T Commands

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

table-map (EIGRP)

To configure a table map with the route map information, use the **table-map** command.

table-map *route-map-name* [**filter**]

Syntax Description		
	route-map-name	Route map name. This string can be a maximum of 63 alphanumeric characters.
	filter	(Optional) Filters routes rejected by the route map and does not download them to the RIB.

Defaults None

Command Modes config-router mode

Supported User Roles network-admin
vdc-admin

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

Usage Guidelines This command requires the Enterprise Services license.

Examples This example shows how to configure a table map with route map information:

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# table-map route-map1 filter
switch(config-router)#
```

Related Commands	Command	Description
	router ospf	Creates a new OSPFv2 instance with the configured instance tag.

table-map (OSPF)

To configure the policy for filtering and modifying the Open Shortest Path First (OSPF) routes before sending them to the Routing Information Base (RIB), use the **table-map** command. To disable this function, use the **no** form of this command.

table-map map-name **[filter]**

no table-map *map-name* **[filter]**

Syntax Description

map-name	Name of table map. The range is 1 to 63 alphanumeric characters. For OSPFv2 and OSPFv3, the *map-name* argument specifies the name of a route map to be used for filtering.
filter	(Optional) Filters routes based on the configuration of the specified route map. A next-hop path is not downloaded to the RIB if it is denied in the route-map configuration.

Defaults

OSPF filters all next-hops from being downloaded in the RIB or deletes all the next-hop paths for a route if a given route is present in RIB.

Command Modes

Router configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(6a)	This command was modified. Support for filtering next-hop paths for an OSPF route was added.
6.2(2)	This command was modified. The **filter** keyword was added.
6.1(1)	This command was introduced.

Usage Guidelines

A table map controls whether routes are downloaded to the RIB. Use this command with the **filter** keyword to filter next-hop paths for an OSPF route based on the configuration in a route map. The route is not downloaded to the RIB if it is denied by the specified route map.

In Cisco NX-OS Release 6.2(6a) and later releases, you can filter next-hop paths for an OSPF route to prevent the path from being added to the RIB. Before Cisco NX-OS Release 6.2(6a), filtering on a specific path is ignored and the entire route is filtered from being added to the RIB.

Before using this command with the **filter** keyword, you must use the **route-map** command in global configuration mode to configure the route map that is to be specified in the **table-map** command.

Unlike a route map, a table map is not followed by **match** or **set** commands.

This command does not require a license.

Examples

The following example shows a route-map configuration for blocking the next hops that are learned through Vlan10:

```
route-map Filter-OSPF deny 10
    match interface Vlan10
route-map Filter-OSPF permit 20
```

The following example show how to configure the **table-map** command with the **filter** keyword to use the preceding route-map configuration (Filter-OSPF) to remove the next-hop path that is learned through VLAN 10 and not the next-hop path that is learned through VLAN 20:

```
switch(config)# router ospf p1
switch(config-router)# table-map Filter-OSPF filter
```

The following example shows how to configure the policy for filtering and modifying OSPF routes before sending them to the RIB:

```
switch(config)# router ospf p1
switch(config-router)# table-map tmap
switch(config-router)#
```

Related Commands

Command	Description
route-map	Enters route-map configuration mode for configuring a route map.
show forwarding distribution	Displays information about the FIB.

table-map (OSPFv3)

To configure the policy for filtering and modifying the Open Shortest Path First (OSPF) routes before sending them to the Routing Information Base (RIB), use the **table-map** command.To disable this function, use the **no** form of this command.

table-map *table-map-name*

no table-map *table-map-name*

Syntax Description

table-map-name	Table-map name. The maximum size is 40 characters.

Defaults

None

Command Modes

OSPFv3 router configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

In OSPFv3, you can add a table map in the address-family ipv6 unicast mode only.

Examples

This example shows how to configure a policy for filtering and modifying OSPF routes before sending them to the RIB:

```
switch(config)# router ospfv3 3
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# table-map tmap
```

Related Commands

Command	Description
show forwarding distribution	Displays information about the FIB.

template (BGP)

To create a peer template and enter a peer template configuration mode, use the **template** command. To remove a peer template, use the **no** form of this command.

template {**peer** *name* | **peer-policy** *name* | **peer-session** *name*}

no template {**peer** *name* | **peer-policy** *name* | **peer-session** *name*}

Syntax Description

peer *name*	Specifies the name of the neighbor template.
peer-policy *name*	Specifies the name of the peer-policy template.
peer-session *name*	Specifies the name of the peer-session template.

Defaults

None.

Command Modes

Neighbor address-family configuration
Router bgp configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **template** command allows you to enable a set of predefined attributes that a neighbor inherits.

Note A Border Gateway Protocol neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong to a peer group or to inherit policies from peer templates only.

Peer-Templates

Peer templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or Network Layer Reachability Information configuration modes are configured with peer templates.

The peer template combines the peer-session and peer-policy templates to form a basic neighbor definition. It is not mandatory to use a neighbor template but you can use it to simplify the BGP configuration.

Peer-Policy Templates

Peer-policy templates are used to group and apply the configuration of commands that are applied within specific address families and the NLRI configuration mode. Peer-policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address families or NLRI configuration modes are configured in a peer-policy template. When you enter the peer-policy template configuration mode, the following commands are available:

- **suppress-inactive**—Advertises the active routes to the peer only. See the **suppress-inactive** command for additional information.
- **exit**—Exits current configuration mode.
- **filter-list** *name* {**in** | **out**}—Creates the AS-PATH filter list on the inbound and the outbound BGP routes. To remove the entry, use the **no** form of this command.
  - **in**—Applies the access list to incoming routes.
  - **out**—Applies the access list to outgoing routes.
- **inherit peer-policy** *policy-name seq-num*—Configures a peer-policy template to inherit the configuration from another peer-policy template. To remove an inherited statement from a peer-policy template, use the **no** form of this command. Range: 1 to 65535. Default: No inherit statements are configured.

  The sequence number specifies the order in which the peer policy template is evaluated. Like a route-map sequence number, the lowest sequence number is evaluated first. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. When multiple peer-policies are configured under a template, only the policy with the lowest sequence number is executed. If a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.

Note A BGP routing process cannot be configured to be a member of a peer group and to use peer templates for group configurations. You must use one method or the other. We recommend peer templates because they provide improved performance and scalability.

- **maximum-prefix** *max*—Specifies the maximum number of prefixes from this neighbor. Range: 1 to 300000. Default: This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. See the **maximum-prefix** command for additional information.
- **next-hop-self**—Configures the router as the next hop for a BGP neighbor or peer group. To disable this feature, use the **no** form of this command. Default: Disabled.
- **next-hop-third-party**—Computes a third-party next hop if possible.
- **no**—Negates a command or sets its defaults.
- **prefix-list** *name* {**in** | **out**}—Specifies the route type to apply the prefix list. To remove the entry, use the **no** form of this command.
  - **in**—Applies the prefix list to incoming routes.
  - **out**—Applies the prefix list to outgoing routes.
- **route-map** *name* {**in** | **out**}—Specifies the route map name to apply the route type to the neighbor.
  - **in**—Applies the route map to incoming routes.
  - **out**—Applies the route map to outgoing routes.

- **route-reflector-client**—Configures the router as a BGP route reflector and configures the specified neighbor as its client. To indicate that the neighbor is not a client, use the **no** form of this command. Default: There is no route reflector in the autonomous system.

  By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, which prevents a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

  If you use route reflectors, all iBGP speakers do not need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

  All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

- **send-community**—Specifies that a community attribute be sent to a BGP neighbor. To remove the entry, use the **no** form of this command.

- **soft-reconfiguration**—Configures the Cisco NX-OS software to start storing updates. To not store received updates, use the **no** form of this command. Default: Disabled. Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

  To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Clearing the BGP session using the **soft-reconfiguration** command has a negative effect on network operations and should only be used as a last resort.

  To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

  ```
  Received route refresh capability from peer.
  ```

  If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

Similar to peer-session templates, peer-policy templates are configured once and applied to many neighbors through the direct application of a peer-policy template or through inheritance from peer-policy templates. The configuration of peer-policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Peer-policy templates support direct and indirect inheritance from up to eight peer-policy templates. Inherited peer-policy templates are configured with sequence numbers like route maps. An inherited peer-policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number and ending with the highest sequence number. However, there is a difference; a peer-policy template will not fall through like a route map. Every sequence is evaluated, and if a BGP policy command is reapplied with different value, it will overwrite any previous value from a lower sequence number.

Peer-policy templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer-policy templates.

Note A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from only peer templates.

Peer-Session Templates

Peer-session templates are used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer-session template. Peer-session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer-session template.

When you enter the peer-session template configuration mode, the following commands are available:

- **description** *description*—Configures a description to be displayed by the local or a peer router. You can enter up to 80 characters including spaces.
- **disable-connected-check**—Disables connection verification for eBGP peers no more than one hop away when the eBGP peer is configured with a loopback interface.
- **ebgp-multihop**—Accepts and attempts BGP connections to external peers that reside on networks that are not directly connected.

Note You should enter this command under the guidance of Cisco technical support staff only.

- **exit**—Exits current configuration mode.
- **inherit peer-session** *session-name*—Configures a peer-session template to inherit the configuration from another peer-session template. To remove an inherit statement from a peer-session template, use the **no** form of this command.
- **local-as**—Allows you to customize the autonomous system number for eBGP peer groupings.
- **neighbor inherit peer-session**—Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
- **neighbor translate-update**—Upgrades a router running BGP in the NLRI format to support multiprotocol BGP.
- **password**—Enables MD5 authentication on a TCP connection between two BGP peers. The following configuration tools are available:
  - **0** *password*—Specifies an unencrypted neighbor password.
  - **3** *password*—Specifies a 3DES encrypted neighbor password
  - *password*—Specifies an unencrypted (cleartext) neighbor password
- **remote-private-as**—Removes the private AS number from outbound updates.
- **show ip bgp template peer-policy**—Displays the locally configured peer policy templates.
- **show ip bgp template peer-session**—Displays the locally configured peer session templates.
- **shutdown**—Disables a neighbor or peer group.
- **timers** *keepalive-time*—Configures keepalive and hold timers in seconds. Range: 0 to 3600. Default: 60.
- **update-source** {**ethernet** *mod/port* | **loopback** *virtual-interface* | **port-channel** *number*[**.***sub-interface*]}—Specifies the source of the BGP session and updates. Range: *virtual-interface* is 0 to 1023; *number* is 0 to 4096; (optional); *.sub-interface* is 1 to 4093.

General session commands can be configured once in a peer-session template and then applied to many neighbors through the direct application of a peer-session template or through indirect inheritance from a peer-session template. The configuration of peer-session templates simplify the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

Peer-session templates support direct and indirect inheritance. A peer can be configured with only one peer-session template at a time, and that peer-session template can contain only one indirectly inherited peer-session template. However, each inherited session template can also contain one indirectly inherited peer-session template. So, only one directly applied peer-session template and up to seven additional indirectly inherited peer-session templates can be applied, allowing you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer-session template and the configurations from up to seven indirectly inherited peer-session templates. Inherited peer-session templates are evaluated first, and the directly applied template will be evaluated and applied last. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template.

Peer-session templates support only general session commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer-policy templates.

This command requires the Enterprise Services license.

Examples

This example shows how to create a peer-session template named CORE1. This example inherits the configuration of the peer-session template named INTERNAL-BGP.

```
switch(config-router)# template peer-session CORE1
switch(config-router-stmp)#
```

This example shows how to create and configure a peer-policy template named CUSTOMER-A:

```
switch(config-router)# template peer-policy CUSTOMER-A
switch(config-router-ptmp)# exit
switch(config-router)# route-map SET-COMMUNITY in
switch(config-router)# filter-list 20 in
switch(config-router)# inherit peer-policy PRIMARY-IN 20
switch(config-router)# inherit peer-policy GLOBAL 10
switch(config-router)# exit-peer-policy
switch(config-router)#
```

This example shows how to configure that the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 1000
```

This example shows how to configure that the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 5000 50
```

This example shows how to configure that the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

This example shows how to configure that the warning messages is displayed when the maximum-prefix limit (500) for the 192.168.4.4 neighbor is exceeded:

```
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 500 warning-only
```

This example shows how to force all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
switch(config)# router bgp 64496
switch(config-router)# next-hop-self
```

This router configuration mode example shows how to configure the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
switch(config)# router bgp 64496
switch(config-router)# send-community
```

The address family configuration mode example shows how to configure that the router belongs to autonomous system 109 send the communities attribute to its neighbor at IP address 172.16.70.23:

```
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# send-community
```

This example shows how to enable inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information is used to generate a new set of inbound updates.

```
switch(config)# router bgp 64496
switch(config-router)# soft-reconfiguration inbound
```

Related Commands

Command	Description
router bgp	Assigns an autonomous system (AS) number to a router and enters the router BGP configuration mode
address-family	Enters the address family mode for the Border Gateway Protocol (BGP).

test forwarding distribution perf

To test the forwarding distribution performance of the Forwarding Information Base (FIB), use the **test forwarding distribution perf** command.

test forwarding distribution perf

Syntax Description This command has no keywords or arguments.

Defaults None

Command Modes Any command mode

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to test the forwarding distribution performance:

```
switch# test forwarding distribution perf
```

Related Commands

Command	Description
show forwarding distribution	Displays information about the FIB.

test forwarding inconsistency

To trigger the Layer 3 inconsistency checker for the Forwarding Information Base (FIB), use the **test forwarding inconsistency** command.

test forwarding inconsistency [**ip** | **ipv4** | **ipv6**] [**unicast**] [**vrf** *vrf-name*] [**module** {*slot* | **all**}] [**stop**]

Syntax Description

ip	(Optional) Specifies the inconsistency check for IPv4 routes.
ipv4	(Optional) Specifies the inconsistency check for IPv4 routes.
ipv6	(Optional) Specifies the inconsistency check for IPv6 routes.
unicast	(Optional) Specifies the inconsistency check for unicast routes.
vrf	(Optional) Specifies the routes for a specific VRF.
vrf-name	(Optional) Specifies the VRF name.
module	(Optional) Specifies the inconsistency check for one or more modules.
slot	Module number. The range depends on the platform.
all	(Optional) Specifies the inconsistency check for all modules.
stop	(Optional) Stops the inconsistency check.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added support for the **ipv6** keyword.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to trigger the Layer 3 inconsistency checker for all modules:

```
switch# test forwarding inconsistency module all
```

This example shows how to stop the Layer 3 inconsistency checker for all modules:

```
switch# test forwarding inconsistency module all stop
```

Related Commands

Command	Description
clear forwarding inconsistency	Clears the FIB inconsistencies.
show forwarding inconsistency	Displays information about the FIB inconsistencies.

threshold percentage

To set a threshold percentage for a tracked object in a list of objects, use the **threshold percentage** command. To disable the threshold percentage, use the **no** form of this command.

threshold percentage {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}

no threshold percentage

Syntax Description

up	Specifies the up threshold.
down	Specifies the down threshold.
number	Threshold value. The range is from 0 to 100.

Defaults

None

Command Modes

Tracking configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

When you configure a tracked list using the **track** *object-number* **list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **percentage** keyword, the **weight** keyword is unavailable. If you specify the **weight** keyword, the **percentage** keyword is unavailable.

You should configure the up percentage first. The valid range is from 1 to 100. The down percentage depends on what you have configured for up. For example, if you configure 50 percent for up, you will see a range from 0 to 49 percent for down.

This command does not require a license.

Examples

This example shows how to configure the tracked list 11 to measure the threshold using an up percentage of 50 and a down percentage of 32:

```
switch(config)# track 11 list threshold percentage
switch(config-track)# object 1
switch(config-track)# object 2
switch(config-track)# threshold percentage up 50 down 32
```

Related Commands

Command	Description
threshold weight	Sets a threshold weight for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

threshold weight

To set a threshold weight for a tracked object in a list of objects, use the **threshold weight** command. To disable the threshold weight, use the **no** form of this command.

threshold weight {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}

no threshold weight

Syntax Description

up	Specifies the up threshold.
down	(Optional) Specifies the down threshold.
number	Threshold value. The range is from 1 to 255.

Defaults

None

Command Modes

Tracking configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

When you configure a tracked list using the **track** *object-number* **list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **percentage** keyword, then the **weight** keyword is unavailable. If you specify the **weight** keyword, then the **percentage** keyword is unavailable.

You should configure the up weight first. The valid range is from 1 to 255. The available down weight depends on what you have configured for the up weight. For example, if you configure 25 for up, you will see a range from 0 to 24 for down.

This command does not require a license.

Examples

This example shows how to configure the tracked list 12 to measure a threshold using a specified weight:

```
switch(config)# track 11 list threshold weight
switch(config-track)# object 1
switch(config-track)# object 2
switch(config-track)# threshold weight up 35 down 22
```

Related Commands

Command	Description
threshold percentage	Sets a threshold percentage for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

timers (GLBP)

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 **timers** command. To return the timers to the default values, use the **no** form of this command.

timers [**msec**] *hellotime* [**msec**] *holdtime*

no timers

Syntax Description

msec	(Optional) Specifies that the following (*hellotime* or *holdtime)* argument value will be expressed in milliseconds.
hellotime	Hello interval. The range is from 1 to 60 seconds. 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 range is from 2 to 180 seconds. The default is 10 seconds (10,000 milliseconds).

Defaults

hellotime: 3 seconds
holdtime: 10 seconds

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you do not configure timers on a gateway, the gateway learns the timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All gateways 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. Typically, the holdtime is greater than three times the value of the hello time, (*holdtime* > 3 * *hellotime*). The range of values for the holdtime force the holdtime to be greater than the hello time.

This command does not require a license.

Examples

This example shows how to configure the timers for GLBP group 10 on Ethernet interface 1/1:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers 5 18
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
timers redirect	Configures the redirect and timeout values for the GLBP group.

timers active-time

To adjust the Enhanced Interior Gateway Routing Protocol (EIGRP) time limit for the active state, use the **timers active-time** command. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description

time-limit	(Optional) Active time limit (in minutes). The range is from 1 to 65535 minutes. The default value is 3.
disabled	(Optional) Disables the timers and permits the routing wait time to remain active indefinitely.

Defaults

Disabled

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers active-time** command to control the time that the router waits (after a query is sent) before declaring the route to be in the stuck in active (SIA) state.

This command requires the Enterprise Services license.

Examples

This example shows how to configure an indefinite routing wait time on the specified EIGRP route:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers active-time disabled
```

timers advertise

To set the advertisement timer in milliseconds, use the **timers advertise** command.

timers advertise *interval*

Syntax Description		
	interval	Interval duration. The range is from 100 to 40950.

Defaults None

Command Modes config-if-vrrpv3-group mode

Supported User Roles network-admin
vdc-admin

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

Usage Guidelines Cisco recommends that you set this timer to a value greater than or equal to 1 second.

This command requires the Enterprise Services license.

Examples This example shows how to set the advertisement timer in milliseconds:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# vrrpv3 5 address-family ipv4
switch(config-if-vrrpv3-group)# address 100.0.1.10 primary
switch(config-if-vrrpv3-group)# description group3
switch(config-if-vrrpv3-group)# match-address
switch(config-if-vrrpv3-group)# preempt delay minimum 30
switch(config-if-vrrpv3-group)# priority 3
switch(config-if-vrrpv3-group)# timers advertise 100
switch(config-if-vrrpv3-group)#
```

Related Commands	Command	Description
	vrrpv3 address-family	Creates a VRRPv3 group and enter VRRPv3 group configuration mode.

timers basic

To adjust the Routing Information Protocol (RIP) network timers, use the **timers basic** command. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description

update	Rate (in seconds) at which updates are sent. The default is 30 seconds.
invalid	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when no updates refresh the route. The route then enters into a *holddown* state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed; it should be at least three times the value of the *update* argument. A route enters into a *holddown* state when an update packet is received that indicates that the route is unreachable. The route is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.
flush	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the sum of the *invalid* argument plus the *holddown* argument. If it is less than this sum, the proper *holddown* interval cannot elapse, which results in a new route being accepted before the *holddown* interval expires. The default is 240 seconds.

Defaults

update: 30 seconds
invalid: 180 seconds
holddown: 180 seconds
flush: 240 seconds

Command Modes

Router address-family configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can modify the basic timing parameters for RIP. These timers must be the same for all routers and servers in the network.

Note You can view the current and default timer values by using the **show ip protocols** command.

This command does not require a license.

Examples

This example shows how to set updates to broadcast every 5 seconds. If Cisco NX-OS does not hear from a router in 15 seconds (the invalid time), it declares the route as unusable. Cisco NX-OS suppresses further information for an additional 15 seconds (the holddown time). At the end of the suppression period, Cisco NX-OS flushes the route from the routing table.

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# timers basic 5  15  15  30
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.

timers lsa-arrival (OSPF)

To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa-arrival** command. To return to the default, use the **no** form of this command.

timers lsa-arrival *milliseconds*

no timers lsa-arrival

Syntax Description

milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa arrival** command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.

We recommend that you keep the *milliseconds* value of the **timers lsa-arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa** command.

This command requires the Enterprise Services license.

Examples

This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:

```
switch(config)# router ospf 1
switch(config-router)# timers lsa-arrival 2000
```

Related Commands

Command	Description
show ip ospf timers rate-limit	Displays all of the LSAs in the rate-limit queue.
timers throttle lsa	Sets rate-limiting values for LSAs being generated.

timers lsa-arrival (OSPFv3)

To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First version 3 (OSPFv3) neighbors, use the **timers lsa-arrival** command. To return to the default, use the **no** form of this command.

timers lsa-arrival *milliseconds*

no timers lsa-arrival

Syntax Description

milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa arrival** command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.

We recommend that you keep the *milliseconds* value of the **timers lsa-arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa** command.

This command requires the Enterprise Services license.

Examples

This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:

```
switch(config)# router ospfv3 1
switch(config-router)# timers lsa-arrival 2000
```

Related Commands

Command	Description
show ospfv3 timers rate-limit	Displays all of the LSAs in the rate-limit queue.
timers throttle lsa	Sets rate-limiting values for LSAs being generated.

timers lsa-group-pacing (OSPF)

To change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command. To return to the default, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Syntax Description

seconds	Time (in seconds) in the interval in which LSAs are grouped and refreshed, checksummed, or aged. The range is from 1 to 1800 seconds. The default value is 10 seconds.

Defaults

The default interval for this command is 10 seconds. OSPF LSA group pacing is enabled by default.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa-group-pacing** command to control the rate at which LSA updates occur and reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. Do not change the packet pacing timers unless you have tried all other options to meet OSPF packet flooding requirements. You should try summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. There are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis.

Cisco NX-OS groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs that the router is handling. For example, if you have about 10,000 LSAs, you should decrease the pacing interval. If you have a very small database (40 to 100 LSAs), you should increase the pacing interval to 10 to 20 minutes.

This command requires the Enterprise Services license.

Examples

This example shows how to configure OSPF group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPF routing process 1:

```
switch(config)# router ospf 1
switch(config-router)# timers lsa-group-pacing 60
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.

timers lsa-group-pacing (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command. To return to the default, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Syntax Description

seconds	Time (in seconds) in the interval in which LSAs are grouped and refreshed, checksummed, or aged. The range is from 1 to 1800 seconds. The default value is 240 seconds.

Defaults

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa-group-pacing** command to control the rate at which LSA updates occur and reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless you have tried all other options to meet OSPFv3 packet flooding requirements. You should try summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. There are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Cisco NX-OS groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs that the router is handling. For example, if you have about 10,000 LSAs, you should decrease the pacing interval. If you have a very small database (40 to 100 LSAs), you should increase the pacing interval to 10 to 20 minutes.

This command requires the Enterprise Services license.

Examples

This example shows how to configure OSPFv3 group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPFv3 routing process 1:

```
switch(config)# router ospfv3 1
switch(config-router)# timers lsa-group-pacing 60
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPFv3 routing processes.

timers nsf converge

To adjust the time limit for nonstop forwarding (NSF) convergence for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **timers nsf converge** command. To disable this function, use the **no** form of this command.

timers nsf converge *seconds*

no timers nsf converge

Syntax Description

seconds	Time limit for convergence after an NSF switchover (in seconds). The range is from 60 to 180 seconds. The default value is 120.

Defaults

120 seconds

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf converge** command to control the time that the router waits for convergence after a switchover.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the NSF convergence time for EIGRP:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf converge 100
```

timers nsf route-hold

To set the timer that determines how long an NSF-aware Enhanced Interior Gateway Routing Protocol (EIGRP) router holds routes for an inactive peer, use the **timers nsf route-hold** command. To return the route hold timer to the default value, use the **no** form of this command.

timers nsf route-hold *seconds*

no timers nsf route-hold

Syntax Description

seconds	Time, in seconds, that EIGRP holds routes for an inactive peer. The range is from 20 to 300 seconds. The default is 240.

Defaults

EIGRP NSF awareness is enabled.
seconds: 240

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf route-hold** command to set the maximum period of time that the NSF-aware router holds known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes (advertising invalid routes) if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

This command requires the Enterprise Services license.

Examples

This example shows how to set the route hold timer value for an NSF-aware router to 2 minutes (120 seconds):

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf route-hold 120
```

timers nsf signal

To set the time limit to signal a nonstop forwarding (NSF) restart for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **timers nsf signal** command. To return the route hold timer to the default, use the **no** form of this command.

timers nsf signal *seconds*

no timers nsf signal

Syntax Description

seconds	Time, in seconds, that EIGRP waits for a peer to signal an NSF restart. The range is from 10 to 30 seconds. The default is 20.

Defaults

EIGRP NSF awareness is enabled.
seconds: 20

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf signal** command to set the maximum period of time that the NSF-aware router waits for an NSF-capable neighbor to signal a restart.

This command requires the Enterprise Services license.

Examples

This example shows how to set the signal timer value for an NSF-aware router to the maximum (30 seconds):

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf signal 30
```

timers prefix-peer-timeout

To configure the Border Gateway Protocol (BGP) prefix peering timeout value, use the **timers prefix-peer-timeout** command. To remove the timeout value, use the **no** form of this command.

timers prefix-peer-timeout *interval*

no timers prefix-peer-timeout

Syntax Description

interval	Timeout value for prefix peering. The range is from 0 to 1200 seconds. The default value is 30.

Defaults

Timeout value is 30.

Command Modes

Router configuration

Neighbor configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

BGP supports the prefix peering timeout for both IPv4 and IPv6, which means that you do not have to add each neighbor to the configuration.

When you are defining a prefix peering, you must specify the remote AS number with the prefix. BGP accepts any peer that connects from that prefix and autonomous system if the prefix peering does not exceed the configured maximum peers allowed.

When a BGP peer that is part of a prefix peering disconnects, Cisco NX-OS holds its peer structures for a defined prefix peer timeout value. An established peer can reset and reconnect without danger of being blocked because other peers have consumed all slots for that prefix peering.

This command requires a Enterprise Services license.

Examples

This example shows how to specify the timeout interval as 100 seconds:

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 100
```

Related Commands

Command	Description
address family (BGP)	Enters the address family configuration mode for BGP.
timers prefix-peer-wait	Configures the BGP prefix peering timeout value.

timers prefix-peer-wait

To configure the Border Gateway Protocol (BGP) prefix peering wait timer, use the **timers prefix-peer-wait** command. To remove the timer value, use the **no** form of this command.

timers prefix-peer-wait *interval*

no timers prefix-peer-wait

Syntax Description

interval	Prefix peer wait timer (seconds). The range is from 0 to 1200. The default value is 90.

Defaults

The prefix peer wait timer interval is 90 seconds.

Command Modes

Router configuration

Neighbor configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(8)	This command was introduced.

Usage Guidelines

You can use the **timers prefix-peer-wait** command to disable the peer prefix wait time so that there is no delay before BGP prefixes are inserted into the routing information base (RIB). This command is supported on a per-VRF basis or on the default VRF.

This timer is only applicable for BGP dynamic neighbors. It is only set when BGP is restarted or is coming up for the first time for the dynamic BGP neighbors.

This prefix-peer wait timer expires:

1. When at least one prefix-peer instance comes up.
2. When the prefix-peer convergence or the bestpath timer expires (this situation is applicable when the prefix-peer wait timer is greater than the best path timer).
3. None of the BGP prefix-peer instances comes up within this time.

Use the **show bgp convergence private** command to display details of the prefix peer wait timer.

This command requires a Enterprise Services license.

Examples

This example shows how to specify the timeout interval as 30 seconds:

```
switch(config)# router bgp 65536
```

```
switch(config-router)# timers prefix-peer-wait 30
```

Command	Description
address family (BGP)	Enters the address family configuration mode for BGP.
timers pre-fix-peer-timeout	Configures the BGP prefix peering timeout value.

timers redirect

To configure the time interval in 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), use the **timers redirect** command. To return the redirect timers to the default values, use the **no** form of this command.

timers redirect *redirect timeout*

no timers redirect *redirect timeout*

Syntax Description

redirect	Redirect timer interval, in seconds. The range is from 0 to 3600 seconds. The default is 300 seconds (5 minutes).
timeout	Time, in seconds, before the secondary virtual forwarder becomes unavailable. The range is from 610 to 64800 seconds. The default is 14,400 seconds (4 hours).

Defaults

redirect: 300 seconds
timeout: 14,400 seconds

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A virtual forwarder that is assigned a virtual MAC address by the AVG is referred to as a primary virtual forwarder. If the virtual forwarder learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.

You can use the redirect timer to set a time delay that starts when a forwarder fails on the network and the AVG assumes that the forwarder will not return. When you set a time delay, the virtual MAC address that the forwarder replies to is still in the Address Resolution Protocol (ARP) replies, but the actual forwarding task is handled by another group in the GLBP group.

The timeout interval is the time delay that begins when a forwarder fails on the network and the MAC address that the forwarder was responsible for becomes inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. You must configure a timeout interval that is long enough to allow all hosts to refresh the ARP cache entry that contained the virtual MAC address.

This command does not require a license.

Examples

This example shows how to configure the redirect and timeout values for GLBP group 1 on Ethernet interface 1/1:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers redirect 600 7200
switch(config-glbp)# ip
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
timers	Configures hello and hold timers for GLBP.

timers throttle lsa (OSPF)

To set rate-limiting values for Open Shortest Path First (OSPF) link-state advertisement (LSA) generation, use the **timers throttle lsa** command. To return to the default values, use the **no** form of this command.

timers throttle lsa *start-time hold-interval max-time*

no timers throttle lsa

Syntax Description

start-time	Start time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 0 to 5000 milliseconds. The default value is 0 milliseconds.
hold-interval	Incremental time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.
max-time	Maximum time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.

Defaults

start-time: 0 milliseconds
hold-interval: 5000 milliseconds
max-time: 5000 milliseconds

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added *start-time* and *max-time* arguments.

Usage Guidelines

Use the **timers throttle lsa** command to rate limit LSA generation.

This command requires the Enterprise Services license.

Examples

This example shows how to customize OSPF LSA throttling:

```
switch(config)# router ospf 1
switch(config-router)# timers throttle lsa 50 5000 6000
```

Related Commands

Command	Description
show ip ospf	Displays information about OSPF routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle lsa (OSPFv3)

To set rate-limiting values for Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) generation, use the **timers throttle lsa** command. To return to the default values, use the **no** form of this command.

timers throttle lsa *start-time hold-interval max-time*

no timers throttle lsa

Syntax Description

start-time	Start time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 50 to 5000 milliseconds. The default value is 50 milliseconds.
hold-interval	Incremental time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.
max-time	Maximum time (in milliseconds) that is used to calculate the subsequent rate-limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.

Defaults

hold-interval: 5000 milliseconds

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added *start-time* and *max-time* arguments.

Usage Guidelines

Use the **timers throttle lsa** command to rate limit LSA generation.

This command requires the Enterprise Services license.

Examples

This example shows how to customize OSPFv3 LSA throttling:

```
switch(config)# router ospfv3 1
switch(config-router)# timers throttle lsa 50 10000 5000
```

Related Commands

Command	Description
show ospfv3	Displays information about OSPFv3 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.

timers throttle spf (OSPF)

To set the shortest-path first (SPF) best-path schedule initial delay time and the minimum hold between the SPF best-path calculation for Open Shortest Path First (OSPF), use the **timers throttle spf** command. To turn off SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-default spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-default spf-max-wait*

Syntax Description

spf-start	Initial SPF schedule delay in milliseconds. The range is from 1 to 6000,00 milliseconds.
spf-hold	Minimum hold time between two consecutive SPF calculations. the range is from 1 to 6000,00 milliseconds. The default is 1000 milliseconds.
spf-default	The default is 200 milliseconds.
spf-max-wait	Maximum wait time between two consecutive SPF calculations. The range is from 1 to 6000,00 milliseconds. The default is 5000 milliseconds.

Defaults

The default configuration for SPF throttling is:

```
timers throttle spf 200,1000,5000
```

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers throttle spf** command to set the SPF timers.

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-maximum* argument. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Examples

This example shows how to configure a router configured with the start, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds:

```
switch(config)# router ospf 1
```

```
switch(config-router)# timers throttle spf 5 1000 90000
```

timers throttle spf (OSPFv3)

To set the shortest-path first (SPF) best-path schedule initial delay time and the minimum hold between the SPF best-path calculation for Open Shortest Path First version 3 (OSPFv3), use the **timers throttle spf** command. To turn off SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-default spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-default spf-max-wait*

Syntax Description

spf-start	Initial SPF schedule delay in milliseconds. The range is from 1 to 600,000 milliseconds.
spf-hold	Minimum hold time between two consecutive SPF calculations. the range is from 1 to 600,000 milliseconds. The default is 1000 milliseconds.
spf-default	The default is 200 milliseconds.
spf-max-wait	Maximum wait time between two consecutive SPF calculations. The range is from 1 to 600,000 milliseconds. The default is 5000 milliseconds.

Defaults

The default configuration for SPF throttling is

timers throttle spf 200,1000,5000

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **timers throttle spf** command to set the SPF timers.

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-maximum* argument. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Examples

This example shows how to configure a router configured with the start, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds:

```
switch(config)# router ospfv3 1
switch(config-router)# address-family ipv6 unicast
```

```
switch(config-router-af)# timers throttle spf 5 1000 90000
```

track (VRRP)

To modify the priority for a virtual router based on a tracked object, use the **track** command. To disable priority tracking for a virtual router, use the **no** form of this command.

track *object-number* [**decrement** *value*]

no track track *object-number* [**decrement** *value*]

Syntax Description

object-number	Number for a configured tracked object. The range is from 1 to 500.
decrement *value*	(Optional) Decrements the VRRP priority if the tracked object is down. The range is from 1 to 254.

Defaults

None

Command Modes

VRRP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modified
4.2(1)	This command was introduced.

Usage Guidelines

Use the **track (VRRP)** command to change the priority of the virtual router based on the state of a configured tracked object. Use the track command to configure the tracked object. When the tracked object is down, the priority reverts to the priority value for the virtual router. When the tracked object is up, the priority of the virtual router is restored to the original value.

This command does not require a license.

Examples

This example shows how to enable object tracking for a virtual router:

```
switch# config t
switch(config)# track 33 ip route 192.0.2.0/24 reachability
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track 33 priority 2
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
track interface (VRRP)	Tracks the state of an interface and modifies the VRRP priority if that interface state goes down.

track interface

To configure object tracking on an interface, use the **track interface** command. To remove the object tracking for this interface, use the **no** form of this command.

track *object-id* **interface** *interface-type number* {{**ip** | **ipv6**} **routing** | **line-protocol**}

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
interface interface-type number	Interface to track. Use the online ? help to see a list of available interface types.
ip routing	Tracks the IP routing state of the interface.
ipv6 routing	Tracks the IPv6 routing state of the interface.
line-protocol	Tracks the line protocol state of the interface.
force	(Optional) Removes the object tracking instance.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	Added the **ipv6** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

Use the **track interface** command to track the line protocol status or IPv4 or IPv6 routing state of an interface. This command enters the object tracking command mode. Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault virtual routing and forwarding (VRF) instance.

This command does not require a license.

Examples

This example shows how to track the IP routing state on interface Ethernet 1/2:

```
switch(config)# track 1 interface ethernet 1/2 ip routing
switch(config-track)#
```

Related Commands

Command	Description
show track	Displays information about object tracking.
track {**ip** | **ipv6**} **route reachability**	Tracks the state of an IPv4 or IPv6 route reachability.
vrf member	Tracks an object in a nondefault VRF.

track interface (VRRP)

To track the priority for a virtual router based on an interface, use the **track interface** command. To disable priority tracking for a virtual router, use the **no** form of this command.

track interface {**ethernet** *interface-num* | **vlan** *vlan-num* | **port-channel** *channel-group-num*}
  priority *value*

no track interface

Syntax Description

ethernet *interface-num*	Specifies the virtual router interface for which to track priority. The range is from 1 to 255.
vlan *vlan-num*	Specifies the VLAN for which to track priority.
port-channel *channel-group-num*	Specifies the port-channel group for which to track priority.
priority *value*	Interface priority for a virtual router. The range of values is from 1 to 255. If this router is the owner of the IP addresses, the value is automatically set to 255.

Defaults

Disabled

Command Modes

VRRP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modified
4.0(1)	This command was introduced.

Usage Guidelines

Use the **track** command to change the priority of the virtual router based on the state of another interface in the switch. When the tracked interface is down, the priority reverts to the priority value for the virtual router. When the tracked interface is up, the priority of the virtual router is restored to the interface state tracking value.

Note Interface state tracking will not be operational unless you enable preemption on the interface.

This command does not require a license.

This example shows how to enable interface state tracking for a virtual router:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track interface ethernet 2/2 priority 2
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
track (VRRP)	Tracks an object to modify the VRRP priority.

track ip route

To configure object tracking on an IP route, use the **track ip route** command. To remove the object tracking for this route, use the **no** form of this command.

track *object-id* **ip route** *ip-prefix/length* **reachability**

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
ip-prefix/length	Prefix of route to track. The IP prefix is in dotted decimal format (X.X.X.X). The length can be from 1 to 32.
reachability	Tracks the reachability state of an IP route.
force	(Optional) Removes the object tracking instance.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **track ip route** command to track IP route reachability. This command enters the object tracking command mode. Use the **vrf member** command to track objects in a nondefault VRF.

This command does not require a license.

Examples

This example shows how to track an IP route:

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)#
```

Related Commands

Command	Description
show track	Displays information about object tracking.
track interface	Tracks an interface.

Command	Description
track ipv6 route reachability	Tracks an IPv6 route reachability.
vrf member	Tracks an object in a nondefault VRF.

track ipv6 route

To configure object tracking on an IPv6 route, use the **track ipv6 route** command. To remove the object tracking for this route, use the **no** form of this command.

track *object-id* **ipv6 route** *ipv6-prefix/length* **reachability**

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
ipv6-prefix/length	Prefix of route to track. The IPv6 prefix format is A:B::C:D/length. The length can be from 1 to 128.
reachability	Tracks the reachability state of an IPv6 route.
force	(Optional) Removes the object tracking instance.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **track ipv6 route** command to track the status of an IPv6 route. This command enters the object tracking command mode. Use the **vrf member** command to track objects in a nondefault VRF.

This command does not require a license.

Examples

This example shows how to track an IPv6 route:

```
switch(config)# track 1 ipv6 route 2001:0DB8::/8 reachability
switch(config-track)#
```

Related Commands

Command	Description
show track	Displays information about object tracking.
track ip route	Tracks an interface.
vrf member	Tracks an object in a nondefault VRF.

track list

To configure object tracking on an object list, use the **track list** command. To remove the object tracking for this object list, use the **no** form of this command.

track *object-id* **list boolean** {**and** | **or**}

track *object-id* **list threshold** {**percentage** | **weight**}

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range is from 1 to 500.
boolean	Combines the tracked object states as a Boolean combination.
and	Combines the tracked object states as a Boolean AND.
or	Combines the tracked object states as a Boolean OR.
threshold	Combines the tracked object states as a percentage or weight combination.
percentage	Combines the tracked object states as a percentage of the total number of tracked objects in the list.
weight	Combines the tracked object states as a combination of their configured weights.
force	(Optional) Removes the object tracking instance.

Command Default

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **track list** command to create a list of objects to combine into one tracked state. Use the **boolean and** keywords to combine the tracked objects as an AND function (that is, all objects must be up for the track list to be up). Use the **boolean or** keywords to combine the tracked objects as an OR (that is, if any object is up, the tracked state is up).

The track list command enters the track command mode. You can configure the following commands in this mode:

- **object**—Configures one or more objects to track in the track list. You can optionally use the **not** keyword to negate the object track state. (That is, an up state becomes a down state if you use the **not** keyword) for boolean tracked lists. You can optionally use the **weight** keyword to assign a weight to an object for a threshold weight tracked list. The default weight is 10.
- **vrf**—Assigns the track list to a VRF.

This command does not require a license.

Examples

This example shows how to create a track list of two objects as a Boolean and AND:

```
switch(config)# track 1 boolean and
switch(config-track)#object 33
switch(config-track)#object 30
```

This example shows how to configure a track list with an up threshold of 70 percent and a down threshold of 30 percent:

```
switch# config t
switch(config)# track 1 list threshold percentage
switch(config-track)# threshold percentage up 70 down 30
switch(config-track)# object 10
switch(config-track)# object 20
switch(config-track)# object 30
```

This example shows how to configure a track list with an up weight threshold of 30 and a down threshold of 10:

```
switch# config t
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
```

In this example, the track list is up if object 10 and object 20 are up, and the track list goes to the down state if all three objects are down.

Related Commands

Command	Description
show track	Displays information about object tracking.
track ip route	Tracks an interface.

transmit-delay (OSPF virtual link)

To set the estimated time required to end a link-state update packet on the interface, use the **transmit-delay** command. To return to the default, use the **no** form of this command.

transmit-delay *seconds*

no transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Defaults

1 second

Command Modes

Virtual interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **transmit-delay** command to account for the transmission and propagation delays for the virtual link.

This command requires the Enterprise Services license.

Examples

This example shows how to set the retransmit delay value to 3 seconds:

```
switch(config)# router ospf 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```

transmit-delay (OSPFv3 virtual link)

To set the estimated time required to end a link-state update packet on the interface, use the **transmit-delay** command. To return to the default, use the **no** form of this command.

transmit-delay *seconds*

no transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Defaults

1 second

Command Modes

Virtual interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **transmit-delay** command to account for the transmission and propagation delays for the virtual link.

This command requires the Enterprise Services license.

Examples

This example shows how to set the retransmit delay value to 3 seconds:

```
switch(config)# router ospfv3 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```