

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*



## **P Commands**

---

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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 ethertype is not set to 4 (IPv4).

**Defaults** All address tests enabled.

**Command Modes** Global configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**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
	<b>platform ip verify address</b>	Configures IPv4 and IPv6 packet verification checks based on addresses.
	<b>platform ip verify length</b>	Configures IPv4 packet verification checks based on length.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

<b>Command</b>	<b>Description</b>
<b>platform ipv6 verify</b>	Configures IPv6 packet verification.
<b>show hardware forwarding ip verify</b>	Displays information about IP packet verification checks.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## 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		
<b>destination zero</b>	Drops IP packets if the destination IPv4 address is 0.0.0.0 or if the IPv6 address is ::..	
<b>identical</b>	Drops IP packets if the source IPv4 or IPv6 address is identical to the destination IPv4 or IPv6 address.	
<b>reserved</b>	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.	
<b>source</b>	Drops IP packets based on the IP source address	
<b>broadcast</b>	Drops IP packets if the IP source address is 255.255.255.255	
<b>multicast</b>	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 enabled.

**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 **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
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

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

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## platform ip verify length

To configure IPv4 packet verification based on packet length, use the **platform ip verify length** command. To return to 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

<b>consistent</b>	Drops IPv4 packets where the Ethernet frame size is greater than or equal to the IP packet length plus the Ethernet header.
<b>maximum</b> { <b>max-frag</b>   <b>max-tcp</b>   <b>udp</b> }	Drops IPv4 packets based on the following: <ul style="list-style-type: none"> <li>• <b>max-frag</b>—Drops IP packets if the maximum fragment offset is greater than 65536.</li> <li>• <b>max-tcp</b>—Drops IP packets if the TCP length is greater than the IP payload length.</li> <li>• <b>udp</b>—Drops IP packets if the IP payload length is less than the UDP packet length.</li> </ul>
<b>minimum</b>	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 enabled.

### 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 **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
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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

<b>length</b>	Drops IPv6 packets based on length.
<b>consistent</b>	Drops IPv6 packets where the Ethernet frame size is greater than or equal to the IPv6 packet length plus the Ethernet header.
<b>maximum {max-frag   max-tcp   udp}</b>	Drops IPv6 packets based on the following: <ul style="list-style-type: none"> <li><b>max-frag</b>—Drops IPv6 packets if the formula (IPv6 Payload Length – IPv6 Extension Header Bytes) + (Fragment Offset * 8) is greater than 65536.</li> <li><b>max-tcp</b>—Drops IPv6 packets if the TCP length is greater than the IP payload length.</li> <li><b>udp</b>—Drops IPv6 packets if the IP payload length is less than the UDP packet length.</li> </ul>
<b>tcp tiny-frag</b>	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.
<b>version</b>	Drops IPv6 packets if the ethertype is not set to 6 (IPv6).

### Defaults

All address tests enabled.

### 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 **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:

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

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

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

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## policy statistics enable (OSPFv3)

To enable Open Shortest Path First version 3 (OSPFv3) policy statistics, use the **policy statistics enable** command. To disable policy statistics, use the **no** form of this command.

**policy statistics enable**

**no policy statistics enable**

**Syntax Description** This command has no keywords or arguments.

**Defaults** Policy statistics are disabled.

**Command Modes** Router configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** Use the **policy statistics enable** command to enable statistics gathering based on route policies applied to this OSPFv3 instance.

This command requires the Enterprise Services license.

**Examples** This example shows how to enable policy statistics gathering on OSPFv3 2:

```
switch(config)# ospfv3 2
switch(config-router)# policy statistics enable
```

Related Commands	Command	Description
	<b>show ospfv3 policy statistics</b>	Shows policy statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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.

**preempt** [**delay minimum** *seconds* | **sync** *seconds*]

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

### Syntax Description

<b>delay minimum</b> <i>seconds</i>	(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.
<b>sync</b> <i>seconds</i>	(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 Administrator  
VDC Administrator

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

This command does not require a license.

### Examples

The following 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

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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		
<b>delay minimum</b> <i>min-delay</i>	(Optional)	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.
<b>reload</b> <i>rel-delay</i>	(Optional)	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.
<b>sync</b> <i>seconds</i>	(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

**SupportedUserRoles** Network administrator  
VDC administrator

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. Note that 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.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## Examples

This example shows how to configure a delay when a router becomes active when its priority 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
<b>feature hsrp</b>	Enables HSRP configuration.
<b>show hsrp</b>	Displays HSRP information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## 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 mode

**SupportedUserRoles** Superuser  
VDC administrator

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:

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**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**

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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**

<b>Syntax Description</b>	<i>level</i>	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.
---------------------------	--------------	--

<b>Defaults</b>	<i>level</i> : 100
-----------------	--------------------

<b>Command Modes</b>	GLBP configuration
----------------------	--------------------

<b>SupportedUserRoles</b>	Network Administrator VDC Administrator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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**

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

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

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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*

**no priority**

<b>Syntax Description</b>	<i>level</i>	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.
---------------------------	--------------	---

<b>Defaults</b>	<i>level</i> : 100
-----------------	--------------------

<b>Command Modes</b>	HSRP configuration or HSRP template mode
----------------------	--

<b>Supported User Roles</b>	Network administrator VDC administrator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>priority</b> 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.
-------------------------	--

<b>Examples</b>	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature hsrp</b>	Enables HSRP configuration.
	<b>show hsrp</b>	Displays HSRP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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** *value*

**no priority**

### Syntax Description

<i>value</i>	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.
--------------	---

### 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 mode

### Supported User Roles

Superuser  
VDC administrator

### Command History

Release	Modification
4.0(1)	This command was introduced.

### 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
```

## ■ priority (VRRP)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

```
switch(config-if-vrrp)# priority 2
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature vrrp</b>	Enables VRRP.
<b>show vrrp</b>	Displays VRRP configuration information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## 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

The following example shows how to disable OSPF 209:

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

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## 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

**SupportedUserRoles** 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
```