Note You must configure all HSRP options before you use the **ip** command to assign a virtual IP address and activate the HSRP group. This helps you to avoid authentication error messages and unexpected state changes that can occur in other routers when a group is enabled first and then there is a delay before the configuration is created. We recommend that you always specify an IP address

This command does not require a license.

Examples

This example shows how to activate HSRP for group 10 on Ethernet interface 1/1. The virtual IP address used by the HSRP group is set to 192.0.2.10.

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# hsrp 10
switch(config-hsrp)# ip 192.0.2.10
```

This example shows how to activate HSRP for group 10 on Ethernet interface 2/1. The virtual IP address used by the HSRP group will be learned from another gateway configured to be in the same HSRP group.

```
switch(config)# interface ethernet 2/1
switch(config-if)# hsrp 10
switch(config-hsrp)# ip
```

This example shows how to activate HSRP for group 2 on Ethernet interface 1/1 and creates a secondary IP address on the interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 20.20.20.1 255.255.255.0 secondary
switch(config-if)# ip address 10.10.10.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 10.10.10.2
switch(config-if-hsrp)# ip 20.20.20.2 secondary
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.
show hsrp	Displays HSRP information.

ip adjacency notify

To specify the notify interval for the IP adjacency manager, use the **ip adjacency notify** command. To remove the notify interval, use the **no** form of this command.

ip adjacency notify interval *interval*

no ip adjacency notify interval *interval*

Syntax Description

interval *interval*	Specifies the notify interval for the adjacency manager. The default is 500 milliseconds.

Defaults

The notify interval is 500 milliseconds.

Command Modes

Global

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(8)	This command was introduced.

Usage Guidelines

To get optimal BGP PIC convergence, the *interval* value should be set to 100 milliseconds.

This command does not require a license.

Examples

This example shows how to specify the notify interval as 100 milliseconds:

```
switch(config)# ip adjacency notify interval 100
```

Related Commands

Command	Description
additional-paths	Configure the capability of sending and receiving additional paths to and from the BGP peers.
address family (BGP)	Enters the address family configuration mode for BGP.

ip arp

To configure a static Address Resolution Protocol (ARP) entry, use the **ip arp** command. To remove a static ARP entry, use the **no** form of this command.

ip arp *ip-address mac-address*

no ip arp *ip-address*

Syntax Description

ip-address	IPv4 address, in A.B.C.D format.
mac-address	MAC address in one of the following formats: • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Support added for multicast static MAC addresses.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a static ARP entry on interface Ethernet 2/1:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip arp 192.0.2.1 0150.5a03.efab
```

Related Commands

Command	Description
show ip arp	Displays ARP entries.

ip arp cache limit

To configure the maximum number of Address Resolution Protocol (ARP) entries in the neighbor adjacency table, use the **ip arp cache limit** command. To delete the ARP entries configuration, use the **no** form of this command.

ip arp cache limit *max-arp-entries* [**syslog** *syslogs-per-second*]

no ip arp cache limit *max-arp-entries* [**syslog** *syslogs-per-second*]

Syntax Description

max-arp-entries	Maximum ARP entries. The range is from 1 to 409600.
syslog	(Optional) Specifies syslog messages. The range is from 1 to 1000.
syslogs-per-second	Syslogs per second.

Defaults

1

Command Modes

Global configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

If you do not configure a limit, system logs appear on the console when you try to add an adjacency after reaching the default limit. If you configure a limit for IPv4 ARP entries, system logs appear when you try to add an adjacency after reaching the configured limit.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the maximum number of ARP entries in the neighbor adjacency table:

```
switch# configuration terminal
switch(config)# ip arp cache limit 4000 syslog 4
switch(config)#
```

This example shows how to delete the ARP cache limit configuration:

```
switch(config)# no ip arp cache limit 4000 syslog 4
switch(config)#
```

Related Commands

Command	Description
show ip adjacency summary	Displays the global limit of the neighbor adjacency table and a summary of throttle adjacencies.

ip arp fast-path

To enable glean optimization, use the **ip arp fast-path** command. To disable enable glean optimization, use the **no** form of this command.

ip arp fast-path

no ip arp fast-path

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines This command requires the Enterprise Services license.

Examples This example shows how to enable glean optimization:

```
switch# configuration terminal
switch(config)# ip arp fast-path
switch(config)#
```

This example shows how to disable glean optimization:

```
switch(config)# no ip arp fast-path
switch(config)#
```

ip arp gratuitous

To enable gratuitous Address Resolution Protocol (ARP), use the **ip arp gratuitous** command. To disable gratuitous ARP, use the **no** form of this command.

ip arp gratuitous {**hsrp duplicate** | **request** | **update**}

no **ip arp gratuitous** {**hsrp duplicate** | **request** | **update**}

Syntax Description

hsrp duplicate	Specifies duplicate HSRP address detection.
request	Enables sending gratuitous ARP requests when a duplicate address is detected.
update	Enables ARP cache updates for gratuitous ARP.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(8)	Added keywords **hsrp duplicate** to the syntax description.
4.0(3)	This command was introduced.

Usage Guidelines

This command is typically useful in case of Data Center interconnection (DCI) scenario between multiple datacenters.

In a DCI scenario, typically it is desirable to have active /standby HSRP pair of routers on all sites so that each site has an active forwarder from the data plane perspective.To achieve this, a PACL denying the HSRP hello packets could be applied on the DCI facing links on each of the sites. This way HSRP hellos are dropped on the DCI links, and each site has a local HSRP active/standby router.

This command helps suppress duplicate IP detection when hosts do an ARP for HSRP active or when HSRP active sends a GARP for its own virtual IP.

This command does not require a license.

Examples

This example shows how to enable HSRP duplicate address detection:

```
switch(config)# interface vlan 10
switch(config-if)# ip arp gratuitous hsrp duplicate
switch(config-if)#
```

This example shows how to enable gratuitous ARP request on interface Ethernet 2/1:

```
switch(config)# interface vlan 10
switch(config-if)# ip arp gratuitous request
switch(config-if)#
```

Related Commands

Command	Description
ip arp	Configures a static ARP entry.

ip as-path access-list

To configure an access-list filter for Border Gateway Protocol (BGP) autonomous system (AS) number, use the **ip as-path access-list** command. To remove the filter, use the **no** form of this command.

ip as-path access-list *name* {**deny** | **permit**} *regexp*

no ip as-path access-list *name* {**deny** | **permit**} *regexp*

Syntax Description

name	AS path access list name. The name can be any alphanumeric string up to 63 characters.
deny	Rejects packets with AS numbers that match the *regexp* argument.
permit	Allows packets with AS numbers that match the *regexp* argument.
regexp	Regular expression to match BGP AS paths. See the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x* at the following URL for details on regular expressions: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fundamentals/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6-x.html

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip as-path access-list** command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the permit or deny condition applies. The autonomous system path should not contain the local autonomous system number.

This command does not require a license.

Examples

This example shows how to configure an AS path filter for BGP to permit AS numbers 55:33 and 20:01 and apply it to a BGP peer for inbound filtering:

```
switch# configure terminal
switch(config)# ip as-path access-list filter1 permit 55:33,20:01
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list filter1 in
```

Related Commands

Command	Description
filter-list	Assigns an AS path filter to a BGP peer.
show ip as-path access-list	Displays information about IP AS path access lists.

ip 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 **ip authentication key-chain eigrp** command. To prevent authentication, use the **no** form of this command.

ip authentication key-chain eigrp *instance-tag name-of-chain*

no ip authentication key-chain eigrp *instance-tag name-of-chain*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
name-of-chain	Group of keys that are valid.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must set the authentication mode using the **ip authentication mode eigrp** command in interface 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

This 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)# interface ethernet 1/2
switch(config-if)# ip authentication key-chain eigrp 209 trees
```

Related Commands

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

ip authentication mode eigrp

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

ip authentication mode eigrp *instance-tag* **md5**

no ip authentication mode eigrp *instance-tag* **md5**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
md5	Specifies Message Digest 5 (MD5) authentication.

Defaults

None

Command Modes

Interface 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 configure the interface to use MD5 authentication:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ip authentication mode eigrp 209 md5
```

Related Commands

Command	Description
authentication mode (EIGRP	Configures 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.

ip bandwidth eigrp

To configure the bandwidth metric on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip bandwidth eigrp** command. To restore the default, use the **no** form of this command.

ip bandwidth eigrp *instance-tag bandwidth*

no ip bandwidth eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
bandwidth	Bandwidth value. The range is from 1 to 2,560,000,000 kilobits.

Defaults

None

Command Modes

Interface 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 configure EIGRP to use a bandwidth metric of 10000 in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip bandwidth eigrp 209 10000
```

Related Commands

Command	Description
ip bandwidth-percent eigrp	Sets the percent of the interface bandwidth that EIGRP can use.

ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip bandwidth-percent eigrp** command. To restore the default, use the **no** form of this command.

ip bandwidth-percent eigrp *instance-tag percent*

no ip bandwidth-percent eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
percent	Percentage of bandwidth that EIGRP may use.

Defaults

percent: 50

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

EIGRP uses up to 50 percent of the bandwidth of a link, as defined by the **ip bandwidth** interface configuration command. Use the **ip bandwidth-percent** command to change this default percent.

This command requires the Enterprise Services license.

Examples

This example shows how to configure EIGRP to use up to 75 percent of an interface in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
ip bandwidth eigrp	Sets the EIGRP bandwidth value for an interface.

ip community-list

To create a community list entry, use the **ip community-list** command. To remove the entry, use the **no** form of this command.

ip community-list standard *list-name* {**deny** | **permit**} {*aa:nn* | **internet** | **local-AS** | **no-advertise** | **no-export**}

no ip community-list standard *list-name*

ip community-list expanded *list-name* {**deny** | **permit**} *regexp*

no ip community-list expanded *list-name*

Syntax Description

standard *list-name*	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
aa:*nn*	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space. You can pick more than one of these optional community keywords.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external). You can pick more than one of these optional community keywords.
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers. You can pick more than one of these optional community keywords.
local-AS	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation. You can pick more than one of these optional community keywords.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external). You can pick more than one of these optional community keywords.

expanded *list-name*	Configures a named expanded community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x* at the following URL for details on regular expressions: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fundamentals/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6-x.html **Note** Regular expressions can be used with expanded community lists only.

Defaults

Community exchange is not enabled by default.

Command Modes

Global configuration (config)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 4-byte number. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. BGP community attribute exchange between BGP peers is enabled when the send-community command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997 and RFC 1998.

BGP community exchange is not enabled by default. Use the **send-community** command in BGP neighbor fix-family configuration mode to enable BGP community attribute exchange between BGP peers.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the **set community** command.

Once you configure a permit value to match a given set of communities, the community list defaults to an implicit deny for all other community values. Use the **internet** community to apply an implicit permit to the community list.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. You can pick more than one of the optional community keywords. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

You can configure up to 32 communities.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

This command does not require a license.

Examples

This example shows how to configure a standard community list where the routes with this community are advertised to all peers (internal and external):

```
switch(config)# ip community-list standard test1 permit internet
switch(config)#
```

In this example, a standard community list is configured that permits routes from:

- Network 40 in autonomous system 65534 and from network 60 in autonomous system 65412.
- Peers in the same autonomous system or from subautonomous system peers in the same confederation.

This example shows how to configure a logical AND condition; all community values must match in order for the list to be processed:

```
switch(config)# ip community-list standard test1 permit 65534:40 65412:60 no-export
switch(config)#
```

This example shows how to configure a standard community list that will deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
switch(config)# ip community-list standard test2 deny 65534:40 65412:60
```

This example shows how to configure a named standard community list that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
switch(config)# ip community-list standard RED permit local-AS

switch(config)# ip community-list standard RED permit 40000:20
switch(config)#
```

In this example, an expanded community list is configured that will deny routes that carry communities from any private autonomous system:

```
switch(config)# ip community-list expanded 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
switch(config)#
```

In this example, a named expanded community list configured that denies routes from network 1 through 99 in autonomous system 50000:

```
switch(config)# ip community-list list expanded BLUE deny 50000:[0-9][0-9]_
switch(config)#
```

Related Commands

Command	Description
feature bgp	Enables BGP.
match community	Matches an community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set community	Sets an community in a route map.

ip delay eigrp

To configure the throughput delay for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip delay eigrp** command. To restore the default, use the **no** form of this command.

ip delay eigrp *instance-tag seconds* **picoseconds**

no ip **delay eigrp instance-tag**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Throughput delay, in microseconds. The range is from 1 to 16777215.
picoseconds	Specifies the delay units in picoseconds.

Defaults

100 (10-microsecond units)

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	Added the **picoseconds** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

You configure the throughput delay on an interface in 10-microsecond units. For example, if you set the **ip delay eigrp** command to 100, the throughput delay is 1000 microseconds.

The **picoseconds** option is supported only supported in 64-bit mode.

This command requires the Enterprise Services license.

Examples

This example shows how to set the delay to 40 microseconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip delay eigrp 1 40
```

Related Commands

Command	Description
ip hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process that is designated by an autonomous system number.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** command. To disable this function, use the no form of this command.

ip directed-broadcast [*acl-name*]

ip directed-broadcast [*acl-name*]

Syntax Description

acl-name	Access control list (ACL) name. An ACL name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is exploded as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet.

When you configure **ip directed-broadcast** *acl-name* command with the acl-name as **hw-assist**, you cannot delete this configuration after the ISSU. This is applicable to releases prior to Cisco NX-OS Release 8.2(1).

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

This command does not require a license.

Examples

This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip directed-broadcast
```

ip distribute-list eigrp

To configure a distribution list for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip distribute-list eigrp** command. To restore the default, use the **no** form of this command.

ip distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

no ip distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
prefix-list *list-name*	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies the route policy to incoming routes.
out	Applies the route policy to outgoing routes.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip distribute-list eigrp** command to configure a route filter policy on an interface. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a route map for all EIGRP routes coming into the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip distribute-list eigrp 209 route-map InputFilter in
```

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

ip domain-list

To configure the IP domain list, use the **ip domain-list** command. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name* [**use-vrf** *name*]

no ip domain-list *domain-name* [**use-vrf** *name*]

Syntax Description

domain-list	Specifies the domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 63 characters.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Global configuration
VRF context configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-list** command to configure additional domain names for the device. Use the **vrf context** command to enter the VRF context mode to configure additional domain names for a particular VRF.

This command does not require a license.

Examples

This example shows how to configure the IP domain list for the default VRF:

```
switch# config terminal
switch(config)# ip domain-list Mysite.com
```

This example shows how to configure the IP domain list for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-list Mysite.com
```

This example configures the IP domain list for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF.

```
switch# config terminal
switch(config)# ip domain-list Mysite.com use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

ip domain-lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-lookup** command to enable DNS.

This command does not require a license.

Examples

This example shows how to configure a DNS server lookup feature:

```
switch# config terminal
switch(config)# ip domain-lookup
```

Related Commands

Command	Description
show hosts	Displays information about the DNS.

ip domain-name

To configure a domain name, use the **ip domain-name** command. To delete a domain name, use the **no** form of the command.

ip domain-name *domain-name* [**use-vrf** *name*]

no ip domain-name *domain-name* [**use-vrf** *name*]

Syntax Description

domain-name	Specifies the domain name. The name can be any case-sensitive, alphanumeric string up to 63 characters.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Global configuration
VRF context configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-name** command to configure the domain name for the device. Use the **vrf context** command to enter the VRF context mode to configure the domain monastery a particular VRF.

This command does not require a license.

Examples

This example shows how to configure the IP domain name for the default VRF:

```
switch# config terminal
switch(config)# ip domain-name Mysite.com
```

This example shows how to configure the IP domain name for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-name Mysite.com
```

This example shows how to configure the IP domain name for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF:

```
switch# config terminal
switch(config)# ip domain-name Mysite.com use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

ip dscp-lop

To set the DSCP value for locally originated packets for IPv4 and IPv6, use the **ip dscp-lop** command. To restore the default, use the **no** form of this command.

ip dscp-lop *dscp-value*

no ip dscp-lop

Syntax Description

dscp-value	The range is from 0 to 63. • af11—AF11 dscp (001010) • af12—AF12 dscp (001100) • af13—AF13 dscp (001110) • af21—AF21 dscp (010010) • af22—AF22 dscp (010100) • af23—AF23 dscp (010110) • af31—AF31 dscp (011010) • af32—AF32 dscp (011100) • af33—AF33 dscp (011110) • af41—AF41 dscp (100010) • af42—AF42 dscp (100100) • af43—AF43 dscp (100110) • cs1—CS1(precedence 1) dscp (001000) • cs2—CS2(precedence 2) dscp (010000) • cs3—CS3(precedence 3) dscp (011000) • cs4—CS4(precedence 4) dscp (100000) • cs5—CS5(precedence 5) dscp (101000) • cs6—CS6(precedence 6) dscp (110000) • cs7—CS7(precedence 7) dscp (111000) • default—Default dscp (000000) • ef—EF dscp (101110)

Defaults

0

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(12)	This command was introduced.

Usage Guidelines

Use the **ip dscp-lop** command to set the dscp value of all locally originated packets unless they are set by the application.

For values 40-63, a warning is also thrown as this could contend with higher priority traffic.

This command applies to IPv4 and IPv6.

This command affects all protocols from the SUP which do not have explicitly specified markers and sets the marker to 0.

For example, if BGP has a dscp marker of cs6 while TFTP has a dscp marker of 0. BGP packets will not be affected by this command.

Examples

This example shows how to set the dscp value to 16:

```
switch# configure terminal
switch(config)# ip dscp-lop 16
```

This example shows how to set the dscp value to 45:

```
switch# configure terminal
switch(config)# ip dscp-lop 45
DSCP 40-63 are used for high priority traffic. Set dscp to a lower value to avoid contention. DSCP for Locally Originated packet for Telnet/SSH/SNMP/Syslog/TFTP/ICMP/Netflow/DNS/TACACS/RADIUS/FTP is set to 45
```

ip eigrp shutdown

To shut down the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip eigrp shutdown** command. To restore the default, use the **no** form of this command.

ip eigrp *instance-tag* **shutdown**

no ip **eigrp** *instance-tag* **shutdown**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip eigrp shutdown** command to shut down the interface for EIGRP and prevent EIGRP adjacency for the interface for maintenance purposes. The network address for the interface does not show up in the EIGRP topology table.

Use the **ip passive-interface eigrp** command to prevent EIGRP adjacency but keep the network address in the topology table.

This command requires the Enterprise Services license.

Examples

This example shows how to disable EIGRP on an interface:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip eigrp 201 shutdown
```

Related Commands

Command	Description
ip passive-interface eigrp	Configures an instance of EIGRP.
router eigrp	Configures an instance of EIGRP.

ip extcommunity-list

To create an extended community list entry, use the **ip extcommunity-list** command. To remove the entry, use the **no** form of this command.

ip extcommunity-list standard *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *aa4*:*nn*

no ip extcommunity-list standard generic {**transitive** | **nontransitive**} *list-name*

ip extcommunity-list expanded *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *regexp*

no ip extcommunity-list expanded generic {**transitive** | **nontransitive**} *list-name*

Syntax Description

standard *list-name*	Configures a named standard extended community list.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
generic	Specifies the generic specific extended community type.
transitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
nontransitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
aa4:*nn*	(Optional) Autonomous system number and network number. This value is configured with a 4-byte AS number and a 2-byte network number separated by a colon. The 4-byte AS number range is from 1 to 4294967295 in plaintext notation, or from 1.0 to 56636.65535 in AS.dot notation. You can enter a single community or multiple communities, each separated by a space.
expanded *list-name*	Configures a named expanded extended community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x* at the following URL for details on regular expressions: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fundamentals/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6-x.html **Note** Regular expressions can be used with expanded extended community lists only.

Defaults

Community exchange is not enabled by default.

Command Modes

Global configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **ip extcommunity-list** command to configure extended community filtering for BGP. Extended community values are configured as a 6-byte number. The first four bytes represent the autonomous system number, and the last two bytes represent a user-defined network number. The BGP generic specific community attribute is defined in draft-ietf-idr-as4octet-extcomm-generic-subtype-00.txt.

BGP extended community exchange is not enabled by default. Use the **send-extcommunity** command in BGP neighbor fix-family configuration mode to enable extended community attribute exchange between BGP peers.

Once you configure a permit value to match a given set of extended communities, the extended community list defaults to an implicit deny for all other extended community values.

Standard Extended Community Lists

Use standard extended community lists to configure specific extended community numbers. You can configure a maximum of 16 extended communities in a standard extended community list.

Expanded Extended Community Lists

Use expanded extended community lists to filter communities using a regular expression. Use regular expressions to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.

Community List Processing

When you configure multiple values in the same extended community list statement, a logical AND condition is created. All extended community values must match to satisfy the AND condition. When you configure multiple values in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

This command does not require a license.

Examples

This example shows how to configure a standard generic specific extended community list that permits routes from network 40 in autonomous system 1.65534 and from network 60 in autonomous system 1.65412.

This example shows how to configure a logical AND condition:

```
switch(config)# ip extcommunity-list standard test1 permit generic transitive 1.65534:40 1.65412:60
switch(config)#
```

All community values must match in order for the list to be processed.

Related Commands

Command	Description
feature bgp	Enables BGP.
match extcommunity	Matches an extended community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set extcommunity	Sets an extended community in a route map.

ip forward

To allow IPv4 traffic on an interface even when there is no IP address configuration on that interface, use the **ip forward** command. To disable this function, use the **no** form of this command.

ip forward

no ip forward

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
6.2(8)	This command was introduced.

Usage Guidelines Beginning with Cisco NX-OS Release 6.2(8), BGP supports RFC 5549 which allows an IPv4 prefix to be carried over an IPv6 next hop.

Use the **ip forward** command to do the following:

- Accept IPv4 packets on an interface that has no IPv4 interface address configured on that interface.
- Reply with IPv4 ICMP over IPv6.

This command requires the Enterprise Services license.

Examples This example shows how allow IPv4 traffic on an interface:

```
switch(config)# interface ethernet 0/2
switch(config-if)# ipv6 address ABCF:1::3/64
switch(config-if)# ip forward
```

Command	Description
ipv6 nd mac-extract	Enables any next hop that matches the IPv6 prefix on that interface to be treated as an MEv6 address,

ip hello-interval eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) hello interval for an interface, use the **ip hello-interval eigrp** command. To restore the default, use the **no** form of this command.

ip hello-interval eigrp *instance-tag seconds*

no ip hello-interval eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Hello interval (in seconds). The range is from 1 to 65535.

Defaults

5 seconds

Command Modes

Interface 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 set the hello interval to 10 seconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip hello-interval eigrp 1 10
```

ip hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip hold-time eigrp** command. To restore the default, use the **no** form of this command.

ip hold-time eigrp *instance-tag seconds*

no ip hold-time eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Hold time (in seconds). The range is from 1 to 65535.

Defaults

15 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip hold-time eigrp** command to increase the default hold time on very congested and large networks,

We recommend that you configure the hold time to be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

This command requires the Enterprise Services license.

Examples

This example shows how to set the hold time to 40 seconds for the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip hold-time eigrp 209 40
```

Related Commands

Command	Description
ip hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process designated by an autonomous system number.

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ip host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host *name address1* [*address2... address6*]

no ip host *name address1* [*address2... address6*]

Syntax Description

name	Host name. The *name* can be any case-sensitive, alphanumeric string up to 80 characters.
address1	IPv4 address in the x.x.x.x format.
address2 ...address6	(Optional) Up to five additional IPv4 addresses in the x.x.x.x format.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip host** command to add a static host name to DNS.

This command does not require a license.

Examples

This example shows how to configure a static hostname:

```
switch(config)# ip host mycompany.com 192.0.2.1
```

Related Commands

Command	Description
ipv6 host	Configures a static host name in the DNS database.

ip load-sharing address

To configure the load-sharing algorithm used by the unicast Forwarding Information Base (FIB), use the **ip load-sharing address** command. To restore the default, use the **no** form of this command.

ip load-sharing address {**destination port destination** | **source-destination** [**port source-destination**]} [**universal-id** *seed*]

no ip load-sharing address {**destination port destination** | **source-destination** [**port source-destination**]} [**universal-id** *seed*]

Syntax Description

destination port destination	Sets the load-sharing algorithm based on destination address and port.
source-destination	Sets the load-sharing algorithm based on source and destination address.
port source-destination	(Optional) Sets the load-sharing algorithm based on source and destination address and port address.
universal-id *seed*	(Optional) Sets the random seed for the load sharing hash algorithm. The range is from 1 to 4294967295.

Defaults

Destination address and port address

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip load-sharing address** command to set the load-sharing algorithm that the unicast FIB uses to select a path from the equal-cost paths in the Router Information Base (RIB).

This command does not require a license.

Examples

This example shows how to set the load-sharing algorithm to use source and destination address:

```
switch(config)# ip load-sharing address source-destination
```

Related Commands

Command	Description
show ip load-sharing	Displays the load-sharing algorithm.
show routing hash	Displays the path the RIB and FIB select for a source/destination pair.

ip load-sharing per-packet

To configure per-packet load sharing on an interface, use the **ip load-sharing per-packet** command. To restore the default, use the **no** form of this command.

ip load-sharing per-packet

no load-sharing per-packet

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines Use the **ip load-sharing per-packet** command to set the load-sharing algorithm on an interface. This command overrides the **ip load-sharing address** command.

Note Using per-packet load sharing can result in out-of-order packets. Packets for a given pair of source-destination hosts might take different paths and arrive at the destination out of order. Make sure you understand the implications of out-of-order packets to your network and applications. Per-packet load sharing is not appropriate for all networks. Per-flow load sharing ensures packets always arrive in the order that they were sent.

You configure per-packet load sharing on the input interface. This configuration determines the output interface that Cisco NX-OS chooses for the packet.

For example, if you have ECMP paths on two output interfaces, Cisco NX-OS uses the following load-sharing methods for input packets on Ethernet 1/1:

- Per-packet load sharing if you configure per-packet load sharing on Ethernet 1/1.
- Per-flow load sharing.

The configuration for the other interfaces have no effect on the load-sharing method used for Ethernet 1/1 in this example.

This command does not require a license.

Examples

This example shows how to enable per-packet load-sharing on interface Ethernet 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip load-sharing per-packet
```

Related Commands

Command	Description
ip load-sharing	Configures the per-flow load-sharing algorithm.
show ip load-sharing	Displays the load-sharing algorithm.

ip name-server

To configure a name server, use the **ip name-server** command. To disable this feature, use the **no** form of the command.

ip name-server *ip-address* [**use-vrf** *name*]

no ip name-server *ip-address* [**use-vrf** *name*]

Syntax Description

ip-address	IP address for the name server.
use-vrf *name*	(Optional) Specifies the virtual routing and forwarding (VRF) to use to reach the name-server. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Global configuration
VRF context configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip name-server** command to configure the name server for the device. Use the **vrf context** command to enter the VRF context mode to configure the domain names for a particular VRF.

This command does not require a license.

Examples

This example shows how to configure the IP name server for the default VRF:

```
switch# config terminal
switch(config)# ip name-server 192.0.2.1
```

This example shows how to configure the IP name server for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip name-server 192.0.2.1
```

This example configures the IP name server for the default VRF to use the management VRF as a backup if show ip rip policy statistics redistributeIP name server cannot be reached through the default VRF:

```
switch# config terminal
```

```
switch(config)# ip name-server 192.0.2.1 use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

ip next-hop-self eigrp

To instruct the Enhanced Interior Gateway Routing Protocol (EIGRP) process to use the local IP address as the next-hop address when advertising these routes, use the **ip next-hop-self eigrp** command. To use the received next-hop value, use the **no** form of this command.

ip next-hop-self eigrp *instance-tag*

no ip next-hop-self eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

EIGRP always sets the IP next-hop value to be itself.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

EIGRP, by default, sets the IP next-hop value to be itself for routes that it is advertising, even when advertising those routes on the same interface from which the router learned them. To change this default, you must use the **no ip next-hop-self eigrp** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes.

Examples

This example shows how to change the default IP next-hop value and instruct EIGRP to use the received next-hop value:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ip next-hop-self eigrp 209
```

ip offset-list eigrp

To configure an offset list for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip offset-list eigrp** command. To restore the default, use the **no** form of this command.

ip offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

no ip **offset-list eigrp** *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
prefix-list *list-name*	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies route policy to incoming routes.
out	Applies route policy to outgoing routes.
offset	Value to add to the EIGRP metric.

Defaults

This command has no defaults.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip offset-list eigrp** command to influence which route is advertised on an interface. Cisco NX-OS adds the configured offset value to any routes that match the configure prefix list or route map. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an offset list filter to add 20 to the metric for EIGRP routes coming into the interface that match the route map OffsetFilter:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip offset-list eigrp 209 route-map OffsetFilter in 20
```

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

ip ospf authentication

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

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

no ip ospf authentication

Syntax Description

key-chain *key-name*	(Optional) Specifies a key chain to use for authentication. The *key-name* argument can be any alphanumeric string.
message-digest	(Optional) Specifies that message-digest authentication will be used.
null	(Optional) Specifies that no authentication is used. Use the keyword to override any other authentication configured for an area.

Defaults

No authentication

Command Modes

Interface configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf authentication** command to configure the authentication mode for an OSPF interface. If you use this command with no keywords, use the **ip ospf authentication-key** command to configure the password. If you use the **message-digest** keyword, use the **ip ospf message-digest-key** command to configure the message-digest key for the interface.

The authentication that you configure on an interface overrides the authentication that you configure for the area.

This command requires the Enterprise Services license.

Examples

This example shows how to configure message-digest authentication:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf message-digest-key 33 md5 0 mypassword
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the password authentication of OSPF.
ip ospf message-digest-key	Configures the OSPF MD5 message-digest key.

ip ospf authentication-key

To assign a password for simple password authentication to be used by neighboring Open Shortest Path First (OSPF) routers, use the **ip ospf authentication-key** command. To remove a previously assigned OSPF password, use the **no** form of this command.

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

no ip ospf authentication-key

Syntax Description

0	(Optional) Configures an unencrypted password.
3	(Optional) Configure a 3DES encrypted password string.
password	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Defaults

Unencrypted password

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf authentication-key** command to configure a password for simple password authentication. The password created by this command is used as a key that is inserted directly into the OSPF header when Cisco NX-OS originates routing protocol packets. You can assign a separate password to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Note Cisco NX-OS uses this key when you enable authentication for an interface with the **ip ospf authentication** interface configuration command or if you configure the area for authentication with the **area authentication** command in router configuration mode.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an unencrypted authentication key with the string yourpass:

```
switch(config-if)# ip ospf authentication-key yourpass
```

Related Commands

Command	Description
area authentication	Specifies the authentication type for an OSPF area.
ip ospf authentication	Specifies the authentication type for an interface.

ip ospf cost

To specify the cost of sending a packet on an interface, use the **ip ospf cost** command. To reset the path cost to the default, use the **no** form of this command.

ip ospf cost *interface-cost*

no ip ospf cost *interface-cost*

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults

Calculates the cost based on the reference bandwidth divided by the configured interface bandwidth. You can configure the reference bandwidth or it defaults to 40 Gb/s.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf cost** command to configure the cost metric manually for each interface. This command overrides any settings for the reference bandwidth that you set using the **reference-bandwidth** command in router configuration mode.

If this command is not used, the link cost is calculated using the following formula:

link cost = reference bandwidth / interface bandwidth

This command requires the Enterprise Services license.

Examples

This example shows how to configure the interface cost value to 65:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf cost 65
```

Related Commands

Command	Description
reference-bandwidth	Specifies the reference bandwidth that OSPF uses to calculate the link cost.

ip ospf dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down, use the **ip ospf dead-interval** command. To restore the default, use the **no** form of this command.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Syntax Description

seconds	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or that neighbor adjacency is removed from the local router and does not participate in routing. The range is from 1 to 65535. The value must be the same for all nodes on the network.

Defaults

The default for *seconds* is four times the interval set by the **ip ospf hello-interval** command.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf dead-interval** command to set the dead interval that OSPF advertises in hello packets. This value must be the same for all networking devices on a specific network.

Aggressive protocol timers are not supported in the Virtual Port-Channel (vPC) environment and they are also not supported from the in-service software updates (ISSU) perspective. We recommend that you retain the default value.

Configure a shorter dead interval to detect down neighbors faster and improve convergence. Very short dead intervals could cause routing instability.

Use the **show ip ospf interface** command to verify the dead interval and hello interval.

This command requires the Enterprise Services license.

Examples

This example shows how to set the OSPF dead interval to 20 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf dead-interval 20
```

Related Commands

Command	Description
ip ospf hello-interval	Interval between hello packets that OSPF sends on the interface.
show ip ospf interface	Displays OSPF-related information.

ip ospf hello-interval

To specify the interval between hello packets that Open Shortest Path First (OSPF) sends on the interface, use the **ip ospf hello-interval** command. To return to the default, use the **no** form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Syntax Description

seconds	Interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Defaults

10 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf hello-interva**l command to set the rate at which OSPF advertises hello packets. Shorter hello intervals allow OSPF to detect topological changes faster. This value must be the same for all routers and access servers on a specific network.

Aggressive protocol timers are not supported in the Virtual Port-Channel (vPC) environment and they are also not supported from the in-service software updates (ISSU) perspective. We recommend that you retain the default value.

This command requires the Enterprise Services license.

Examples

This example shows how to set the interval between hello packets to 15 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf hello-interval 15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.

ip ospf message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key** command. To remove an old MD5 key, use the **no** form of this command.

ip ospf message-digest-key *key-id* **md5** [0 | 3] *key*

no ip ospf message-digest-key *key-id*

Syntax Description

key-id	Identifier in the range from 1 to 255.
0	(Optional) Specifies an unencrypted password to generate the md5 key.
3	(Optional) Specifies an encrypted 3DES password to generate the md5 key.
key	An alphanumeric password of up to 16 bytes.

Defaults

Unencrypted

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf message-digest-key** command when you configure the MD5 digest authentication mode. All neighbor routers must have the same *key* value on the network.

This command requires the Enterprise Services license.

Examples

This example shows how to set key 19 with the password 8ry4222:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies the authentication type for an interface.

ip ospf mtu-ignore

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on received Database Descriptor (DBD) packets, use the **ip ospf mtu-ignore** command. To return to the default, use the **no** form of this command.

ip ospf mtu-ignore

no **ip ospf mtu-ignore**

Syntax Description

This command has no arguments or keywords.

Defaults

OSPF MTU mismatch detection is enabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf mtu-ignore** command to disable MTU mismatch detection on an interface. By default, OSPF checks whether neighbors are using the same MTU on a common interface. If the receiving MTU is higher than the IP MTU configured on the incoming interface, OSPF does not establish adjacencies. Use the **ip ospf mtu-ignore** command to disable this check and allow adjacencies when the MTU value differs between OSPF neighbors.

This command requires the Enterprise Services license.

Examples

This example shows how to disable MTU mismatch detection on received DBD packets:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf mtu-ignore
```

ip ospf network

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for an interface, use the **ip ospf network** command. To return to the default, use the **no** form of this command.

ip ospf network {**broadcast** | **point-to-point**}

no ip ospf network

Syntax Description

broadcast	Sets the network type as broadcast.
point-to-point	Sets the network type as point-to-point.

Defaults

Depends on the network type.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The network type influences the behavior of the OSPF interface. OSPF network type is usually broadcast, which uses OSPF multicasting capabilities. Under this network type a designated router and backup designated router are elected. For point-to-point networks there are only two neighbors and multicast is not required. For routers on an interface to become neighbors the network type for all should match.

This command overrides the **medium** {**broadcast** | **p2p**} command in interface configuration mode.

This command requires the Enterprise Services license.

Examples

This example shows how to set an OSPF network as a broadcast network:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.33 255.255.255.0
switch(config-if)# ip ospf network broadcast
```

ip ospf passive-interface

To suppress Open Shortest Path First (OSPF) routing updates on an interface, use the **ip ospf passive-interface** command. To return to the default, use the **no** form of this command.

ip ospf passive-interface

no ip ospf passive-interface

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines If an interface is configured as passive-interface it does not participate in the OSPF protocol and will not establish adjacencies or send routing updates. However the interface is announced as part of the routing network.

This command requires the Enterprise Services license.

Examples This example shows how to set an interface as passive:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf passive-interface
```

ip ospf priority

To set the router priority for an Open Shortest Path First (OSPF) interface, use the **ip ospf priority** command. To return to the default, use the **no** form of this command.

ip ospf priority *number-value*

no ip ospf priority *number-value*

Syntax Description

number-value	Number value that specifies the priority of the router. The range is from 0 to 255.

Defaults

Priority of 1

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf priority** command to set the router priority, which determines the designated router for this network. When two routers are attached to a network, both attempt to become the designated router. The router with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero cannot become the designated router or backup designated router.

Cisco NX-OS uses this priority value when you configure OSPF for broadcast networks using the **neighbor** command in router configuration mode.

This command requires the Enterprise Services license.

Examples

This example shows how to set the router priority value to 4:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf priority 4
```

Related Commands

Command	Description
ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.

ip ospf retransmit-interval

To specify the time between Open Shortest Path First (OSPF) link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** command. To return to the default, use the **no** form of this command.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. The time must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf retransmit-interval** command to set the time between LSA retransmissions. When a router sends an LSA to its neighbor, it keeps the LSA until it receives an acknowledgment message from the neighbor. If the router receives no acknowledgment within the retransmit interval, the local router resends the LSA.

This command requires the Enterprise Services license.

Examples

This example shows how to set the retransmit interval value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf retransmit-interval 8
```

ip ospf shutdown

To shut down an Open Shortest Path First (OSPF) interface, use the **ip ospf shutdown** command. To return to the default, use the **no** form of this command.

ip ospf shutdown

no ip ospf shutdown

Syntax Description This command has no keywords or arguments.

Defaults None

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Use the **ip ospf shutdown** command to shut down OSPF on this interface.

This command requires the Enterprise Services license.

Examples This example shows how to shut down OSPF on an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf shutdown
```

ip ospf transmit-delay

To set the estimated time required to send an Open Shortest Path First (OSPF) link-state update packet on the interface, use the **ip ospf transmit-delay** command. To return to the default, use the **no** form of this command.

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 450 seconds.

Defaults

1 second

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf transmit-delay** command to set the estimated time needed to send an LSA update packet. OSPF increments the LSA age time by transmit delay amount before transmitting the LSA update. You should take into account the transmission and propagation delays for the interface when you set this value.

This command requires the Enterprise Services license.

Examples

This example shows how to set the transmit delay value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf transmit-delay 8
```

ip passive-interface eigrp

To suppress all routing updates on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip passive-interface eigrp** command. To re-enable the sending of routing updates, use the **no** form of this command. To remove the interface-level configuration for the passive-interface, use the **default ip passive-interface eigrp** command.

ip passive-interface eigrp *instance-tag*

no ip passive-interface eigrp *instance-tag*

default ip passive-interface eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Routing updates are sent on the interface.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
6.2(2)	The default form of this command was added.

Usage Guidelines

Use the **ip passive-interface eigrp** command to stop all routing updates on an interface and suppress the formation of EIGRP adjacencies. The network address for the interface remains in the EIGRP topology table. To remove this command from the interface, use the **default ip passive-interface eigrp** command. The final behavior of this command depends on **passive-interface default (EIGRP)** command.

The following table sums up the behavior of this command:

Table 1 Behavior of combination of commands

VRF mode (deafult passive-interface)	Interface mode (passive)	Result (interface passive ?)
TRUE	FALSE	FALSE
TRUE	TRUE	TRUE
TRUE	NONE	TRUE

Table 1 Behavior of combination of commands

VRF mode (deafult passive-interface)	Interface mode (passive)	Result (interface passive ?)
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE
FALSE	NONE	FALSE

Default configuration at interface-level corresponds to NONE state.

This command requires the Enterprise Services license.

Examples

This example shows how to stop EIGRP routing updates on Ethernet 2/1:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip passive-interface eigrp 201
```

Related Commands

Command	Description
passive-interface default (EIGRP)	Suppresses the EIGRP hellos.

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** command. To remove the route map, use the **no** form of this command.

ip policy route-map *name*

no ip policy route-map [*name*]

Syntax Description

name	Name of the route map. The name can be any alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip policy route-map** command to identify a route map to use for policy routing. Use the **route-map** command to create the rout map. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing is allowed for the interface, based on the destination IP address of the packet. The **set** commands specify the set actions—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

You can perform policy-based routing on any match criteria that can be defined in an expanded IP access list when using the **match ip address** command and referencing an expanded IP access list.

You must enable policy-based routing with the **feature pbr** command before you can use the **ip policy route-map** command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a policy-based route map to an interface:

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ip policy route-map policymap
```

Related Commands

Command	Description
feature pbr	Enabled the policy-based routing feature.
route-map	Creates a route map.
show route-map pbr-statistics	Displays statistics about policy-based route maps

ip port-unreachable

To enable the generation of Internet Control Message Protocol (ICMP) port unreachable messages, use the **ip port-unreachable** command. To disable this function, use the no form of this command.

ip port-unreachable

no ip port-unreachable

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled

Command Modes

Interface 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

This example shows how to enable the generation of ICMP port unreachable messages, as appropriate, on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip port-unreachable
```

Related Commands

Command	Description
ip unreachables	Sends ICMP unreachable messages.

ip prefix-list

To create a prefix list to match IP packets or routes against, use the **ip prefix-list** command. To remove the prefix-list, use the **no** form of this command.

ip prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [**le** *length*]]

no prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [**le** *length*]]

Syntax Description

name	IP prefix list name. The name can be any alphanumeric string up to 63 characters.
seq *number*	(Optional) Specifies the number to order entries in the prefix list. The range is from 1 to 4294967294.
permit	Allows routes or IP packets that match the prefix list.
deny	Rejects routes or IP packets that match the prefix list.
prefix	IP prefix in A.B.C.D/length format.
eq *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
ge *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
le *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. You configure prefix lists with permit or deny keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IP address and a bit mask. The bit mask is entered as a number from 1 to 32. An implicit deny is applied to traffic that does not match any prefix-list entry.

You can configure prefix lists to match an exact prefix length or a prefix range. Use the **ge** and **le** keywords to specify a range of the prefix lengths to match, providing more flexible configuration than can be configured with just the network/length argument. Cisco NX-OS processes the prefix list using an exact match when you do not configure either neither the **ge** nor **le** keyword. If you configure both the **ge** *ge-length* and **le** l*e-length* keywords and arguments, the allowed prefix length range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

network/length < ge ge-length < le le-length <= 32

If you do not configure a sequence number, Cisco NX-OS applies a a default sequence number of 5 to the prefix list, and subsequent prefix list entries will be increment by 5 (for example, 5, 10, 15, and onwards). If you configure a sequence number for the first prefix list entry but not subsequent entries, then Cisco NX-OS increments the subsequent entries by 5 (For example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword.

Cisco NX-OS evaluates prefix lists starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the **permit** or **deny** statement is applied to that network and the rest of the list is not evaluated.

Tip For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The seq number keyword and argument can be used for resequencing.

The prefix list is applied to inbound or outbound updates for specific peer by entering the **prefix-list** command in neighbor address-family mode. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

This command does not require a license.

Examples

This example shows how to configure a prefix list and apply it to a BGP peer:

```
switch# config t
switch(config)# ip prefix-list allowprefix 10 permit 192.0.2.0 eq 24
switch(config)# ip prefix-list allowprefix 20 permit 209.165.201.0 eq 27
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

Related Commands

Command	Description
clear ip prefix-list	Clears counters for IP prefix lists.
prefix-list	Applies a prefix list to BGP peer.
show ip prefix-list	Displays information about IP prefix lists.

ip prefix-list description

To configure a description string for an IP prefix-list, use the **ip prefix-list description** command. To revert to default, use the **no** form of this command.

ip prefix-list *name* **description** *string*

no ip prefix-list *name* **description**

Syntax Description

name	Name of prefix list. The name can be any alphanumeric string up to 63 characters.
string	Descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.

Defaults

None

Command Modes

Global 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

This example shows how to configure a description for an IP prefix list:

```
switch# configure terminal
switch(config)# ip prefix-list test1 description “this is a test”
```

Related Commands

Command	Description
ip prefix-list	Creates an IPv6 prefix list
show ip prefix-list	Displays information about IPv6 prefix lists.

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command. To disable proxy ARP on the interface, use the **no** form of this command.

ip proxy-arp

no ip proxy-arp

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Interface 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 This example shows how to enable proxy ARP:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip proxy-arp
```

ip rip authentication key-chain

To enable authentication for the Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface, use the **ip rip authentication key-chain** command in interface configuration mode. To prevent authentication, use the **no** form of this command.

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain [*name-of-chain*]

Syntax Description

name-of-chain	Group of keys that are valid.

Defaults

No authentication is provided for RIP packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication key-chain trees
```

Related Commands

Command	Description
key-chain	Creates a set of keys that can be used by an authentication method.

ip rip authentication mode

To specify the type of authentication used in the Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication mode** command in interface configuration mode. To restore clear text authentication, use the **no** form of this command.

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Syntax Description

text	Specifies the clear text authentication.
md5	Specifies the message Digest 5 (MD5) authentication.

Defaults

Clear text authentication is provided for RIP packets if you configured a key chain.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

RIP for IPv6 uses the authentication built into IPv6.

This command does not require a license.

Examples

This example shows how to configure the interface to use MD5 authentication:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication mode md5
```

Related Commands

Command	Description
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
key chain	Enables authentication for routing protocols.

ip rip metric-offset

To add an additional value to the incoming IP Routing Information Protocol (RIP) route metric for an interface, use the **ip rip metric-offset** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ip rip metric-offset *value*

no ip rip metric-offset

Syntax Description

value	Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.

Defaults

value: 1

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip route metric-offset** command to influence which routes are used by Cisco NX-OS. This command allows you to add a fixed offset to the route metric of all incoming routes on an interface. For example, if you set the metric-offset to 5 on an interface and the incoming route metric is 5,.Cisco NX-OS adds the route to the route table with a metric of 10.

This command does not require a license.

Examples

This example shows how to configure a metric offset of 10 for all incoming RIP routes on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip rip metric-offset 10
```

Related Commands

Command	Description
ip rip offset-list	Adds an offset value to incoming RIP route metrics.

ip rip offset-list

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **ip rip offset-list** command in interface configuration mode. To remove an offset list, use the **no** form of this command.

ip rip offset-list *value*

no ip rip offset-list

Syntax Description

value	Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.

Defaults

value: 1

Command Modes

Router address-family 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

This example shows how to configure an offset of 10 for all incoming RIP routes on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip rip offset-list 10
```

Related Commands

Command	Description
ip rip metric-offset	Adds an offset value to incoming RIP route metrics.

ip rip passive-interface

To suppress the sending of the Routing Information Protocol (RIP) updates on an interface, use the **ip rip passive-interface** command in interface configuration mode. To unsuppress updates, use the **no** form of this command.

ip rip passive-interface

no ip rip passive-interface

Syntax Description This command has no arguments or keywords.

Defaults RIP updates are sent on the interface.

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines While RIP stops sending routing updates to the multicast (or broadcast) address on a passive interface, RIP continues to receive and process routing updates from its neighbors on that interface.

This command does not require a license.

Examples This example shows how to configure Ethernet 1/2 as a passive interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip passive-interface
```

ip rip poison-reverse

To enable poison-reverse processing of the Routing Information Protocol (RIP) router updates, use the **ip rip poison-reverse** command in interface configuration mode. To disable poison-reverse processing of RIP updates, use the **no** form of this command.

ip rip poison-reverse

no ip rip poison-reverse

Syntax Description This command has no arguments or keywords.

Defaults Split horizon is always enabled. Poison-reverse processing is disabled.

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Use the **ip rip poison-reverse** command to enable poison-reverse processing of RIP router updates. By default, Cisco NX-OS does not advertise RIP routes out the interface over which they were learned (split horizon). If you configure both poison reverse and split horizon, then Cisco NX-OS advertises the learned routes as unreachable over the interface on which the route was learned.

This command does not require a license.

Examples This example shows how to enable poison-reverse processing for an interface running RIP:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip poison-reverse
```

ip rip route-filter

To filter the Routing Information Protocol (RIP) routes coming in or out of an interface, use the **route-filter** command in interface configuration mode. To remove filtering from an interface, use the **no** form of this command.

ip rip route filter {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description

prefix-list *list-name*	Associates a prefix list to filter RIP packets.
route-map *map-name*	Associates a route map to set the redistribution policy for RIP.
in	Filters incoming routes.
out	Filters outgoing routes.

Defaults

Route filtering is disabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip rip route-filter** command to filter incoming or outgoing routes on an interface.

This command does not require a license.

Examples

This example shows how to use a route map to filter routes for a RIP interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip route-filter route-map InRipFilter in
```

Related Commands

Command	Description
route-map	Creates a route map.
prefix-list	Creates a prefix list.

ip rip summary-address

To configure a summary aggregate address under an interface for the Routing Information Protocol (RIP), use the **ip rip summary-address** command in interface configuration mode. To disable summarization of the specified address or subnet, use the **no** form of this command.

ip rip summary-address *ip-prefix/mask*

no ip rip summary-address *ip-prefix/mask*

Syntax Description

ip-prefix/length	IP prefix and prefix length to be summarized.

Defaults

Disabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **ip rip summary-address** command summarizes an address or subnet under a specific interface.

This command does not require a license.

Examples

This example shows how to configure the summary address192.0.2.0 that is advertised out Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip summary-address rip 192.0.2.0/24
```

ip route

To configure a static route, use the **ip route** command. To remove the static route, use the **no** form of this command.

ip route *ip-prefix/mask* {[*interface*] *next-hop*} [*preference*] [**tag** *id*] [**name** *nexthop-name*]

no ip route *ip-prefix/mask* {[*interface*] *next-hop*}} [*preference*] [**tag** *id*] [**name** *nexthop-name*]

Syntax Description

ip-prefix/length	IP prefix and prefix length. The format is x.x.x.x/length. The length is 1 to 32.
interface	(Optional) The interface on which all packets are sent to reach this route. Use **?** to display a list of supported interfaces.
next-hop	IP address of the next-hop that can be used to reach that network. You can specify an IP address and an interface type and interface number. The format is x.x.x.x/length. The length is 1 to 32.
preference	(Optional) Sets the route preference, used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag *id*	(Optional) Assigns a route tag that can be used to match against in a route map. The range is from 0 to 4294967295. The default is 0.
name	(Optional) Specifies the name of the nexthop.
nexthop-name	(Optional) Name of the nexthop. The maximum size is 50 characters.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	Added **name** *nexthop-name* option in the syntax description.
4.0(1)	This command was introduced.

Usage Guidelines

Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precedence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100.

This command does not require a license.

Examples

This example shows how to create a static route for destinations with the IP address prefix 192.168.1.1/32, reachable through the next-hop address 10.0.0.2:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2
```

This example shows how to assign a tag to the previous example so that you can configure a route map that can match on this static route:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2 tag 5
```

This example shows how to choose a preference of 110. In this case, packets for prefix 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic route information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0/8 172.31.3.4 110
```

Related Commands

Command	Description
ipv6 route	Configures an IPv6 static route.
match tag	Matches the tag value associated with a route.

ip route track

To configure a static route associated with the track object, use the **ip route track** command.

ip route track route *ip-prefix ip-mask ip-addr* **track** *object-number*

Syntax Description

ip-prefix	IP address prefix.
ip-mask	IP mask.
ip-addr	IPv4 or IPv6 address.
track	(Optional) Specifies the object to be tracked.
object-number	Object number. The range is from 1 to 500.

Defaultsc

None

Command Modes

Global configuration mode.

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a static route associated with the track object:

```
switch# configure terminal
switch(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.242 track 123
switch(config)#
```

Related Commands

Command	Description
show static-route track-table	Displays information about the IPv4 or IPv6 static-route track table.

ip router eigrp

To specify the Enhanced Interior Gateway Routing Protocol (EIGRP) instance for an interface, use the **ip router eigrp** command. To return to the default, use the **no** form of this command.

ip router eigrp *instance-tag*

no ip router eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip router eigrp** command to specify the EIGRP instance for the interface.

This command requires the Enterprise Services license.

Examples

This example shows how to set the EIGRP instance for an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router eigrp Base
```

ip router ospf area

To specify the Open Shortest Path First (OSPF) instance and area for an interface, use the **ip router ospf area** command. To return to the default, use the **no** form of this command.

ip router ospf *instance-tag* **area** *area-id* [**secondaries none**]

no ip router ospf *instance-tag* **area** *area-id* [**secondaries none]**

Syntax Description

instance-tag	Instance tag. Specify as an alphanumeric string.
area-id	Identifier for the OSPF area where you want to enable authentication. Specify as either a positive integer value or an IP address.
secondaries none	(Optional) Excludes secondary IP addresses.

Defaults

10 seconds

Command Modes

Interface configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip router ospf area** command to specify the area and OSPF instance for the interface.

This command requires the Enterprise Services license.

Examples

This example shows how configure an interface for OSPF:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf Base area 33
```

ip router ospf multi-area

To configure multi-area adjacency on an Open Shortest Path First (OSPF) interface, use the **ip router ospf multi-area** command. To return to the default, use the **no** form of this command.

ip router ospf *instance-tag* **multi-area** *area-id*

no ip router ospf *instance-tag* **multi-area** *area-id*

Syntax Description

instance-tag	Instance tag. Specify as an case-sensitive alphanumeric string up to 63 characters.
area-id	Identifier for the OSPF area where you want to add as another area to the primary interface. Specify as either a positive integer value or an IP address.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **ip router ospf multi-area** command to specify additional areas on an OSPF interface.

This command requires the Enterprise Services license.

Examples

This example shows how to configure multi-area adjacency:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf Base area 33
switch(config-if)# ip router ospf Base multi-area 99
```

ip source-route

To handle IP datagrams with source routing header options, use the **ip source-route** command. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description This command has no keywords or arguments.

Defaults Enabled

Command Modes Global configuration

Interface 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 This example shows how to enable the handling of IP datagrams with source routing header options:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip source-route
```

ip split-horizon eigrp

To enable split horizon for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **ip split-horizon eigrp** command. To disable split horizon, use the **no** form of this command.

ip split-horizon eigrp *instance-tag*

no ip split-horizon eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **no ip split-horizon eigrp** command to disable split horizon on an interface.

This command requires the Enterprise Services license.

Examples

This example shows how to disable split horizon an an Ethernet link:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ip split-horizon eigrp 209
```

ip summary-address eigrp

To configure a summary aggregate address for the specified Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip summary-address eigrp** command. To disable a configuration, use the **no** form of this command.

ip summary-address eigrp *instance-tag* {*ip-address /length* | *ip-address mask*} [*admin-distance*]

no ip summary-address eigrp *instance-tag* {*ip-address /length* | *ip-address mask*}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
ip-address/length	Summary IP prefix and prefix length to apply to an interface in four-part, dotted-decimal notation. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If *length* is used, the slash is required.
ip-address	Summary IP address to apply to an interface in four-part, dotted-decimal notation.
mask	IP address mask.
admin-distance	(Optional) Administrative distance. The range is from 1 to 255.

Defaults

An administrative distance of 5 is applied to EIGRP summary routes.
No summary addresses are predefined.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip summary-address eigrp** command to configure interface-level address summarization. EIGRP summary routes are given an administrative distance of 5.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an administrative distance of 95 on an EIGRP interface for the 192.168.0.0/16 summary address:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
```

```
switch(config-if)# ip summary-address eigrp 209 192.168.0.0/16 95
```

ip tcp path-mtu-discovery

To enable path MTU discovery on an IPv4 or IPv6 interface, use the **ip tcp path-mtu discovery** command. To disable this feature, use the **no** form of this command.

ip ip tcp path-mtu discovery

no ip tcp path-mtu discovery

Syntax Description This command has no keywords or arguments

Defaults Disabled

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
5.0(2)	Added support for IPv6 path MTU discovery.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable path MTU discovery for both IPv4 and IPV6:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip tcp path-mtu-discovery
```

ip unreachables

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachables** command. To disable this function, use the **no** form of this command.

ip unreachables

no ip unreachables

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Use the **ip unreachables** command to enable the generation of ICMP unreachable messages on a Layer-3 VLAN interface.

Hosts use maximum transmission unit (MTU) path discovery to find the largest MTU along the path. They do this by setting the DF bit and sending a large packet. If the packet exceeds the physical port or port-channel MTU, the packet is dropped and GIANTS and INPUT DISCARDS are incremented in the **show interface** command output.

By default, a Cisco Nexus 7000 Series switch does not send back an ICMP Unreachable Packet-Too-Big message that notifies the host that the MTU of a packet is too large. The switch silently drops inbound packets that are larger than the physical port, port-channel, or Layer-3 VLAN interface MTU.

If a packet is routed, the Layer-3 VLAN MTU is checked and if the packet is too big, the output of the **show ip traffic** command indicates outfrag fails and packets with DF increments.

The system jumbomtu sets the upper limit for configuration of the MTU on a Cisco Nexus 7000 Series switch and can be seen with the **show run all | include jumbomtu** command.

The **show run all** command shows the default commands. The default MTU for interfaces and physical ports is 1500 bytes (1472 in pings with encapsulation overhead).

This command does not require a license.

Examples

This example shows how to enable the generation of ICMP unreachable messages, as appropriate, on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip unreachables
```

Related Commands

Command	Description
ip port-unreachable	Sends ICMP port unreachable messages.

ip wccp

To enable a Web Cache Communication Protocol (WCCP) service in a service group, use the **ip wccp** command. To disable the service group, use the **no** form of this command.

ip wccp {*service-number* | **web-cache** [**hia-timeout** *timeout seconds* | **mode** {**open** [**redirect-list** *access-list*] | **closed service-list** *service-access-list*}] [**password** [**0**-**7**] *password*]

no ip wccp {*service-number* | **web-cache** [**hia-timeout** *timeout seconds* | **mode** {**open** [**redirect-list** *access-list*] | **closed service-list** *service-access-list*}] [**password** [**0**-**7**] *password*]

Syntax Description

service-number	Dynamic service identifier. The *service-number* range is from 1 to 255.
web-cache	Specifies the web-cache well-known service.
hia-timeout	(Optional) Specifies the service group timeout.
timeout seconds	Timeout in seconds. The range is from 2 to 15 seconds.
mode	(Optional) Configures a a route tag value for local or direct routes.
open	Identifies the service as open.
redirect-list *access-list*	(Optional) Specifies the access list that controls traffic redirected to this service group. The *access-list* can be any case-sensitive, alphanumeric string up to 64 characters.
closed service-list *service-access-list*	(Optional) Identifies the service as closed. The service list identifies a named IP access list that defines the packets that match the service. The s*ervice-access-list* can be any case-sensitive, alphanumeric string up to 64 characters.
password [**0**-**7**]	(Optional) Configures the message digest algorithm 5 (MD5) authentication for messages received from the service group. WCCP discards messages that are not accepted by the authentication. The encryption type can be any value between 0 and 7 (inclusive), where 0 is unencrypted and 7 indicates proprietary encryption.
password	MD5 password. The *password* can be any case-sensitive, alphanumeric string up to eight characters.

Defaults

None

Command Modes

Global configuration

VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	Added the **hia-timeout** keyword to the syntax description.
4.2(1)	This command was introduced.

Usage Guidelines

The **redirect-list** keyword instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group. The **access list** specifies the traffic that is permitted to be redirected. The default is to redirect TCP traffic.

Use the **service-list** keyword only for closed mode services. When a WCCP service is closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create a secure connection between the router and the cache engine.

Use **password 0** *pwstring* to store the password in clear text. Use **password 7** *pwstring* to store the password in encrypted form. You can use the **password 7** keywords for an already encrypted password.

If you set the timer to 2 seconds and the timeout occurs at 10 seconds then at every 5 second interval, the service is lost due to the removal query.

Wildcard masks are not supported for the WCCPv2 redirect list.

Note You must enter the **ip wccp** command with all your required parameters. Any subsequent entry of the **ip wccp** command overwrites the earlier configuration.

This command does not require a license.

Examples

This example shows how to configure a service group timeout in seconds:

```
switch(config)# ip wccp 23 hia-timeout 14
switch(config)#
```

This example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
switch(config)# access-list 100
switch(config-acl)# permit ip any any
switch(config-acl)# exit
switch(config)# ip wccp web-cache redirect-list 100
switch(config)# interface ethernet 2/1
switch(config-if)# ip wccp web-cache redirect out
```

This example shows how to configure a closed WCCP service:

```
switch(config)# ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
show ip wccp	Displays the status of the WCCP service group.

ip wccp redirect

To redirect a packet on an outbound or inbound interface using the Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command.

ip wccp {*service-number* | **web-cache**} **redirect** {**in** | **out**}

no ip wccp {*service-number* | **web-cache**} **redirect** {**in** | **out**}

Syntax Description

service-number	Dynamic service identifier. The *service-number* range is from 1 to 255.
web-cache	Specifies the web-cache well-known service.
in	Redirects a packet on an inbound interface.
out	Redirects a packet on an outbound interface.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

WCCPv2 is only supported on Layer 3 interfaces, including Layer 3 subinterfaces, VLAN interfaces, Layer 3 and port channels.

Use the **ip wccp redirect in** command to configure WCCP redirection on an interface that receives inbound network traffic. When you configure the command on an interface, all packets that arrive at that interface are compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they are redirected.

Use the **ip wccp redirect out** command to configure the WCCP redirection check at an outbound interface.

You can also include a redirect list when you configure a service group. The redirect list allows you to deny packets with a NAT (source) IP address and prevent redirection. See the **ip wccp** command for information about configuring the redirect list and service group.

To prevent redirection of any packets from the cache engine, use the **ip wccp redirect exclude in** command on the router interface that faces the cache engine.

Note Do not use the **ip wccp redirect** {**in** | **out**} command and the **ip wccp redirect exclude in** command on the same interface. The **ip wccp redirect exclude in** command overrides the **ip wccp redirect** {**in** | **out**} command.

This command does not require a license.

Examples

This example shows how to configure a session in which WCCP redirects outgoing packets on Ethernet interface 2/2 to a cache engine:

```
switch(config)# ip wccp 99
switch(config)# interface ethernet 2/2
switch(config-if)# ip wccp 99 redirect out
```

This example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 2/1 is redirected to a cache engine:

```
switch(config)# ip wccp web-cache
switch(config)# interface ethernet 0/1
switch(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
ip wccp redirect exclude in	Excludes WCCP redirection on an interface.
show ip wccp	Displays the status of the WCCP service group.

ip wccp redirect exclude in

To exclude inbound packets on an interface from Web Cache Communication Protocol (WCCP) redirection checks, use the **ip wccp redirect exclude** in command. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines Use the **ip wccp redirect exclude in** command to exclude inbound packets on an interface from any redirection check that may occur at the outbound interface. This command is affects all the services and should be applied to any inbound interface that will be excluded from redirection.

Note Do not use the **ip wccp redirect** {**in** | **out**} command and the **ip wccp redirect exclude in** command on the same interface. The **ip wccp redirect exclude in** command overrides the **ip wccp redirect** {**in** | **out**} command.

This command does not require a license.

Examples This example shows how to exclude packets that arrive on Ethernet interface 2/1 from all WCCP redirection checks:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip wccp redirect exclude in
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
ip wccp redirect	Configures WCCP redirection on an interface.
show ip wccp	Displays the status of the WCCP service group.

ipv4 local policy route-map

To configure IPv4 local policy route maps for packets generated by the device, use the **ipv4 local policy route-map** command.

ipv4 local policy route-map *map-name*

Syntax Description		
	map-name	Map name. The *map-name* string can be up to 63 alphanumeric characters.

Defaults None

Command Modes Global configuration mode

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

Usage Guidelines This command requires the Enterprise Services license.

Examples This example shows how to configure IPv4 local policy route maps for packets generated by the device:

```
switch# configure terminal
switch(config)# ip local policy route-map pbr-src-90
switch(config)#
```

Related Commands	Command	Description
	ipv6 local policy route-map	Configures IPv6 local policy route maps for packets generated by the device.

ipv6 address

To configure an IPv6 address on an interface, use the **ipv6 address** command. To remove the address, use the **no** form of this command.

ipv6 address {*addr* [**eui64**] [**route-preference** *preference*] [**secondary**] **tag** *tag-id*] | **use-link-local-only**]

no ipv6 address {*addr* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*] | **use-link-local-only**

Syntax Description

addr	IPv6 address. The format is A:B::C:D/length. The length range is 1 to 128.
eui64	(Optional) Configures the Extended Unique Identifier (EUI64) for the low-order 64 bits of the address.
route-preference *preference*	(Optional) Sets the route preference for local or direct routes. The range is from 0 to 255.
secondary	(Optional) Creates a secondary IPv6 address.
tag *tag-id*	(Optional) Configures a a route tag value for local or direct routes.
use-link-local-only	Specifies IPv6 on the interface using only a single link-local.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Added **tag** keyword.

Usage Guidelines

Use the **ipv6 address** command to configure an IPv6 address or secondary address on an interface.

This command does not require a license.

Examples

This example shows how to configure an IPv6 address:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8::3/48
```

Related Commands

Command	Description
ip address	Configures an IPv4 address on an interface.

ipv6 authentication key-chain eigrp

To enable authentication for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets and to specify the set of keys that can be used on an interface, use the **ipv6 authentication key-chain eigrp** command. To prevent authentication, use the **no** form of this command.

ipv6 authentication key-chain eigrp *instance-tag name-of-chain*

no ipv6 authentication key-chain eigrp *instance-tag name-of-chain*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
name-of-chain	Name of a key chain. The key chain name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You must set the authentication mode using the **ipv6 authentication mode eigrp** command in interface 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

This 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)# interface ethernet 1/2
switch(config-if)# ipv6 authentication key-chain eigrp 209 trees
```

Related Commands

Command	Description
ipv6 authentication mode eigrp	Sets the authentication mode for EIGRP for an IPv6 interface.
key-chain	Creates a set of keys that can be used by an authentication method.

ipv6 authentication mode eigrp

To specify the type of authentication used in the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication mode eigrp** command. To remove authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *instance-tag* **md5**

no ipv6 authentication mode eigrp *instance-tag* **md5**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
md5	Specifies Message Digest 5 (MD5) authentication.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the interface to use MD5 authentication:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ipv6 authentication mode eigrp 209 md5
```

Related Commands

Command	Description
authentication mode (EIGRP	Configures the authentication mode for EIGRP in address-family mode.
iv6p 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.

ipv6 bandwidth eigrp

To configure the bandwidth metric on an Enhanced Interior Gateway Routing Protocol (EIGRP) for the IPv6 interface, use the **ipv6 bandwidth eigrp** command. To restore the default, use the **no** form of this command.

ipv6 bandwidth eigrp *instance-tag bandwidth*

no ipv6 bandwidth eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
bandwidth	Bandwidth value. The range is from 1 to 2,560,000,000 kilobits.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure EIGRP to use a bandwidth metric of 10000 in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 bandwidth eigrp 209 10000
```

Related Commands

Command	Description
ipv6 bandwidth-percent eigrp	Sets the percent of the interface bandwidth that EIGRP can use.

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 bandwidth-percent eigrp** command. To restore the default, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *instance-tag percent*

no ipv6 bandwidth-percent eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
percent	Percentage of bandwidth that EIGRP may use.

Defaults

percent: 50

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

EIGRP uses up to 50 percent of the bandwidth of a link, as defined by the **ip bandwidth** interface configuration command. Use the **ip bandwidth-percent** command to change this default percent.

This command requires the Enterprise Services license.

Examples

This example shows how to configure EIGRP to use up to 75 percent of an interface in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
ipv6 bandwidth eigrp	Sets the EIGRP bandwidth value for an interface.

ipv6 delay eigrp

To configure the throughput delay for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 delay eigrp** command. To restore the default, use the **no** form of this command.

ipv6 delay eigrp *instance-tag seconds*

no ipv6 delay eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Throughput delay, in tens of microseconds. The range is from 1 to 16777215.

Defaults

100 (10-microsecond units)

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You configure the throughput delay on an interface in 10-microsecond units. For example, if you set the **ipv6 delay eigrp** command to 100, the throughput delay is 1000 microseconds.

This command requires the Enterprise Services license.

Examples

This example shows how to set the delay to 400 microseconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 delay eigrp 1 40
```

Related Commands

Command	Description
ipv6 hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process that is designated by an autonomous system number.

ipv6 distribute-list eigrp

To configure a distribution list for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 distribute-list eigrp** command. To restore the default, use the **no** form of this command.

ipv6 distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

no ipv6 distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
prefix-list *list-name*	Specifies the name of an IPv6 prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies the route policy to incoming routes.
out	Applies the route policy to outgoing routes.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 distribute-list eigrp** command to configure a route filter policy on an interface. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a route map for all EIGRP routes coming into the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 distribute-list eigrp 209 route-map InputFilter in
```

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

ipv6 eigrp shutdown

To shut down the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 eigrp shutdown** command. To restore the default, use the **no** form of this command.

ipv6 eigrp *instance-tag* **shutdown**

no ipv6 eigrp *instance-tag* **shutdown**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to disable EIGRP on an interface:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 eigrp 201 shutdown
```

Related Commands

Command	Description
router eigrp	Configures an instance of EIGRP.

ipv6 hello-interval eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 hello interval for an interface, use the **ipv6 hello-interval eigrp** command. To restore the default, use the **no** form of this command.

ipv6 hello-interval eigrp *instance-tag seconds*

no ipv6 hello-interval eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Hello interval (in seconds). The range is from 1 to 65535.

Defaults

5 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to set the hello interval to 10 seconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 hello-interval eigrp 1 10
```

ipv6 hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 hold-time eigrp** command. To restore the default, use the **no** form of this command.

ipv6 hold-time eigrp *instance-tag seconds*

no ipv6 **hold-time eigrp** *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
seconds	Hold time (in seconds). The range is from 1 to 65535.

Defaults

15 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 hold-time eigrp** command to increase the default hold time on very congested and large networks.

We recommend that you configure the hold time to be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

This command requires the Enterprise Services license.

Examples

This example shows how to set the hold time to 40 seconds for the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 hold-time eigrp 209 40
```

Related Commands

Command	Description
ipv6 hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process designated by an autonomous system number.

ipv6 host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ipv6 host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ipv6 host *name address1* [*address2... address6*]

no ipv6 host *name address1* [*address2... address6*]

Syntax Description

name	Hostname. The *name* can be any case-sensitive, alphanumeric string up to 80 characters.
address1	IPv6 address in the A:B::C:D format.
address2 ...address6	(Optional) Up to five additional IPv6 addresses in the A:B::C:D format.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 host** command to add a static hostname to DNS.

This command does not require a license.

Examples

This example shows how to configure a static hostname:

```
switch(config)# ipv6 host mycompany.com 2001:0DB8::4
```

Related Commands

Command	Description
ip host	Configures a static hostname.

ipv6 local policy route-map

To configure IPv6 local policy route maps for packets generated by the device, use the **ipv6 local policy route-map** command.

ipv6 local policy route-map *map-name*

Syntax Description		
	map-name	Map name. The *map-name* string can be up to 63 alphanumeric characters.

Defaults None

Command Modes Global configuration mode

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

Usage Guidelines This command requires the Enterprise Services license.

Examples This example shows how to configure IPv6 local policy route maps for packets generated by the device:

```
switch# configure terminal
switch(config)# ip local policy route-map pbr-src-90
switch(config)#
```

Related Commands	Command	Description
	ipv4 local policy route-map	Configures IPv4 local policy route maps for packets generated by the device.

c

ipv6 nd cache limit

To configure the maximum number of entries in the neighbor adjacency table, use the **ipv6 nd cache limit max-nd-adj** command.

ipv6 nd cache limit *max-nd-adj* [**syslog** *syslogs-per-second*]

Syntax Description

max-nd-adj	Maximum number of entries in the neighbor adjacency table. The range is from 1 to 409600.
syslog	(Optional) Specifies syslog messages.
syslogs-per-second	Number of system logs per second. The range is from 1 to 1000.

Defaults

None

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the maximum number of entries in the neighbor adjacency table:

```
switch# configure terminal
switch(config-if)# interface ethernet 2/1
switch(config-if)# ipv6 nd cache 1000 syslog 100
switch(config)#
```

Related Commands

Command	Description
ipv6 nd dad attempts	Sets the number of consecutive neighbor solicitation messages that the device sends from the IPv6 interface for duplicate address detection (DAD) validation.
ipv6 nd fast-path	Improves the performance of glean packets by reducing the processing of the packets in the supervisor.

ipv6 nd dad attempts

To set the number of consecutive neighbor solicitation messages that the device sends from the IPv6 interface for the duplicate address detection (DAD) validation, use the **ipv6 nd dad attempts** command.

ipv6 nd dad attempts *number*

Syntax Description

number	Number of attempts.

Defaults

1

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to set the number of consecutive neighbor solicitation messages that the device sends from the IPv6 interface for the DAD validation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd dad attempts 3
switch(config-if)#
```

Related Commands

Command	Description
ipv6 nd cache limit	Configures the maximum number of entries in the neighbor adjacency table.
ipv6 nd fast-path	Improves the performance of glean packets by reducing the processing of the packets in the supervisor.

ipv6 nd fast-path

To improve the performance of glean packets by reducing the processing of the packets in the supervisor, use the **ipv6 nd fast-path** command. To remove the fast path configuration, use the **no** form of this command.

ipv6 nd fast-path

no ipv6 nd fast-path

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

config-router-neighbor-af mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to improve the performance of glean packets by reducing the processing of the packets in the supervisor:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd fast-path
switch(config-if)#
```

This example shows how to delete the fast path configuration:

```
switch(config-if)# no ipv6 nd fast-path
```

Related Commands

Command	Description
ipv6 nd dad attempts	Sets the number of consecutive neighbor solicitation messages that the device sends from the IPv6 interface for duplicate address detection (DAD) validation.

ipv6 nd hop-limit

To advertise the hop limit in IPv6 neighbor discovery packets, use the **ipv6 nd hop-limit** command. To return to default, use the **no** form of this command.

ipv6 nd hop-limit *hop-limit*

no ipv6 nd hop-limit [*hop-limit*]

Syntax Description

hop-limit	Hop limit in IPv6 header. The range is from 0 to 255.

Defaults

64

Command Modes

Interface 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

This example shows how to configure the IPv6 hop limit:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd hop-limit 55
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd mac-extract

To enable any next hop that matches the IPv6 prefix on that interface to be treated as a MAC Embedded IPv6 (MEv6) address, use the **ipv6 nd mac-extract** command. To disable this function, use the **no** form of this command.

ipv6 nd mac-extract

no ipv6 nd mac-extract

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
6.2(8)	This command was introduced.

Usage Guidelines Beginning with Cisco NX-OS Release 6.2(8), BGP supports RFC 5549 which allows an IPv4 prefix to be carried over an IPv6 next hop.

The IPv6 next hop is leveraged to remove neighbor discover (ND) related traffic from the network by embedding the MAC address directly in the global IPv6 next-hop address. This address is called a MAC Embedded IPv6 (MEv6) address. The router extracts the MAC address directly from the MEv6 address instead of through ND.

This command requires the Enterprise Services license.

Examples This example shows how to configure an IPv4 route over an IPv6 next-hop:

```
switch(config)# interface ethernet 0/1
switch(config-if)# mac-address mac3
switch(config-if)# ipv6 address ABCD:1::/64 eui-64
switch(config-if)# ipv6 nd mac-extract
switch(config-if)# ip forward

switch(config)# interface ethernet 0/2
switch(config-if)# ipv6 address ABCF:1::3/64
switch(config-if)# ip forward
```

Related Commands

Command	Description
ip forward	Allows IPv4 traffic on an interface even when there is no IP address configuration on that interface.

ipv6 nd managed-config-flag

To advertise in ICMPv6 Router-Advertisement messages to use stateful address auto-configuration to obtain address information, use the **ipv6 nd managed-config-flag** command. To revert to default, use the **no** form of this command.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax Description This command has no keywords or arguments.

Defaults None

Command Modes Interface 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 This example shows how to advertise in ICMPv6 Router-Advertisement messages to use stateful address auto-configuration to obtain address information:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd mtu

To advertise the Maximum Transmission Unit (MTU) in ICMPv6 Router-Advertisement messages on this link, use the **ipv6 nd mtu** command. To revert to default, use the **no** form of this command.

ipv6 nd mtu *mtu*

no ipv6 nd mtu [*mtu*]

Syntax Description

mtu	MTU in bytes. The range is from 1280 to 65535.

Defaults

1500

Command Modes

Interface 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

This example shows how to configure the MTU value to advertise on a link:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd mtu 1280
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd ns-interval

To configure the retransmission interval between IPv6 neighbor solicitation messages, use the **ipv6 nd ns-interval** command. To revert to default, use the **no** form of this command.

ipv6nd ns-interval *interval*

no ipv6 nd ns-interval [*interval*]

Syntax Description

interval	Interval in milliseconds. The range is from 1000 to 3600000.

Defaults

1000

Command Modes

Interface 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

This example shows how to configure the neighbor solicitation interval:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ns-interval 1280
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd other-config-flag

To indicate in ICMPv6 router advertisement messages that hosts use stateful auto configuration to obtain nonaddress related information, use the **ipv6 nd other-config-flag** command. To revert to the default, use the **no** form of this command.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Interface 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

This example shows how to configure stateful autoconfiguration in ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd prefix

To advertise the IPv6 prefix in the router advertisement messages, use the **ipv6 nd prefix** command. To revert to the default, use the **no** form of this command.

ipv6 nd prefix {*ipv6-address/prefix-length* | **default**} {*valid-lifetime* | **infinite** | **no-advertise**} {*preferred-lifetime* | **infinite**} [**no-autoconfig**] [**no-onlink**] [**off-link**]

no ipv6 nd prefix {*ipv6-address* | **default**}

Defaults

ipv6-address	IPv6 prefix.
/prefix-length	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
default	Specifies that default values are used.
valid-lifetime	Amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The range is from 0 to 4294967295.
infinite	Specifies that the valid lifetime is infinite.
no-advertise	Specifies that the prefix is not advertised.
preferred-lifetime	Amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. The range is from 0 to 4294967295.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The prefix is advertised with the A-bit clear.
no-onlink	(Optional) Configures the specified prefix as not on-link. The prefix is advertised with the L-bit clear.
off-link	(Optional) Configures the specified prefix as off-link. The prefix is advertised with the L-bit clear. The prefix is not inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured using the **ipv6 address** command), it will be removed.

Defaults

All prefixes are advertised as an autoconfiguration prefix (for example, the A-bit is set in the advertisement).

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(8)	The **no-autoconfig** keyword was added.
5.2(1)	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, only these prefixes are advertised.

Default Parameters

The **default** keyword can be used to set default parameters for all prefixes.

Prefix Lifetime and Expiration

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix is no longer advertised.

On-Link

When on-link is on (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. When autoconfiguration is on (the default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 neighbor discovery (ND) router advertisement, and presence of the prefix in the routing table, as follows:

- Default L=1 A=1 In Routing Table
- no-onlink L=0 A=1 In Routing Table
- no-autoconfig L=1 A=0 In Routing Table
- no-onlink no-autoconfig L=0 A=0 In Routing Table
- off-link L=0 A=1 Not in Routing Table
- off-link no-autoconfig L=0 A=0 Not in Routing Table

This command does not require a license.

Examples

This example shows how to include the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds:

```
switch(config)# interface ethernet 0/0
switch(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd ra-interval

To configure the interval between sending ICMPv6 router advertisement messages, use the **ipv6 nd ra-interval** command. To revert to default, use the **no** form of this command.

ipv6 nd ra-interval *interval*

no ipv6 nd ra-interval [*interval*]

Syntax Description

interval	Interval between sending router advertisement messages in seconds. The range is from 4 to 1800.

Defaults

600

Command Modes

Interface 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

This example shows how to configure the ICMPv6 router advertisement message interval:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ra-interval 500
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd ra-lifetime

To advertise the router lifetime of a default router in ICMPv6 router advertisement messages, use the **ipv6 nd ra-lifetime** command. To revert to the default, use the **no** form of this command.

ipv6 nd ra-lifetime *lifetime*

no ipv6 nd ra-lifetime [*lifetime*]

Syntax Description

lifetime	Lifetime in seconds. The range is from 0 to 9000. If 0, this router will not be the default router.

Defaults

Three times the router advertisement interval.

Command Modes

Interface 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

This example shows how to configure the ICMPv6 router advertisement message lifetime:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ra-lifetime 1500
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd reachable-time

To advertise the time when a node considers a neighbor up after receiving a reachability confirmation in ICMPv6 router advertisement messages, use the **ipv6 nd reachable-time** command. To revert to the default, use the **no** form of this command.

ipv6 nd reachable-time *time*

no ipv6 nd reachable-time [*time*]

Syntax Description

lifetime	Lifetime in seconds. The range is from 0 to 9000. If 0, this router will not be the default router.

Defaults

0

Command Modes

Interface 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

This example shows how to configure the ICMPv6 router advertisement reachability time:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd reachable-time 1500
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd redirects

To enable sending ICMPv6 redirect messages, use the **ipv6 redirects** command. To revert to the default, use the **no** form of this command.

ipv6 nd redirects

no ipv6 nd redirects

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Interface 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 This example shows how to disable the ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no ipv6 nd redirects
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd retrans-timer

To advertise the time between neighbor solicitation (NS) messages in ICMPv6 router advertisement messages, use the **ipv6 nd retrans-timer** command. To revert to the default, use the **no** form of this command.

ipv6 nd retrans-timer *time*

no ipv6 nd retrans-timer [*time*]

Syntax Description

lifetime	Lifetime in seconds. The range is from 0 to 9000. If 0, this router will not be the default router.

Defaults

0

Command Modes

if-igp configuration (config-xxx)

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

This example shows how to configure the ICMPv6 router advertisement reachability time:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd retrans-timer
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 nd suppress-ra

To disable sending ICMPv6 router advertisement messages, use the **ipv6 nd suppress-ra** command. To revert to default, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description This command has no keywords or arguments.

Defaults Enabled

Command Modes Interface 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 This example shows how to disable the ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *pv6-address interface-type interface-number hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*

Syntax Description

ipv6-address	IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type	Interface type. For supported interface types, use the question mark (?) online help function.
interface-number	Interface number.
hardware-address	Local data-link address (a 48-bit address).

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor** command to create a static entry. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- INCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries. See the show ipv6 neighbors command for descriptions of the INCMP and REACH states for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to INCMP).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

This example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 neighbor 2001:0DB8::45A ethernet 2/10002.7D1A.9472
```

ipv6 next-hop-self eigrp

To instruct the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 process to use the local IPv6 address as the next-hop address when advertising these routes, use the **next-hop-self eigrp** command. To use the received next-hop value, use the **no** form of this command.

ipv6 next-hop-self eigrp *instance-tag*

no ipv6 next-hop-self eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

EIGRP always sets the IPv6 next-hop value to be itself.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

EIGRP, by default, sets the IPv6 next-hop value to be itself for routes that it is advertising, even when advertising those routes on the same interface from which the router learned them. To change this default, you must use the **no ipv6 next-hop-self eigrp** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes.

Examples

This example shows how to change the default IPv6 next-hop value and instruct EIGRP to use the received next-hop value:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ipv6 next-hop-self eigrp 209
```

ipv6 offset-list eigrp

To configure an offset list for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 offset-list eigrp** command. To restore the default, use the **no** form of this command.

ipv6 offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

no ipv6 offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
prefix-list *list-name*	Specifies the name of an IPv6 prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies a route policy to incoming routes.
out	Applies a route policy to outgoing routes.
offset	Value to add to the EIGRP metric.

Defaults

This command has no defaults.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 offset-list eigrp** command to influence which route is advertised on an interface. Cisco NX-OS adds the configured offset value to any routes that match the configure prefix list or route map. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an offset list filter to add 20 to the metric for EIGRP routes coming into the interface that match the route map OffsetFilter:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 offset-list eigrp 209 route-map OffsetFilter in 20
```

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

ipv6 passive-interface eigrp

To suppress all routing updates on an Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 passive-interface eigrp** command. To reenable the sending of routing updates, use the **no** form of this command.

ipv6 passive-interface eigrp *instance-tag*

no ipv6 passive-interface eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Routing updates are sent on the interface.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 passive-interface eigrp** command to stop all routing updates on an interface and suppress the formation of EIGRP adjacencies.

This command requires the Enterprise Services license.

Examples

This example shows how to stop EIGRP routing updates on Ethernet 2/1:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 passive-interface eigrp 201
```

ipv6 policy route-map

To identify a route map to use for policy routing on an interface, use the **ipv6 policy route-map** command. To remove the route map, use the **no** form of this command.

ipv6 policy route-map *name*

no ipv6 policy route-map [*name*]

Syntax Description

name	Name of the route map. The name can be any alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **iv6 policy route-map** command to identify a route map to use for policy routing on an IPv6 interface. Use the **route-map** command to create the rout map. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing is allowed for the interface, based on the destination IPv6 address of the packet. The **set** commands specify the set actions—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ipv6 policy route-map** command deletes the pointer to the route map.

You can perform policy-based routing on any match criteria that can be defined in an IPv6 access list when using the **match ipv6 address** command and referencing an IPv6 access list.

You must enable policy-based routing with the **feature pbr** command before you can use the **ipv6 policy route-map** command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a policy-based route map to an interface:

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 policy route-map policymap
```

Related Commands

Command	Description
feature pbr	Enabled the policy-based routing feature.
route-map	Creates a route map.
show route-map pbr-statistics	Displays statistics about policy-based route maps
show ipv6 policy	Displays information about IPv6 policies

ipv6 prefix-list

To create a prefix list to match IPv6 packets or routes again, use the **ipv6 prefix-list** command. To remove the prefix-list, use the **no** form of this command.

ipv6 prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [*le length*]]

no ipv6 prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [*le length*]]

Syntax Description

name	IPv6 prefix list name. The name can be any alphanumeric string up to 63 characters.
seq *number*	(Optional) Specifies the sequence number to order entries in the prefix list. The range is from 1 to 4294967294.
permit	Allows routes or IP packets that match the prefix list.
deny	Rejects routes or IP packets that match the prefix list.
prefix	IP prefix in A:B::C:D/length format.
eq *length*	(Optional) Specifies the exact prefix length to match. The range is from 1 to 128.
ge *length*	(Optional) Specifies the maximum prefix length to match. The range is from 1 to 128.
le *length*	(Optional) Specifies the minimum prefix length to match. The range is from 1 to 128.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 prefix-list** command to configure IPv6 prefix filtering. You configure prefix lists with permit or deny keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IPv6 address and a bit mask. The bit mask is entered as a number from 1 to 128. An implicit deny is applied to traffic that does not match any prefix-list entry.

You can configure prefix lists to match an exact prefix length or a prefix range. Use the **ge** and **le** keywords to specify a range of the prefix lengths to match, providing more flexible configuration than can be configured with just the network/length argument. Cisco NX-OS processes the prefix list using

an exact match when you do not configure either the **ge** nor **le** keyword. If you configure both the **ge** *ge-length* and **le** l*e-length* keywords and arguments, the allowed prefix length range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

network/length < ge ge-length < le le-length <= 32

If you do not configure a sequence number, Cisco NX-OS applies a a default sequence number of 5 to the prefix list, and subsequent prefix list entries will be increment by 5 (for example, 5, 10, 15, and onwards). If you configure a sequence number for the first prefix list entry but not subsequent entries, then Cisco NX-OS increments the subsequent entries by 5 (For example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the no form of this command with the **seq** keyword.

Cisco NX-OS evaluates prefix lists starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the **permit** or **deny** statement is applied to that network and the rest of the list is not evaluated.

Tip For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The seq number keyword and argument can be used for resequencing.

The prefix list is applied to inbound or outbound updates for specific peer by entering the **prefix-list** command in neighbor address-family mode. Prefix list information and counters are displayed in the output of the **show ipv6 prefix-list** command. Prefix-list counters can be reset by entering the **clear ipv6 prefix-list** command.

This command does not require a license.

Examples

This example shows how to configure an IPv6 prefix list and apply it to a BGP peer:

```
switch# config t
switch(config)# ipv6 prefix-list allowprefix 10 permit 2001:0DB8::/48 eq 24
switch(config) router bgp 65536:20
switch(config-router)# neighbor 2001:0DB8::1/64 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

Related Commands

Command	Description
clear ip prefix-list	Clears counters for IP prefix lists.
prefix-list	Applies a prefix list to BGP peer.
show ip prefix-list	Displays information about IP prefix lists.

ipv6 prefix-list description

To configure a description string for an IPv6 prefix-list, use the **ipv6 prefix-list description** command. To revert to default, use the **no** form of this command.

ipv6 prefix-list *name* **description** *string*

no ipv6 prefix-list *name* **description**

Syntax Description

name	Name of the prefix list. The name can be any alphanumeric string up to 63 characters.
string	Descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.

Defaults

None

Command Modes

Global 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

This example shows how to configure a description for an IPv6 prefix list:

```
switch# configure terminal
switch(config)# ipv6 prefix-list test1 description “this is a test”
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an IPv6 prefix list.
show ipv6 prefix-list	Displays information about IPv6 prefix lists.

ipv6 route

To configure a static IPv6 route, use the **ipv6 route** command. To remove this static route, use the **no** form of this command.

ipv6 route *ipv6-prefix/length* {{*next-hop-addr* | *next-hop-prefix*} | *interface* | *link-local-addr*} [*preference*] [**tag** *tag-id*]

no ipv6 route *ipv6-prefix/length*

Syntax Description

ipv6-prefix/length	IPv6 prefix and prefix length. The format is A:B::C:D/length. The length range is from 1 to 128.
next-hop-addr	Next-hop address. The format is A:B::C:D.
next-hop-prefix	Next-hop prefix and length. The format is A:B::C:D/length. The length range is from 1 to 128.
interface	Interface to reach this route. Use **?** to display a list of supported interfaces.
link-local-addr	IPv6 link-local address. The format is A:B::C:D.
preference	(Optional) Sets the route preference, used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag *id*	(Optional) Assigns a route tag that can be used to match against in a route map. The range is from 0 to 4294967295. The default is 0.

Defaults

Disabled

Command Modes

Global 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

This example shows how to create an IPv6 static route:

```
switch(config)# ipv6 route 2001:0DB8::/48 2b11::2f01:4c
```

Related Commands

Command	Description
ip route	Configures an IPv4 static route.

ipv6 router eigrp

To specify the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 router eigrp** command. To return to the default, use the **no** form of this command.

ipv6 router eigrp *instance-tag*

no ipv6 router eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 router eigrp** command to specify the EIGRP instance for the interface.

This command requires the Enterprise Services license.

Examples

This example shows how to set the EIGRP instance for an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router eigrp Base
```

ipv6 router ospfv3 area

To specify the Open Shortest Path First version 3(OSPFv3) instance and area for an interface, use the **ipv6 router ospfv3 area** command. To return to the default, use the **no** form of this command.

ipv6 router ospfv3 *instance-tag* area *area-id* [**secondaries none**]

no ipv6 router ospfv3 *instance-tag* area *area-id* [**secondaries none**]

Syntax Description

instance-tag	Instance tag. Specify as an alphanumeric string.
area-id	Identifier for the OSPFv3 area where you want to enable authentication. Specify as either a positive integer value or an IP address.
secondaries none	(Optional) Excludes secondary IP addresses.

Defaults

None

Command Modes

Interface configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 router ospfv3 area** command to specify the area and OSPFv3 instance for the interface.

This command requires the Enterprise Services license.

Examples

This example shows how configure an interface for OSPFv3:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router ospfv3 Base area 33
```

ipv6 router ospfv3 multi-area

To configure multi-area adjacency on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 router ospfv3 multi-area** command. To return to the default, use the **no** form of this command.

ipv6 router ospfv3 *instance-tag* **multi-area** *area-id*

no ipv6 router ospfv3 *instance-tag* **multi-area** *area-id*

Syntax Description

instance-tag	Instance tag. Specify as an case-sensitive alphanumeric string up to 63 characters.
area-id	Identifier for the OSPF area where you want to add as another area to the primary interface. Specify as either a positive integer value or an IP address.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 router ospfv3 multi-area** command to specify additional areas on an OSPFv3 interface.

This command requires the Enterprise Services license.

Examples

This example shows how to configure multi-area adjacency:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router ospfv3 Base area 33
switch(config-if)# ipv6 router ospfv3 Base multi-area 99
```

ipv6 split-horizon eigrp

To enable split horizon for an Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 process, use the **ipv6 split-horizon eigrp** command. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *instance-tag*

no ipv6 split-horizon eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **no ipv6 split-horizon eigrp** command to disable split horizon on an interface.

This command requires the Enterprise Services license.

Examples

This example shows how to disable split horizon an an Ethernet link:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ipv6 split-horizon eigrp 209
```

ipv6 summary-address eigrp

To configure a summary aggregate address for the specified Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 summary-address eigrp** command. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *instance-tag* {*ipv6-address /length*} [*admin-distance*]

no ipv6 summary-address eigrp *instance-tag* {*ipv6-address /length*}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 63 characters.
ipv6-address/length	Summary IPv6 prefix and prefix length to apply to an interface in A:B::C:D/length format. The length range is from 1 to 128.
admin-distance	(Optional) Administrative distance. The range is from 1 to 255.

Defaults

An administrative distance of 5 is applied to EIGRP summary routes.
No summary addresses are predefined.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 summary-address eigrp** command to configure interface-level summary address. EIGRP summary routes are given an administrative distance of 5.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an administrative distance of 95 on an EIGRP interface for the 2001:0DB8::/48 summary address:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 summary-address eigrp 209 2001:0DB8::/48 95
```

ipv6 unreachables

To enable sending ICMPv6 unreachable messages, use the **ipv6 unreachables** command. To revert to default, use the **no** form of this command.

ipv6 [**icmp**] **unreachables**

no ipv6 [**icmp**] **unreachables**

Syntax Description

icmp	(Optional) Specifies ICMPv6 commands.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Port-unreachable messages are always rate limit enabled.

This command does not require a license.

Examples

This example shows how to enable the ICMPv6 unreachable messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 unreachables
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

is-type

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the **is-type** command. To reset the default value, use the **no** form of this command.

is-type {**level-1** | **level-1-2** | **level-2**}

no is-type {**level-1** | **level-1-2** | **level-2**}

Syntax Description

level-1	Specifies that the router performs only level-1 (intraarea) routing.
level-1-2	Specifies that the router performs both level-1 and level-2 routing.
level-2	Specifies that the routing process acts as a level-2 (interarea) router only.

Command Default

Routers typically act as both a level-1 (intraarea) and a level-2 (interarea) router by default. In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a level-1-2 (intraarea and interarea) router. The remaining instances of the IS-IS process configured by default are level-1 routers.

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

The routing levels for an instance of the IS-IS routing process are defined as follows:

- **level-1—**Specifies that the router performs only level-1 (intraarea) routing. This router learns only about destinations inside its area. Level-2 (interarea) routing is performed by the closest level-1-2 router.
- **level-1-2—**Specifies that the router performs both level-1 and level-2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (level-1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (level-2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
- **level-2—**Specifies that the routing process acts as a level-2 (interarea) router only. This router is part of the backbone, and does not communicate with level-1-only routers in its own area.

We recommend that you configure the type of IS-IS routing process. If you are configuring multiarea IS-IS, you must configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the router isis command is a level-1-2 router.

If only one area is in the network, there is no need to run both level-1 and level-2 routing algorithms. If IS-IS is used for IP routing only (and there is only one area), you can run level-2 only everywhere. Areas you add after the level-1-2 area exists are by default level-1 areas.

If the router instance has been configured for level-1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove level-2 (interarea) routing for the area using the is-type command. You can also use the is-type command to configure level-2 routing for an area, but it must be the only instance of the IS-IS routing process configured for level-2 on the Cisco device.

This command requires the Enterprise Services license.

Examples

This example specifies an area router:

```
switch(config)# router isis
switch(config-router)# is-type level-2-only
```

Related Commands

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

isis authentication key-chain

To enable authentication for Intermediate System-to-Intermediate System (IS-IS) for an individual IS-IS interface, use the **isis authentication key-chain** command. To disable authentication, use the **no** form of this command.

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

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

Syntax Description

auth-key	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

Interface configuration

Supported User Roles

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 **isis 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 **isis authentication key-chain** command, the first authentication key chain is overridden.

You can configure key-chain authentication per IS-IS instance by using the **authentication key-chain** configuration command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure IS-IS to accept and send any key belonging to the key chain named site1 on a specific interface:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication key-chain site1 level-1
switch(config-if)#
```

Related Commands

Command	Description
authentication key-chain	Enables authentication per IS-IS instance.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

isis 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) from an interface, use the **isis authentication-check** 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

Interface configuration

Usage Guidelines

Enter the **isis authentication-check** command before configuring the authentication mode and authentication key chain. Entering the **isis 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 isis 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 check per IS-IS instance by using the **authentication-check** configuration mode command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure IS-IS level-1 packets on a specific interface to use clear text authentication on packets being sent (not received):

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-check level-1
switch(config-if)# isis authentication key-chain site1 level-1
switch(config-if)#
```

Related Commands

Command	Description
authentication-check	Specifies that authentication is performed only on IS-IS packets being sent (not received).
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

isis authentication-type

To specify the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets on a specific interface, use the **isis authentication-type** command. To restore clear text authentication, use the **no** form of this command.

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

no isis 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

Interface 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 authentication type per IS-IS instance by using the **authentication-type** configuration mode command.

This command requires the Enterprise Services license.

Examples

This example configures for the IS-IS instance that Message Digest 5 (MD5) authentication is performed on level-1 packets on a specific interface:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-type md5 level-1
switch(config-router)#
```

Related Commands

Command	Description
authentication-type	Specifies the authentication type per IS-IS instance.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** command. To reset the circuit type to Level l and Level 2, use the **no** form of this command.

isis circuit-type {**level-1** | **level-1-2** | **level-2-only**}

no isis circuit-type

Syntax Description

level-1	Configures a router for Level 1 adjacency only.
level-1-2	Configures a router for Level 1 and Level 2 adjacency.
level-2-only	Configures a router for Level 2 adjacency only.

Command Default A Level 1 and Level 2 adjacency is established.

Command Modes Interface configuration

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines You do not have to configure this command. We recommend that you configure a router as a Level 1-only, Level 1-2, or Level 2-only system. Only on routers that are between areas (Level 1-2 routers) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Note that on point-to-point interfaces, the Level 1 and Level 2 hellos are in the same packet.

A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies will never be established over this interface.

A Level 1 and Level 2 adjacency is established if the neighbor is also configured as level-1-2 and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.

Level 2 adjacencies are established if the other routers are Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies will never be established over this interface.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an adjacency. In this example other routers on the Ethernet interface 2/5 are in the same area. Other routers on Ethernet interface 1 are in other areas, so the router will stop sending Level 1 hellos.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis circuit-type level-2-only
switch(config-if)#
```

isis csnp-interval

To configure the Intermediate System-to-Intermediate System (IS-IS) complete sequence number (CSNPs) interval, use the **isis csnp-interval** command. To restore the default value, use the **no** form of this command.

isis csnp-interval *seconds* {**level-1** | **level-2**}

no isis csnp-interval [**level-1** | **level-2**]

Syntax Description

seconds	Interval of time (in seconds) between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. Range: 0 to 65535. Default: 10.
level-1	Configures the interval of time between transmission of CSNPs for Level 1 independently.
level-2	Configures the interval of time between transmission of CSNPs for Level 2 independently.

Command Default

The default settings are as follows:

- 10 seconds
- Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Normally, you will not have to change the default value of this command.

This command applies only for the designated router or a specified interface. Only designated routers send CSNP packets in order to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2.

The **isis csnp-interval** command on point-to-point subinterfaces should be used only in combination with the IS-IS mesh-group feature.

This command requires the Enterprise Services license.

Examples

This example configures Ethernet interface 2/5 for sending CSNPs every 30 seconds:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis csnp-interval 30 level-1
switch(config-if)#
```

Related Commands

show isis interface	Displays IS-IS information.

isis hello padding

To reenable Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level, use the **isis hello padding** command. To disable IS-IS hello padding, use the **no** form of this command.

isis hello padding

no isis hello padding

Syntax Description This command has no arguments or keywords.

Command Default IS-IS hello padding is enabled.

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode. To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the **no hello padding** command in router configuration mode.

This command requires the Enterprise Services license.

Examples This example shows how to turn off hello padding at the interface level for the Ethernet interface 0/0, and enter interface configuration mode:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# no isis hello padding
switch(config-if)#
```

Related Commands

Command	Description
hello padding	Reenables IS-IS hello padding at the router level.

isis hello-interval

To specify the length of time between hello packets that the Cisco NX-OS software sends, use the **isis hello-interval** command. To restore the default value, use the **no** form of this command.

isis hello-interval *seconds* {**level-1** | **level-2**}

no isis hello-interval {**level-1** | **level-2**}

Syntax Description

seconds	Length of time between hello packets, in seconds. By default, a value three times the hello interval *seconds* is advertised as the hold time in the hello packets sent. (Change the multiplier of 3 by specifying the **isis hello-multiplier** command.) With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. Range: 0 to 65535. Default: 10. **Note** On designated intermediate system (DIS) interfaces, only one third of the configured value is used. The full value of the configured hello intervals is used only by non-DIS interfaces.
level-1	Configures the hello interval for Level 1 independently. Use this on X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multiaccess networks.
level-2	Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

Command Default

The default settings are as follows:

- 10 seconds
- Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The hello interval multiplied by the hello multiplier equals the hold time.

The hello interval can be configured independently for Level 1 and Level 2. The **level-1** and **level-2** keywords are used on LAN interfaces.

A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network. A slower hello interval saves bandwidth and CPU usage. Especially when used in combination with a higher hello multiplier, configuration of the slower hello interval may increase overall network stability. When the hello interval is configured on DIS interfaces, only one third of the interval value is used. Therefore, the hold time (hello interval multiplied by the hello multiplier) for DIS interfaces will also be one third the hold time for non-DIS interfaces.

Tune the hello interval and hello multiplier on point-to-point interfaces instead of LAN interfaces.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the Ethernet interface 2/3 to advertise hello packets every 5 seconds. The router is configured to act as a station router. This configuration will cause more traffic than the traffic generated by configuring a longer interval, but topological changes will be detected earlier.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# isis hello-interval 5 level-1
switch(config-if)#
```

Related Commands

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets that a neighbor must miss before the router should declare the adjacency as down.

isis hello-multiplier

To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **isis hello-multiplier** command. To restore the default value, use the **no** form of this command.

isis hello-multiplier *multiplier* {**level-1** | **level-2**}

no isis hello-multiplier {**level-1** | **level-2**}

Syntax Description

multiplier	Integer value. Range: 3 to 1000. Default: 3.
level-1	Configures the hello multiplier independently for Level 1 adjacencies.
level-2	Configures the hello multiplier independently for Level 2 adjacencies.

Command Default

The default settings are as follows:

- *multiplier*: 3
- Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The holding time carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated. The advertised hold time in IS-IS hello packets will be set to the hello multiplier times the hello interval. Neighbors will declare an adjacency to this router down after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on a per-interface basis, and can be different between different routers in one area.

Using a smaller hello multiplier will give fast convergence, but can result in more routing instability. Increment the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier lower than the default value of 3.

Use the **isis hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval (**isis hello-interval** command) correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

On point-to-point links, there is only one hello for both Level 1 and Level 2, so different hello multipliers should be configured only for multiaccess networks such as Ethernet and FDDI. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM. However, we recommend that you run IS-IS over point-to-point subinterfaces over WAN NBMA media.

This command requires the Enterprise Services license.

Examples

This example shows how to increase network stability by making sure an adjacency will go down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This configuration will ensure that the network remains stable, even when the link is fully congested.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# ip router isis
switch(config-if)# isis hello-interval 6 level-1
switch(config-if)# isis hello-multiplier 10 level-1
```

Related Commands

Command	Description
isis hello-interval	Specifies the length of time between hello packets that the Cisco NX-OS software sends.

isis ipv6 metric

To differentiate between the link costs for Intermediate System-to-Intermediate System (IS-IS) IPv6 traffic, use the **isis ipv6 metric** command. To restore the default, use the **no** form of this command.

isis ipv6 metric *metric-value* {**level-1** | **level-2**}

no isis ipv6 metric *metric-value* {**level-1** | **level-2**}

Syntax Description

metric-value	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range: 1 to 16777215. Default: 10.
level-1	Specifies that this metric should be used only in the SPF calculation for Level 1 (intraarea) routing.
level-2	Specifies that this metric should be used only in the SPF calculation for Level 2 (interarea) routing.

Command Default

The default metric value is set to 10.

The metric is enabled on routing Level 1 and Level 2.

Command Modes

Address-family configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

Specifying the **level-1** or **level-2** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We recommend that you configure metrics on all interfaces. If you do not configure metrics on all interfaces, the IS-IS metrics are similar to hop-count metrics.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an IS-IS IPv6 metric:

```
switch(config)# router isis test1
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# isis ipv6 metric 5 level-1
```

Related Commands

Command	Description
isis metric	Configures the value of an IS-IS metric,

isis lsp-interval

To configure the time delay between successive Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) transmissions, use the **isis lsp-interval** command. To restore the default value, use the **no** form of this command.

isis lsp-interval *milliseconds*

no isis lsp-interval

Syntax Description

milliseconds	Time delay between successive LSPs (in milliseconds). Range: 10 to 65535.

Command Default

The default time delay is 33 milliseconds.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

In topologies with a large number of IS-IS neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows the LSP transmission rate (and the reception rate of other systems) to be reduced.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the system to send LSPs every 100 milliseconds (10 packets per second) on Ethernet interface 0/0:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Configures the time between retransmission of each LSP (IS-IS link-state PDU) over point-to-point links.

isis mesh-group

To optimize link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies, use the **isis mesh-group** command. To remove a subinterface from a mesh group, use the **no** form of this command.

isis mesh-group {*number* | **blocked**}

no isis mesh-group {*number* | **blocked**}

Syntax Description

number	Number identifying the mesh group of which this interface is a member. Range: 1 to 4294967295.
blocked	Specifies that no LSP flooding take place on this subinterface.

Command Default

The interface performs normal flooding.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The LSPs that are first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

The LSPs that are first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If you enter the **blocked** keyword on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally, you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios no router will be logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

This command requires the Enterprise Services license.

Examples

This example shows how to configure six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs received first through Ethernet 1/0.1 are flooded to all interfaces except Ethernet 1/0.2 (which is part of the same mesh group) and Ethernet 1/2.1, which is blocked.
- LSPs received first through Ethernet 1/1.2 are flooded to all interfaces except Ethernet 1/1.1 (which is part of the same mesh group) and Ethernet 1/2.1, which is blocked.
- LSPs received first through Ethernet 1/2.1 are not ignored, but flooded as usual to all interfaces. LSPs received first through Ethernet 1/2.2 are flooded to all interfaces, except Ethernet 1/2.1, which is blocked.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.1
switch(config-if)# isis mesh-group 10

switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.2
switch(config-if)# isis mesh-group 10

switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.1
switch(config-if)# isis mesh-group 11

switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.2
switch(config-if)# isis mesh-group 11

switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.1
switch(config-if)# isis mesh-group blocked

switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.2
switch(config-if)# isis mesh-group 12
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

isis metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) metric, use the **isis metric** command. To restore the default metric value, use the **no** form of this command.

isis metric *metric-value* {**level-1** | **level-2**}

no isis metric *metric-value* {**level-1** | **level-2**}

Syntax Description

metric-value	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range: 1 to 16777215. Default: 10.
level-1	Specifies that this metric should be used only in the SPF calculation for Level 1 (intraarea) routing. If you do not specify an optional keyword, the metric is enabled on routing Level 1 and Level 2.
level-2	Specifies that this metric should be used only in the SPF calculation for Level 2 (interarea) routing. If you do not specify a level, the metric is enabled on routing Level 1 and Level 2.

Command Default

The default metric value is set to 10.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Specifying the **level-1** or **level-2** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We recommend that you configure metrics on all interfaces. If you do not configure metrics on all interfaces, the IS-IS metrics are similar to hop-count metrics.

We recommend that you use the **metric-style wide** command to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv4 information in link-state packets (LSPs) are defined to use only expanded metrics. The Cisco NX-OS software provides support of a 24-bit metric field, the 24-bit metric field is called the *wide metric*. Using the new metric style, link metrics now have a maximum value of 16777215 with a total path metric of 4261412864.

This command requires the Enterprise Services license.

Examples

This example shows how to configure Ethernet interface 3/2 for a link-state metric cost of 15 for Level 1:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis metric 15 level-1
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

isis passive

To suppress adjacency forming on the interface, but still advertise the prefix associated with the interface, use the **isis passive** command. To disable suppression, use the **no** form of this command.

isis passive {**level-1** | **level-1-2** | **level-2-only**}

no isis passive {**level-1** | **level-1-2** | **level-2-only**}

Syntax Description

level-1	Suppresses Level 1 PDU only.
level-1-2	Suppresses Level 1 and Level 2 PDU.
level-2-only	Suppresses Level 2 PDU only.

Defaults

The default settings are as follows:

- This command is disabled by default.
- If enabled, the default is **level-1-2**.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not necessary on a loopback interface. Use the **ip router isis** command in interface configuration mode on a loopback interface to associate that interface with the IS-IS instance.

This command requires the Enterprise Services license.

Examples

This example suppresses adjacency for Ethernet interface 3/2 at Level 1:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis passive level-1
```

isis passive-interface

To block sending of routing updates on an Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis passive-interface** command. To revert to the default settings, use the **no** form of this command.

isis passive-interface {**level-1** | **level-1-2** | **level-2**}

Syntax Description

level-1	Suppresses level-1 PDU.
level-1-2	Suppresses level-1 and level-2 PDU.
level-2	Suppresses level-2 PDU.

Defaults

None

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to block the sending of routing updates on an IS-IS interface:

```
switch# configure terminal
switch(config)# router isis 1
switch(config-router)# passive-interface default level-1
switch(config-router)# exit
switch# configure terminal
switch(config)# interface GigabitEthernet 0/0/0/
switch(config-if# isis passive-interface level-1
switch(config-if#
```

Related Commands

Command	Description
no isis passive-interface	Re-enables sending of routing updates on an IS-IS interface and activates only those interfaces that need adjacencies.

isis priority

To configure the priority of designated routers, use the **isis priority** command in interface configuration mode. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]

no isis priority [**level-1** | **level-2**]

Syntax Description

number-value	Priority of a router and is a number from 0 to 127. The default value is 64.
level-1	(Optional) Sets the priority for Level 1 independently.
level-2	(Optional) Sets the priority for Level 2 independently.

Defaults

Priority of 64
Level 1 and Level 2

Command Modes

Interface configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying the **level-1** or **level-2** keyword resets priority only for Level 1 or Level 2 routing, respectively.

The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.

In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

This command requires the Enterprise Services license.

Examples

This example shows how to set the priority level to 80. So that the router is now more likely to become the DIS:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
```

```
switch(config-if)# isis priority 80 level-1
```