P Commands

This chapter describes the Cisco NX-OS Ethernet and virtual Ethernet commands that begin with P.

pinning

To configure pinning options for an interface, use the **pinning** command. To revert to the default settings, use the **no** form of this command.

pinning {**control-vlan** | **packet-vlan**} *sub_group_ID*

no pinning {**control-vlan** | **packet-vlan**}

Syntax Description

control-vlan	Configures pinning for control VLANs.
packet-vlan	Configures pinning for packet VLANs.
sub_group_ID	Sub-group ID. The range is from 0 to 31.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure packet VLAN pinning for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# pinning packet-vlan 5
switch(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the running system configuration information.

pinning id (virtual Ethernet interface)

To pin virtual Ethernet interface traffic to a specific subgroup, use the **pinning id** command. To remove the configuration, use the **no** form of this command.

pinning id *sub-group-id*

no pinning id

Syntax Description

sub-group-id	ID number of the subgroup. The range is from 0 to 31.

Command Default

None

Command Modes

Virtual Ethernet interface configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to pin a virtual Ethernet interface to subgroup 3:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# pinning id 3
switch(config-if)#
```

Related Commands

Command	Description
show interface vethernet	Displays the virtual Ethernet interface configuration information.
show running-config intefrace vethernet	Displays the running configuration information for a specific virtual Ethernet interface, including the pinning configuration.

port

To configure a unified port on a Cisco Nexus 5548UP switch or Cisco Nexus 5596UP switch, use the **port** command. To remove the unified port, use the **no** form of this command.

port *port-number* **type** {**ethernet** | **fc**}

no port *port-number* **type** {**ethernet** | **fc**}

Syntax Description

port-number	Port number. The range is from 1 to 199.
type	Specifies the type of port to configure on a slot in a chassis.
ethernet	Specifies an Ethernet port.
fc	Specifies a Fibre Channel (FC) port.

Command Default

None

Command Modes

Slot configuration mode

Command History

Release	Modification
5.0(3)N1(1)	This command was introduced.

Usage Guidelines

Unified ports allow you to configure ports as Ethernet, native Fibre Channel or Fibre Channel over Ethernet (FCoE) ports. By default, the ports are Ethernet ports but you can change the port mode to Fibre Channel on the following unified ports:

- Any port on the Cisco Nexus 5548UP switch or the Cisco Nexus 5596UP switch.
- The ports on the Cisco N55-M16UP expansion module that is installed in a Cisco Nexus 5548P switch.

You must configure Ethernet ports and FC ports in a specified order:

- FC ports must be configured from the last port of the module.
- Ethernet ports must be configured from the first port of the module.

If the order is not followed, the following errors are displayed:

```
ERROR: Ethernet range starts from first port of the module
ERROR: FC range should end on last port of the module
```

On a Cisco Nexus 5548UP switch, the 32 ports of the main slot (slot1) are unified ports. The Ethernet ports start from port 1/1 to port 1/32. The FC ports start from port 1/32 backwards to port 1/1.

Examples

This example shows how to configure a unified port on a Cisco Nexus 5548UP switch or Cisco Nexus 5596UP switch:

```
switch# configure terminal
```

```
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure a unified port on a Cisco N55-M16UP expansion module:

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure 20 ports as Ethernet ports and 12 as FC ports:

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Related Commands

Command	Description
slot	Enables preprovisioning of features or interfaces of a module on a slot in a chassis.
reload	Reloads the switch and all attached Fabric Extender chassis or a specific Fabric Extender.

port-channel load-balance ethernet

To configure the load-balancing method among the interfaces in the channel-group bundle, use the **port-channel load-balance ethernet** command. To return the system priority to the default value, use the **no** form of this command.

port-channel load-balance ethernet *method* [*hash-polynomial*]

no port-channel load-balance ethernet [*method*]

Syntax Description

method	Load-balancing method. See the "Usage Guidelines" section for a list of valid values.
hash-polynomial	(Optional) Hash polynomial that is used to determine the egress port selected for a port channel. See the "Usage Guidelines" section for a list of valid values. **Note** This is applicable only on a Cisco Nexus 5548 switch and a Cisco Nexus 5596 switch.

Command Default

Loads distribution on the source and destination MAC address.
The default hash polynomial is CRC8a.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.0(3)N2(1)	Support for configurable hash polynomials was added.

Usage Guidelines

The valid load-balancing *method* values are as follows:

- **destination-ip**—Loads distribution on the destination IP address.
- **destination-mac**—Loads distribution on the destination MAC address.
- **destination-port**—Loads distribution on the destination port.
- **source-destination-ip**—Loads distribution on the source and destination IP address.
- **source-destination-mac**—Loads distribution on the source and destination MAC address.
- **source-destination-port**—Loads distribution on the source and destination port.
- **source-ip**—Loads distribution on the source IP address.
- **source-mac**—Loads distribution on the source MAC address.
- **source-port**—Loads distribution on the source port.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in that EtherChannel; using source addresses or IP addresses might result in better load balancing.

Beginning with Cisco NX-OS Release 5.0(3)N2(1), the Cisco Nexus 5548 switch and Cisco Nexus 5596 switch support 8 hash polynomials that can be used for compression on the hash-parameters (software-configurable selection of source and destination MAC addresses, source and destination IP addresses, and source and destination TCP and UDP ports). Depending on variations in the load-balancing method for egress traffic flows from a port channel, different polynomials could provide different load distribution results.

The valid load-balancing *hash-polynomial* values are as follows:

- **CRC8a**—Hash polynomial CRC8a.
- **CRC8b**—Hash polynomial CRC8b.
- **CRC8c**—Hash polynomial CRC8c.
- **CRC8d**—Hash polynomial CRC8d.
- **CRC8e**—Hash polynomial CRC8e.
- **CRC8f**—Hash polynomial CRC8f.
- **CRC8g**—Hash polynomial CRC8g.
- **CRC8h**—Hash polynomial CRC8h.

Note The hash polynomial that you choose affects both the multicast and unicast traffic egressing from all the local port channels. The hash polynomial does not affect the port channels whose member ports are on a Cisco Nexus 2148T Fabric Extender, Cisco Nexus 2232P Fabric Extender, or Cisco Nexus 2248T Fabric Extender.

Examples

This example shows how to set the load-balancing method to use the source IP:

```
switch(config)# port-channel load-balance ethernet source-ip
```

This example shows how to set the load-balancing method to use the source IP and the CRC8c polynomial to hash a flow to obtain a numerical value that can be used to choose the egress physical interface on a Cisco Nexus 5548 switch:

```
switch(config)# port-channel load-balance ethernet source-ip CRC8c
```

Related Commands

Command	Description
show port-channel load-balance	Displays information on EtherChannel load balancing.

private-vlan

To configure private VLANs, use the **private-vlan** command. To return the specified VLANs to normal VLAN mode, use the **no** form of this command.

private-vlan {**isolated** | **community** | **primary**}

no private-vlan {**isolated** | **community** | **primary**}

Syntax Description

isolated	Designates the VLAN as an isolated secondary VLAN.
community	Designates the VLAN as a community secondary VLAN.
primary	Designates the VLAN as the primary VLAN.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must enable private VLANs by using the **feature private-vlan** command before you can configure private VLANs. The commands for configuring private VLANs are not visible until you enable private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. When you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. If you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and are reenabled when you recreate the specified VLAN and configure it as the previous secondary VLAN.

You cannot configure VLAN1 or the internally allocated VLANs as private VLANs.

A private VLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. An isolated VLAN's traffic is blocked on all other private ports in the same VLAN. Its traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

A promiscuous port is defined as a private port that is assigned to a primary VLAN.

A community VLAN is defined as the VLAN that carries the traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

A primary VLAN is defined as the VLAN that is used to convey the traffic from the routers to customer end stations on private ports.

Multiple community and isolated VLANs are allowed. If you enter a range of primary VLANs, the system uses the first number in the range for the association.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

If VLAN Trunking Protocol (VTP) is enabled on a switch, you can configure private VLANs only on a device configured in Transparent mode.

Examples

This example shows how to assign VLAN 5 to a private VLAN as the primary VLAN:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

This example shows how to assign VLAN 100 to a private VLAN as a community VLAN:

```
switch# configure terminal
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

This example shows how to assign VLAN 109 to a private VLAN as an isolated VLAN:

```
switch# configure terminal
switch(config)# vlan 109
switch(config-vlan)# private-vlan isolated
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show vlan	Displays information about VLANs.
show vlan private-vlan	Displays information about private VLANs.

private-vlan association

To configure the association between a primary VLAN and a secondary VLAN on a private VLAN, use the **private-vlan association** command. To remove the association, use the **no** form of this command.

private-vlan association {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}

no private-vlan association

Syntax Description

add	(Optional) Associates a secondary VLAN to a primary VLAN.
secondary-vlan-list	Number of the secondary VLAN.
remove	Clears the association between a secondary VLAN and a primary VLAN.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must enable private VLANs by using the **feature private-vlan** command before you can configure private VLANs. The commands for configuring private VLANs are not visible until you enable private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. However, when you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. However, if you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and return when you recreate the specified VLAN and configure it as the previous secondary VLAN.

The *secondary-vlan-list* argument cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single secondary VLAN ID or a hyphenated range of secondary VLAN IDs. The *secondary-vlan-list* parameter can contain multiple secondary VLAN IDs.

A private VLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

Multiple community and isolated VLANs are allowed. If you enter a range of primary VLANs, the system uses the first number in the range for the association.

Isolated and community VLANs can only be associated with one primary VLAN. You cannot configure a VLAN that is already associated to a primary VLAN as a primary VLAN.

Note A private VLAN-isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1Q encapsulation and cannot be used as a trunk port.

Examples

This example shows how to create a private VLAN relationship between the primary VLAN 14, the isolated VLAN 19, and the community VLANs 20 and 21:

```
switch(config)# vlan 19
switch(config-vlan)# private-vlan isolated
switch(config)# vlan 20
switch(config-vlan)# private-vlan community
switch(config)# vlan 21
switch(config-vlan)# private-vlan community
switch(config)# vlan 14
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 19-21
```

This example shows how to remove isolated VLAN 18 and community VLAN 20 from the private VLAN association:

```
switch(config)# vlan 14
switch(config-vlan)# private-vlan association remove 18,20
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.
show vlan	Displays information about VLANs.
show vlan private-vlan	Displays information about private VLANs.

private-vlan synchronize

To map the secondary VLANs to the same Multiple Spanning Tree (MST) instance as the primary VLAN, use the **private-vlan synchronize** command.

private-vlan synchronize

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

MST configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

If you do not map secondary VLANs to the same MST instance as the associated primary VLAN when you exit the MST configuration mode, the device displays a warning message that lists the secondary VLANs that are not mapped to the same instance as the associated VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples

This example shows how to initialize private VLAN synchronization:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
```

Related Commands

Command	Description
show spanning-tree mst configuration	Displays information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

protocol vmware-vim

To enable the VMware Infrastructure Software Development Kit (VI SDK), use the **protocol vmware-vim** command. To disable the VI SDK, use the **no** form of this command.

protocol vmware-vim

no protocol vmware-vim

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

SVS connection configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

The VMware VI SDK is published by VMware and it allows clients to talk to a vCenter server.

You must first create an SVS connection before you enable the VMware VI SDK.

This command does not require a license.

Examples

This example shows how to enable the VMware VI SDK:

```
switch# configure terminal
switch(config)# svs connection SVSConn
switch(config-svs-conn)# protocol vmware-vim
switch(config-svs-conn)#
```

This example shows how to disable the VMware VI SDK:

```
switch# configure terminal
switch(config)# svs connection SVSConn
switch(config-svs-conn)# no protocol vmware-vim
switch(config-svs-conn)#
```

Related Commands

Command	Description
interface vethernet	Creates a virtual Ethernet interface.
show svs connections	Displays SVS connection information.
svs connection	Enables an SVS connection.

provision

To preprovision a module in a chassis slot, use the **provision** command. To remove a preprovisioned module from a slot, use the **no** form of this command.

provision model *model-name*

no provision model [*model-name*]

Syntax Description

model	Specifies the type of module to be provisioned.
model-name	Module name. The supported modules are as follows: • **N2K-C2148T**—Cisco Nexus 2000 Series Fabric Extender 48x1G 4x10G Module • **N2K-C2232P**—Cisco Nexus 2000 Series Fabric Extender 32x10G Module • **N2K-C2232TM**—Cisco Nexus 2000 Series Fabric Extender 32x10G Module • **N2K-C2248T**—Cisco Nexus 2000 Series Fabric Extender 48x1G 4x10G Module • **N2K-N2224TP**—Cisco Nexus 2000 Series Fabric Extender 24x1G 2x10G SFP+ Module • **N55-M16FP**—Cisco 16 port Port Fiber Channel Expansion Module 16 x SFP • **N55-M16P**—Cisco 16x10-Gigabit Ethernet Expansion Module • **N55-M16UP**—Cisco 16x10-Gigabit Flexible Ethernet Expansion Module • **N55-M8P8FP**—Cisco 8 Port 1/2/4/8-Gigabit Fibre Channel + 8 Port 10-Gigabit Ethernet Expansion Module • **N5K-M1008**—Cisco 8 Port Fiber Channel Expansion Module 8 x SFP • **N5K-M1060**—Cisco 6 Port Fiber Channel Expansion Module 6 x SFP • **N5K-M1404**—Expansion Module 4 x 10GBase-T LAN, 4 x Fiber Channel • **N5K-M1600**—Cisco 6-port 10 Gigabit Ethernet SFP Module 6 x SFP

Command Default

None

Command Modes

Slot configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use this command to define the modules (line card or Cisco Nexus 2000 Series Fabric Extender) to preprovision. If the card type does not match the card in the slot or the module is not compatible with the chassis, you see the following messages:

```
ERROR: The card type does not match the card in slot
```

or

```
ERROR: This module cannot be configured for this chassis
```

You can configure features or interfaces (Ethernet, Fibre Channel) on the modules before the modules are inserted in the switch chassis. You can also use this command to manage the configuration of these features or interfaces when the module is offline due to a failure or scheduled downtime. These configurations are applied when the module comes online.

When you preprovision a module by specifying the type of module, platform manager will allow only modules of matching type to come online. If you configure the interfaces for the module without specifying the module type, the configuration is applied when the module comes online, regardless of the module type.

You can preprovision modules and interfaces in a switch profile. The modules and interfaces are preprovisioned when you apply (commit) the switch profile. Once the module is inserted and interfaces are created, the preprovisioning module passes on the configuration to the respective applications before the interfaces come up.

Mutual exclusion is a mechanism where configuration outside the switch profile is not allowed in the switch profile and vice-versa. This requirement is to ensure that configuration in the switch profile is exactly the same on both switches. Preprovisioned configuration is the same as a configuration when the module is online, so mutual exclusion checks would continue to apply normally.

When you downgrade from Cisco NX-OS release 5.0(2)N1(1), which supports preprovisioning, to an earlier release of Cisco NX-OS that does not support module preprovisioning, you will be prompted to remove preprovisioning configuration that you configured on the switch.

Examples

This example shows how to preprovision a module in slot 2 of the chassis:

```
switch(config)# slot 2
switch(config-slot)# provision model N5K-M1404
switch(config-slot)#
```

This example shows how to configure a switch profile to enable a chassis slot for preprovisioning of a module:

```
switch# config sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# slot 2
switch(config-sync-sp-slot)# provision model N5K-M1600
switch(config-sync-sp-slot)#
```

This example shows how to remove a preprovisioned module from a chassis slot:

```
switch(config)# slot 2
```

```
switch(config-slot)# no provision model N5K-M1404
switch(config-slot)#
```

This example shows how to remove all preprovisioned modules or line cards from a chassis slot:

```
switch(config)# slot 2
switch(config-slot)# no provision model
switch(config-slot)#
```

Related Commands

Command	Description
show module	Displays module information.
show provision	Displays provisioned modules.
show switch-profile	Displays switch profile information.
show running-config exclude-provision	Displays the running configuration excluding the preprovisioned features.
slot	Enables a slot for preprovisioning a module.
switch-profile	Configures a switch profile.