H Commands

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

hardware ejector enable

To enable the hardware when both ejectors are open, card is powered down, use the **hardware ejector enable** command.

hardware ejector enable

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration mode

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

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable the hardware when both ejectors are open:

```
switch(config)# hardware ejector enable
```

Related Commands

Command	Description
show hardware forwarding dynamic-allocation	Displays information about dynamic TCAM allocation for each module.

hardware forwarding dynamic-allocation

To enable or disable dynamic TCAM block allocation in the Forwarding Information Base (FIB), use the **hardware forwarding dynamic-allocation** command.

hardware forwarding dynamic-allocation {**enable** | **disable**}

Syntax Description

enable	Enables dynamic TCAM allocation.
disable	Disables dynamic TCAM allocation.

Defaults

Enabled

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.
5.0(x)	This command was deprecated.

Usage Guidelines

As of Cisco NX-OS Release 5.0(x), dynamic TCAM allocation is enabled by default and cannot be disabled.

Use the **hardware forwarding dynamic-allocation enable** command to reallocate unused blocks in the FIB.

Use the **hardware forwarding dynamic-allocation disable** command to disable the dynamic TCAM allocation. This command returns the TCAM to the default allocation if there are no routes in the reallocated blocks.

This command does not require a license.

Examples

This example shows how to enable dynamic TCAM allocation:

```
switch(config)# hardware forwarding dynamic-allocation enable
```

Related Commands

Command	Description
show hardware forwarding dynamic-allocation	Displays information about dynamic TCAM allocation for each module.

hardware forwarding l3 resource route non-deterministic

To expand the number of routes available on the Cisco NX-OS device, use the **hardware forwarding l3 resource route non-deterministic** command. To set the revert to the default settings, use the **no** form of the command.

hardware forwarding l3 resource route non-deterministic

no hardware forwarding l3 resource route non-deterministic

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

We recommend that you use the **hardware forwarding l3 resource route non-deterministic** command only under the advisement of Cisco.

This command does not require a license.

Examples

This example shows how to expand the number of routes available on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# hardware forwarding l3 resource route non-deterministic
```

This example shows how to remove the route expansion on the Cisco NX-OS device:

```
switch(config)# no hardware forwarding l3 resource route non-deterministic
switch(config)#
```

Related Commands

Command	Description
hardware forwarding dynamic-allocation	Enable or disable dynamic TCAM block allocation in the Forwarding Information Base (FIB).

hardware ip glean throttle

To enable Address Resolution Protocol (ARP) throttling, use the **hardware ip glean throttle** command. To return to the default setting, use the **no** form of this command.

hardware ip glean throttle

no hardware ip glean throttle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.
4.2(8)	This command was introduced.

Usage Guidelines

Note We recommend that you configure the IP glean throttle feature by using the **hardware ip glean throttle** command to filter the unnecessary glean packets that are sent to the supervisor for ARP resolution for the next hops that are not reachable or do not exist. IP glean throttling boosts software performance and helps to manage traffic more efficiently.

This command does not require a license.

Examples

This example shows how to enable ARP throttling:

```
switch(config)# hardware ip glean throttle
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

hardware ip glean throttle maximum

To limit the maximum number of drop adjacencies that will be installed in the Forwarding Information Base (FIB), use the **hardware ip glean throttle maximum** command. If **no** form is used, default limits will be applied.

hardware ip glean throttle maximum *count*

no **hardware ip glean throttle maximum** *count*

Syntax Description

count	Maximum count. The range is from 0 to 2147483647.

Defaults

The default value for count is 1000. The minimum value is 0 and the maximum value is 32767 entries

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.
4.2(8)	This command was introduced.

Usage Guidelines

If the maximum number of entries are exceeded, the packets for which ARP is not resolved continue to be processed in the software instead of getting dropped in the hardware.

This command does not require a license.

Examples

This example shows how to limit the maximum number of drop adjacencies that are installed in the FIB:

```
switch(config)# hardware ip glean throttle maximum 2134
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

hardware ip glean throttle syslog

To generate a syslog if the number of packets that get dropped for a specific flow exceeds the configured packet count, use the **hardware ip glean throttle syslog** command. To return to the default setting, use the **no** form of this command.

hardware ip glean throttle syslog *pkt-count*

no hardware ip glean throttle syslog *pkt-count*

Syntax Description

pkt-count	Packet count. The range is from 0 to 2147483647.

Defaults

The default value for count is 10000. The minimum value is 0 and the maximum value is 64 k (65535) packets

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.
4.2(8)	This command was introduced.

Usage Guidelines

After the timeout period is exceeded, the drop adjacencies are removed from the FIB.

This command does not require a license.

Note The Adjmgr generates a syslog for the configured packet count that will not be accurate to the glean packets dropped hit in FIB. The drop statistics collected from the FIB in S/w (Adjmgr) occurs every two minutes. The Adjmgr generates a syslog only after it receives the stats from the FIB every two minutes only for the adjacencies where the drop count exceeds the configured packet count.

Examples

This example shows how to generate a syslog if the number of packets that get dropped for a specific flow exceed the configured packet count:

```
switch(config)# hardware ip glean throttle syslog 1030
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

hardware ip glean throttle timeout

To configure a timeout for the installed drop adjacencies to remain in the Forwarding Information Base (FIB), use the **hardware ip glean throttle timeout** command. To return to the default setting, use the **no** form of this command.

hardware ip glean throttle timeout *timeout-in-sec*

no hardware ip glean throttle timeout *timeout-in-sec*

Syntax Description

timeout -in-sec	Timeout value in seconds. The range is from 300 to 1800.

Defaults

300 seconds

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.
4.2(8)	This command was introduced.

Usage Guidelines

After the timeout period is exceeded, the drop adjacencies are removed from the FIB.

This command does not require a license.

Examples

This example shows how to limit the maximum number of drop adjacencies that are installed in the FIB:

```
switch(config)# hardware ip glean throttle timeout 300
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

hardware ip verify

To configure IP packet verification, use the **hardware ip verify** command. To disable IP packet verification, use the **no** form of this command.

hardware ip verify {**checksum** | **fragment** | **protocol** | **tcp tiny-frag** | **version**}

no hardware ip verify {**checksum** | **fragment**}

Syntax Description

checksum	Drops IPv4 or IPv6 packets if the checksum is invalid.
fragment	Drops IPv4 or IPv6 packets if the packet fragment has a nonzero offset and the DF bit is active.
protocol	Drops IPv4 or IPv6 packets if the packet fragment has an invalid IP protocol number.
tcp tiny-frag	Drops IPv4 packets if the IP fragment offset is 1, or if the IP fragment offset is 0 and the IP payload length is less than 16.
version	Drops IPv4 packets if the Ethertype is not set to 4 (IPv4).

Defaults

All address tests disabled (since Cisco NX-OS Release 5.1(3)).

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.
4.2(2)	Added **protocol** keyword.

Usage Guidelines

Use the **hardware ip verify** command to configure packet verification tests on IPv4 and IPv6 packets based on checksum or fragments.

This command is not supported in F Series modules.

This command replaces the **platform ip verify** command.

This command does not require a license.

Examples

This example shows how to drop fragmented IPv4 or IPv6 packets:

```
switch(config)# hardware ip verify fragment
```

Related Commands

Command	Description
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ip verify length	Configures IPv4 packet verification checks based on length.
hardware ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

hardware ip verify address

To enable packet verification tests on IP addresses, use the **hardware ip verify address** command. To disable packet verification tests, use the **no** form of this command.

hardware ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

no hardware ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

Syntax Description

destination zero	Drops IP packets if the destination IPv4 address is 0.0.0.0 or if the IPv6 address is ::.
identical	Drops IP packets if the source IPv4 or IPv6 address is identical to the destination IPv4 or IPv6 address.
reserved	Drops IP packets if the IPv4 address is in the 127.x.x.x range or if the IPv6 address is in the ::1 range.
source	Drops IP packets based on the IP source address.
broadcast	Drops IP packets if the IP source address is 255.255.255.255.
multicast	Drops IP packets if the IPv4 source address is in the 224.x.x.x range or if the IPv6 source address is in the FF00::/8 range.

Defaults

All values are disabled (since Cisco NX-OS Release 5.1(3)).

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **hardware ip verify address** command to configure packet verification tests on IPv4 and IPv6 packets based on addresses.

This command replaces the **platform ip verify address** command.

Prior to Cisco NX-OS Release 5.1(3), for Fabric Extender (FEX), you must manually disable the **hardware ip verify address reserved** option.

In Cisco NX-OS Release 5.1(3), you must disable the **hardware ip verify address identical** option before enabling the Multiprotocol Label Switching (MPLS) feature.

This command is not supported in F-Series modules.

This command does not require a license.

Examples

This example shows how to drop broadcast IPv4 packets:

```
switch(config)# hardware ip verify address source broadcast
```

Related Commands

Command	Description
hardware ip verify	Configures IPv4 and IPv6 packet verification checks based on checksum or fragments.
hardware ip verify length	Configures IPv4 packet verification checks based on length.
hardware ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

hardware ip verify length

To configure IPv4 packet verification tests based on packet length, use the **hardware ip verify length** command. To disable the tests, use the **no** form of this command.

hardware ip verify length {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **minimum**}

no hardware ip verify length {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **minimum**}

Syntax Description

consistent	Drops IPv4 packets where the Ethernet frame size is greater than or equal to the IP packet length plus the Ethernet header.
maximum	Drops IP packets if the Ethernet frame length is more than the IP packet length.
max-frag	Drops IP packets if the maximum fragment offset is greater than 65536.
max-tcp	Drops IP packets if the TCP length is greater than the IP payload length.
udp	Drops IP packets if the IP payload length is less than the UDP packet length.
minimum	Drops IP packets if the Ethernet frame length is less than the IP packet length plus four octets (the CRC length).

Defaults

All address tests are enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **hardware ip verify length** command to configure packet verification tests on IPv4 and IPv6 packets based on packet length.

This command replaces the **platform ip verify length** command.

This command is not supported in F Series modules.

This command does not require a license.

Examples

This example shows how to drop minimum-length IPv4 packets:

```
switch(config)# hardware ip verify length minimum
```

Related Commands

Command	Description
hardware ip verify	Configures IPv4 packet verification checks based on checksum or fragments.
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

hardware ipv6 verify

To configure IPv6 packet verification tests, use the **hardware ipv6 verify** command. To disable the tests, use the **no** form of this command.

hardware ipv6 verify {**length** {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **tcp tiny-frag** | **version**}

no hardware ip verify {**checksum** | **fragment**}

Syntax Description

length	Drops IPv6 packets based on length.
consistent	Drops IPv6 packets where the Ethernet frame size is greater than or equal to the IPv6 packet length plus the Ethernet header.
maximum	Drops IP packets if the Ethernet frame length is more than the IP packet length.
max-frag	Drops IP packets if the maximum fragment offset is greater than 65536.
max-tcp	Drops IP packets if the TCP length is greater than the IP payload length.
udp	Drops IP packets if the IP payload length is less than the UDP packet length.
tcp tiny-frag	Drops IPv6 packets if the IP fragment offset is 1, or if the IPv6 fragment offset is 0 and the IPv6 payload length is less than 16.
version	Drops IPv6packets if the Ethertype is not set to 6 (IPv6).

Defaults

All address tests are enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **hardware ipv6 verify** command to configure packet verification tests on IPv6 packets.

This command replaces the **platform ipv6 verify** command.

This command does not require a license.

Examples

This example shows how to drop all IPv4 packets:

```
switch(config)# hardware ipv6 verify version
```

Related Commands

Command	Description
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ip verify length	Configures IPv4 packet verification checks based on length.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

hardware proxy layer-3 forwarding

To configure hardware proxy layer 3 forwarding information, use the **hardware proxy layer-3 forwarding** command. To set the default value, use the **no** form of the command.

hardware proxy layer-3 forwarding {**exclude** | **use**} {{**none**} {**interface ethernet** *slot/port* | **module** *slot-number*} [**module-type f1**]}

no hardware proxy layer-3 forwarding

Syntax Description

use	Specifies members.
exclude	Specifies all available members to exclude.
none	Specifies no modules or interface.
module	Specifies modules.
slot-number	Slot number. The range is from 1 to 18.
interface	Specifies interfaces.
slot/port	Slot or port number. The range is from 1 to 253.
module-type f1	(Optional) Specifies type of modules to perform proxyl ayer 3 forwarding for hardware proxy layer 3 forwarding exclude interface ethernet F1 modules.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

The N7K-F132-15 module only runs Layer 2 switching. So, when you have both this module and an M Series module in one Nexus 7000 Series chassis and you are performing Layer 3 procedures, the system uses proxy routing.

This command does not require a license.

Examples

This example shows how to configure hardware proxy forwarding information:

```
switch(config)# hardware proxy layer-3 forwarding exclude interface ethernet 2/1-16,
ethernet 3/1, ethernet 4/1-2
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays detail information on the proxylayer 3 functionality.

hello-interval (OSPF virtual link)

To specify the interval between hello packets that Cisco NX-OS sends on an Open Shortest Path First (OSPF) virtual link, use the **hello-interval** command. To return to the default, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

seconds	Hello interval (in seconds). The value must be the same for all nodes on a specific virtual link. The range is from 1 to 65535.

Defaults

10 seconds

Command Modes

Virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **hello-interval** command in virtual link configuration mode to set the hello interval for OSPF across a virtual link. A shorter hello interval detects topological changes faster but causes more routing traffic. The hello interval must be the same for all devices on a virtual link.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the hello interval to 15 seconds:

```
switch(config)# router ospf 202
switch(config-router)# ip ospf area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (virtual link)	Sets the time period to declare a neighbor as down if the local device receives no hello packets.

hello-interval (OSPFv3 virtual link)

To specify the interval between hello packets that Cisco NX-OS sends on an Open Shortest Path First version 3 (OSPFv3) virtual link, use the **hello-interval** command. To return to the default, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

seconds	Hello interval (in seconds). The value must be the same for all nodes on a specific virtual link. The range is from 1 to 65535.

Defaults

10 seconds

Command Modes

Virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **hello-interval** command in virtual link configuration mode to set the hello interval for OSPFv3 across a virtual link. A shorter hello interval detects topological changes faster but causes more routing traffic. The hello interval must be the same for all devices on a virtual link.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the hello interval to 15 seconds:

```
switch(config)# router ospfv3 202
switch(config-router)# ipv6 ospfv3 area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (OSPFv3 virtual link)	Sets the time period to declare a neighbor as down if the local device receives no hello packets.

hostname dynamic

To enable the exchange of the dynamic host name for IS-IS, use the **hostname dynamic** configuration mode command. To disable the exchange of the dynamic host name for IS-IS, use the **no** form of this command

hostname dynamic

no hostname dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

Dynamic hostname is disabled 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

The **hostname dynamic** command allows you to enable the IS-IS routers to flood their host name to system ID mapping information across the IS-IS network.

This command requires the Enterprise Services license.

Examples

This example shows how to enable the exchange of the dynamic host name for IS-IS:

```
switch(config-router)# hostname dynamic
switch(config-router)#
```

This example shows how to disable the exchange of the dynamic host name for IS-IS:

```
switch(config-router)# no hostname dynamic
switch(config-router)#
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.
show isis hostname	Displays the IS-IS dynamic host name exchange information.

hsrp

To enter Hot Standby Router Protocol (HSRP) configuration mode and create an HSRP group, use the **hsrp** command. To disable HSRP, use the **no** form of this command.

hsrp *group-number* [**ipv4** | **ipv6**]

no hsrp *group-number* [**ipv4** | **ipv6**]

Syntax Description

group-number	Number of HSRP groups that can be configured on a Gigabit Ethernet port, including the main interfaces and subinterfaces. For HSRP version 1, the range is from 0 to 255. For HSRP version 2, the range is from 0 to 4096. The default value is 0.
ipv4	(Optional) Sets the HSRP group for IPv4.
ipv6	(Optional) Sets the HSRP group for IPv6.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added the IPv4 keyword.
5.0(2)	Added the IPv6 keyword.
5.1(1)	Added an example on how to configure an IPv6 HSRP group.

Usage Guidelines

You must globally enable HSRP before you can configure any HSRP options or create an HSRP group.

The switch creates an IPv4 HSRP group if the **ipv6** keyword is not specified.

The keyword **ipv4** is optional if only IPv4 with the group ID exists on the interface. If both the IPv4 and IPv6 groups exist on the same interface, you must specify the address type as IPv4 or IPv6.

To configure IPv6 HRSP groups, you must configure HSRP version 2 on the interface.

The IPv4 and IPv6 groups can share the same group ID within an interface.

This command does not require a license.

Examples

This example shows how to create and activate an HSRP group:

```
switch# configure t
switch(config)# interface ethernet 0
switch(config-if)# ip address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)#
```

This example shows how to create and activate an IPv6 HSRP group:

```
switch# configure t
switch(config)# interface ethernet 5/2
switch(config)# ipv6 address 2001:0DB8:0001:0001:/64
switch(config-if-hsrp)# hsrp version 2
switch(config-if)# hsrp 10 ipv6
switch(config-if-hsrp)#
```

Related Commands

Command	Description
feature hsrp	Enables HSRP configuration.
show hsrp	Displays HSRP information.
ip address	Creates a virtual IP address for the HSRP group. The IP address must be in the same subnet as the interface IP address

hsrp ipv6

To create an Hot Standby Redundancy Protocol (HSRP) group and enter HSRP configuration mode, use the **hsrp** command. To remove the HSRP group configuration, use the **no** form of this command.

hsrp *group-number* [**ipv6**]

no hsrp *group-number* [**ipv6**]

Syntax Description

group-number	Group number. The range is from 0 to 4095.
ipv6	(Optional) Specifies the IPv6 address.

Defaults

None

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to create an HSRP group and enter HSRP configuration mode:

```
switch# configure terminal
switch(config)# interface ethernet 3/5
switch(config-if)# ip address 11.0.0.1/24
switch(config-if)# hsrp version 2
switch(config-if)# hsrp 10
switch(config-if-hsrp)#
```

This example shows how to remove the HSRP group configuration:

```
switch(config-if)# no hsrp 10
switch(config-if)#
```

Related Commands

Command	Description
hsrp version 2	Configures the HSRP version 2.

hsrp mac-refresh

To configure the MAC refresh interval for the Hot Standby Redundancy Protocol (HSRP) slave group, use the **hsrp mac-refresh** command.

hsrp mac-refresh *seconds*

Syntax Description

seconds	Interval in seconds. The range is from 0 to 10000.

Defaults

60 seconds

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

You can use the **hsrp mac-refresh** command to minimize the number of hello messages that are sent out and reduce HSRP protocol overheads and CPU utilization when multiple subinterfaces are configured.

The **hsrp mac-refresh** command is not available for individual subinterfaces. It applies to all groups on all subinterfaces.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the MAC refresh interval for an HSRP slave group:

```
switch# configure terminal
switch(config)# interface ethernet 3/5
switch(config-if)# ip address 11.0.0.1/24
switch(config-if)# hsrp version 2
switch(config-if)# hsrp mac-refresh 90
switch(config-if)#
```

Related Commands

Command	Description
follow	Configures a regular HSRP group as a slave group.

hsrp timers extended-hold

To enabled extended hold timers for the Hot Standby Router Protocol (HSRP), use the **hsrp timers extended-hold** command. To revert to default, use the **no** form of this command.

hsrp timers extended-hold [*timer*]

no hsrp timers extended-hold

Syntax Description

timer	(Optional) Extended hold time, in seconds. The range is from 10 to 255.

Defaults

10 seconds

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 **hsrp timers extended-hold** command to configure extended Non-stop Forwarding (NSF) support for HSRP.

Note You must configure extended hold timers on all HSRP routers if you configure non-default extended hold timers. You can configure different extended holdtimer values on each HSRP routers, based on the expected system switchover delays.

This command does not require a license.

Examples

This example shows how to configure the extended hold time for HSRP:

```
switch(config)# hsrp timers extended-hold 30
```

Related Commands

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

hsrp version 2

To configure the Hot Standby Redundancy Protocol (HSRP) version 2, use the **hsrp version 2** command.

hsrp version 2

Syntax Description This command has no arguments or keywords.

Defaults Version 1

Command Modes Interface configuration mode

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines Because the multiple group optimization (MGO) supports only HSRP version 2, you must set the HSRP version to version 2.

This command requires the Enterprise Services license.

Examples This example shows how to configures the HSRP version:

```
switch# configure terminal
switch(config)# interface ethernet 3/5
switch(config-if)# ip address 11.0.0.1/24
switch(config-if)# hsrp version 2
switch(config-if)#
```

Related Commands

Command	Description
hsrp	Configures the HSRP version.