S Commands

- shut (ERSPAN), on page 3
- shutdown, on page 4
- shutdown (virtual Ethernet interface), on page 6
- slot, on page 7
- snmp-server enable traps vtp, on page 9
- source (SPAN, ERSPAN), on page 10
- spanning-tree bpdufilter, on page 13
- spanning-tree bpduguard, on page 15
- spanning-tree bridge assurance, on page 17
- spanning-tree cost, on page 18
- spanning-tree domain, on page 20
- spanning-tree guard, on page 21
- spanning-tree link-type, on page 22
- spanning-tree loopguard default, on page 23
- spanning-tree mode, on page 24
- spanning-tree mst configuration, on page 25
- spanning-tree mst cost, on page 27
- spanning-tree mst forward-time, on page 28
- spanning-tree mst hello-time, on page 29
- spanning-tree mst max-age, on page 30
- spanning-tree mst max-hops, on page 31
- spanning-tree mst port-priority, on page 32
- spanning-tree mst pre-standard, on page 33
- spanning-tree mst priority, on page 34
- spanning-tree mst root, on page 35
- spanning-tree mst simulate pvst, on page 36
- spanning-tree mst simulate pvst global, on page 38
- spanning-tree pathcost method, on page 40
- spanning-tree port type edge, on page 41
- spanning-tree port type edge bpduguard default, on page 43
- spanning-tree port type edge bpdufilter default, on page 45
- spanning-tree port type edge default, on page 47
- spanning-tree port type network, on page 49

- spanning-tree port type network default, on page 51
- spanning-tree port type normal, on page 52
- spanning-tree vlan port-priority, on page 53
- spanning-tree vlan cost, on page 54
- spanning-tree vlan, on page 55
- spanning-tree pseudo-information, on page 57
- spanning-tree port-priority, on page 58
- speed (interface), on page 59
- state, on page 61
- svs veth auto-setup, on page 62
- svi enable, on page 63
- svs veth auto-delete, on page 64
- svs connection, on page 65
- switchport private-vlan trunk allowed vlan, on page 66
- switchport port-security violation, on page 68
- switchport private-vlan host-association, on page 69
- switchport private-vlan association trunk, on page 71
- switchport priority extend, on page 72
- switchport monitor rate-limit, on page 74
- switchport port-security maximum, on page 75
- switchport port-security mac-address, on page 77
- switchport port-security aging, on page 79
- switchport port-security, on page 80
- switchport mode private-vlan host, on page 81
- switchport mode private-vlan trunk, on page 83
- switchport mode private-vlan promiscuous, on page 84
- switchport access vlan, on page 85
- switchport mode, on page 87
- switchport host, on page 89
- switchport block, on page 90
- switchport backup interface, on page 92
- system vlan reserve, on page 95
- system private-vlan fex trunk, on page 96
- switchport private-vlan mapping, on page 97
- switchport private-vlan trunk native, on page 100
- switchport trunk allowed vlan, on page 101
- switchport trunk native vlan, on page 103
- switchport voice vlan, on page 104

shut (ERSPAN)

To shut down an Encapsulated Remote Switched Port Analyzer (ERSPAN) or an Ethernet Switched Port Analyzer (SPAN) session, use the **shut** command. To enable an ERSPAN or SPAN session, use the **no** form of this command.

shut
no shut

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

ERSPAN session configuration mode

network-adminvdc-admin

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to shut down an ERSPAN session:

```
switch#configureterminal
switch(config)#monitor session 1 type erspan-source
switch(config-erspan-src)#shut
switch(config-erspan-src)#
```

This example shows how to enable an ERSPAN session:

```
switch#configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)#no shut
switch(config-erspan-src)#
```

Related Commands

Command	Description
monitor session	Enters the monitor configuration mode.
show monitor session	Displays the virtual SPAN or ERSPAN configuration.

shutdown

To shut down the local traffic on an interface, use the **shutdown** command. To return the interface 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

Interface configuration mode

Subinterface configuration mode

Virtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.0(3)N1(1)	Support for Layer 3 interfaces and subinterfaces, and virtual Ethernet interface was added.
5.1(3)N1(1)	Support for virtual Ethernet interface was added.

Usage Guidelines

You can use this command on the following interfaces:

- Layer 2 interface (Ethernet interface, EtherChannel interface, subinterface)
- Layer 3 interface

Note Use the **no switchport** command to configure an interface as a Layer 3 interface.

- Layer 3 subinterface
- Management interface
- Virtual Ethernet interface

Examples

This example shows how to shut down, or disable, a Layer 2 interface:

```
switch(config)#interface ethernet 1/10
switch(config-if)# shutdown
switch(config-if)#
```

This example shows how to shut down a Layer 3 Ethernet subinterface:

```
switch(config)# interface ethernet 1/5.1
switch(config-subif)# shutdown
switch(config-subif)#
```

This example shows how to shut down a virtual Ethernet interface:

```
switch(config)# interface vethernet 10
switch(config-if)# shutdown
switch(config-if)#
```

Related Commands

Command	Description
no switchport	Converts an interface to a Layer 3 routed interface.
show interface ethernet	Displays the Ethernet interface configuration information.
show interface port-channel	Displays information on traffic about the specified EtherChannel interface.
show interface vethernet	Displays the virtual Ethernet interface configuration information.

shutdown (virtual Ethernet interface)

To shut down the local traffic on a virtual Ethernet interface, use the **shutdown** command. To return a virtual Ethernet interface 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

Virtual Ethernet interface configuration mode

Command History

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

Examples

This example shows how to shut down, or disable, a virtual Ethernet interface:

```
switch#
configure terminal
switch(config)# interface vethernet 10
switch(config-if)# shutdown
switch(config-if)#
```

Related Commands

Command	Description
show interface vethernet	Displays the virtual Ethernet interface configuration information.

slot

To enable preprovisioning on a slot in a chassis, use the **slot** command. To disable the slot for preprovisioning, use the **no** form of this command.

slot *slot-number*
no slot *slot-number*

Syntax Description

slot-number	Slot number in the chassis. The range is from 2 to 199.

Command Default

None

Command Modes

Global configuration mode

Configuration synchronization mode

Command History

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

Usage Guidelines

Use this command to enable preprovisioning of features or interfaces of a module on a slot in a chassis. Preprovisioning allows you configure features or interfaces (Ethernet, Fibre Channel) on modules before the modules are inserted in the switch chassis.

Examples

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

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

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

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

This example shows how to disable a chassis slot for preprovisioning of a module:

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

Related Commands

Command	Description
port	Configures ports as Ethernet, native Fibre Channel or Fibre Channel over Ethernet (FCoE) ports.

Command	Description
provision	Preprovisions a module in a slot.
show running-config exclude-provision	Displays the running configuration excluding the preprovisioned features.

snmp-server enable traps vtp

To enable the Simple Network Management Protocol (SNMP) notifications for a VLAN Trunking Protocol (VTP) domain, use the **snmp-server enable traps vtp** command. To disable SNMP notifications on a VTP domain, use the **no** form of this command.

snmp-server enable traps vtp
no snmp-server enable traps vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

Examples

This example shows how to enable SNMP notifications on a VTP domain:

```
switch(config)# snmp-server enable traps vtp
switch(config)#
```

This example shows how to disable all SNMP notifications on a VTP domain:

```
switch(config)# no snmp-server enable traps vtp
switch(config)#
```

Related Commands

Command	Description
show snmp trap	Displays the SNMP notifications enabled or disabled.
show vtp status	Displays VTP information.

source (SPAN, ERSPAN)

To add an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) source port, use the **source** command. To remove the source SPAN or ERSPAN port, use the **no** form of this command.

source {**interface** {**ethernet** *slot* /[*QSFP-module* /] *port*|**port-channel** *channel-num*|**vethernet** *veth-num*} [{**both**|**rx**|**tx**}]|**vlan** *vlan-num*|**vsan** *vsan-num*}
no source {**interface** {**ethernet** *slot* /[*QSFP-module* /] *port*|**port-channel** *channel-num*|**vethernet** *veth-num*} [{**both**|**rx**|**tx**}]|**vlan** *vlan-num*|**vsan** *vsan-num*}

Syntax Description

interface	Specifies the interface type to use as the source SPAN port.
ethernet *slot /port*	Specifies the Ethernet interface to use as the source SPAN port. The slot number is from 1 to 255 and the port number is from 1 to 128.
port-channel *channel-num*	Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
vethernet *veth-num*	Specifies the virtual Ethernet interface to use as the source SPAN or ERSPAN port. The virtual Ethernet interface number is from 1 to 1048575.
both	(Optional) Specifies both ingress and egress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
rx	(Optional)Specifies only ingress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
tx	(Optional) Specifies only egress traffic on the source port. **Note** This keyword applies to the ERSPAN source port.
vlan *vlan-num*	Specifies the VLAN inteface to use as the source SPAN port. The range is from 1 to 3967 and 4048 to 4093.
vsan *vsan-num*	Specifies the virtual storage area network (VSAN) to use as the source SPAN port. The range is from 1 to 4093.

Command Default

None

Command Modes

SPAN session configuration mode

ERSPAN session configuration mode

Command History

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

Release	Modification
5.0(2)N1(1)	Port Channel and SAN Port Channel interfaces can be configured as ingress or egress source ports. The limit on the number of egress (TX) sources in a monitor session has been lifted.
5.1(3)N1(1)	Support for a virtual Ethernet interface and ERSPAN was added.

Usage Guidelines

A source port (also called a *monitored port*) is a switched port that you monitor for network traffic analysis. In a single local SPAN session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both).

A source port can be an Ethernet port, port channel, SAN port channel, VLAN, or a VSAN port. It cannot be a destination port.

Note For Cisco NX-OS Release 4.2(1)N2(1) and earlier, the Cisco Nexus 5010 Switch and the Cisco Nexus 5020 Switch supports a maximum of two egress SPAN source ports.

Beginning with Cisco NX-OS Release 5.0(2)N2(1):

- There is no limit to the number of egress SPAN source ports.
- SAN Port Channel interfaces can be configured as ingress or egress source ports.
- The limit on the number of egress (TX) sources in a monitor session has been lifted.
- Port-channel interfaces can be configured as egress sources.

For ERSPAN, if you do not specify **both**, **rx**, or **tx**, the source traffic is analyzed for both directions.

Examples

This example shows how to configure an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 9 type local
switch(config-monitor)# description A Local SPAN session
switch(config-monitor)# source interface ethernet 1/1
switch(config-monitor)#
```

This example shows how to configure a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 5

switch(config-monitor)#
```

This example shows how to configure an ERSPAN source port to receive traffic on the port:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# source interface ethernet 1/5 rx
switch(config-erspan-src)#
```

Related Commands

Command	Description
destination (SPAN, ERSPAN)	Configures a destination SPAN port.
monitor session	Creates a new SPAN session configuration.
show monitor session	Displays SPAN session configuration information.
show running-config monitor	Displays the running configuration information of a SPAN session.

spanning-tree bpdufilter

To enable bridge protocol data unit (BPDU) Filtering on the interface, use the **spanning-tree bpdufilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {**enable**|**disable**}
no spanning-tree bpdufilter

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 bpdufilter 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 bpdufilter 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 bpdufilter 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 bpdufilter 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 bpdufilter 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 bpdufilter enable
```

Related Commands

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

spanning-tree bpduguard

To enable bridge protocol data unit (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 bpdufilter 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 the **spanning-tree port type edge bpdufilter default** command 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**—E nables BPDU Guard on the interface if it is an operational spanning tree edge port and if the **spanning-tree port type edge bpdufilter 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.

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.

spanning-tree bridge assurance

To enable Spanning Tree Protocol (STP) Bridge Assurance on all network ports on the switch, use the **spanning-tree bridge assurance** command. To disable Bridge Assurance, use the **no** form of this command.

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You can use Bridge Assurance to protect against certain problems that can cause bridging loops in the network.

Note Bridge Assurance is supported only by Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST). Legacy 802.1D spanning tree does not support Bridge Assurance.

Bridge Assurance is enabled by default and can only be disabled globally.

Bridge Assurance is enabled globally by default but is disabled on an interface by default. You can enable Bridge Assurance on an interface by using the **spanning-tree port type network** command.

For more information on Bridge Assurance, see the Cisco Nexus 5000 Series *NX-OS Layer 2 Switching Configuration Guide* .

This command does not require a license.

Examples

This example shows how to enable Bridge Assurance globally on the switch:

```
switch# configure terminal
switch(config)# spanning-tree bridge assurance
switch(config)#
```

Related Commands

Command	Description
show spanning-tree bridge	Displays the status and configuration of the local Spanning Tree Protocol (STP) bridge.
spanning-tree port type network	Configures an interface as a network spanning tree port.

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 *vlan-id*	(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.
value	Value of the port cost. The available cost range depends on the path-cost calculation method as follows: • short—The range is from 1 to 65536. • long—The range is from 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface (refer the table below, Default Port Cost, 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 the table below on Default Port Cost). See the **spanning-tree pathcost method** command for information on setting the path cost calculation method for Rapid per VLAN Spanning Tree Plus (Rapid PVST+).

Table 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.

The EtherChannel bundle is considered as 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.

spanning-tree domain

To configure a Spanning Tree Protocol (STP) domain, use the **spanning-tree domain** command. To remove an STP domain, use the **no** form of this command.

spanning-tree domain *domain-num*
no spanning-tree domain *domain-num*

Syntax Description

domain-num	STP domain number. The range is from 1 to 1023.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a spanning-tree domain:

```
switch# configure terminal
switch(config)# spanning-tree domain 1
switch(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays the configuration information of the Spanning Tree Protocol (STP).

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.

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.

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 arguments or keywords.

Command Default

Disabled

Command Modes

Global 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 **spanning-tree guard loop** command for the specified interface overrides this global Loop Guard command.

Examples

This example shows how to enable Loop Guard:

```
switch(config)# spanning-tree loopguard default
```

Related Commands

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

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

Global 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

This example shows how to switch to MST mode:

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

Related Commands

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

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 arguments or keywords.

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 Common and Internal Spanning Tree (CIST) instance.
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global 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.

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.

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

instance-id	Instance ID number. The range is from 0 to 4094.
cost	Port cost for an instance. The range 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 EtherChannel bundle is considered as 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
```

Related Commands

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

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

seconds	Number of seconds to set the forward-delay timer for all the instances on the switch. The range is from 4 to 30 seconds.

Command Default

15 seconds

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set the forward-delay timer:

```
switch(config)# spanning-tree mst forward-time 20
```

Related Commands

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

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

seconds	Number of seconds to set the hello-time delay timer for all the instances on the switch. The range is from 1 to 10 seconds.

Command Default

2 seconds

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the hello-time delay timer:

```
switch(config)# spanning-tree mst hello-time 3
```

Related Commands

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

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

seconds	Number of seconds to set the max-age timer for all the instances on the switch. The range is from 6 to 40 seconds.

Command Default

20 seconds

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This parameter is used only by Instance 0 or the IST.

Examples

This example shows how to set the max-age timer:

```
switch(config)# spanning-tree mst max-age 40
```

Related Commands

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

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

hop-count	Number of possible hops in the region before a BPDU is discarded. The range is from 1 to 255 hops.

Command Default

20 hops

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to set the number of possible hops:

```
switch(config)# spanning-tree mst max-hops 25
```

Related Commands

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

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

instance-id	Instance ID number. The range is from 0 to 4094.
priority	Port priority for an instance. The range 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 the port priority for the default STP, which is Rapid PVST+.

spanning-tree mst pre-standard

To force a prestandard Multiple Spanning Tree (MST) bridge protocol data unit (BPDU) transmission on an interface port, use the **spanning-tree mst pre-standard** command. To revert to the defaults, use the **no** form of this command.

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to force a prestandard MST BPDU transmission on port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# spanning-tree mst pre-standard
switch(config-if)#
```

Related Commands

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

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

instance-id	Instance identification number. The range is from 0 to 4094.
priority-value	Bridge priority. See the "Usage Guidelines" section for valid values and additional information.

Command Default

Bridge priority default is 32768.

Command Modes

Global 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 *priority-value* argument to 0 to make the switch root.

You can enter the *instance-id* 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.

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

instance-id	Instance identification number. The range 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, if the primary root fails.
diameter *dia*	(Optional) Specifies the timer values for the bridge that are based on the network diameter .
hello-time *hello-time*	(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

Global 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
```

Related Commands

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

spanning-tree mst simulate pvst

To reenable specific interfaces to automatically interoperate between Multiple Spanning Tree (MST) and Rapid per VLAN Spanning Tree Plus (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 arguments or keywords.

Command Default

Enabled. By default, all interfaces on the switch interoperate seamlessly between MST and Rapid PVST+. See the **spanning-tree mst simulate pvst global** command 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) bridge protocol data unit (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.

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+.

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 Plus (Rapid PVST+), use the **spanning-tree mst simulate pvst global** command. To return to the default settings, which is a seamless operation between MST and Rapid PVST+ on the switch, use the **no 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 arguments or keywords.

Command Default

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

Command Modes

Global 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.

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.

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

Global 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 valued 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 per VLAN Spanning Tree Plus (Rapid PVST+) spanning tree mode, which is the default mode. When you are using Multiple Spanning Tree (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:

```
switch(config)#
spanning-tree pathcost method long
```

Related Commands

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

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 **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 a 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
```

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 **no 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 a linkup:

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

Related Commands

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

spanning-tree port type edge bpduguard default

To enable bridge protocol data unit (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 arguments or keywords.

Command Default

Disabled

Command Modes

Global 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 the **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
```

Related Commands

Command	Description
show spanning-tree summary	Displays the information about the spanning tree configuration.
spanning-tree bpduguard	Enables BPDU guard on the interface.

Command	Description
spanning-tree port type edge	Configures an interface as a spanning tree edge port.

spanning-tree port type edge bpdufilter default

To enable bridge protocol data unit (BPDU) Filtering by default on all spanning tree edge ports, use the **spanning-tree port type edge bpdufilter default** command. To disable BPDU Filtering by default on all edge ports, use the **no** form of this command.

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

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Notification
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 bpdufilter default** command by configuring BPDU Filtering at the interface level. See the **spanning-tree bpdufilter** 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.

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 bpdufilter default
```

Related Commands

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

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

Global 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
```

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.

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 mode

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 **no 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.

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.

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

Global 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
```

Related Commands

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

spanning-tree port type normal

To configure an interface as a normal spanning tree port, use the **spanning-tree port type normal** command. To revert to the default settings, use the **no** command.

spanning-tree port type normal
no spanning-tree port type normal

Syntax Description

This command has no arguments or keywords.

Command Default

Default spanning tree port type is normal.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an interface as a normal port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# spanning-tree port type normal
switch(config-if)#
```

Related Commands

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

spanning-tree vlan port-priority

To change the spanning tree port priority of an interface, use the **spanning-tree vlan port-priority** command. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* **port-priority** *port_priority_value*
no spanning-tree vlan *vlan-id* **port-priority** *port_priority_value*

Syntax Description

vlan-id	VLAN identification number. The VLAN ID range is from 0 to 4094.
port_priority_value	Port priority. The range is from 0 to 224 in increments of 32.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to change the spanning tree port priority of an interface to 20:

```
switch#
configure terminal
switch(config)#
interface ethernet 1/5
switch(config-if)#
spanning-tree vlan 5 port-priority 20
switch(config-if)#
```

This example shows how to revert the interface to the default configuration:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no spanning-tree vlan 5 port-priority 20
switch(config-if)#
```

Related Commands

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

spanning-tree vlan cost

To change the spanning tree port path-cost of an interface, use the **spanning-tree vlan cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* **cost** {*port_path_cost*|**auto**}
no spanning-tree vlan *vlan-id* **cost** {*port_path_cost*|**auto**}

Syntax Description

vlan-id	VLAN identification number. The VLAN ID range is from 0 to 4094.
port_path_cost	Port path cost. The range is from 1 to 200,000,000.
auto	Determines the cost based on the media speed of this interface.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to change the spanning tree port path cost of an interface:

```
switch#
configure terminal
switch(config)#
interface ethernet 1/5
switch(config-if)# spanning-tree vlan 5 cost 200
switch(config-if)#
```

This example shows how to revert the interface to the default configuration:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no spanning-tree vlan 5 cost 200
switch(config-if)#
```

Related Commands

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

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

vlan-id	VLAN identification number. The VLAN ID range is from 0 to 4094.
forward-time *value*	(Optional) Specifies the STP forward-delay time. The range is from 4 to 30 seconds.
hello-time *value*	(Optional) Specifies the number of seconds between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds.
max-age *value*	(Optional) Specifies the maximum number of seconds that the information in a bridge protocol data unit (BPDU) is valid. The range is from 6 to 40 seconds.
priority *value*	(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 *dia*	(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

Global configuration mode

Command History

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

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the no spanning-tree vlan *vlan-id* co mmand, 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 the bridge priority of the current bridge 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.

spanning-tree pseudo-information

To configure spanning tree pseudo information parameters for two Layer 2 gateway switches, use the **spanning-tree pseudo-information** command.

spanning-tree pseudo-information

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Use this command in a topology with hybrid switches (for example, a virtual port channel [vPC] connected to a non-vPC switch) to configure VLAN-based load balancing.

To meet the VLAN-based load-balancing criteria, you must configure a different Spanning Tree Protocol (STP) bridge priority value for the root bridge and the designated bridge.

This command does not require a license.

Examples

This example shows how to enable Bridge Assurance globally on the switch:

```
switch# configure terminal
switch(config)# spanning-tree pseudo-information
switch(config-pseudo)#
```

Related Commands

Command	Description
mst (STP)	Configures the Multiple Spanning Tree (MST) designated bridge and root bridge priority.
show running-config spanning-tree	Displays the running configuration information for spanning trees.
show spanning-tree summary	Displays the summary information of the STP.
vlan (STP)	Configures the designated bridge and root bridge priority for VLANs.

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 *vlan-id*	(Optional) Specifies the VLAN identification number. The range is from 0 to 4094 .
value	Port priority. The range is 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 per VLAN Spanning Tree Plus (Rapid PVST+) spanning tree mode, which is the default STP mode. To configure the port priority for Multiple Spanning Tree (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.

speed (interface)

To configure the transmit and receive speed for an interface, use the **speed** command. To reset to the default speed, use the **no** form of this command.

speed {**100**|**1000**|**10000**|**auto**}
no speed

Syntax Description

100	Sets the interface speed to 100 Mbps. **Note** This keyword is not supported on a management interface.
1000	Sets the interface speed to 1 Gbps.
10000	Sets the interface speed to 10 Gbps. This is the default speed. **Note** This keyword is not supported on a management interface.
auto	Specifies that the speed of the interface is auto negotiated.

Command Default

The default speed is 10000 (10-Gigabit).

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.
5.1(3)N1(1)	Interface speed of 100 Mbps and the **auto** keyword was introduced.

Usage Guidelines

The first 8 ports of a Cisco Nexus 5010 switch and the first 16 ports of a Cisco Nexus 5020 switch are switchable 1-Gigabit and 10-Gigabit ports. The default interface speed is 10-Gigabit. To configure these ports for 1-Gigabit Ethernet, insert a 1-Gigabit Ethernet SFP transceiver into the applicable port and then set its speed with the speed command.

Note If the interface and transceiver speed is mismatched, the SFP validation failed message is displayed when you enter the **show interface ethernet** *slot /port* command. For example, if you insert a 1-Gigabit SFP transceiver into a port without configuring the **speed 1000** command, you will get this error.By default, all ports on a Cisco Nexus 5000 Series switch are 10 Gigabits.

Examples

This example shows how to set the speed for a 1-Gigabit Ethernet port:

```
switch# configure terminal
```

```
switch(config)# interface ethernet 2/1
switch(config-if)# speed 1000
```

This example shows how to set the an interface port to automatically negotiate the speed:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# speed auto
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

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.

svs veth auto-setup

To enable the Virtual Supervisor Module (VSM) to automatically create a virtual Ethernet interface when a new port is activated on a host, use the **svs veth auto-setup** command. To remove this control, use the **no** form of this command.

svs veth auto-setup
no svs veth auto-setup

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable automatic creation and configuration of virtual Ethernet interfaces:

```
switch# configure terminal
switch(config)# svs veth auto-setup
switch(config)#
```

This example shows how to disable automatic creation and configuration of virtual Ethernet interfaces:

```
switch# configure terminal
switch(config)# no svs veth auto-setup
switch(config)#
```

Related Commands

Command	Description
interface vethernet	Creates a virtual Ethernet interface.
show svs connections	Displays SVS connection information.
svs veth auto-delete	Enables the VSM to automatically delete DVPorts no longer used by a vNIC or hypervisor port.

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

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N1(1)	This command was deprecated and replaced with the **feature interface-vlan** command. For backwards compatibility, it will be maintained for a number of releases.

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.

svs veth auto-delete

To enable the Virtual Supervisor Module (VSM) to automatically delete Distributed virtual ports (dvPorts) no longer used by a virtual NIC (vNIC) or hypervisor port, use the **svs veth auto-delete** command. To disable this control, use the **no** form of this command.

svs veth auto-delete
no svs veth auto-delete

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

When enabled (the default), any virtual Ethernet interfaces that are in the administratively down state will be deleted after confirming with the vCenter server that no corresponding vNICs are in use.

This command does not require a license.

Examples

This example shows how to enable the Virtual Supervisor Module (VSM) to automatically delete dvPorts no longer used by a vNIC or hypervisor port:

```
switch# configure terminal
switch(config)# svs veth auto-delete
switch(config)#
```

This example shows how to disable the automatic deletion of dvPorts that are no longer used by a vNIC or hypervisor port:

```
switch# configure terminal
switch(config)# no svs veth auto-delete
switch(config)#
```

Related Commands

Command	Description
interface vethernet	Creates a virtual Ethernet interface.
show svs connections	Displays SVS connection information.
svs veth auto-setup	Enables the VSM to automatically create a virtual Ethernet interface when a new port is activated on a host.

svs connection

To enable an SVS connection to connect a vCenter Server to a Cisco Nexus 5000 Series switch, use the **svs connection** command. To disable an SVS connection, use the **no** form of this command.

svs connection *svs-name*
no svs connection *svs-name*

Syntax Description

svs-name	Name of the SVS connection. The name can be a maximum of 64 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Only one SVS connection can be enabled per session.

This command does not require a license.

Examples

This example shows how to enable an SVS connection:

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

This example shows how to disable an SVS connection:

```
switch# configure terminal
switch(config)# no svs connection SVSConn
switch(config)#
```

Related Commands

Command	Description
connect	Initiates a connection with a vCenter server.
protocol vmware-vim	Enables the VMware VI SDK.
show svs connections	Displays SVS connection information.
remote	Connects to remote machines.
vmware dvs	Creates a VMware virtual switch.

switchport private-vlan trunk allowed vlan

To configure the allowed VLANs for the private trunk interface, use the **switchport private-vlan trunk allowed vlan** command. To remove the allowed VLANs, sue the **no** form of this command.

switchport private-vlan trunk allowed vlan {*vlan-list*|{**add**|**except**|**remove**} *vlan-list*|**all**|**none**}
no switchport private-vlan trunk allowed vlan {*vlan-list*|{**add**|**all**|**except**|**remove**} *vlan-list*|**none**}

Syntax Description

vlan-list	VLAN IDs of the allowed VLANs when the interface is in private-vlan trunking mode. The range is from 1 to 4094, except for the VLANs reserved for internal use. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, 20,70-100,142.
add	Specifies the VLANs to be added to the current list.
except	Specifies all VLANs to be added to the current list, except the specified VLANs.
remove	Specifies the VLANs to be removed from the current list.
all	Specifies all VLANs to be added to the current list.
none	Specifies that no VLANs be added to the current list.

Command Default

Allows only associated VLANs on the private VLAN trunk interface.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

The primary VLANs do not need to be explicitly added to the allowed VLAN list. They are added automatically once there is a mapping between primary and secondary VLANs.

Examples

This example shows how to add VLANs to the list of allowed VLANs on an Ethernet private VLAN trunk port:

```
switch(config)# interface ethernet 1/3
switch(config-if)# switchport private-vlan trunk allowed vlan 15-20
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command. To revert to the default settings, use the **no** form of this command.

switchport port-security violation {**protect**|**restrict**|**shutdown**}
no switchport port-security violation {**protect**|**restrict**|**shutdown**}

Syntax Description

protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
shutdown	Shuts down the port if there is a security violation.

Command Default

shutdown

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the port security violation mode on a port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security violation protect
switch(config-if)#
```

This example shows how to set the port security violation mode on a port to the default value:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport port-security violation protect
switch(config-if)#
```

Related Commands

Command	Description
show port-security	Displays the port security configuration information.

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

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship. The range is from 1 to 3967 and 4048 to 4093.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship. The range is from 1 to 3967 and 4048 to 4093.

Command Default

None

Command Modes

Interface configuration modeVirtual Ethernet 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.
5.1(3)N1(1)	Support was added for virtual Ethernet interfaces.

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 pr imary VLANs, secondary VLANS, and isolated or community ports.

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

Examples

This example shows how to 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
```

This example shows how to configure a virtual Ethernet interface host private VLAN port with a primary VLAN (VLAN 5) and a secondary VLAN (VLAN 23):

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport private-vlan host-association 5 23
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
show vlan private-vlan	Displays information on private VLANs.

switchport private-vlan association trunk

To associate an isolated trunk port with the primary and secondary VLANs of a private VLAN, use the **switchport private-vlan association trunk** command. To remove the isolated trunk port association, use the **no** form of this command.

switchport private-vlan association trunk primary-id secondary-id
no switchport private-vlan association trunk

Syntax Description

primary-id	Primary VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.
secondary-id	Secondary VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

The secondary VLAN should be an isolated VLAN. Only one isolated VLAN under a given primary VLAN can be associated to an isolated trunk port.

Examples

This example shows how to map the secondary VLANs to the primary VLAN:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk secondary
switch(config-if)# switchport private-vlan association trunk 5 100
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

switchport priority extend

To configure the switch to override the priority of frames arriving on the Cisco IP phone port from connected devices, use the **switchport priority extende** command. To return the port to its default setting, use the **no** form of this command.

switchport priority extend {**cos** *cos-value*|**trust**}
no switchport priority extend

Syntax Description

cos	Specifies that the switch will send CDP packets to instruct the Cisco IP phone to mark data traffic with class of service (CoS) value.
cos-value	CoS value. The range is from 0 to 7.
trust	Specifies that the switch will send CDP packets to instruct the Cisco IP phone to trust tagged data traffic.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)N2(1)	This command was introduced.

Examples

This example shows how to set the Cisco IP phone port to trust tagged data traffic:

```
switch(config)# interface ethernet 1/28

switch(config-if)# switchport priority extend trust
switch(config-if)#
```

This example shows how to set the Cisco IP phone port to mark data traffic with CoS value:

```
switch(config)# interface ethernet 1/28

switch(config-if)# switchport priority extend cos 3
switch(config-if)#
```

This example shows how to return to the default settings:

```
switch(config)# interface ethernet 1/28

switch(config-if)# no switchport priority extend
switch(config-if)#
```

Related Commands

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

switchport monitor rate-limit

To configure a rate limit to monitor traffic on an interface, use the **switchport monitor rate-limit** command. To remove a rate limit, use the **no** form of this command.

switchport monitor rate-limit 1G
no switchport monitor rate-limit [1G]

Syntax Description

1G	(Optional) Specifies that the rate limit is 1 GB.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command is applicable to the following Cisco Nexus 5000 Series switches:

- Cisco Nexus 5010 Series
- Cisco Nexus 5020 Series

This command does not require a license.

Examples

This example shows how to limit the bandwidth on Ethernet interface 1/2 to 1 GB:

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport monitor rate-limit 1G
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport private-vlan association trunk	Associates the isolated trunk port with the primary and secondary VLANs of a private VLAN.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum** command. To revert to the default settings, use the **no** form of this command.

switchport port-security maximum *max-addr* [**vlan** *vlan-ID*]
no switchport port-security maximum *max-addr* [**vlan** *vlan-ID*]

Syntax Description

max-addr	Maximum number of secure MAC addresses for the interface; valid values are from 1 to 1025.
vlan *vlan-ID*	(Optional) Specifies the VLAN on which the MAC address should be secured. The range is from 1 to 4094.

Command Default

1

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the maximum number of secure MAC addresses on a port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security maximum 5
switch(config-if)#
```

This example shows how to override the maximum number of secure MAC addresses set for a specific VLAN:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security maximum 3 vlan 10
switch(config-if)#
```

This example shows how to set the maximum number of secure MAC addresses on a port to the default value:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport port-security maximum 5
switch(config-if)#
```

Related Commands

Command	Description
show port-security	Displays the port security configuration information.

switchport port-security mac-address

To add a static secure MAC address on a Layer 2 interface or to enable sticky MAC address learning on an interface, use the **switchport port-security mac-address** command. To revert to the default settings, use the **no** form of this command.

switchport port-security mac-address {*MAC-addr* [**vlan** *vlan-ID*]|**sticky**}
no switchport port-security mac-address {*MAC-addr* [**vlan** *vlan-ID*]|**sticky**}

Syntax Description

MAC-addr	MAC address in the format *E .E .E* .
vlan *vlan-ID*	(Optional) Specifies the VLAN on which the MAC address should be secured. The range is from 1 to 4094.
sticky	Configures the dynamic MAC addresses as sticky on an interface.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a static secure MAC address on a port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security mac-address 0050.3e8d.6400
switch(config-if)#
```

This example shows how to enable port security with sticky MAC addresses on a port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)#
```

This example shows how to remove a MAC address from the list of secure MAC addresses:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport port-security mac-address 0050.3e8d.6400
switch(config-if)#
```

Related Commands

Command	Description
show port-security	Displays the port security configuration information.

switchport port-security aging

To enable port security aging on a Layer 2 port, use the **switchport port-security aging** command. To disable port security on a port, use the **no** form of this command.

switchport port-security aging {**time** *aging-time*|**type** {**absolute**|**inactivity**}}
no switchport port-security aging {**time** *aging-time*|**type** {**absolute**|**inactivity**}}

Syntax Description

time *aging-time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging.
inactivity	Specifies that the timer starts to run only when there is no traffic.

Command Default

Aging time is 0

Aging type is **absolute**

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the secure MAC address aging type on a port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security aging type absolute
switch(config-if)#
```

This example shows how to set the secure MAC address aging time to 2 minutes:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security aging time 2
switch(config-if)#
```

Related Commands

Command	Description
show port-security	Displays the port security configuration information.
switchport port-security	Configures the switchport parameters to establish port security.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security on a port, use the **no** form of this command.

switchport port-security
no switchport port-security

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable port security on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport port-security
switch(config-if)#
```

This example shows how to disable port security on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport port-security
switch(config-if)#
```

Related Commands

Command	Description
show port-security	Displays the port security configuration information.

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. To remove the configuration, use the **no** form of this command.

switchport mode private-vlan host
no switchport mode

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration modeVirtual Ethernet 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.
5.1(3)N1(1)	Support was added for virtual Ethernet interfaces.

Usage Guidelines

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

- 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.

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 becomes inactive.

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
```

This example shows how to set a virtual Ethernet interface port to host mode for private VLANs:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport mode private-vlan host
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
show interface switchport	Displays information on all interfaces configured as switch ports.
show vlan private-vlan	Displays the status of the private VLAN.

switchport mode private-vlan trunk

To configure the port as a secondary trunk port for a private VLAN, use the **switchport mode private-vlan trunk** command. To remove the isolated trunk port, use the **no** form of this command.

switchport mode private-vlan trunk [{**promiscous**|**secondary**}]
no switchport mode private-vlan trunk [{**promiscous**|**secondary**}]

Syntax Description

promiscous	(Optional) Specifies the promiscous port.
secondary	(Optional) Specifies the secondary port.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

In a private VLAN domain, isolated trunks are part of a secondary VLAN. Isolated trunk ports can carry multiple isolated VLANs.

Examples

This example shows how to configure Ethernet interface 1/1 as a promiscuous trunk port for a private VLAN:

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk promiscous
switch(config-if)#
```

This example shows how to configure Ethernet interface 1/5 as a secondary trunk port for a private VLAN:

```
switch(config)# interface ethernet 1/5
switch(config-if)# switchport mode private-vlan trunk secondary
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport private-vlan association trunk	Associates the isolated trunk port with the primary and secondary VLANs of a private VLAN.

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 arguments or keywords.

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.
show vlan private-vlan	Displays the status of the private VLAN.

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

vlan-id	VLAN to set when the interface is in access mode. The range is from 1 to 4094, except for the VLANs reserved for internal use.

Command Default

VLAN 1

Command Modes

Interface configuration modeVirtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.1(3)N1(1)	Support for virtual Ethernet interface was added.

Usage Guidelines

Use the no form of the **switchport access vlan** com mand 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#
configure terminal
switch(config)#
interface ethernet 1/7

switch(config-if)#
switchport access vlan 2

switch(config-if)#
```

This example shows how to configure a virtual Ethernet interface to join VLAN 5:

```
switch#
configure terminal
switch(config)#
interface vethernet 1

switch(config-if)#
switchport access vlan 5
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a port.
show interface vethernet	Displays the virtual Ethernet interface information.

switchport mode

To configure the interface as a nontrunking nontagged single-VLAN Ethernet or virtual Ethernet interface, use the **switchport mode** command. To remove the configuration and restore the default, use the **no** form of this command.

switchport mode {**access**|**trunk**|**vntag**}
no switchport mode {**access**|**trunk**|**vntag**}
no switchport mode

Syntax Description

access	Specifies that the interface is in access mode.
trunk	Specifies that the interface is in trunk mode.
vntag	Specifies that the interface is in port mode. **Note** This keyword doe not apply to a virtual Ethernet interface.

Command Default

An access port carries traffic for VLAN 1.

Command Modes

Interface configuration modeVirtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.1(3)N1(1)	Support for a virtual Ethernet interface was added.

Usage Guidelines

An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN 1. To set the access port to carry traffic for a different VLAN, use the **switchport access vlan** command.

The VLAN must exist before you can specify that VLAN as an access VLAN. The system shuts down an access port that is assigned to an access VLAN that does not exist.

A virtual network tag (VNTag) port helps to identify the virtual interfaces on that physical port.

For a virtual Ethernet interface, use the **no** form of the command without the keywords.

Examples

This example shows how to set an interface as an Ethernet access port that carries traffic for a specific VLAN only:

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

This example shows how to set an interface as a VNTag port:

```
switch(config)# interface ethernet 1/5

switch(config-if)# switchport mode vntag

switch(config-if)#
```

This example shows how to set a virtual Ethernet interface in trunk port mode:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport mode trunk
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
show interface ethernet	Displays information about a specified Ethernet interface.
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport access vlan	Sets the access VLAN when the interface is in access mode.

switchport host

To configure the interface to be an access host port, use the **switchport host** command. To remove the host port, use the **no** form of this command.

switchport host
no switchport host

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Ensure that you are configuring the correct interface. It must be an interface that is connected to an end station.

An access host port handles the Spanning Tree Protocol (STP) like an edge port and immediately moves to the forwarding state without passing through the blocking and learning states. Configuring an interface as an access host port also disables EtherChannel on that interface.

Examples

This example shows how to set an interface as an Ethernet access host port with EtherChannel disabled:

```
switch(config)# interface ethernet 2/1

switch(config-if)# switchport host
switch(config-if)#
```

Related Commands

Command	Description
show interface brief	Displays a summary of the interface configuration information.
show interface switchport	Displays information on all interfaces configured as switch ports.

switchport block

To prevent the unknown multicast or unicast packets from being forwarded, use the **switchport block** 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 modeVirtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.1(3)N1(1)	Support for virtual Ethernet interface was added.

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
switch(config-if)#
```

This example shows how to block the unknown unicast traffic on a virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport block uniicast
switch(config-if)#
```

Related Commands

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

switchport backup interface

To configure Flex Links, which are two interfaces that provide backup to each other, on a Layer 2 interface, use the **switchport backup interface** command. To remove the Flex Links configuration, use the **no** form of this command.

Syntax Description

ethernet *slot /port*	Specifies the backup Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.
port-channel *channel-no*	Specifies the port channel interface. The interface number is from 1 to 4096.
multicast	(Optional) Specifies to configure the multicast parameters.
fast-convergence	(Optional) Configures fast convergence on the backup interface.
preemption	(Optional) Specifies to configure a preemption scheme for a backup interface pair.
delay *delay-time*	(Optional) Specifies a preemption delay. The range is from 1 to 300 seconds.
mode	(Optional) Specifies the preemption mode.
bandwidth	(Optional) Specifies that the interface with the higher available bandwidth always preempts the backup.
forced	(Optional) Specifies the interface that always preempts the backup.
off	(Optional) Specifies no preemption occurs from backup to active.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)N2(1)	This command was introduced.

Usage Guidelines

Note This command is applicable to the Cisco Nexus 5548 Series switch and the Cisco Nexus 5596 Series switch.

Before you use this command, make sure that you enable Flex Links on the switch by using the **feature flexlink** command.

Note Make sure the virtual port channel (vPC) is disabled on the switch.

A Flex Links port can be a physical Ethernet port or a port channel.

You cannot configure Flex Links port on the following types of interface:

- Fabric Extender (FEX) fabric port and FEX host port
- Virtual Fibre Channel interface
- Virtual network tag (VNTag)
- Interface with port security enabled
- Layer 3 interface
- Switched Port Analyzer (SPAN) destination
- Port channel member
- Interface configured with private VLAN
- Endnode mode
- Fabric path core interface (Layer 2 multipath)

Examples

This example shows how to configure Ethernet 1/1 and Ethernet 1/12 as Flex Links:

```
switch# configure terminal

switch(config)# interface ethernet 1/1
switch(config-if)# switchport backup interface ethernet 1/12
switch(config-if)#
```

This example shows how to configure EtherChannel 100 and EtherChannel 101 as Flex Links:

```
switch# configure terminal

switch(config)# interface port-channel 100
switch(config-if)# switchport backup interface port-channel 101
switch(config-if)#
```

This example shows how to configure the Ethernet interface to always preempt the backup:

```
switch# configure terminal
switch(config)# interface ethernet1/10
switch(config-if)# switchport backup interface ethernet1/2 preemption mode forced
switch(config-if)#
```

This example shows how to configure the Ethernet interface preemption delay time:

```
switch# configure terminal
switch(config)# interface ethernet1/1
switch(config-if)# switchport backup interface ethernet1/12 preemption delay 150
switch(config-if)#
```

This example shows how to configure fast convergence on the backup interface:

```
switch# configure terminal
switch(config)# interface ethernet1/1
switch(config-if)# switchport backup interface ethernet1/12 multicast fast-convergence
switch(config-if)#
```

Related Commands

Command	Description
feature flexlink	Enables Flex Links for Layer 2 interfaces.

Command	Description
show interface switchport backup	Displays backup interfaces.

system vlan reserve

To configure a reserved VLAN range, use the **system vlan reserve** command. To delete the reserved VLAN range configuration, use the **no** form of this command.

system vlan *vlan-start* **reserve**
no system vlan *vlan-start* **reserve**

Syntax Description

vlan-start	Starting VLAN ID. 80 VLANs are reserved starting from the start VLAN ID. For example, if you specify the starting VLAN ID as 1006, the reserved VLAN range is from 2006 to 1085.

Command Default

3968-4096

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The user-configured system reserved VLAN range comes in to effect only after a reload.

This command does not require a license.

Examples

This example shows how to configure a reserved VLAN range:

```
switch(config)# system vlan 1006 reserve

This will delete all configs on vlans 1006-1085. Continue anyway? (y/n) [no] yes

Note: After switch reload, VLANs 1006-1085 will be reserved for internal use.
      This requires copy running-config to startup-config before
      switch reload.  Creating VLANs within this range is not allowed.
```

This example shows how to remove the reserved VLAN configuration:

```
switch# no system vlan 1006 reserve
This will delete all configs on vlans 3968-4047. Continue anyway? (y/n) [no] yes

Note: After switch reload, VLANs 3968-4047 will be reserved for internal use.
      This requires copy running-config to startup-config before
      switch reload.  Creating VLANs within this range is not allowed.
```

Related Commands

Command	Description
show system vlan reserved	Displays information about the reserved VLAN usage.

system private-vlan fex trunk

To configure a PVLAN FEX trunk on port, use the **system private-vlan fex trunk** command. To remove the PVLAN FEX trunk ports, use the **no** form of this command.

system private-vlan fex trunk
no system private-vlan fex trunk

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.1(3)N2(1)	This command was introduced.

Usage Guidelines

You must disable all the FEX Isolated trunk ports before configuring PVLANs on the FEX trunk ports. If the FEX Isolated trunk ports and the FEX trunk ports are both enabled, unwanted traffic might occur.

Examples

This example shows how to configure PVLAN over a FEX trunk port:

```
switch# configure terminal
switch(config-if)# System private-vlan fex trunk
switch(config-if)# copy running-config startup-config
```

Related Commands

Command	Description
feature private-vlan	Enables private VLANs.

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*|**trunk** *primary-vlan-id*} {*secondary-vlan-id*|{**add**|**remove**} *secondary-vlan-id*}
no switchport private-vlan mapping [{*primary-vlan-id*|**trunk** *primary-vlan-id*} *secondary-vlan-id*]

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
trunk	Specifies the private VLAN promiscuous trunk port. **Note** This keyword applies to only Layer 2 interfaces.
add	(Optional) Associates the secondary VLANs to the primary VLAN.
secondary-vlan-id	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 modeVirtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.0(2)N2(1)	Number of secondary VLANs is limited to 16.
5.1(3)N1(1)	Support was added for virtual Ethernet interfaces.

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 pr imary VLANs, secondary VLANS, and isolated or community ports.

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

Note Beginning with Cisco NX-OS Release 5.0(2)N2(1), the number of mappings on a private-vlan trunk port is limited to 16.

Examples

This example shows how to configure the associated primary VLAN 18 to secondary isolated VLAN 20 on a private VLAN promiscuous port:

```
switch#
configure terminal
switch(config)#
interface ethernet 1/1
switch(config-if)#
switchport mode private-vlan promiscous
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#
configure terminal
switch(config)#
interface ethernet 1/2
switch(config-if)#
switchport mode private-vlan promiscous
switch(config-if)#
switchport private-vlan mapping 18 add 21
```

This example shows how to configure the associated primary VLAN 30 to secondary isolated VLANs 20-32 on a private VLAN promiscuous trunk port:

```
switch#
configure terminal
switch(config)#
interface ethernet 1/21
switch(config-if)#
switchport mode private-vlan promiscous trunk
switch(config-if)#
switchport private-vlan mapping trunk 30 20-32
switch(config-if)#
```

This example shows the error message that appears when you configure the associated primary VLAN 30 to secondary isolated VLANs 50-100 (beyond the total permissible limit of 16 secondary VLANs) on a private VLAN promiscuous trunk port:

```
switch#
configure terminal
switch(config)#
interface ethernet 1/12
switch(config-if)#
switchport mode private-vlan promiscous trunk
switch(config-if)#
switchport private-vlan mapping trunk 30 50-100
ERROR: secondary VLAN list contains primary VLAN id in trunk promiscuous port mapping.
switch(config-if)#
```

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

```
switch#
configure terminal
switch(config)#
interface ethernet 1/5
switch(config-if)#
no switchport private-vlan mapping
switch(config-if)#
```

This example shows how to configure the primary VLAN 12 to secondary isolated VLAN 20 on a virtual Ethernet interface host:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport private-vlan mapping 12 20
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
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.

switchport private-vlan trunk native

To configure the native VLAN ID for the private VLAN trunk, use the **switchport private-vlan trunk native** command. To remove the native VLAN ID from the private VLAN trunk, use the **no** form of this command.

switchport private-vlan trunk native vlan *vlan-list*
no switchport private-vlan trunk native vlan *vlan-list*

Syntax Description

vlan *vlan-list*	Specifies the VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.

Command Default

VLAN 1

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Secondary VLANs cannot be configured with a native VLAN ID on promiscuous trunk ports. Primary VLANs cannot be configured with a native VLAN ID on isolated trunk ports.

Examples

This example shows how to map the secondary VLANs to the primary VLAN:

```
switch(config)# interface ethernet 1/1

switch(config-if)# switchport private-vlan trunk native vlan 5
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switch ports.
switchport mode private-vlan trunk	Configures the port as a secondary trunk port for a private VLAN.
show vlan private-vlan	Displays the status of the private VLAN.

switchport trunk allowed vlan

To configure the allowed VLANs for a virtual Ethernet interface, use the **switchport trunk allowed vlan** command. To remove the configuration, use the **no** form of this command.

switchport trunk allowed vlan {{**add**|**except**|**remove**} *vlan_list*|**all**|**none**}
no switchport trunk allowed vlan

Syntax Description

add	Specifies the VLANs to be added to the current list.
except	Specifies all VLANs to be added to the current list, except the specified VLANs.
remove	Specifies the VLANs to be removed from the current list.
vlan_list	VLAN IDs of the allowed VLANs when the interface is in trunking mode. The range is from 1 to 4094, except for the VLANs reserved for internal use. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, 20,70-100,142.
all	Specifies all VLANs to be added to the current list.
none	Specifies that no VLANs be added to the current list.

Command Default

None

Command Modes

Interface configuration modeVirtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add VLANs to the list of allowed VLANs on a virtual Ethernet interface trunk port:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport trunk allowed vlan 5-15
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.

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

switchport trunk native vlan

To configure the native VLAN ID for the virtual Ethernet interface, use the **switchport trunk native vlan** command. To remove the native VLAN ID from the virtual Ethernet interface, use the **no** form of this command.

switchport trunk native vlan *vlan_ID*
no switchport trunk native vlan

Syntax Description

vlan_ID	VLAN ID of the native VLAN when this port is in trunking mode. The range is from 1 to 4094.

Command Default

None

Command Modes

Interface configuration modeVirtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set VLAN 3 as the native trunk port:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# switchport trunk native vlan 3
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
show running-config	Displays the running system configuration information.

switchport voice vlan

To configure the voice VLAN on a port, use the **switchport voice vlan** command. To remove a voice VLAN, use the **no** form of this command.

switchport voice vlan {*vlan-list*|**dot1p**|**untagged**}
no switchport voice vlan

Syntax Description

vlan-list	VLAN ID. The range is from 1 to 3967 and from 4048 to 4093.
dot1p	Specifies that the Cisco IP phone uses priority tagging and uses an 802.1P VLAN ID of 0 for voice traffic.
untagged	Specifies that the Cisco IP phone does not tag frames for voice traffic.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)N2(1)	This command was introduced.

Examples

This example shows how to configure VLAN 3 as the voice VLAN:

```
switch(config)# interface ethernet 1/28

switch(config-if)# switchport voice vlan 3
switch(config-if)#
```

This example shows how to configure an Ethernet port to send CDP packets that configure the Cisco IP phone to transmit voice traffic in 802.1p frames:

```
switch(config)# interface ethernet 1/28

switch(config-if)# switchport voice vlan dot1p
switch(config-if)#
```

This example shows how to configure an Ethernet port to send CDP packets that configure the Cisco IP phone to transmit untagged voice traffic:

```
switch(config)# interface ethernet 1/28

switch(config-if)# switchport voice vlan untagged
switch(config-if)#
```

This example shows how to stop voice traffic on an Ethernet port:

```
switch(config)# interface ethernet 1/28
```

```
switch(config-if)# no switchport voice vlan
switch(config-if)#
```