IP Commands

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** command in user EXEC or privileged EXEC mode.

clear ip nhrp[{**vrf** {*vrf-name* | **global**}}] [{*dest-ip-address* [{*dest-mask*}] | **tunnel** *number* | **counters** [{**interface tunnel** *number*}] | **stats** [{**tunnel** *number* [{**vrf** {*vrf-name* | **global**}}]}]}]

Syntax Description

vrf	(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the VRF address family to which the command is applied.
global	(Optional) Specifies the global VRF instance.
dest-ip-address	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.
dest-mask	(Optional) Destination network mask.
counters	(Optional) Clears the NHRP counters.
interface	(Optional) Clears the NHRP mapping entries for all interfaces.
tunnel *number*	(Optional) Removes the specified interface from the NHRP cache.
stats	(Optional) Clears all IPv4 statistic information for all interfaces.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The **clear ip nhrp** command does not clear any static (configured) IP-to-NBMA address mappings from the NHRP cache.

Examples

The following example shows how to clear all dynamic entries from the NHRP cache for an interface:

```
Switch# clear ip nhrp
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

debug nhrp

To enable Next Hop Resolution Protocol (NHRP) debugging, use the **debug nhrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } | **umatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate**}]
no debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } **unmatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate** }]

Syntax Description

attribute	(Optional) Enables NHRP attribute debugging operations.
cache	(Optional) Enables NHRP cache debugging operations.
condition	(Optional) Enables NHRP conditional debugging operations.
interface tunnel *number*	(Optional) Enables debugging operations for the tunnel interface.
nbma	(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.
ipv4-nbma-address	(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.
nbma-name	(Optional) NBMA network name.
IPv6-address	(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. **Note** The *IPv6-address* argument is not supported in Cisco IOS XE Denali 16.3.1.
vrf *vrf-name*	(Optional) Enables debugging operations for the virtual routing and forwarding instance.
detail	(Optional) Displays detailed logs of NHRP debugs.
error	(Optional) Enables NHRP error debugging operations.
extension	(Optional) Enables NHRP extension processing debugging operations.
group	(Optional) Enables NHRP group debugging operations.

packet	(Optional) Enables NHRP activity debugging.
rate	(Optional) Enables NHRP rate limiting.
routing	(Optional) Enables NHRP routing debugging operations.

Command Default

NHRP debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *IPv6-nbma-address* argument although available on the switch, will not work if configured.

Use the **debug nhrp detail** command to view the NHRP attribute logs.

The **Virtual-Access** *number* keyword-argument pair is visible only if the virtual access interface is available on the device.

Examples

The following sample output from the **debug nhrp** command displays NHRP debugging output for IPv4:

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

fhrp delay

To specify the delay period for the initialization of First Hop Redundancy Protocol (FHRP) clients, use the **fhrp delay** command in interface configuration mode. To remove the delay period specified, use the **no** form of this command.

fhrp delay { [**minimum**] [**reload**] *seconds* }
no fhrp delay { [**minimum**] [**reload**] *seconds* }

Syntax Description

minimum	(Optional) Configures the delay period after an interface becomes available.
reload	(Optional) Configures the delay period after the device reloads.
seconds	Delay period in seconds. The range is from 0 to 3600.

Command Default

None

Command Modes

Interface configuration (config-if)

Examples

This example shows how to specify the delay period for the initialization of FHRP clients:

```
Device(config-if)# fhrp delay minimum 90
```

Related Commands

Command	Description
show fhrp	Displays First Hop Redundancy Protocol (FHRP) information.

fhrp version vrrp v3

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) and Virtual Router Redundancy Service (VRRS) configuration on a device, use the **fhrp version vrrp v3** command in global configuration mode. To disable the ability to configure VRRPv3 and VRRS on a device, use the **no** form of this command.

fhrp version vrrp v3
no fhrp version vrrp v3

Syntax Description

This command has no keywords or arguments.

Command Default

VRRPv3 and VRRS configuration on a device is not enabled.

Command Modes

Global configuration (config)

Usage Guidelines

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable.

Examples

In the following example, a tracking process is configured to track the state of an IPv6 object using a VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20:

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

Related Commands

Command	Description
track (VRRP)	Enables an object to be tracked using a VRRPv3 group.

glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

glbp *group-number***authentication** {**text** *string* | **md5** {**key-string** [{**0** | **7**}] *key* | **key-chain** *name-of-chain*}}
no glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [{**0** | **7**}] *key* | **key-chain** *name-of-chain*}}

Syntax Description

group-number	GLBP group number in the range from 0 to 1023.
text *string*	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

Usage Guidelines

The same authentication method must be configured on all the devices that are configured to be members of the same GLBP group, to ensure interoperation. A device will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

Examples

The following example configures stringxyz as the authentication string required to allow GLBP devices in group 10 to interoperate:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain “AuthenticateGLBP” to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp forwarder preempt

To configure a device to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]
no glbp *group* **forwarder preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the device will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was introduced..

Examples

The following example shows a device being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the device preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ip

To activate the Gateway Load Balancing Protocol (GLBP), use the **glbp ip** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

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

Syntax Description

group	GLBP group number in the range from 0 to 1023.
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.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was introduced.

Usage Guidelines

The **glbp ip** command activates GLBP on the configured interface. If an IP address is specified, that address is used as the designated virtual IP address for the GLBP group. If no IP address is specified, the designated address is learned from another device configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one device on the cable must have been configured with the designated address. A device must be configured with, or have learned, the virtual IP address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ip** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP 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.

Examples

The following example activates GLBP for group 10 on GigabitEthernet interface 1/0/1. The virtual IP address to be used by the GLBP group is set to 10.21.8.10.

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

glbp *group* **load-balancing** [{**host-dependent** | **round-robin** | **weighted**}]
no glbp *group* **load-balancing**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
host-dependent	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
round-robin	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default

The round-robin method is the default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was introduced..

Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same device. Use the weighted method of GLBP load balancing when you need unequal load balancing because devices in the GLBP group have different forwarding capacities.

Examples

The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip 10.21.8.10
Device(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

glbp *group-number* **name** *group-name*
no glbp *group-number* **name** *group-name*

Syntax Description

group-number	GLBP group number. Range is from 0 to 1023.
group-name	GLBP group name specified as a character string. Maximum number of characters is 255.

Command Default

IP redundancy for a group is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines

The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

Examples

The following example assigns the abccomp name to GLBP group 10:

```
Device(config-if)# glbp 10 name abccomp
```

Related Commands

Command	Description
glbp authentication	Configures an authentication string for the GLBP.
glbp forwarder preempt	Configures a device to take over as AVF for a GLBP group if it has higher priority than the current AVF.
glbp ip	Activates GLBP.
glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.
glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
glbp priority	Sets the priority level of the gateway within a GLBP group.

Command	Description
glbp timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **preempt** [**delay minimum** *seconds*]
no glbp *group* **preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the device will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

A GLBP device with a higher priority than the current AVG cannot assume the role of AVG. The default delay value is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Examples

The following example shows a device being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the device preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the device within a GLBP group.

glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

glbp *group* **priority** *level*
no glbp *group* **priority** *level*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
level	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Command Default

The GLBP virtual gateway preemptive scheme is disabled

Command Modes

Interface configuration (config-if)

Usage Guidelines

Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

Examples

The following example shows a virtual gateway being configured with a priority of 254:

```
Device(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp preempt	Configures a device to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

glbp *group* **timers** {*hellotime* {*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}
no glbp *group* **timers** {*hellotime* {*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}

Syntax Description

group	GLBP group number in the range from 0 to 1023.
msec	(Optional) Specifies that the following (*hellotime* or *holdtime)* argument value will be expressed in milliseconds rather than seconds.
hellotime	Hello interval. The default is 3 seconds (3000 milliseconds).
holdtime	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).
redirect	Specifies time interval during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF) and time-out values for failed forwarders.
time-interval-to-redirect	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). **Note** The zero value for the *time-interval-to-redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and*time-interval-to-redirect*, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a device fails, new hosts continue to be assigned to the failed device instead of being redirected to the backup.
timeout	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

GLBP timers are set to their default values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

Devices on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All devices in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, (*holdtime* > 3 * *hellotime*). The range of values for holdtime force the holdtime to be greater than the hello time.

Examples

The following example shows the GLBP group 10 on GigabitEthernet interface 1/0/1 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip
Device(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no**form of this command.

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
no glbp *group* **weighting**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
maximum	Maximum weighting value in the range from 1 to 254. Default value is 100.
lower *lower*	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper *upper*	(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Command Default

The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the device fails, the weighting value of the device may fall from the maximum value to below the lower threshold, causing the device to give up its role as a virtual forwarder. When the weighting value of the device rises above the upper threshold, the device can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a device goes down, the weighting for the device can be reduced by a specified value.

Examples

The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

Related Commands

Command	Description
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	Configures an interface to be tracked.

glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

glbp *group* **weighting track** *object-number* [**decrement** *value*]
no glbp *group* **weighting track** *object-number* [**decrement** *value*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
object-number	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the **track** command to configure the tracked object.
decrement *value*	(Optional) Specifies an amount by which the GLBP weighting for the device is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

Command Default

Objects are not tracked for GLBP weighting changes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines

This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, GigabitEthernet interface 1/0/1 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp** command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the device. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Usage Guidelines

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the device.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type* is the Ethernet interface where the command is configured and *interface-type number* is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

If a Cisco device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the device. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the device.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 1: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the device in the option 12 field.
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the device in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a device configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

The DISCOVER message sent by a device configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a Dynamic Host Configuration Protocol (DHCP) pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

ip address pool *name*
no ip address pool

Syntax Description

name	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in *name*.

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

Usage Guidelines

Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the device. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.

Examples

The following example specifies that the IP address of GigabitEthernet interface 1/0/1 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
interface GigabitEthernet 1/0/1
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

ip http server
no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server uses the standard port 80 by default.

HTTP/TCP port 8090 is open by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.

ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

ip http secure-server
no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.

Caution When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip nhrp map

To statically configure the IP-to-nonbroadcast multiaccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** command in interface configuration mode. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ip nhrp map *ip-address* {*ip-nbma-address* | *destination-mask* [{*ip-nbma-address ipv6-nbma-address*}] *ipv6-nbma-address*}
no ip nhrp map *ip-address* {*ip-nbma-address* | *destination-mask* [{*ip-nbma-address ipv6-nbma-address*}] *ipv6-nbma-address*}

Syntax Description

ip-address	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
ip-nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium; for example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.
destination-mask	Destination address mask.
ipv6-nbma-address	IPv6 NBMA address. **Note** This argument is not supported in Cisco IOS XE Denali 16.3.1.

Command Default

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration(config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

In Cisco IOS XE Denali 16.3.1, NHRP supports only hub-to-spoke communication; spoke-to-spoke communication is not supported.

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

Configure at least one static mapping to reach the next-hop server. To statistically configure multiple IP-to-NBMA address mappings, configure this command multiple times.

When using the routing protocols, Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), configure the **ip ospf network point-to-multipoint** (when OSPF is used for hub-to-spoke communication) and **ip split-horizon eigrp** (when EIGRP is used) commands on the tunnel to allow the traffic.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured as 192.0.2.1 and the NBMA address for 10.0.1.3 is 198.51.100.1.

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip nhrp nhs 10.0.0.1
Switch(config-if)# ip nhrp nhs 10.0.1.3
Switch(config-if)# ip nhrp map 10.0.0.1 192.0.2.1
Switch(config-if)# ip nhrp map 10.0.1.3 198.51.100.1
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
ip split-horizon eigrp	Enables EIGRP split horizon.
ip ospf network point-to-multipoint	Configures the OSPF network type to point-to-multipoint.

ip nhrp map multicast

To configure nonbroadcast multiaccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast**command in interface configuration mode. To remove the destinations, use the **no** form of this command.

ip nhrp map multicast {*ip-nbma-address ipv6-nbma-address* | **dynamic**}
no ip nhrp map multicast {*ip-nbma-address ipv6-nbma-address* | **dynamic**}

Syntax Description

ip-nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium that you are using.

ipv6-nbma-address	IPv6 NBMA address. **Note** This argument is not supported in Cisco IOS XE Denali 16.3.1.
dynamic	Dynamically learns destinations from client registrations on the hub.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

This command applies only to tunnel interfaces. This command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2:

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

Command	Description
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
tunnel destination	Specifies the destination for a tunnel interface.

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

ip nhrp network-id *number*
no ip nhrp network-id [{*number*}]

Syntax Description

number	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.

Command Default

NHRP is disabled on an interface.

Command Modes

Interface configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example enables NHRP on the interface:

```
Switch(config-if)# ip nhrp network-id 1
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

Syntax Description

nhs-address	Address of the next-hop server being specified.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies the use of NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10.
max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Command Default

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating the **ip nhrp nhs** command with the same *nhs-address* argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

ipv6 address-validate

To enable IPv6 address validation, use the **ipv6 address-validate** in global configuration mode. To disable IPv6 address validation, use the **no** form of this command.

ipv6 address-validate
no ipv6 address-validate

Command Default

This command is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The **ipv6 address-validate** command is used to validate whether the interface identifiers in an assigned IPv6 address are a part of the reserved IPv6 interface identifiers range, as specified in RFC5453. If the interface identifiers of the assigned IPv6 address are a part of the reserved range, a new IPv6 address is assigned.

Only auto-configured addresses or addresses configured by DHCPv6 are validated.

Note The **no ipv6-address validate** command disables the IPv6 address validation and allows assigning of IPv6 addresses with interface identifiers that are a part of the reserved IPv6 interface identifiers range. We do not recommend the use of this command.

Examples

The following example shows how to re-enable IPv6 address validation if it is disabled using the no ipv6-address validate command:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 address-validate
```

ipv6 nd cache expire

To configure the duration of time before an IPv6 neighbor discovery cache entry expires, use the **ipv6 nd cache expire** command in the interface configuration mode. To remove this configuration, use the **no** form of this command.

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

Syntax Description

Syntax Description

expire-time-in-seconds	The time range is from 1 through 65536 seconds. The default is 14400 seconds or 4 hours.
refresh	(Optional) Automatically refreshes the neighbor discovery cache entry.

Command Modes

Interface configuration (config-if)

Command History

Command History

Release	Modificat
Cisco IOS XE 3.3SE	This com introduce

Usage Guidelines

By default, a neighbor discovery cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds or 4 hours. The **ipv6 nd cache expire** command allows the expiry time to vary and to trigger auto refresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, a neighbor discovery cache entry is auto refreshed. The entry moves into the DELAY state and the neighbor unreachability detection process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation is sent and then retransmitted as per the configuration.

Examples

The following example shows that the neighbor discovery cache entry is configured to expire in 7200 seconds or 2 hours:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

Related Commands

Command	Description
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd na glean

To configure the neighbor discovery to glean an entry from an unsolicited neighbor advertisement, use the **ipv6 nd na glean** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Command Modes

Interface configuration

Command History

Release
Cisco IOS XE 3.3SE

Usage Guidelines

IPv6 nodes may emit a multicast unsolicited neighbor advertisement packet following the successful completion of duplicate address detection (DAD). By default, other IPv6 nodes ignore these unsolicited neighbor advertisement packets. The **ipv6 nd na glean** command configures the router to create a neighbor advertisement entry on receipt of an unsolicited neighbor advertisement packet (assuming no such entry already exists and the neighbor advertisement has the link-layer address option). Use of this command allows a device to populate its neighbor advertisement cache with an entry for a neighbor before data traffic exchange with the neighbor.

Examples

The following example shows how to configure neighbor discovery to glean an entry from an unsolicited neighbor advertisement:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery cache entry expires.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd nud retry

To configure the number of times the neighbor unreachability detection process resends neighbor solicitations, use the **ipv6 nd nud retry** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}
no ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}

Syntax Description

base	The neighbor unreachability detection process base value.
interval	The time interval, in milliseconds, between retries. The range is from 1000 to 32000.
max-attempts	The maximum number of retry attempts, depending on the base value. The range is from 1 to 128.
final-wait-time	The waiting time, in milliseconds, on the last probe. The range is from 1000 to 32000.

Command Modes

Interface configuration (config-if)

Command History

Release
Cisco IOS XE 3.3SE

Usage Guidelines

When a device runs neighbor unreachability detection to resolve the neighbor detection entry for a neighbor again, it sends three neighbor solicitation packets 1 second apart. In certain situations, for example, spanning-tree events, or high-traffic events, or end-host reloads), three neighbor solicitation packets that are sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for neighbor solicitation retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm^n

here,

- t = Time interval
- m = Base (1, 2, or 3)
- n = Current neighbor solicitation number (where the first neighbor solicitation is 0).

Therefore, **ipv6 nd nud retry 3 1000 5** command retransmits at intervals of 1,3,9,27,81 seconds. If the final wait time is not configured, the entry remains for 243 seconds before it is deleted.

The **ipv6 nd nud retry** command affects only the retransmit rate for the neighbor unreachability detection process, and not for the initial resolution, which uses the default of three neighbor solicitation packets sent 1 second apart.

Examples

The following example shows how to configure a fixed interval of 1 second and three retransmits:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example shows how to configure a retransmit interval of 1, 2, 4, and 8:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example shows how to configure the retransmit intervals of 1, 3, 9, 27, 81:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

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

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.

Command Default

No key chain exists.

Command Modes

Global configuration (config)

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example shows how to specify key chain:

```
Device(config-keychain-key)# key-string chestnut
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string key-string *text*
no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Examples

The following example shows how to specify the authentication string for a key:

```
Device(config-keychain-key)# key-string key1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

key-id	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Usage Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example shows how to specify a key to identify authentication on a key-chain:

```
Device(config-keychain)# key 1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

capability [*interface-type interface-number*]
interface-type interface-number [*group-number*] [*state*] [**brief**]

Syntax Description

capability	(Optional) Displays the GLBP capability interfaces.
interface-type interface-number	(Optional) Interface type and number for which output is displayed.
group-number	(Optional) GLBP group number in the range from 0 to 1023.
state	(Optional) State of the GLBP device, one of the following: **active**, **disabled**, **init**, **listen**, and **standby**.
brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines

Use the **show glbp** command to display information about GLBP groups on a device. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder. The **capability** keyword displays all GLBP-capable interfaces.

Examples

The following is sample output from the **show glbp** command that displays GLBP group 10:

```
Device# show glbp GigabitEthernet 1/0/1 10
```

```
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
  Virtual IP address is 10.21.8.10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.608 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is unknown
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ac7e.8a35.6364 (10.21.8.32) local
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:04:41
    MAC address is 0007.b400.0a01 (default)
    Owner ID is ac7e.8a35.6364
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

The table below describes the significant fields shown in the displays.

Table 2: show glbp Field Descriptions

Field	Description
GigabitEthernet1/0/1 - Group	Interface type and number and GLBP group number for the interface.
State is	State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following: • Active--The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled--The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial--The virtual IP address has been configured or learned, but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen--The virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable. • Speak--The virtual gateway is attempting to become the active or standby virtual gateway. • Standby--The gateway is next in line to be the AVG.

Field	Description
Virtual IP address is	The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the device has failed to defend its ARP cache entry.
Hello time, hold time	The hello time is the time between hello packets (in seconds or milliseconds). The hold time is the time (in seconds or milliseconds) before other devices declare the active device to be down. All devices in a GLBP group use the hello- and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello- and hold-time values.
Next hello sent in	The time until GLBP will send the next hello packet (in seconds or milliseconds).
Preemption	Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) for which a higher-priority nonactive device will wait before preempting the lower-priority active device. This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.
Active is	The active state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the current AVG. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
Standby is	The standby state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	The initial weighting value with lower and upper threshold values.
Track object	The list of objects that are being tracked and their corresponding states.
IP redundancy name is	The name of the GLBP group.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other devices declare the active GLBP device to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs**command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [{*interface*}] [**detail**] [{**redundancy** [{**cluster** *number* | **preempted** | **running** | **waiting**}]}]

Syntax Description

interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays information about NHS redundancy stacks.
cluster *number*	(Optional) Displays redundancy cluster information.
preempted	(Optional) Displays information about NHS that failed to become active and is preempted.
running	(Optional) Displays NHSs that are currently in Responding or Expecting replies states.
waiting	(Optional) Displays NHSs awaiting to be scheduled.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 3: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
ANI	0 to 1000	Autonomic-Networking virtual interface
Auto-Template	1 to 999	Auto-Template interface
GMPLS	0 to 1000	Multiprotocol Label Switching (MPLS) interface
GigabitEthernet	0 to 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 to 9	Internal interface

Valid Types	Number Ranges	Interface Descriptions
LISP	0 to 65520	Locator/ID Separation Protocol (LISP) virtual interface
loopback	0 to 2147483647	Loopback interface
Null	0 to 0	Null interface
PROTECTION_GROUP	0 to 0	Protection-group controller
Port-channel	1 to 128	Port channel interface
TenGigabitEthernet	0 to 9	TenGigabitEthernet interface
Tunnel	0 to 2147483647	Tunnel interface
Tunnel-tp	0 to 65535	MPLS Transport Profile interface
Vlan	1 to 4094	VLAN interface

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
   10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

The table below describes the significant field shown in the display.

Table 4: show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

show key chain

To display the keychain, use the **show key chain** command.

show key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the key chain command.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

Privileged EXEC (#)

Examples

The following is sample output from the **show key chain** command:

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

Related Commands

Command	Description
key-string	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [{*object-number* **[brief]** | **application [brief]** | **interface [brief]** | **ip[route [brief]** | **[sla [brief]]** | **ipv6 [route [brief]]** | **list [route [brief]]** | **resolution [ip** | **ipv6]** | **stub-object [brief]** | **summary** | **timers**}]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
application	(Optional) Displays tracked application objects.

interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP route objects.
ip sla	(Optional) Displays tracked IP SLA objects.
ipv6 route	(Optional) Displays tracked IPv6 route objects.
list	(Optional) Displays the list of boolean objects.
resolution	(Optional) Displays resolution of tracked parameters.
summary	(Optional) Displays the summary of the specified object.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was integrated into Cisco IOS XE Release 2.1.
	This command was introduced.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Device# show track 1

Track 1
 Interface GigabitEthernet 1/0/1 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

The table below describes the significant fields shown in the displays.

Table 5: show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface GigabitEthernet 1/0/1 ip routing	Interface type, interface number, and object that is being tracked.

Field	Description
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.

Related Commands

Command	Description
show track resolution	Displays the resolution of tracked parameters.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

track

To configure an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface, use the **track** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}
no track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}

Syntax Description

object-number	Object number in the range from 1 to 1000 representing the interface to be tracked.
interface *type number*	Interface type and number to be tracked.
line-protocol	Tracks whether the interface is up.
ip routing	Tracks whether IP routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.
ipv6 routing	Tracks whether IPv6 routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.

Command Default

The state of the interfaces is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
	This command was introduced..

Usage Guidelines

Use the **track** command in conjunction with the **glbp weighting** and **glbp weighting track** commands to configure parameters for an interface to be tracked. If a tracked interface on a GLBP device goes down, the

weighting for that device is reduced. If the weighting falls below a specified minimum, the device will lose its ability to act as an active GLBP virtual forwarder.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, TenGigabitEthernet interface 0/0/1 tracks whether GigabitEthernet interfaces 1/0/1 and 1/0/3 are up. If either of the GigabitEthernet interface goes down, the GLBP weighting is reduced by the default value of 10. If both GigabitEthernet interfaces go down, the GLBP weighting will fall below the lower threshold and the device will no longer be an active forwarder. To resume its role as an active forwarder, the device must have both tracked interfaces back up, and the weighting must rise above the upper threshold.

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

vrrp

To create a Virtual Router Redundancy Protocol version 3 (VRRPv3) group and enter VRRPv3 group configuration mode, use the **vrrp**. To remove the VRRPv3 group, use the **no** form of this command.

vrrp *group-id* **address-family** {**ipv4** | **ipv6**}
no vrrp *group-id* **address-family** {**ipv4** | **ipv6**}

Syntax Description

group-id	Virtual router group number. The range is from 1 to 255.
address-family	Specifies the address-family for this VRRP group.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

Command Default

None

Command Modes Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced..

Usage Guidelines

Examples

The following example shows how to create a VRRPv3 group and enter VRRP configuration mode:

```
Device(config-if)# vrrp 3 address-family ipv4
```

Related Commands

Command	Description
timers advertise	Sets the advertisement timer in milliseconds.

vrrp description

To assign a description to the Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *text*
no description

Syntax Description

text	Text (up to 80 characters) that describes the purpose or use of the group.

Command Default There is no description of the VRRP group.

Command Modes VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was introduced.

Examples

The following example enables VRRP. VRRP group 1 is described as Building A – Marketing and Administration.

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

vrrp preempt

To configure the device to take over as the current primary virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current primary virtual router, use the **preempt** command in VRRP configuration mode. To disable this function, use the **no** form of this command.

preempt [**delay minimum** *seconds*]
no preempt

Syntax Description

delay minimum *seconds*	(Optional) Number of seconds that the device will delay before issuing an advertisement claiming primary ownership. The default delay is 0 seconds.

Command Default

This command is enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

By default, the device being configured with this command will take over as primary virtual router for the group if it has a higher priority than the current primary virtual router. You can configure a delay, which will cause the VRRP device to wait the specified number of seconds before issuing an advertisement claiming primary ownership.

Note The device that is the IP address owner will preempt, regardless of the setting of this command.

Examples

The following example configures the device to preempt the current primary virtual router when its priority of 200 is higher than that of the current primary virtual router. If the device preempts the current primary virtual router, it waits 15 seconds before issuing an advertisement claiming it is the primary virtual router.

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
priority	Sets the priority level of the device within a VRRP group.

vrrp priority

To set the priority level of the device within a Virtual Router Redundancy Protocol (VRRP) group, use the **priority** command in interface configuration mode. To remove the priority level of the device, use the **no** form of this command.

priority *level*
no priority *level*

Syntax Description

level	Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.

Command Default

The priority level is set to the default value of 100.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

Use this command to control which device becomes the primary virtual router.

Examples

The following example configures the device with a priority of 254:

```
Device(config-if-vrrp)# priority 254
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
vrrp preempt	Configures the device to take over as primary virtual router for a VRRP group if it has higher priority than the current primary virtual router.

vrrp timers advertise

To configure the interval between successive advertisements by the primary virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the **timers advertise** command in VRRP configuration mode. To restore the default value, use the **no** form of this command.

timers advertise [**msec**] *interval*
no timers advertise [**msec**] *interval*

Syntax Description

group	Virtual router group number. The group number range is from 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.

interval	Time interval between successive advertisements by the primary virtual router. The unit of the interval is in seconds, unless the **msec** keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the **msec** keyword is specified, the valid range is 50 to 999 milliseconds.

Command Default

The default interval of 1 second is configured.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 16.2.1	This command was introduced.

Usage Guidelines

The advertisements being sent by the primary virtual router communicate the state and priority of the current primary virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the primary router to be down. Routers or access servers on which timer values are not configured can learn timer values from the primary router. The timers configured on the primary router always override any other timer settings. All routers in a VRRP group must use the same timer values. If the same timer values are not set, the devices in the VRRP group will not communicate with each other and any misconfigured device will change its state to primary.

Examples

The following example shows how to configure the primary virtual router to send advertisements every 4 seconds:

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
timers learn	Configures the device, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the primary virtual router.

vrrs leader

To specify a leader's name to be registered with Virtual Router Redundancy Service (VRRS), use the **vrrs leader** command. To remove the specified VRRS leader, use the **no** form of this command.

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description

vrrs-leader-name	Name of VRRS Tag to lead.

Command Default

A registered VRRS name is unavailable by default.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
	This command was introduced.

Examples

The following example specifies a leader's name to be registered with VRRS:

```
Device(config-if-vrrp)# vrrs leader leader-1
```

Related Commands

Command	Description
vrrp	Creates a VRRP group and enters VRRP configuration mode.