

Send comments to nx5000-docfeedback@cisco.com



CHAPTER 2

Cisco Nexus 5000 Series Ethernet Commands

This chapter describes the Cisco NX-OS Ethernet and virtual Ethernet commands available on Cisco Nexus 5000 Series switches.

Send comments to nx5000-docfeedback@cisco.com

channel-group (Ethernet configuration)

To assign and configure a physical interface to a port channel group, use the **channel-group** command. To remove the channel group configuration from the interface, use the **no** form of this command.

```
channel-group number [mode { active | on | passive}]

no channel-group [number]
```

Syntax Description	<i>number</i>	Number of channel group. The <i>number</i> range is from 1 to 4096. Cisco NX-OS creates the port channel associated with this channel group if the port channel does not already exist.
	mode	(Optional) Specifies the port channel mode of the interface.
	active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. Interface is in active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
	on	This is the default channel mode. All port channels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the switch returns an error message. After you enable LACP globally, by using the feature lacp command, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group. The default mode is on .
	passive	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected. The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.
Command Default	None.	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines

Use this command to create a channel group that includes the interface that you are working on and to add or remove specific interfaces from the channel group. Use this command to move a port from one channel group to another. You enter the channel group that you want the port to move to; the switch automatically removes the specified port from its present channel group and adds it to the specified channel group.

After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either **active** or **passive**. A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. The port channel does not run LACP.

You cannot change the mode for an existing port channel or any of its interfaces if that port channel is not running LACP; the channel mode remains as **on**. The system returns an error message if you attempt to change the mode.

Use the **no** form of this command to remove the physical interface from the port channel. When you delete the last physical interface from a port channel, the port channel remains. To delete the port channel completely, use the **no** form of the **interface port-channel** command.

The compatibility check includes the following operational attributes:

- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- SPAN (cannot be SPAN source or destination port)
- Storm control

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** for static port channels, that is, without a configured aggregation protocol. You can only add interfaces configured with the channel mode as **active** or **passive** to port channels that are running LACP.

You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, Cisco NX-OS suspends that port in the port channel.

When the interface joins a port channel, some of its individual parameters are overridden with the values on the port channel, as follows:

- MAC address
- Spanning Tree Protocol (STP)
- Service policy
- Quality of service (QoS)
- Access control lists (ACLs)

Interface parameters, such as the following, remain unaffected when the interface joins or leaves a port channel:

- Description
- Cisco Discovery Protocol (CDP)
- LACP port priority
- Debounce

Send comments to nx5000-docfeedback@cisco.com

- Rate mode
- Shutdown
- SNMP trap

If interfaces are configured for the port channel interface and a member port is removed from the port channel, the configuration of the port channel interface is not propagated to the member ports.

Any configuration changes that you make in any of the compatibility parameters to the port channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel but are part of the channel group).

Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
switch(config)# interface ethernet 1/1  
switch(config-if)# channel-group 5 mode active
```

Related Commands

Command	Description
show interface port-channel	Displays information about the traffic on the specified port-channel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the port channels.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

clear mac access-list counters

To clear statistical information from the access list, use the **clear mac access-list counters** command.

clear mac access-list counters [*name*]

Syntax Description	<i>name</i> (Optional) Name a specific counter to clear.	
Command Default	None.	
Command Modes	Any command mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
Usage Guidelines	None.	
Examples	This example shows how to clear statistical information from the access list: switch# clear mac access-list counters	
Related Commands	Command	Description
	show mac access-lists	Displays the information about the MAC address table.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

clear mac dynamic

To clear dynamic entries from the forwarding table, use the **clear mac dynamic** command.

clear mac dynamic [**address** *mac_addr*] [**interface** {*type slot/port* | **port-channel** *number*}] [**vlan** *vlan_id*]

Syntax Description

address <i>mac_addr</i>	(Optional) Specifies the MAC address to remove from the table. Use the format EEEE.EEEE.EEEE.
interface <i>type slot/port</i>	(Optional) Specifies the interface for which MAC addresses should be removed from the table. The type can be either ethernet or vethernet. Specify the appropriate slot or virtual interface group number and port number.
port-channel <i>number</i>	(Optional) Specifies the port channel for which MAC addresses should be removed from the table. Use the port channel number.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN from which MAC addresses should be removed from the table. The range of valid values is from 1 to 4094.

Command Default

None.

Command Modes

Any command mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to clear all the dynamic entries from the MAC address table:

```
switch# clear mac dynamic
```

This example shows how to clear a dynamic entry for VLAN 2 from the MAC address table:

```
switch# clear mac dynamic address 001b.2106.58bc vlan 2
```

This example shows how to clear all dynamic entries for a virtual Ethernet from the MAC address table:

```
switch# clear mac dynamic interface vethernet 1/1
```

This example shows how to clear all dynamic entries for VLAN 2 from the MAC address table:

```
switch# clear mac dynamic vlan 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show mac dynamic	Displays the dynamic addresses in the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

clear mac-address-table dynamic

To clear the dynamic address entries from the MAC address table, use the **clear mac-address-table dynamic** command.

```
clear mac-address-table dynamic [[address mac_addr] | [interface {type slot/port | port-channel
number}]] [vlan vlan_id]
```

Syntax Description	address <i>mac_addr</i>	(Optional) Specifies the MAC address to remove from the table. Use the format EEEE.EEEE.EEEE.
	interface <i>type slot/port</i>	(Optional) Specifies the interface for which MAC addresses should be removed from the table. The type can be either ethernet or vethernet. Specify the appropriate slot or virtual interface group number and port number.
	port-channel <i>number</i>	(Optional) Specifies the port channel for which MAC addresses should be removed from the table. Use the port channel number.
	vlan <i>vlan_id</i>	(Optional) Specifies the VLAN from which MAC addresses should be removed from the table. The range of valid values is from 1 to 4094.

Command Default None.

Command Modes Any command mode

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

Usage Guidelines

Use the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

To clear static MAC addresses from the table, use the **no mac-address-table static** command in configuration mode.

If the **clear mac-address-table dynamic** command is entered with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, the switch removes all addresses on the specified interfaces.

Examples

This example shows how to clear all the dynamic entries from the MAC address table:

```
switch# clear mac-address-table dynamic
```

This example shows how to clear all the dynamic entries from the MAC address table for VLAN 2:

```
switch# clear mac-address-table dynamic vlan 2
```


Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show mac-address-table	Displays the information about the MAC address table.

Send comments to nx5000-docfeedback@cisco.com

clear ntp session

To clear the Network Time Protocol (NTP) session, use the **clear ntp session** command.

clear ntp session

Syntax Description	This command has no other arguments or keywords.
---------------------------	--

Command Default	None.
------------------------	-------

Command Modes	Any command mode.
----------------------	-------------------

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

Usage Guidelines	None.
-------------------------	-------

Examples	The following example shows how to discard the NTP CFS distribution session in progress: switch# clear ntp session
-----------------	--

Related Commands	Command	Description
	show ntp	Displays NTP information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

clear ntp statistics

To clear the Network Time Protocol (NTP) session, use the **clear ntp session** command.

clear ntp statistics {all-peers | io | local | memory}

Syntax Description	all-peers	Clears all peer transaction statistics.
	io	Clears I/O statistics.
	local	Clears local statistics.
	memory	Clears memory statistics.

Command Default	None.
------------------------	-------

Command Modes	Any command mode.
----------------------	-------------------

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

Usage Guidelines	None.
-------------------------	-------

Examples	The following example shows how to discard the NTP I/O statistics:
-----------------	--

```
switch# clear ntp statistics io
```

Related Commands	Command	Description
	show ntp	Displays NTP information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

clear spanning-tree counters

To clear the counters for the Spanning Tree Protocol (STP), use the **clear spanning-tree counters** command.

```
clear spanning-tree counters [interface {ethernet interface-num | port-channel channel-num |  
                                vethernet interface-num}] [vlan vlan-id]
```

Syntax Description	interface	(Optional) Specifies the interface type.
	ethernet <i>interface-num</i>	Slot and port number.
	port-channel <i>channel-num</i>	Port-channel number.
	vethernet <i>interface-num</i>	Slot and port number.
	vlan <i>vlan-id</i>	(Optional) Specifies the VLAN. The range is from 1 to 4094.

Command Default	None.
------------------------	-------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	You can clear all the STP counters on the entire switch, per VLAN, or per interface.
-------------------------	--

Examples	This example shows how to clear the STP counters for VLAN 5:
-----------------	--

```
switch# clear spanning-tree counters vlan 5
```

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning tree state.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

clear spanning-tree detected-protocol

To restart the protocol migration, use the **clear spanning-tree detected-protocol** command. With no arguments, the command is applied to every port of the switch.

```
clear spanning-tree detected-protocol [interface {ethernet interface | port-channel channel |  
vethernet interface}]
```

Syntax Description	interface	(Optional) Specifies the interface type.
	ethernet <i>interface</i>	Slot and port number.
	port-channel <i>channel</i>	Port-channel number.
	vethernet <i>interface</i>	Slot and port number.

Command Default	None.
-----------------	-------

Command Modes	Any command mode
---------------	------------------

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

Usage Guidelines

Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a switch running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy device. An MST switch can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region.

These mechanisms are not always able to revert to the most efficient mode. For example, a Rapid PVST+ switch that is designated for a legacy 802.1D bridge stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges to which it is connected have joined the same region.

To force a port to renegotiate with its neighbors, enter the **clear spanning-tree detected-protocol** command.

Examples	This example shows how to restart the protocol migration on a specific interface:
----------	---

```
switch# clear spanning-tree detected-protocol interface ethernet 1/4
```

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

feature interface-vlan

To enable the creation of VLAN interfaces, use the **feature interface-vlan** command. To disable the VLAN interface feature, use the **no** form of this command.

feature interface-vlan

no feature interface-vlan

Syntax Description This command has no arguments or keywords.

Command Default VLAN interfaces are disabled.

Command Modes Configuration mode

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

Usage Guidelines You must use the **feature interface-vlan** or the **svi enable** command before you can create VLAN interfaces.

Examples This example shows how to enable the interface VLAN feature on the switch:

```
switch(config)# feature interface-vlan
```

Related Commands	Command	Description
	interface vlan	Creates a VLAN interface.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

feature lacp

To enable Link Aggregation Control Protocol (LACP), which bundles a number of physical ports together to form a single logical channel, use the **feature lacp** command. To disable LACP on the switch, use the **no** form of this command.

feature lacp

no feature lacp

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

Command Default	LACP is disabled.
------------------------	-------------------

Command Modes	Configuration mode
----------------------	--------------------

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

Usage Guidelines	You must remove all the LACP configuration parameters from all port channels on the switch before you can disable LACP.
	Even after you enable LACP globally, you do not have to run LACP on all port channels on the switch. You enable LACP on each channel mode using the channel-group mode command.

Examples	This example shows how to enable LACP port channeling on the switch:
	<pre>switch(config)# feature lacp</pre>

Related Commands	Command	Description
	show lacp	Displays information on LACP.

Send comments to nx5000-docfeedback@cisco.com

feature private-vlan

To enable private VLANs, use the **feature private-vlan** command. To return to the default settings, use the **no** form of this command.

feature private-vlan

no feature private-vlan

Syntax Description None.

Command Default Private VLANs are disabled.

Command Modes Configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
	4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

Usage Guidelines The private VLAN commands are not available until you enable the private VLAN feature. You cannot disable the private VLANs if there are operational ports on the switch that are in private VLAN mode.



Note

A PVLAN 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 enable private VLAN functionality on the switch:

```
switch(config)# feature private-vlan
```

Related Commands	Command	Description
	private-vlan	Configures a VLAN as either a community, isolated, or primary private VLAN.
	show vlan private-vlan	Displays information on private VLANs. If the feature is not enabled, this command is not available.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

instance vlan

To map a VLAN or a set of VLANs to a Multiple Spanning Tree instance (MSTI), use the **instance vlan** command. To delete the instance and return the VLANs to the default instance (common and internal spanning tree [CIST]), use the **no** form of this command.

instance *instance-id* **vlan** *vlan-id*

no instance *instance-id* [**vlan** *vlan-id*]

Syntax Description

<i>instance-id</i>	Instances to which the specified VLANs are mapped; the range of valid values is from 0 to 4094.
vlan <i>vlan-id</i>	Number of the VLANs that you are mapping to the specified MSTI; the range of valid values is from 1 to 4094.

Command Default

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration mode

Command History

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

Usage Guidelines

The VLAN identifier is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added to or removed from the existing instances.

Any unmapped VLAN is mapped to the CIST instance.



Caution

When you change the VLAN-to-MSTI mapping, the system restarts MST.

Examples

This example shows how to map a range of VLANs to MSTI 4:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 4 vlan 100-200
```

Send comments to nx5000-docfeedback@cisco.com

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

Send comments to nx5000-docfeedback@cisco.com

interface ethernet

To enter interface configuration mode for a 10-Gigabit Ethernet IEEE 802.3 interface, use the **interface ethernet** command.

interface ethernet *slot/port*

Syntax Description	<i>slot</i>	Specifies a slot from 1 to 3. The following list defines the slots available: <ul style="list-style-type: none"> Slot 1 includes all the fixed ports. Slot 2 includes the ports on the upper expansion module (if populated). Slot 3 includes the ports on the lower expansion module (if populated).
	<i>port</i>	Specifies the port number within a particular slot.

Command Default	None.
-----------------	-------

Command Modes	Configuration mode
---------------	--------------------

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

Usage Guidelines	None.
------------------	-------

Examples	<p>This example shows how to enter configuration mode for Ethernet interface 1/4:</p> <pre>switch(config)# interface ethernet 1/4 switch(config-if)#</pre>
----------	---

Related Commands	Command	Description
	interface vethernet	Configures a virtual Ethernet interface.
	show interface ethernet	Displays various parameters of a 10-Gigabit Ethernet IEEE 802.3 interface.

Send comments to nx5000-docfeedback@cisco.com

interface port-channel

To create a port-channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port-channel interface or subinterface, use the **no** form of this command.

```
interface port-channel channel-number

no interface port-channel channel-number
```

Syntax Description	channel-number	Channel number that is assigned to this port-channel logical interface. The range of valid values is from 1 to 4096.
--------------------	----------------	--

Command Default	None.
-----------------	-------

Command Modes	Configuration mode
---------------	--------------------

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

Usage Guidelines	A port can belong to only one channel group.
	When you use the interface port-channel command, follow these guidelines: <ul style="list-style-type: none"> If you are using CDP, you must configure it only on the physical interface and not on the port-channel interface. If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned. The MAC address of the port channel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

Examples	This example shows how to create a port-channel group interface with channel-group number 50:
	<pre>switch(config)# interface port-channel 50 switch(config-if)#</pre>

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show interface port-channel	Displays information on traffic on the specified port-channel interface.
	show lacp	Displays LACP information.
	show port-channel summary	Displays information on the port channels.

Send comments to nx5000-docfeedback@cisco.com

interface vethernet

To enter interface configuration mode for a virtual Ethernet interface, use the **interface vethernet** command.

interface vethernet *vig-num/port*

Syntax Description

<i>vig-num</i>	Specifies the virtual interface group (VIG) number. You must have previously created the VIG.
<i>port</i>	The only valid number for the port is 1.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enter configuration mode for virtual Ethernet interface 16/1:

```
switch(config)# interface vethernet 16/1
switch(config-if)#
```

Related Commands

Command	Description
interface ethernet	Configures a 10-Gigabit Ethernet IEEE 802.3 interface.
show interface vethernet	Displays various parameters of a virtual Ethernet interface.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

ip igmp snooping (EXEC)

To enable Internet Group Management Protocol (IGMP), use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no other arguments or keywords.

Command Default

IGMP snooping is enabled.



Note

If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to enable IGMP snooping:

```
switch# ip igmp snooping
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information and configuration.

Send comments to nx5000-docfeedback@cisco.com

ip igmp snooping (VLAN)

To configure Internet Group Management Protocol (IGMP) on a VLAN, use the **ip igmp snooping** command. To negate the command or return to the default settings, use the **no** form of this command

ip igmp snooping *parameter*

no ip igmp snooping *parameter*

Syntax Description

<i>parameter</i>	Parameter to configure. See the “Usage Guidelines” section for additional information.
------------------	--

Command Default

The default settings are as follows:

- **explicit-tracking**—enabled
- **fast-leave**—disabled for all VLANs
- **last-member-query-interval** *seconds*—1
- **querier** *IP-address*—disabled
- **report-suppression**—enabled

Command Modes

VLAN configuration mode

Command History

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

Usage Guidelines

The valid values for *parameter* are as follows:

Keyword and Argument	Description
explicit-tracking	Enables tracking IGMPv3 membership reports for each port on a per-VLAN basis. The default is enabled on all VLANs.
fast-leave	Enables IGMPv3 snooping fast-leave processing. The default is disabled for all VLANs.
last-member-query-interval <i>seconds</i>	Removes the group if no hosts respond to an IGMP query message. Valid value is from 1 to 25 seconds. The default is 1 second.
mrouter interface <i>interface</i>	Configures a static connection to a multicast router. The specified interface is Ethernet or port channel.
querier <i>IP-address</i>	Configures a snooping querier. The IP address is used as the source in messages. The default is disabled.

Send comments to nx5000-docfeedback@cisco.com

Keyword and Argument	Description
report-suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
static-group <i>group-ip-addr</i> [source <i>source-ip-addr</i>] interface <i>interface</i>	Configures an interface belonging to a VLAN as a static member of a multicast group. The specified interface is Ethernet, port channel, or virtual Ethernet.

Examples

This example shows how to shows configure IGMP snooping parameters for VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface vethernet 4/1
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information and configuration.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

lacp port-priority

To set the priority for the physical interfaces for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command. To return the port priority to the default value, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

<i>priority</i>	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.
-----------------	--

Command Default

System priority value is 32768.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Each port configured to use LACP has an LACP port priority. You can configure a value between 1 and 65535. LACP uses the port priority in combination with the port number to form the port identifier. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put into standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.



Note

When setting the priority, note that a *higher* number means a *lower* priority.

Examples

This example shows how to set the LACP port priority for the interface to 2000:

```
switch(config-if)# lacp port-priority 2000
```

Related Commands

Command	Description
show lacp	Displays LACP information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

lacp system-priority

To set the system priority of the switch for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command. To return the system priority to the default value, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

<i>priority</i>	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.
-----------------	--

Command Default

System priority value is 32768.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

Each device that runs LACP has an LACP system priority value. You can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems.

When setting the priority, note that a *higher* number means a *lower* priority.

Examples

This example shows how to set the LACP system priority for the device to 2500:

```
switch(config)# lacp system-priority 2500
```

Related Commands

Command	Description
show lacp	Displays LACP information.

Send comments to nx5000-docfeedback@cisco.com

mac-address-table aging-time

To configure the aging time for entries in the MAC address table, use the **mac-address-table aging-time** command. To return to the default settings, use the **no** form of this command.

mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

no mac-address-table aging-time [**vlan** *vlan_id*]

Syntax Description	<i>seconds</i>	Specifies the aging time for MAC address table entries. The range is from 0 to 1000000 seconds. The default is 300 seconds. Entering 0 disables MAC address aging.
	vlan <i>vlan_id</i>	(Optional) Specifies the VLAN to which the changed aging time should be applied.

Command Default	300 seconds.
------------------------	--------------

Command Modes	EXEC mode
----------------------	-----------

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

Usage Guidelines

Enter 0 seconds to disable the aging process.

The age value may be rounded off to the nearest multiple of 5 seconds. If the system rounds the value to a different value from that specified by the user (from the rounding process), the system returns an informational message.

When you use this command in EXEC mode, the age values of all VLANs for which a configuration has not been specified are modified and those VLANs with specifically modified aging times are not modified. When you use the **no** form of this command without the VLAN parameter, only those VLANs that have not been specifically configured for the aging time reset to the default value. Those VLANs with specifically modified aging times are not modified.

When you use this command and specify a VLAN, the aging time for only the specified VLAN is modified. When you use the **no** form of this command and specify a VLAN, the aging time for the VLAN is returned to the current global configuration for the aging time, which may or may not be the default value of 300 seconds depending if the global configuration of the switch for aging time has been changed.

Aging time is counted from the last time that the switch detected the MAC address.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to change the length of time an entry remains in the MAC address table to 500 seconds for the entire switch:

```
switch(config)# mac-address-table aging-time 500
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC address table.
show mac-address-table aging-time	Displays information about the MAC address aging time.

Send comments to nx5000-docfeedback@cisco.com

mac-address-table notification

To configure log message notification of MAC address table events, use the **mac-address-table notification** command. To disable log message notifications, use the **no** form of this command.

mac-address-table notification { **mac-move** | **threshold** [**limit** *percentage* **interval** *seconds*] }

no mac-address-table notification { **mac-move** | **threshold** }

Syntax Description

mac-move	Sends a notification message if the MAC address is moved.
threshold	Sends a notification message if the MAC address table threshold is exceeded.
limit <i>percentage</i>	(Optional) Specifies the percentage limit (1 to 100) beyond which threshold notifications are enabled.
interval <i>seconds</i>	(Optional) Specifies the minimum time in seconds (10 to 10000) between two notifications.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

This example shows how to configure log message notification when the threshold exceeds 45 percent, restricting the update interval to once every 1024 seconds:

```
switch(config)# mac-address-table notification threshold limit 45 interval 1024
```

Related Commands

Command	Description
show mac-address-table	Displays information about MAC address table.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

mac-address-table static

To configure a static entry for the MAC address table, use the **mac-address-table static** command. To delete the static entry, use the **no** form of this command.

mac-address-table static *mac_address* **vlan** *vlan_id* { **drop** | **interface** { *type slot/port* | **port-channel** *number* } } [**auto-learn**]

no mac-address-table static *mac_address* { **vlan** *vlan_id* }

Syntax Description

<i>mac_address</i>	Specifies the MAC address to add to the table. Use the format EEEE.EEEE.EEEE.
vlan <i>vlan_id</i>	Specifies the VLAN to apply static MAC address; valid values are from 1 to 4094.
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
interface <i>type slot/port</i>	Specifies the interface. The type can be either ethernet or vethernet. Specify the appropriate slot or virtual interface group number and port number.
port-channel <i>number</i>	Specifies the interface. Use the port channel number.
auto-learn	(Optional) Allows moving of this MAC address.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

You cannot apply the **mac-address-table static** *mac_address* **vlan** *vlan_id* **drop** command to a multicast MAC address.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

Examples

This example shows how to add a static entry to the MAC address table:

```
switch(config)# mac-address-table static 0050.3e8d.6400 vlan 3 interface ethernet 1/4
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	<code>show mac-address-table</code>	Displays information about MAC address table.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

monitor session

Create a new SPAN session configuration or add to an existing session configuration with the **monitor session** command. To clear SPAN sessions, use the **no** form of this command.

monitor session {*number* | **all**} [**suspend**]

no monitor session {*number* | **all**} [**suspend**]

Syntax Description	<i>number</i>	Specifies the SPAN session to create or configure. Select session 1 to 18.
	all	Specifies to apply configuration information to all SPAN sessions.
	suspend	(Optional) Specifies to suspend the referenced SPAN session.

Command Default	None.
-----------------	-------

Command Modes	Configuration mode
---------------	--------------------

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

Usage Guidelines	To ensure that you are working with a completely new session, you can clear the desired session number or all SPAN sessions.
------------------	--

Examples	This example shows how to create a SPAN session: switch# configure terminal switch(config)# monitor session 2
----------	---

Related Commands	Command	Description
	show monitor session	Displays SPAN session configuration information.

Send comments to nx5000-docfeedback@cisco.com

name (VLAN configuration)

To set the name for a VLAN, use the **name** command. To remove the user-configured name from a VLAN, use the **no** form of this command.

name *vlan_name*

no name

Syntax Description	<i>vlan_name</i> Name of the VLAN; you can use up to 32 alphanumeric, case-sensitive characters. The default name is VLANxxxx where xxxx represents four numeric digits (including leading zeroes) equal to the VLAN ID number, for example, VLAN0002.	
Command Default	None.	
Command Modes	VLAN configuration mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
Usage Guidelines	You cannot change the name for the default VLAN, VLAN 1, or for the internally allocated VLANs.	
Examples	This example shows how to name VLAN 2:	
	<pre>switch(config)# vlan 2 switch(config-vlan)# name accounting</pre>	
Related Commands	Command	Description
	show vlan	Displays VLAN information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

name (MST configuration)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

<i>name</i>	Name to assign to the MST region. It can be any string with a maximum length of 32 alphanumeric characters.
-------------	---

Command Default

None.

Command Modes

MST configuration mode

Command History

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

Usage Guidelines

Two or more switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.



Caution

Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the switch in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
```

Related Commands

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

Send comments to nx5000-docfeedback@cisco.com

ntp

To configure the NTP peers and servers for the switch, use the **ntp** command. Use the **no** form of this command to remove configured peers and servers.

ntp {**peer** *hostname* | **server** *hostname*}

no ntp {**peer** *hostname* | **server** *hostname*}

Syntax Description

peer <i>hostname</i>	The hostname or IP address of an NTP peer.
server <i>hostname</i>	The hostname or IP address of the NTP server.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

This example forms a server association with a server:

```
switch(config)# ntp server ntp.cisco.com
```

You can specify multiple associations. This example forms a peer association with a peer:

```
switch(config)# ntp peer 10.20.10.0
```

This example deletes an association with a peer:

```
switch(config)# no ntp peer 10.20.10.0
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

ntp abort

To discard the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress, use the **ntp abort** command.

ntp abort

Syntax Description	This command has no other arguments or keywords.
---------------------------	--

Command Default	None.
------------------------	-------

Command Modes	Configuration mode.
----------------------	---------------------

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

Usage Guidelines	None.
-------------------------	-------

Examples	The following example shows how to discard the NTP CFS distribution session in progress: <pre>switch(config)# ntp abort</pre>
-----------------	--

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

Send comments to nx5000-docfeedback@cisco.com

ntp commit

To apply the pending configuration pertaining to the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ntp commit** command.

ntp commit

Syntax Description This command has no other arguments or keywords.

Command Default None.

Command Modes Configuration mode.

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

Usage Guidelines None.

Examples The following example shows how to commit changes to the active NTP configuration:

```
switch(config)# ntp commit
```

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

Send comments to nx5000-docfeedback@cisco.com

ntp distribute

To enable Cisco Fabric Services (CFS) distribution for Network Time Protocol (NTP), use the **ntp distribute** command. To disable this feature, use the **no** form of the command.

ntp distribute

no ntp distribute

Syntax Description	This command has no other arguments or keywords.
---------------------------	--

Command Default	Disabled.
------------------------	-----------

Command Modes	Configuration mode.
----------------------	---------------------

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

Usage Guidelines	Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the ntp commit command.
-------------------------	--

Examples	The following example shows how to distribute the active NTP configuration to the fabric: <pre>switch(config)# ntp distribute</pre>
-----------------	--

Related Commands	Command	Description
	ntp commit	Commits the NTP configuration changes to the active configuration.
	show ntp	Displays NTP information.

Send comments to nx5000-docfeedback@cisco.com

ntp sync-retry

To retry synchronization with the configured NTP servers, use the **ntp sync-retry** command.

ntp sync-retry

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

Command Default	None.
------------------------	-------

Command Modes	EXEC mode.
----------------------	------------

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

Usage Guidelines	None.
-------------------------	-------

Examples	<p>The following example shows how to retry synchronization with the configured NTP servers:</p> <pre>switch# ntp sync-retry</pre>
-----------------	---

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

port-channel load-balance ethernet

To set 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*

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

Syntax Description

<i>method</i>	Load-balancing method. See the “Usage Guidelines” section for a list of valid values.
---------------	---

Command Default

Loads distribution on the source and destination MAC address.

Command Modes

Configuration mode

Command History

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

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 a port channel is going only to a single MAC address and you use the destination MAC address as the basis of port channel load balancing, the port channel always chooses the same link in that port channel; using source addresses or IP addresses might result in better load balancing.

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
```

Send comments to nx5000-docfeedback@cisco.com

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

Send comments to nx5000-docfeedback@cisco.com

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.
	4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

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.

Send comments to nx5000-docfeedback@cisco.com

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 PVLAN 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 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(config-vlan)# exit
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(config-vlan)# exit
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.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

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.
	<i>secondary_vlan_list</i>	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.

Send comments to nx5000-docfeedback@cisco.com

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 PVLAN 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.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

private-vlan synchronize

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

private-vlan synchronize

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

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 PVLAN 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.

Send comments to nx5000-docfeedback@cisco.com

revision

To set the revision number for the Multiple Spanning Tree (MST) region configuration, use the **revision** command. To return to the default settings, use the **no** form of this command.

revision *version*

no revision *version*

Syntax Description	<i>version</i>	Revision number for the MST region configuration; the range of valid values is from 0 to 65535.
---------------------------	----------------	---

Command Default	Revision 0.
------------------------	-------------

Command Modes	MST configuration mode
----------------------	------------------------

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

Usage Guidelines	Two or more switches with the same VLAN mapping and name are considered to be in different MST regions if the configuration revision numbers are different.
-------------------------	---



Caution

Be careful when using the **revision** command to set the revision number of the MST region configuration because a mistake can put the switch in a different region.

Examples	This example shows how to set the revision number of the MST region configuration:
-----------------	--

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
```

Related Commands	Command	Description
	show spanning-tree mst	Displays information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

shutdown (VLAN configuration)

To shut down the local traffic on a VLAN, use the **shutdown** command. To return a VLAN to its default operational state, use the **no** form of this command.

shutdown

no shutdown

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

Command Default	Not shut down.
------------------------	----------------

Command Modes	VLAN configuration mode
----------------------	-------------------------

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

Usage Guidelines	<p>You cannot shut down, or disable, VLAN 1 or VLANs 1006 to 4094.</p> <p>After you shut down a VLAN, the traffic ceases to flow on that VLAN. Access ports on that VLAN are also brought down; trunk ports continue to carry traffic for the other VLANs allowed on that port. However, the interface associations for the specified VLAN remain, and when you reenables, or recreates, that specified VLAN, the switch automatically reinstates all the original ports to that VLAN.</p>
-------------------------	--

To find out if a VLAN has been shut down internally, check the Status field in the **show vlan** command output. If a VLAN is shut down internally, one of these values appears in the Status field:

- act/lshut—VLAN status is active and shut down internally.
- sus/lshut—VLAN status is suspended and shut down internally.



Note

If the VLAN is suspended and shut down, you use both the **no shutdown** and **state active** commands to return the VLAN to the active state.

Examples	<p>This example shows how to restore local traffic on VLAN 2 after you have shut down, or disabled, the VLAN:</p>
-----------------	---

```
switch(config)# vlan 2
switch(config-vlan)# no shutdown
```

 shutdown (VLAN configuration)

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree bpdudfilter

To enable BPDU Filtering on the interface, use the **spanning-tree bpdudfilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdudfilter {enable | disable}

no spanning-tree bpdudfilter

Syntax Description	enable	Enables BPDU Filtering on this interface.
	disable	Disables BPDU Filtering on this interface.

Command Default The setting that is already configured when you enter the **spanning-tree port type edge bpdudfilter default** command.

Command Modes Interface configuration mode

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

Usage Guidelines Entering the **spanning-tree bpdudfilter enable** command to enable BPDU Filtering overrides the spanning tree edge port configuration. That port then returns to the normal spanning tree port type and moves through the normal spanning tree transitions.



Caution

Be careful when you enter the **spanning-tree bpdudfilter enable** command on specified interfaces. Explicitly configuring BPDU Filtering on a port this is not connected to a host can cause a bridging loop because the port will ignore any BPDU that it receives, and the port moves to the STP forwarding state.

Use the **spanning-tree port type edge bpdudfilter default** command to enable BPDU Filtering on all spanning tree edge ports.

Examples This example shows how to explicitly enable BPDU Filtering on the Ethernet spanning tree edge port 1/4:

```
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdudfilter enable
```

This example shows how to explicitly enable BPDU Filtering on a virtual Ethernet interface:

```
switch (config)# interface vethernet 4/1
switch(config-if)# spanning-tree bpdudfilter enable
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree bpduguard

To enable BPDU Guard on an interface, use the **spanning-tree bpduguard** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard {enable | disable}

no spanning-tree bpduguard

Syntax Description	enable	Enables BPDU Guard on this interface.
	disable	Disables BPDU Guard on this interface.

Command Default The setting that is already configured when you enter the **spanning-tree port type edge bpduguard default** command.

Command Modes Interface configuration mode

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

Usage Guidelines BPDU Guard prevents a port from receiving BPDUs. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure.



Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When you enable this BPDU Guard command globally, the command applies only to spanning tree edge ports. See **spanning-tree port type edge bpduguard default** for more information on the global command for BPDU Guard. However, when you enable this feature on an interface, it applies to that interface regardless of the spanning tree port type.

This command has three states:

- **spanning-tree bpduguard enable**—Unconditionally enables BPDU Guard on the interface.
- **spanning-tree bpduguard disable**—Unconditionally disables BPDU Guard on the interface.
- **no spanning-tree bpduguard**—Enables BPDU Guard on the interface if it is an operational spanning tree edge port and if the **spanning-tree port type edge bpduguard default** command is configured.

Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to enable BPDU Guard on this interface:

```
switch(config-if)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree [**vlan** *vlan_id*] **cost** { *value* | **auto** }

no spanning-tree [**vlan** *vlan_id*] **cost**

Syntax Description		
vlan <i>vlan_id</i>	(Optional) Lists the VLANs on this trunk interface for which you want to assign the path cost. You do not use this parameter on access ports. The range is from 1 to 4094.	
<i>value</i>	Value of the port cost. The available cost range depends on the path-cost calculation method as follows:	
	<ul style="list-style-type: none"> short—The range is 1 to 65536. long—The range is 1 to 200,000,000. 	
auto	Sets the value of the port cost by the media speed of the interface (see to Table 2-1 for the values).	

Command Default	Port cost is set by the media speed.
------------------------	--------------------------------------

Command Modes	Interface configuration mode
----------------------	------------------------------

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

Usage Guidelines

The STP port path cost default value is determined from the media speed and path cost calculation method of a LAN interface (see [Table 2-1](#)). See the **spanning-tree pathcost method** command for information on setting the path cost calculation method for Rapid PVST+.

Table 2-1 Default Port Cost

Bandwidth	Short Path Cost Method Port Cost	Long Path Cost Method Port Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1-Gigabit Ethernet	4	20,000
10-Gigabit Ethernet	2	2,000

When you configure the *value*, higher values will indicate higher costs.

On access ports, assign the port cost by port. On trunk ports, assign the port cost by VLAN; you can configure all the VLANs on a trunk port as the same port cost.

Send comments to nx5000-docfeedback@cisco.com

The port channel bundle is considered a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.



Note

Use this command to set the port cost for Rapid PVST+. Use the **spanning-tree mst cost** command to set the port cost for MST.

Examples

This example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN that is associated with that interface:

```
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree cost 250
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree configuration.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree guard

To enable or disable Loop Guard or Root Guard, use the **spanning-tree guard** command. To return to the default settings, use the **no** form of this command.

spanning-tree guard {loop | none | root}

no spanning-tree guard

Syntax Description	loop	Enables Loop Guard on the interface.
	none	Sets the guard mode to none.
	root	Enables Root Guard on the interface.

Command Default	Disabled.
-----------------	-----------

Command Modes	Interface configuration mode
---------------	------------------------------

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

Usage Guidelines	You cannot enable Loop Guard if Root Guard is enabled, although the switch accepts the command to enable Loop Guard on spanning tree edge ports .
------------------	--

Examples	This example shows how to enable Root Guard: switch(config-if)# spanning-tree guard root
----------	--

Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command. To return to the default settings, use the **no** form of this command.

spanning-tree link-type { **auto** | **point-to-point** | **shared** }

no spanning-tree link-type

Syntax Description

auto	Sets the link type based on the duplex setting of the interface.
point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type set automatically based on the duplex setting.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Fast transition (specified in IEEE 802.1w) functions only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.



Note

On a Cisco Nexus 5000 Series switch, port duplex is not configurable.

Examples

This example shows how to configure the port as a shared link:

```
switch(config-if) # spanning-tree link-type shared
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning tree state.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree loopguard default

To enable Loop Guard as a default on all spanning tree normal and network ports, use the **spanning-tree loopguard default** command. To disable Loop Guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description	This command has no additional arguments or keywords.
---------------------------	---

Command Default	Disabled.
------------------------	-----------

Command Modes	Configuration mode
----------------------	--------------------

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

Usage Guidelines	Loop Guard provides additional security in the bridge network. Loop Guard prevents alternate or root ports from becoming the designated port because of a failure that could lead to a unidirectional link.
	Loop Guard operates only on ports that are considered point-to-point links by the spanning tree, and it does not run on spanning tree edge ports.
	Entering the Loop Guard command, spanning-tree guard loop , for the specified interface overrides this global Loop Guard command.

Examples	This example shows how to enable Loop Guard:
	<pre>switch(config)# spanning-tree loopguard default</pre>

Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mode

To switch between Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) Spanning Tree Protocol (STP) modes, use the **spanning-tree mode** command. To return to the default settings, use the **no** form of this command.

spanning-tree mode {rapid-pvst | mst}

no spanning-tree mode


Syntax Description	rapid-pvst	Sets the STP mode to Rapid PVST+.
	mst	Sets the STP mode to MST.

Command Default	Rapid PVST+.
-----------------	--------------

Command Modes	Configuration mode
---------------	--------------------

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

Usage Guidelines	You cannot simultaneously run MST and Rapid PVST+ on the switch.
------------------	--


Caution

Be careful when using the **spanning-tree mode** command to switch between Rapid PVST+ and MST modes. When you enter the command, all STP instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause the user traffic to be disrupted.

Examples	<p>This example shows how to switch to MST mode:</p> <pre>switch(config)# spanning-tree mode mst switch(config-mst)#</pre>
----------	---

Related Commands	Command	Description
	show spanning-tree summary	Displays the information about the spanning tree configuration.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst configuration

To enter the Multiple Spanning Tree (MST) configuration mode, use the **spanning-tree mst configuration** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no keywords or arguments.

Command Default

The default value for the MST configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping—See the [instance vlan](#) command.
- Region name—See the [name \(MST configuration\)](#) command.
- Configuration revision number—See the [revision](#) command.

The **abort** and **exit** commands allow you to exit MST configuration mode. The difference between the two commands depends on whether you want to save your changes or not:

- The **exit** command commits all the changes before leaving MST configuration mode.
- The **abort** command leaves MST configuration mode without committing any changes.

If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST configuration mode, the following warning message is displayed:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

See the [switchport mode private-vlan host](#) command to fix this problem.

Changing an MST configuration mode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST configuration mode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the **exit** keyword.

Send comments to nx5000-docfeedback@cisco.com

In the unlikely event that two administrators commit a new configuration at exactly the same time, this warning message is displayed:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration mode:

```
switch(config)# spanning-tree mst configuration
switch(config-mst)#
```

This example shows how to reset the MST configuration (name, instance mapping, and revision number) to the default settings:

```
switch(config)# no spanning-tree mst configuration
```

Related Commands

Command	Description
instance vlan	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst cost

To set the path-cost parameter for any Multiple Spanning Tree (MST) instance (including the common and internal spanning tree [CIST] with instance ID 0) use the **spanning-tree mst cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance_id* **cost** {*cost* | **auto**}

no spanning-tree mst *instance_id* **cost**

Syntax Description

<i>instance_id</i>	Instance ID number; the range of valid values is from 0 to 4094.
<i>cost</i>	Port cost for an instance; the range of valid values is from 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface.

Command Default

Automatically set port cost values:

- 10 Mbps—2,000,000
- 100 Mbps—200,000
- 1-Gigabit Ethernet—20,000
- 10-Gigabit Ethernet—2,000

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

The port cost depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.

Higher cost values indicate higher costs. When entering the cost, do not include a comma in the entry; for example, enter 1000, not 1,000.

The port-channel bundle is considered a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.

Examples

This example shows how to set the interface path cost:

```
switch(config-if)# spanning-tree mst 0 cost 17031970
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the switch, use the **spanning-tree mst forward-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description	<i>seconds</i> Number of seconds to set the forward-delay timer for all the instances on the switch; the range of valid values is from 4 to 30 seconds.					
Command Default	15 seconds.					
Command Modes	Configuration mode					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification					
4.0(0)N1(1a)	This command was introduced.					
Usage Guidelines	None.					
Examples	<p>This example shows how to set the forward-delay timer:</p> <pre>switch(config)# spanning-tree mst forward-time 20</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show spanning-tree mst</td><td>Displays the information about the MST protocol.</td></tr></table>		Command	Description	show spanning-tree mst	Displays the information about the MST protocol.
Command	Description					
show spanning-tree mst	Displays the information about the MST protocol.					

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the switch, use the **spanning-tree mst hello-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description	<i>seconds</i> Number of seconds to set the hello-time delay timer for all the instances on the switch; the range of valid values is from 1 to 10 seconds.	
Command Default	2 seconds.	
Command Modes	Configuration mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
Usage Guidelines	If you do not specify the <i>hello-time</i> value, the value is calculated from the network diameter.	
Examples	This example shows how to set the hello-time delay timer:	
	<pre>switch(config)# spanning-tree mst hello-time 3</pre>	
Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst max-age

To set the max-age timer for all the instances on the switch, use the **spanning-tree mst max-age** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description	<i>seconds</i> Number of seconds to set the max-age timer for all the instances on the switch; the range of valid values is from 6 to 40 seconds.					
Command Default	20 seconds.					
Command Modes	Configuration mode					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification					
4.0(0)N1(1a)	This command was introduced.					
Usage Guidelines	<p>This parameter is used only by Instance 0 or the IST.</p> <p>This command does not require a license.</p>					
Examples	<p>This example shows how to set the max-age timer:</p> <pre>switch(config)# spanning-tree mst max-age 40</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show spanning-tree mst</td><td>Displays the information about the MST protocol.</td></tr></table>		Command	Description	show spanning-tree mst	Displays the information about the MST protocol.
Command	Description					
show spanning-tree mst	Displays the information about the MST protocol.					

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hop_count*

no spanning-tree mst max-hops

Syntax Description	<i>hop_count</i> Number of possible hops in the region before a BPDU is discarded; the range of valid values is from 1 to 255 hops.					
Command Default	20 hops.					
Command Modes	Configuration mode					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification					
4.0(0)N1(1a)	This command was introduced.					
Usage Guidelines	None.					
Examples	<p>This example shows how to set the number of possible hops:</p> <pre>switch(config)# spanning-tree mst max-hops 25</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show spanning-tree mst</td><td>Displays the information about the MST protocol.</td></tr></table>		Command	Description	show spanning-tree mst	Displays the information about the MST protocol.
Command	Description					
show spanning-tree mst	Displays the information about the MST protocol.					

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst port-priority

To set the port-priority parameters for any Multiple Spanning Tree (MST) instance, including the common and internal spanning tree (CIST) with instance ID 0, use the **spanning-tree mst port-priority** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance_id* **port-priority** *priority*

no spanning-tree mst *instance_id* **port-priority**

Syntax Description

<i>instance_id</i>	Instance ID number; valid values are from 0 to 4094.
<i>priority</i>	Port priority for an instance; the range of valid values is from 0 to 224 in increments of 32.

Command Default

Port priority value is 128.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Higher **port-priority** *priority* values indicate smaller priorities.

The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected.

Examples

This example shows how to set the interface priority:

```
switch(config-if)# spanning-tree mst 0 port-priority 64
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Configures port priority for default STP, which is Rapid PVST+.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst priority

To set the bridge priority, use the **spanning-tree mst priority** command. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance_id* **priority** *priority_value*

no spanning-tree mst *instance_id* **priority**

Syntax Description	<i>instance_id</i>	Instance identification number; the range of valid values is from 0 to 4094.
	<i>priority_value</i>	Bridge priority; see the “Usage Guidelines” section for valid values and additional information.

Command Default	Bridge priority default is 32768.
------------------------	-----------------------------------

Command Modes	Configuration mode
----------------------	--------------------

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

Usage Guidelines	You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
	You can set the <i>priority_value</i> argument to 0 to make the switch root.
	You can enter the <i>instance_id</i> argument as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples	This example shows how to set the bridge priority:
	switch(config)# spanning-tree mst 0 priority 4096

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst root

To designate the primary and secondary root and set the timer value for an instance, use the **spanning-tree mst root** command. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst instance_id root {primary | secondary} [diameter dia [hello-time
hello_time]]
```

```
no spanning-tree mst instance_id root
```

Syntax Description

<i>instance_id</i>	Instance identification number; the range of valid values is from 0 to 4094.
primary	Specifies the high priority (low value) that is high enough to make the bridge root of the spanning-tree instance.
secondary	Specifies the switch as a secondary root, should the primary root fail.
diameter <i>dia</i>	(Optional) Specifies the timer values for the bridge that are based on the network diameter.
hello-time <i>hello_time</i>	(Optional) Specifies the duration between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds; the default is 2 seconds.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

You can enter the *instance_id* argument as a single instance or a range of instances, for example, 0-3,5,7-9.

If you do not specify the **hello-time** argument, the argument is calculated from the network diameter. You must first specify the **diameter** *dia* keyword and argument before you can specify the **hello-time** *hello_time* keyword and argument.

Examples

This example shows how to designate the primary root:

```
switch(config)# spanning-tree mst 0 root primary
```

This example shows how to set the priority and timer values for the bridge:

```
switch(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree mst simulate pvst

To reenable specific interfaces to automatically interoperate between Multiple Spanning Tree (MST) and Rapid per VLAN Spanning Tree (Rapid PVST+), use the **spanning-tree mst simulate pvst** command. To prevent specific MST interfaces from automatically interoperating with a connecting device running Rapid PVST+, use the **spanning-tree mst simulate pvst disable** command. To return specific interfaces to the default settings that are set globally for the switch, use the **no** form of this command.

spanning-tree mst simulate pvst

spanning-tree mst simulate pvst disable

no spanning-tree mst simulate pvst

Syntax Description This command has no keywords or arguments.

Command Default Enabled. By default, all interfaces on the switch interoperate seamlessly between MST and Rapid PVST+. See [spanning-tree mst simulate pvst global](#) to change this setting globally.

Command Modes Interface configuration mode

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

Usage Guidelines MST interoperates with Rapid PVST+ with no need for user configuration. The PVST simulation feature enables this seamless interoperability. However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a Rapid PVST+-enabled port.

When you use the **spanning-tree mst simulate pvst disable** command, specified MST interfaces that receive a Rapid PVST+ (SSTP) BPDU move into the STP blocking state. Those interfaces remain in the inconsistent state until the port stops receiving Rapid PVST+ BPDUs, and then the port resumes the normal STP transition process.



Note To block automatic MST and Rapid PVST+ interoperability for the entire switch, use **no spanning-tree mst simulate pvst global** command.

This command is useful when you want to prevent accidental connection with a device running Rapid PVST+.

To reenable seamless operation between MST and Rapid PVST+ on specific interfaces, use the **spanning-tree mst simulate pvst** command.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to prevent specified ports from automatically interoperating with a connected device running Rapid PVST+:

```
switch(config-if)# spanning-tree mst simulate pvst disable
```

Related Commands

Command	Description
spanning-tree mst simulate pvst global	Enables global seamless interoperation between MST and Rapid PVST+.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree mst simulate pvst global

To prevent the Multiple Spanning Tree (MST) switch from automatically interoperating with a connecting device running Rapid per VLAN Spanning Tree (Rapid PVST+), use the **no spanning-tree mst simulate pvst global** command. To return to the default settings, which is seamless operation between MST and Rapid PVST+ on the switch, use the **spanning-tree mst simulate pvst global** command.

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description This command has no keywords or arguments.

Command Default Enabled. By default, the switch interoperates seamlessly between MST and Rapid PVST+.

Command Modes
Configuration mode
Interface configuration mode

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

Usage Guidelines MST does not require user configuration to interoperate with Rapid PVST+. The PVST simulation feature enables this seamless interoperability. However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a Rapid PVST+-enabled port.

When you use the **no spanning-tree mst simulate pvst global** command, the switch running in MST mode moves all interfaces that receive a Rapid PVST+ (SSTP) bridge protocol data unit (BPDU) into the Spanning Tree Protocol (STP) blocking state. Those interfaces remain in the inconsistent state until the port stops receiving Rapid PVST+ BPDUs, and then the port resumes the normal STP transition process.

You can also use this command from the interface mode, and the configuration applies to the entire switch.



Note To block automatic MST and Rapid PVST+ interoperability for specific interfaces, see the [spanning-tree mst simulate pvst](#) command.

This command is useful when you want to prevent accidental connection with a device not running MST. To return the switch to seamless operation between MST and Rapid PVST+, use the **spanning-tree mst simulate pvst global** command.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to prevent all ports on the switch from automatically interoperating with a connected device running Rapid PVST+:

```
switch(config)# no spanning-tree mst simulate pvst global
```

Related Commands

Command	Description
spanning-tree mst simulate pvst	Enables seamless interoperation between MST and Rapid PVST+ by the interface.


[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

Syntax Description	long	Specifies the 32-bit based values for port path costs.
	short	Specifies the 16-bit based values for port path costs.
Command Default	Short.	
Command Modes	Configuration mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
Usage Guidelines	The long path-cost calculation method uses all 32 bits for path-cost calculations and yields values in the range of 2 through 2,00,000,000.	
	The short path-cost calculation method (16 bits) yields values in the range of 1 through 65535.	
 Note	This command applies only to the Rapid PVST+ spanning tree mode, which is the default mode. When you are using MST spanning tree mode, the switch uses only the long method for calculating path cost; this is not user-configurable for MST.	
Examples	This example shows how to set the default pathcost method to long: <pre>switch(config)# spanning-tree pathcost method long</pre>	
Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge

To configure an interface connected to a host as an edge port, which automatically transitions the port to the spanning tree forwarding state without passing through the blocking or learning states, use the **spanning-tree port type edge** command. To return the port to a normal spanning tree port, use the **spanning-tree port type normal** command or the **no spanning-tree port type** command.

- spanning-tree port type edge [trunk]**
- spanning-tree port type normal**
- no spanning-tree port type**


Syntax Description	trunk (Optional) Configures the trunk port as a spanning tree edge port.
--------------------	---

Command Default	The default is the global setting for the default port type edge that is configured when you entered the spanning-tree port type edge default command. If you did not configure a global setting, the default spanning tree port type is normal.
-----------------	---

Command Modes	Interface configuration mode
---------------	------------------------------

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


Usage Guidelines	You can also use this command to configure a port in trunk mode as a spanning tree edge port.
------------------	---



Caution

You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When linkup occurs, spanning tree edge ports are moved directly to the spanning tree forwarding state without waiting for the standard forward-time delay.



Note

This is the same functionality that was previously provided by the Cisco-proprietary PortFast feature.

When you use this command, the system returns a message similar to the following:

```
Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

Send comments to nx5000-docfeedback@cisco.com

When you use this command without the **trunk** keyword, the system returns an additional message similar to the following:

```
%Portfast has been configured on Ethernet1/40 but will only  
have effect when the interface is in a non-trunking mode.
```

To configure trunk interfaces as spanning tree edge ports, use the **spanning-tree port type trunk** command. To remove the spanning tree edge port type setting, use the **spanning-tree port type normal** command.

The default spanning tree port type is normal.

Examples

This example shows how to configure an interface connected to a host as an edge port, which automatically transitions that interface to the forwarding state on linkup:

```
switch(config-if)# spanning-tree port type edge
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge bpdupfilter default

To enable BPDU Filtering by default on all spanning tree edge ports, use the **spanning-tree port type edge bpdupfilter default** command. To disable BPDU Filtering by default on all edge ports, use the **no** form of this command.

```
spanning-tree port type edge bpdupfilter default

no spanning-tree port type edge bpdupfilter default
```


Syntax Description	This command has no keywords or arguments.				
Command Default	Disabled.				
Command Modes	Configuration mode				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification				
4.0(0)N1(1a)	This command was introduced.				

Usage Guidelines

To enable BPDU Filtering by default, you must do the following:

- Configure the interface as a spanning tree edge port, using the **spanning-tree port type edge** or the **spanning-tree port type edge default** command.
- Enable BPDU Filtering.


Use this command to enable BPDU Filtering globally on all spanning tree edge ports. BPDU Filtering prevents a port from sending or receiving any BPDUs.



Caution

Be cautious when using this command; incorrect usage can cause bridging loops.

You can override the global effects of this **spanning-tree port type edge bpdupfilter default** command by configuring BPDU Filtering at the interface level. See the **spanning-tree bpdupfilter** command for complete information on using this feature at the interface level.



Note

The BPDU Filtering feature’s functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU Filtering is applied only on ports that are operational spanning tree edge ports. Ports send a few BPDUs at a linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, that port immediately becomes a normal spanning tree port with all the normal transitions and BPDU Filtering is disabled. When enabled locally on a port, BPDU Filtering prevents the switch from receiving or sending BPDUs on this port.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to enable BPDU Filtering globally on all spanning tree edge operational ports by default:

```
switch(config)# spanning-tree port type edge bpdudfilter default
```

Related Commands

Command	Description
<code>show spanning-tree summary</code>	Displays the information about the spanning tree configuration.
<code>spanning-tree bpdudfilter</code>	Enables BPDU Filtering on the interface.
<code>spanning-tree port type edge</code>	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge bpduguard default

To enable BPDU Guard by default on all spanning tree edge ports, use the **spanning-tree port type edge bpduguard default** command. To disable BPDU Guard on all edge ports by default, use the **no** form of this command.

spanning-tree port type edge bpduguard default
no spanning-tree port type edge bpduguard default

Syntax Description This command has no keywords or arguments.

Command Default Disabled.

Command Modes Configuration mode

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

Usage Guidelines


To enable BPDU Guard by default, you must do the following:

- Configure the interface as spanning tree edge ports by entering the **spanning-tree port type edge** or the **spanning-tree port type edge default** command.
- Enable BPDU Guard.

Use this command to enable BPDU Guard globally on all spanning tree edge ports. BPDU Guard disables a port if it receives a BPDU.

Global BPDU Guard is applied only on spanning tree edge ports.

You can also enable BPDU Guard per interface; see **spanning-tree bpduguard** command for more information.


Note

We recommend that you enable BPDU Guard on all spanning tree edge ports.

Examples

This example shows how to enable BPDU Guard by default on all spanning tree edge ports:

```
switch(config)# spanning-tree port type edge bpduguard default
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	<code>show spanning-tree summary</code>	Displays the information about the spanning tree configuration.
	<code>spanning-tree bpduguard</code>	Enables BPDU guard on the interface.
	<code>spanning-tree port type edge</code>	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type edge default

To configure all access ports that are connected to hosts as edge ports by default, use the **spanning-tree port type edge default** command. To restore all ports connected to hosts as normal spanning tree ports by default, use the **no** form of this command.

spanning-tree port type edge default

no spanning-tree port type edge default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

Use this command to automatically configure all interfaces as spanning tree edge ports by default. This command will not work on trunk ports.



Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

When a linkup occurs, an interface configured as an edge port automatically moves the interface directly to the spanning tree forwarding state without waiting for the standard forward-time delay. (This transition was previously configured as the Cisco-proprietary PortFast feature.)

When you use this command, the system returns a message similar to the following:

```
Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.
```

You can configure individual interfaces as edge ports using the **spanning-tree port type edge** command. The default spanning tree port type is normal.

Examples

This example shows how to globally configure all ports connected to hosts as spanning tree edge ports:

```
switch(config)# spanning-tree port type edge default
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree configuration.
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type network

To configure the interface that connects to a switch as a network spanning tree port, regardless of the global configuration, use the **spanning-tree port type network** command. To return the port to a normal spanning tree port, use the **spanning-tree port type normal** command or use the **no** form of this command.

spanning-tree port type network

spanning-tree port type normal

no spanning-tree port type

Syntax Description

This command has no arguments or keywords.

Command Default

The default is the global setting for the default port type network that is configured when you entered the **spanning-tree port type network default** command. If you did not configure a global setting, the default spanning tree port type is normal.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to configure an interface that connects to a switch as a spanning tree network port. Bridge Assurance runs only on Spanning Tree Protocol (STP) network ports.



Note

If you mistakenly configure ports connected to hosts as STP network ports and enable Bridge Assurance, those ports will automatically move into the blocking state.



Note

Bridge Assurance is enabled by default, and all interfaces configured as spanning tree network ports have Bridge Assurance enabled.

To configure a port as a spanning tree network port, use the **spanning-tree port type network** command. To remove this configuration, use the **spanning-tree port type normal** command. When you use the **no spanning-tree port type** command, the software returns the port to the global default setting for network port types.

You can configure all ports that are connected to switches as spanning tree network ports by default by entering the **spanning-tree port type network default** command.

The default spanning tree port type is normal.

Send comments to nx5000-docfeedback@cisco.com

Examples

This example shows how to configure an interface connected to a switch or bridge as a spanning tree network port:

```
switch(config-if)# spanning-tree port type network
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning tree configuration per specified interface.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port type network default

To configure all ports as spanning tree network ports by default, use the **spanning-tree port type network default** command. To restore all ports to normal spanning tree ports by default, use the **no** form of this command.

- spanning-tree port type network default**
- no spanning-tree port type network default**

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Configuration mode

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

Usage Guidelines Use this command to automatically configure all interfaces that are connected to switches as spanning tree network ports by default. You can then use the **spanning-tree port type edge** command to configure specified ports that are connected to hosts as spanning-tree edge ports.



Note If you mistakenly configure ports connected to hosts as Spanning Tree Protocol (STP) network ports and Bridge Assurance is enabled, those ports will automatically move into the blocking state.

Configure only the ports that connect to other switches as network ports because the Bridge Assurance feature causes network ports that are connected to hosts to move into the spanning tree blocking state. You can identify individual interfaces as network ports by using the **spanning-tree port type network** command. The default spanning tree port type is normal.

Examples This example shows how to globally configure all ports connected to switches as spanning tree network ports:

```
switch(config)# spanning-tree port type network default
```


Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show spanning-tree summary	Displays information about the spanning tree configuration.

Send comments to nx5000-docfeedback@cisco.com

spanning-tree port-priority

To set an interface priority when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To return to the default settings, use the **no** form of this command.

spanning-tree [**vlan** *vlan_id*] **port-priority** *value*

no spanning-tree [**vlan** *vlan_id*] **port-priority**

Syntax Description	vlan <i>vlan_id</i>	(Optional) Specifies the VLAN identification number; the range of valid values is from 0 to 4094.
	<i>value</i>	Port priority; valid values are from 1 to 224 in increments of 32.

Command Default Port priority default value is 128.

Command Modes Interface configuration mode

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

Usage Guidelines Do not use the **vlan** *vlan_id* parameter on access ports. The software uses the port priority value for access ports and the VLAN port priority values for trunk ports.

The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected.



Note

Use this command to configure the port priority for Rapid PVST+ spanning tree mode, which is the default STP mode. To configure the port priority for MST spanning tree mode, use the **spacing-tree mst port-priority** command.

Examples This example shows how to increase the probability that the spanning tree instance on access port interface 2/0 is chosen as the root bridge by changing the port priority to 32:

```
switch(config-if)# spanning-tree port-priority 32
```

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning tree state.
	spanning-tree interface priority	Displays information on the spanning tree port priority for the interface.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

spanning-tree vlan

To configure Spanning Tree Protocol (STP) parameters on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan_id* [**forward-time** *value* | **hello-time** *value* | **max-age** *value* | **priority** *value* | [**root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *value*]]]]

no spanning-tree vlan *vlan_id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description	
<i>vlan_id</i>	VLAN identification number; the range of valid values is from 0 to 4094.
forward-time <i>value</i>	(Optional) Specifies the STP forward-delay time; the range of valid values is from 4 to 30 seconds.
hello-time <i>value</i>	(Optional) Specifies the number of seconds between the generation of configuration messages by the root switch; the range of valid values is from 1 to 10 seconds.
max-age <i>value</i>	(Optional) Specifies the maximum number of seconds that the information in a bridge protocol data unit (BPDU) is valid; the range of valid values is from 6 to 40 seconds.
priority <i>value</i>	(Optional) Specifies the STP-bridge priority; the valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Forces this switch to be the root switch if the primary root fails.
diameter <i>dia</i>	(Optional) Specifies the maximum number of bridges between any two points of attachment between end stations.

Command Default The defaults are as follows:

- **forward-time**—15 seconds
- **hello-time**—2 seconds
- **max-age**—20 seconds
- **priority**—32768

Command Modes Configuration mode

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

Send comments to nx5000-docfeedback@cisco.com

Usage Guidelines



Caution

When disabling spanning tree on a VLAN using the **no spanning-tree vlan *vlan_id*** command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.



Caution

We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When setting the **max-age *seconds***, if a bridge does not see BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** alters this switch's bridge priority to 24576. If you enter the **spanning-tree root primary** command and the switch does not become the root, then the bridge priority is changed to 4096 less than the bridge priority of the current bridge. The command fails if the value required to be the root bridge is less than 1. If the switch does not become the root, an error results.

If the network devices are set for the default bridge priority of 32768 and you enter the **spanning-tree root secondary** command, the software alters this switch's bridge priority to 28762. If the root switch fails, this switch becomes the next root switch.

Use the **spanning-tree root** commands on the backbone switches only.

Examples

This example shows how to enable spanning tree on VLAN 200:

```
switch(config)# spanning-tree vlan 200
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning tree state.

Send comments to nx5000-docfeedback@cisco.com

state

To set the operational state for a VLAN, use the **state** command. To return a VLAN to its default operational state, use the **no** form of this command.

state {active | suspend}

no state

Syntax Description

active	Specifies that the VLAN is actively passing traffic.
suspend	Specifies that the VLAN is not passing any packets.

Command Default

The VLAN is actively passing traffic.

Command Modes

VLAN configuration mode

Command History

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

Usage Guidelines

You cannot suspend the state for VLAN 1 or VLANs 1006 to 4094.
VLANs in the suspended state do not pass packets.

Examples

This example shows how to suspend VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)# state suspend
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

svi enable

To enable the creation of VLAN interfaces, use the **svi enable** command. To disable the VLAN interface feature, use the **no** form of this command.

svi enable

no svi enable

Syntax Description This command has no arguments or keywords.

Command Default VLAN interfaces are disabled.

Command Modes Configuration mode

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

Usage Guidelines You must use the **feature interface-vlan** or the **svi enable** command before you can create VLAN interfaces.

Examples This example shows how to enable the interface VLAN feature on the switch:

```
switch(config)# svi enable
```

Related Commands	Command	Description
	interface vlan	Creates a VLAN interface.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

switchport access vlan

To set the access VLAN when the interface is in access mode, use the **switchport access vlan** command. To reset the access-mode VLAN to the appropriate default VLAN for the switch, use the **no** form of this command.

switchport access vlan *vlan_id*

no switchport access vlan

Syntax Description	<i>vlan_id</i>	VLAN to set when the interface is in access mode; valid values are from 1 to 4094, except for the VLANs reserved for internal use.
---------------------------	----------------	--

Command Default	VLAN 1.
------------------------	---------

Command Modes	Interface configuration mode
----------------------	------------------------------

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

Usage Guidelines	Use the no form of the switchport access vlan command to reset the access-mode VLAN to the appropriate default VLAN for the switch. This action may generate messages on the device to which the port is connected.
-------------------------	---

Examples	This example shows how to configure an Ethernet interface to join VLAN 2:
-----------------	---

```
switch(config)# interface ethernet 1/7
switch(config-if)# switchport access vlan 2
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a port.

Send comments to nx5000-docfeedback@cisco.com

switchport block

To prevent the unknown multicast or unicast packets from being forwarded, use the **switchport block** interface configuration command. To allow the unknown multicast or unicast packets to be forwarded, use the **no** form of this command.

switchport block {multicast | unicast}

no switchport block {multicast | unicast}

Syntax Description

multicast	Specifies that the unknown multicast traffic should be blocked.
unicast	Specifies that the unknown unicast traffic should be blocked.

Command Default

Unknown multicast and unicast traffic are not blocked. All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can block the unknown multicast or unicast traffic on the switch ports.

Blocking the unknown multicast or unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.

Examples

This example shows how to block the unknown multicast traffic on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport block multicast
```

Related Commands

Command	Description
show interface switchport	Displays the switch port information for a specified interface or all interfaces.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

switchport mode private-vlan host

To set the interface type to be a host port for a private VLAN, use the **switchport mode private-vlan host** command.

switchport mode private-vlan host

Syntax Description	This command has no additional keywords or arguments.
---------------------------	---

Command Default	None.
------------------------	-------

Command Modes	Interface configuration mode
----------------------	------------------------------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
	4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

Usage Guidelines	<p>When you configure a port as a host private VLAN port and one of the following applies, the port becomes inactive:</p> <ul style="list-style-type: none">• The port does not have a valid private VLAN association configured.• The port is a Switched Port Analyzer (SPAN) destination.• The private VLAN association is suspended. <p>If you delete a private VLAN port association, or if you configure a private port as a SPAN destination, the deleted private VLAN port association or the private port that is configured as a SPAN destination, that port becomes inactive.</p>
-------------------------	---

**Note**

We recommend that you enable spanning tree BPDU Guard on all private VLAN host ports.

Examples	This example shows how to set a port to host mode for private VLANs:
-----------------	--

```
switch(config-if)# switchport mode private-vlan host
```

Related Commands	Command	Description
	show interface switchport	Displays information on all interfaces configured as switch ports.

Send comments to nx5000-docfeedback@cisco.com

switchport mode private-vlan promiscuous

To set the interface type to be a promiscuous port for a private VLAN, use the **switchport mode private-vlan promiscuous** command.

switchport mode private-vlan promiscuous

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes Interface configuration mode

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

Usage Guidelines When you configure a port as a promiscuous private VLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid private VLAN mapping configured.
- The port is a Switched Port Analyzer (SPAN) destination.

If you delete a private VLAN port mapping or if you configure a private port as a SPAN destination, the deleted private VLAN port mapping or the private port that is configured as a SPAN destination becomes inactive.

See the [private-vlan](#) command for more information on promiscuous ports.

Examples This example shows how to set a port to promiscuous mode for private VLANs:

```
switch(config-if)# switchport mode private-vlan promiscuous
```

Related Commands	Command	Description
	show interface switchport	Displays information on all interfaces configured as switch ports.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

switchport private-vlan host-association

To define a private VLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the private VLAN association from the port, use the **no** form of this command.

switchport private-vlan host-association {*primary_vlan_id*} {*secondary_vlan_id*}

no switchport private-vlan host-association

Syntax Description

<i>primary_vlan_id</i>	Number of the primary VLAN of the private VLAN relationship.
<i>secondary_vlan_id</i>	Number of the secondary VLAN of the private VLAN relationship.

Command Default

None.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(0)N1(2)	Support for configuring a virtual Ethernet port as a host port for a private VLAN was enabled.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-host mode. If the port is in private VLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive. The port also may be inactive when the association between the private VLANs is suspended.

The secondary VLAN may be an isolated or community VLAN.

See the [private-vlan](#) command for more information on primary VLANs, secondary VLANs, and isolated or community ports.



Note

A PVLAN 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 configure a Layer 2 host private VLAN port with a primary VLAN (VLAN 18) and a secondary VLAN (VLAN 20):

```
switch(config-if)# switchport private-vlan host-association 18 20
```

This example shows how to remove the private VLAN association from the port:

```
switch(config-if)# no switchport private-vlan host-association
```

 switchport private-vlan host-association

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show vlan private-vlan	Displays information on private VLANs.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

switchport private-vlan mapping

To define the private VLAN association for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

```
switchport private-vlan mapping {primary_vlan_id} {[add] secondary_vlan_id | remove
secondary_vlan_id}
```

```
no switchport private-vlan mapping
```

Syntax Description

<i>primary_vlan_id</i>	Number of the primary VLAN of the private VLAN relationship.
add	(Optional) Associates the secondary VLANs to the primary VLAN.
<i>secondary_vlan_id</i>	Number of the secondary VLAN of the private VLAN relationship.
remove	Clears the association between the secondary VLANs and the primary VLAN.

Command Default

None.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-promiscuous mode. If the port is in private VLAN-promiscuous mode but the primary VLAN does not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

See the [private-vlan](#) command for more information on primary VLANs, secondary VLANs, and isolated or community ports.



Note

A PVLAN 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 configure the associate primary VLAN 18 to secondary isolated VLAN 20 on a private VLAN promiscuous port:

```
switch(config-if)# switchport private-vlan mapping 18 20
```

This example shows how to add a VLAN to the association on the promiscuous port:

```
switch(config-if)# switchport private-vlan mapping 18 add 21
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to remove the all private VLAN association from the port:

```
switch(config-if)# no switchport private-vlan mapping
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
show interface private-vlan mapping	Displays the information about the private VLAN mapping for VLAN interfaces, or SVIs.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

vlan (EXEC mode)

To add a VLAN or to enter the VLAN configuration mode, use the **vlan** command. To delete the VLAN and exit the VLAN configuration mode, use the **no** form of this command.

vlan {*vlan_id* | *vlan_range*}

no vlan {*vlan_id* | *vlan_range*}

Syntax Description	<i>vlan_id</i>	Number of the VLAN; the range of valid values is from 1 to 4094.
	Note	You cannot create, delete, or modify VLAN 1 or any of the internally allocated VLANs.
	<i>vlan_range</i>	Range of configured VLANs; see the “Usage Guidelines” section for a list of valid values.

Command Default None.

Command Modes Configuration mode



Note

You can also create and delete VLANs in the VLAN configuration mode using these same commands.

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

Usage Guidelines When you enter the **vlan** *vlan_id* command, a new VLAN is created with all default parameters and causes the CLI to enter VLAN configuration mode. If the *vlan_id* argument that you entered matches an existing VLAN, nothing happens except that you enter VLAN configuration mode.

You can enter the *vlan_range* using a comma (,), a dash (-), and the number.

VLAN 1 parameters are factory configured and cannot be changed; you cannot create or delete this VLAN. Additionally, you cannot create or delete VLAN 4095 or any of the internally allocated VLANs.

When you delete a VLAN, all the access ports in that VLAN are shut down and no traffic flows. On trunk ports, the traffic continues to flow for the other VLANs allowed on that port, but the packets for the deleted VLAN are dropped. However, the system retains all the VLAN-to-port mapping for that VLAN, and when you reenables, or recreate, that specified VLAN, the switch automatically reinstates all the original ports to that VLAN.

Examples This example shows how to add a new VLAN and enter VLAN configuration mode:

```
switch(config)# vlan 2
switch(config-vlan)#
```

Send comments to nx5000-docfeedback@cisco.com

This example shows how to add a range of new VLANs and enter VLAN configuration mode:

```
switch(config)# vlan 2,5,10-12,20,25,4000  
switch(config-vlan)#
```

This example shows how to delete a VLAN:

```
switch(config)# no vlan 2
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Send comments to nx5000-docfeedback@cisco.com

vrf context

To create a virtual routing and forwarding instance (VRF) and enter VRF configuration mode, use the **vrf context** command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description	<i>name</i>	Name of the VRF.
	management	Specifies a configurable VRF name.

Command Default	None.
-----------------	-------

Command Modes	Configuration mode
---------------	--------------------

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

Usage Guidelines	When you enter the VRF configuration mode, the following commands are available:
	<ul style="list-style-type: none">• exit—Exits from the current command mode.• ip—Enables configuration of IP features. <p>Additional commands available in IP configuration mode:</p> <ul style="list-style-type: none">– domain-list—Adds additional domain names.– domain-lookup—Enables or disables DNS lookup.– domain-name—Specifies the default domain name.– host—Adds an entry to the IP hostname table– name-server—Specifies the IP address of a DNS name server– route—Adds route information by specifying IP addresses of the next hop servers. <ul style="list-style-type: none">• no—Negates a command or set its defaults.• shutdown—Shuts down the current VRF context.

Examples	This example shows how to enter VRF context mode:
----------	---

```
switch(config)# vrf context management
switch(config-vrf)#
```

Send comments to nx5000-docfeedback@cisco.com

Related Commands	Command	Description
	show vrf	Displays VRF information.