P Commands

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

passive-interface

To suppress routing updates on an interface, use the **passive-interface** command. To revert to the default settings, use the no form of this command.

passive-interface default

no passive-interface default

Syntax Description

default	Specifies interfaces that are passive by default.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to suppress routing updates on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 5/4
switch(config-if)# router ospf 2
switch(config-router)# passive-interface default
switch(config-router)#
```

This example shows how to remove the configuration for the routing updates suppression:

```
switch# configure terminal
switch(config)# interface ethernet 5/4
switch(config-if)# router ospf 2
switch(config-router)# no passive-interface default
```

Related Commands

Command	Description
ip ospf passive-interface	Suppresses (OSPF routing updates on an interface.

passive-interface default

To remove the **passive-interface** commands on the interface (if any) and return the interface to the default configuration, use the **passive-interface default** command.

passive-interface default {**level-1** | **level-1-2** | **level-2**}

Syntax Description

level-1	Suppresses level-1 PDU.
level-1-2	Suppresses level-1 and level-2 PDU.
level-2	Suppresses level-2 PDU.

Defaults

None

Command Modes

Router configuration (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 remove the **passive-interface** commands on the interface and return the interface to the default configuration:

```
switch# configure terminal
switch(config)# router isis 1
switch(config-router)# passive-interface default level-1
switch(config-router)# exit
switch(config)#
```

Related Commands

Command	Description
router isis	Creates a new IS-IS instance and enters router configuration mode.

passive-interface default (EIGRP)

To suppress Enhanced Interior Gateway Routing Protocol (EIGRP) hellos, use the **passive-interface default** command. To revert to the default, use the **no** form of this command.

passive-interface default

no passive-interface default

Syntax Description This command has no arguments or keywords.

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 Suppressing the EIGRP hellos prevents neighbors from forming and sending routing updates on all EIGRP interfaces.

This command requires the Enterprise Services license.

Examples This example shows how to suppress EIGRP hellos:

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# passive-interface default
switch(config-router)#
```

Related Commands

Command	Description
router isis	Creates a new IS-IS instance and enters router configuration mode.
ip passive-interface eigrp	Suppresses all routing updates on EIGRP interface.

platform ip verify

To configure IP packet verification, use the **platform ip verify** command. To return to default, use the **no** form of this command.

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

no platform 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.
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 Drops IPv6packets if the Ethertype is not set to 4 (IPv4).

Defaults

All address tests are enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the **hardware ip verify** command.

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

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

platform ip verify address

To packet verification on IP addresses, use the **platform ip verify address** command. To return to default, use the **no** form of this command.

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

no platform 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 address tests are enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the **hardware ip verify address** command.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to drop broadcast IPv4 packets:

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

Related Commands

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

platform ip verify length

To configure IPv4 packet verification based on packet length, use the **platform ip verify length** command. To return to the default, use the **no** form of this command.

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

no platform 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	Specifies maximum IP packets.
max-frag	Specifies the IP packets if the maximum fragment offset is greater than 65536.
max-tcp	Specifies the IP packets if the TCP length is greater than the IP payload length.
udp	Specifies the IP packets if the IP payload length is less than the UDP packet length.
minimum	Specifies the 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
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the **hardware ip verify length** command.

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

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

platform ipv6 verify

To configure IPv6 packet verification, use the **platform ipv6 verify** command. To return to default, use the **no** form of this command.

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

no platform 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	Specifies maximum IP packets.
max-frag	Specifies the IP packets if the maximum fragment offset is greater than 65536.
max-tcp	Specifies the IP packets if the TCP length is greater than the IP payload length.
udp	Specifies the 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 IPv6 packets 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
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the **hardware ipv6 verify** command.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to drop all IPv4 packets:

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

Related Commands

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

preempt (GLBP)

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

Cisco NX-OS Release 4.1(3) and later syntax:

preempt [**delay minimum** *seconds*]

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

Cisco NX-OS Release 4.1(2) and earlier syntax:

preempt [**delay minimum** *seconds*]

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

Syntax Description

delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the gateway delays before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.
sync *seconds*	(Optional) Specifies a number of seconds that the gateway waits for the synchronization to complete. The range is from 0 to 3600 seconds.

Defaults

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

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	Removed **sync** the keyword.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a router to preempt the current AVG when its priority of 254 is higher than the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

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

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
priority	Sets the priority level of the router within a GLBP group.

preempt (HSRP)

To configure a preemption delay, use the **preempt** command. To disable this feature, use the **no** form of this command.

preempt [**delay {minimum** *min-delay* | **reload** *rel-delay* | **sync** *sync-delay*}]

no preempt [**delay {minimum** *min-delay* | **reload** *rel-delay* | **sync** *sync-delay*}]

Syntax Description

delay minimum *min-delay*	(Optional) Specifies the minimum number of seconds that preemption is delayed to allow routing tables to be updated before a router becomes active. The default value is 0.
reload *rel-delay*	(Optional) Specifies the time delay after the router has reloaded. This period applies only to the first interface-up event after the router has reloaded. The default value is 0.
sync *sync-delay*	(Optional) Specifies the maximum number of seconds to allow IP redundancy clients to prevent preemption. When this period expires, preemption occurs regardless of the state of the IP redundancy clients. The default value is 0.

Defaults

The default delay time for all options is 0 seconds.

Command Modes

Interface configuration or HSRP template 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.

Specifying a minimum delay allows routing tables to be updated before a router becomes active. When a router first comes up, it does not have a complete routing table. A high-priority router will only delay preemption if it first receives a Hello packet from a low-priority active router. If the high-priority router does not receive a Hello packet from the low-priority active router when it is starting up, then it assumes there is no active router for the group and will become active as soon as possible.

Examples

This example shows how to configure a delay when a router becomes active when its priority is 110:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 110
switch(config-if-hsrp)# preempt
switch(config-if-hsrp)# authentication text sanjose
switch(config-if-hsrp)# ip 10.0.0.3
switch(config-if-hsrp)# end
```

Related Commands

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

preempt (VRRP)

To enable a high-priority backup virtual router to preempt the low-priority master virtual router, use the **preempt** command. To disable a high-priority backup virtual router from preempting the low-priority master virtual router, use the **no** form of this command.

preempt

no preempt

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes VRRP configuration

Supported User Roles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a high-priority virtual router backup that has become available.

By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master. If you disable preemption, then the backup virtual router that is elected to become the virtual router master remains the master until the original virtual router master recovers and becomes the master again.

If the virtual IP address is also the IP address for the interface, then preemption is applied.

No license is required to use this command.

Examples This example shows how to enable the backup high-priority virtual router to preempt the low-priority master virtual router:

Note This preemption does not apply to the primary IP address.

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

Related Commands

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

peer-gateway exclude

To exclude a VLAN from peer gateway, when a VLAN interface is used for Layer 3 backup routing on the virtual port-channel (vPC) peer devices and an F1 module is used as peer-link, use the **vpc peer-gateway exclude-vlan** command. To revert to the default settings, use the **no** form of this command.

peer-gateway exclude-vlan *vlan-number*

peer-gateway exclude-vlan *vlan-number*

Syntax Description

vlan-number	VLAN number. The range is from 1 to 2499 and from 2628 to 4093.

Defaults

None

Command Modes

vPC configuration (config-vpc-domain)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.1(3)	This command was introduced.

Usage Guidelines

Use the **peer-gateway exclude-vlan** command to configure a Layer 3 backup routing VLAN whenever you use the vPC peer-gateway feature.

If the vPC peer link is configured on a Cisco Nexus 32-port 1/10 Gigabit Ethernet (F1-Series) module (N7K-F132XP-15), then you must include the Layer 3 backup routing VLAN in the VLAN list specified by the **vpc peer-gateway exclude** command.

If the vPC peer link is configured on an M1 series module, then you should include the Layer 3 backup routing VLAN in the VLAN list specified by the **vpc peer-gateway exclude** command, but it is not required.

The peer-gateway functionality is not enabled for those VLANs specified in the exclude VLAN list. If no exclude VLAN list is specified, then this functionality is enabled for all VLANs.

The latest occurrence of this configuration overwrites all previous configurations.

The **no vpc peer-gateway** command also disables IP redirects on all VLANs.

This command does not require a license.

Examples

This example shows how to exclude a VLAN from peer gateway:

```
switch# configure terminal
```

```
switch(config)# vpc domain 2
switch(config-vpc-domain)# peer-gateway exclude-vlan 1-34, 2700-2900
switch(config-vpc-domain)#
```

This example shows how to disable the peer-gateway functionality:

```
switch(config-vpc-domain)# no peer-gateway
switch(config-vpc-domain)#
```

Related Commands

Command	Description
vpc domain	Creates a virtual port-channel (vPC) domain.

priority (GLBP)

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

priority *level*

no priority

Syntax Description

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

Defaults

level: 100

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **priority** command to control which virtual gateway becomes the active virtual gateway (AVG). GLBP compares the priorities of all virtual gateways in the GLBP group and selects the gateway with the numerically highest priority as the AVG. If two virtual gateways have equal priority, GLBP selects the gateway with the highest IP address.

This command does not require a license.

Examples

This example shows how to configure a virtual gateway with a priority of 254:

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

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
preempt	Configures a gateway to take over as the AVG for a GLBP group if it has a higher priority than the current AVG.

priority (HSRP)

To set the priority level within a Hot Standby Router Protocol (HSRP) group, use the **priority** command. To remove the priority level, use the **no** form of this command.

priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

no priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

Syntax Description

level	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, then the value is automatically set to 255. The default is 100.
forwarding-threshold	(Optional) Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
lower *lower-value*	(Optional) Sets the low threshold value. The *lower-value* range is from 1 to 255. The default is 1.
upper *upper-value*	(Optional) Sets the upper threshold value. The *upper-value* range is from 1 to 255. The default is 255.

Defaults

level: 100
lower-value: 1
upper-value: 255

Command Modes

HSRP configuration or HSRP template mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	Added support for **forwarding-threshold**, **lower**, and **upper** keywords**.**

Usage Guidelines

Use the **priority** command to control which virtual router becomes the active router. HSRP compares the priorities of all virtual routers in the HSRP group and selects the router with the numerically highest priority. If two virtual routers have equal priority, HSRP selects the router with the highest IP address.

This command does not require a license.

Examples

This example shows how to configure a virtual router with a priority of 254:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 254
```

Related Commands

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

priority (VRRP)

To set the priority for the Virtual Router Redundancy Protocol (VRRP), use the **priority** command. To revert to the default value, use the **no** form of this command.

priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

no priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

Syntax Description

level	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, then the value is automatically set to 255. The default is 100.
forwarding-threshold	(Optional) Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
lower *lower-value*	(Optional) Sets the low threshold value. The *lower-value* range is from 1 to 255. The default is 1.
upper *upper-value*	(Optional) Sets the upper threshold value. The *upper-value* range is from 1 to 255. The default is 255.

Defaults

The default value is 100. For switches whose interface IP address is the same as the primary virtual IP address, the default value is 255.

Command Modes

VRRP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added support for **forwarding-threshold**, **lower**, and **upper** keywords**.**

Usage Guidelines

The priority determines whether or not a VRRP router functions as a virtual router backup, the order of ascendancy for the VRRP router to become a virtual router master if the virtual router master fails, the role that each VRRP router plays, and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, then this router will function as a virtual router master.

By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master. If you disable preemption, then the backup virtual router that is elected to become the virtual router master remains the master until the original virtual router master recovers and becomes the master again.

No license is required to use this command.

Examples

This example shows how to specify the priority for a virtual router:

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

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.

protocol shutdown (OSPF)

To shut down an Open Shortest Path First (OSPF) instance, use the **protocol shutdown** command. To disable this function, use the **no** form of this command.

protocol shutdown

no protocol shutdown

Syntax Description This command has no keywords or arguments.

Defaults The OSPF instance is enabled by default when configured.

Command Modes 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 **protocol shutdown** command to configure disable an instance of OSPF without removing the configuration.

This command requires the Enterprise Services license.

Examples This example shows how to disable OSPF 209:

```
switch(config) router ospf 209
switch(config-router)# protocol shutdown
```

protocol shutdown (OSPFv3)

To shut down an Open Shortest Path First version 3 (OSPFv3) instance, use the **protocol shutdown** command. To disable this function, use the **no** form of this command.

protocol shutdown

no protocol shutdown

Syntax Description

This command has no keywords or arguments.

Defaults

The OSPFv3 instance is enabled by default when configured.

Command Modes

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 **protocol shutdown** command to configure disable an instance of OSPFv3 without removing the configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to disable OSPFv3 209:

```
switch(config) router ospfv3 209
switch(config-router)# protocol shutdown
```