S Commands

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

auto

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

By default, the device 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.

If you designate a port as a shared link, you cannot use the fast transition feature, regardless of the duplex setting.

This command does not require a license.

Examples

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

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

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 ports of a given bridge, 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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.

When you enter the Loop Guard command for the specified interface, that **spanning-tree guard loop** command overrides this command.

This command does not require a license.

Examples

This example shows how to enable Loop Guard:

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

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You cannot use both Rapid PVST+ and MST in a single virtual device context (VDC). You can, however, use Rapid PVST+ in one VDC and MST in another VDC.

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.

This command does not require a license.

Examples

This example shows how to switch to MST mode:

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

This example shows how to return to the default mode (Rapid PVST+):

```
switch(config)# no spanning-tree mode
switch(config)#
```

Related Commands

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

spanning-tree mst configuration

To enter the Multiple Spanning Tree (MST) configuration submode, 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 CIST instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 submode. 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 submode.

The **abort** command leaves MST configuration submode 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 submode, 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 submode parameter can cause a connectivity loss. To reduce service disruptions, when you enter mst configuration submode, 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, or you can exit the submode without committing any change to the configuration by using the abort keyword.

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message appears:

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

This command does not require a license.

Examples

This example shows how to enter MST-configuration submode:

```
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
switch(config)#
```

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 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 of valid values is from 0 to 4094.
cost	Port cost for an instance; the range of valid values is from 1 to 200,000,000.
auto	Sets the value of the port cost by the media speed of the interface.

Command Default

auto

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

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

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

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

This command does not require a license.

Examples

This example shows how to set the interface path cost:

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

Related Commands

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

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the device, 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 device; the range of valid values is from 4 to 30 seconds.

Command Default

15

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

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

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

Related Commands

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

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the device, 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 device; the range of valid values is from 1 to 10 second s.

Command Default

2

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

Note We recommend not to change any of STP timer values.

This command does not require a license.

Examples

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

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

Related Commands

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

spanning-tree mst max-age

To set the max-age timer for all the instances on the device, 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 device; the range of valid values is from 6 to 40 seconds.

Command Default

20

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
show spanning-tree mst	Displays 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 of valid values is from 1 to 255 hops.

Command Default

20

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
show spanning-tree mst	Displays 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; valid values are from 0 to 4094.
priority	Port priority for an instance; the range of valid values is from 0 to 224 in increments of 32.

Command Default

priority is 128.

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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
switch(config-if)#
```

Related Commands

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

Command	Description
spanning-tree port-priority	Configures the port priority for default STP, which is Rapid PVST+.

spanning-tree mst pre-standard

To force the specified interface to send pre-standard, rather than standard, Multiple Spanning Tree (MST) messages, use the **spanning-tree mst pre-standard** command. To return to the default setting, 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

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(2)	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* argument to 0 to make the device root.

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

This command does not require a license.

Examples

This example shows how to set the bridge priority:

```
switch(config)# spanning-tree mst pre-standard 0 root priority 4096
switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays 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 of valid values is from 0 to 4094.
priority-value	Bridge priority; see the “Usage Guidelines” section for valid values and additional information.

Command Default

priority-value default is 32768.

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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* argument to 0 to make the device root.

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

This command does not require a license.

Examples

This example shows how to set the bridge priority:

```
switch(config)# spanning-tree mst priority 4096
switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays 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 of valid values is from 0 to 4094.
primary	Specifies the high priority (low value) that is high enough to make the bridge root of the spanning-tree instance.
secondary	Specifies the device as a secondary root, should the primary root fail.
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 device. The range is from 1 to 10 seconds; the default is 2 seconds.

Command Default

spanning-tree mst root has no default settings.

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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.

The **diameter** *dia* and **hello-time** *hello-time* keywords and arguments are available for instance 0 (IST) only.

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.

This command does not require a license.

Examples

This example shows how to designate the primary root:

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

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
switch(config)# spanning-tree mst 5 root primary
switch(config)#
```

Related Commands

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

spanning-tree mst simulate pvst

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

spanning-tree mst simulate pvst

no spanning-tree mst simulate pvst

spanning-tree mst simulate pvst disable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled. By default, all interfaces on the device interoperate seamlessly between MST and Rapid PVST+. See the **spanning-tree mst simulate pvst global command** to change this behavior globally.

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Note The interfaces must be in Layer 2 port mode to use this command.

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 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.

Note To block automatic MST and Rapid PVST+ interoperability for the entire device, use the **no spanning-tree mst simulate pvst global** command, which can be used in interface command mode.

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.

This command does not require a license.

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
switch(config-if)#
```

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

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 device 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 device.

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 device to seamless operation between MST and Rapid PVST+, use the **spanning-tree mst simulate pvst global** command.

This command does not require a license.

Examples

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

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

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Note This command applies only to the Rapid Per VLAN Spanning Tree Plus (PVST+) spanning tree mode, which is the default mode. When you are using MST spanning tree mode, the device uses only the long method for calculating path cost; this is not user-configurable for MST.

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.

This command does not require a license.

Examples

This example shows how to set the default pathcost method to long:

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

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 Layer 2 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 **no spanning-tree port type** command or the **spanning-tree port type normal** command.

spanning-tree port type edge [trunk]

no spanning-tree port type

spanning-tree port type normal

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 device and network operation.

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

Note This 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 a message similar to the following:

```
%Portfast has been configured on GigabitEthernet2/8 but will only
 have effect when the interface is in a non-trunking mode.
```

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

The default spanning tree port type is normal.

This command does not require a license.

Examples

This example shows how to configure an interface connected to a Layer 2 host as an edge port, which automatically transitions that interface to the forwarding state on linkup:

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

Related Commands

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

spanning-tree port type edge bpdufilter default

To enable 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 by 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 careful when using this command. Using this command incorrectly 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 Be careful when enabling BPDU Filtering. The 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 device from receiving or sending BPDUs on this port.

This command does not require a license.

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
switch(config)#
```

Related Commands

Command	Description
show spanning-tree summary	Displays 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 bpduguard default

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

spanning-tree port type edge bpduguard default

no spanning-tree port type edge bpduguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 {enable | disable} command for more information.

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

This command does not require a license.

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
switch(config)#
```

Related Commands

Command	Description
show spanning-tree summary	Displays information about the spanning tree configuration.
spanning-tree bpduguard {enable | disable}	Enables BPDU Guard 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 Layer 2 hosts as edge ports by default, use the **spanning-tree port type edge default** command. To restore all ports connected to Layer 2 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use this command to automatically configure all interfaces as spanning tree edge ports by default. This command does 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 device 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.

This command does not require a license.

Examples

This example shows how to globally configure all ports connected to Layer 2 hosts as spanning tree edge ports:

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

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 Layer 2 switch or bridge 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.

spanning-tree port type network

no spanning-tree port type

spanning-tree port type normal

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use this command to configure an interface that connects to a Layer 2 switch or bridge 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 Layer 2 hosts as STP network ports and enable Bridge Assurance, those ports automatically move into the blocking state.

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

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

You can configure all ports that are connected to Layer 2 switches or bridges 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.

This command does not require a license.

Examples

This example shows how to configure an interface connected to a Layer 2 switch or bridge as a spanning tree network port:

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

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use this command to automatically configure all interfaces that are connected to Layer 2 switches or bridges as spanning tree network ports by default. Then, you can use the spanning-tree port type edge command to configure specified ports that are connected to Layer 2 hosts as spanning-tree edge ports.

Note If you mistakenly configure ports connected to Layer 2 hosts as Spanning Tree Protocol (STP) network ports and Bridge Assurance is enabled, those ports automatically move into the blocking state.

If you have enabled Bridge Assurance on the device, all network ports automatically run that feature. To enable Bridge Assurance, see the spanning-tree bridge assurance command.

Configure only the ports that connect to other Layer 2 switches or bridges as network ports because the Bridge Assurance feature causes network ports that are connected to Layer 2 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.

This command does not require a license.

Examples

This example shows how to globally configure all ports connected to Layer 2 switches or bridges as spanning tree network ports:

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

Related Commands

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

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 of valid values is from 0 to 4094 .
value	Port priority; valid values are from 1 to 224 in increments of 32.

Command Default

value is 128 .

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelin

Note Use this command to configure the port priority for Rapid Per VLAB Spanning Tree Plus (PVST+) spanning tree mode, which is the default Spanning Tree Protocol (STP) mode. To configure the port priority for Multiple Spanning Tree (MST) spanning tree mode, use the **spacing-tree mst port-priority** command.

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.

This command does not require a license.

Examples

This example shows how to increase the likelihood 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
switch(config-if)#
```

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.

spanning-tree pseudo-information

To configure the spanning tree pseudo information, 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the spanning tree pseudo information:

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

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.

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** *hello-time*]]]]

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

Syntax Description

vlan-id	VLAN identification number; the range of valid values is from 0 to 4094.
forward-time *value*	(Optional) Specifies the STP forward-delay time; the range of valid values is from 4 to 30 seconds.
hello-time*value*	(Optional) Specifies the number of seconds between the generation of configuration messages by the root device; the range of valid values 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 of valid values 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 device to be the root bridge.
root secondary	(Optional) Forces this device 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

- **priority32768**

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelin

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

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

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

Valid values for *protocol* are **dec—**Digital STP, **ibm—**IBM STP, **ieee—**IEEE Ethernet STP, and **vlan-bridge—**VLAN Bridge STP.

The spanning-tree root primary alters this device's bridge priority to 24576. If you enter the spanning-tree root primary command and the device does not become the root, 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 device does not become the root, an error results.

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

Use the spanning-tree root command on the backbone switches only.

Note We recommend that you configure the hello time to be 4 seconds when you are working with virtual port channels (vPCs).

This command does not require a license.

Examples

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

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

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

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

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

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

Related Commands

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

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

active

Command Modes

VLAN configuration submode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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.

This command does not require a license.

Examples

This example shows how to suspend VLAN 2:

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

Related Commands

Command	Description
show vlan	Displays VLAN information.

switchport mode private-vlan host

To set the interface type to be a Layer 2 host port for a private VLAN, use the **switchport mode private-vlan host** command.

switchport mode private-vlan host

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You must first use the **switchport** command on the interface before you can use the **switchport mode private-vlan host** command.

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.

This command does not require a license.

Examples

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

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

Related Commands

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

switchport mode private-vlan promiscuous

To set the interface type to be a Layer 2 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You must first use the **switchport** command on the interface before you can use the **switchport mode private-vlan promiscuous** command.

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.

This command does not require a license.

Examples

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

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

Related Commands

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

switchport mode private-vlan promiscuous trunk

To set the interface type to be a Layer 2 promiscuous trunk port for a private VLAN, use the **switchport mode private-vlan promiscuous trunk** command.

switchport mode private-vlan promiscuous trunk

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Note See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide* for more information on trunk interfaces.

You must first use the **switchport** command on the interface before you can use the **switchport mode private-vlan promiscuous trunk** command. To return to the default Layer 3 port mode, enter the no switchport command.

Beginning with Cisco Release 5.0(2) for the Cisco Nexus 7000 Series devices, you can configure private VLAN promiscuous trunk ports to carry traffic for multiple primary VLANs and their mapped secondary VLANs.

You must map the primary and secondary VLANs, by entering the **private-vlan mapping** command, before the pair you are mapping to a promiscuous trunk port can become operational. You can map 16 pairs of primary and secondary VLANs to a private VLAN promiscuous trunk port.

This command does not require a license.

Examples

This example shows how to set a port to be a promiscuous trunk port for private VLANs:

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

Related Commands

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

switchport mode private-vlan trunk promiscuous

To set the interface type to be a Layer 2 trunk port and a promiscuous port that carries traffic for multiple primary VLANs, use the **switchport mode private-vlan trunk promiscuous** command.

switchport mode private-vlan trunk promiscuous

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use this command to configure a private VLAN promiscuous port to carry traffic for multiple pimary VLANs as well as normal VLANs. You can configure a maximum of 16 private VLAN primary and secondary pairs on each promiscuous trunk port.

You must first use the **switchport** command on the interface before you can use the **switchport mode private-vlan trunk promiscuous** command.

When you configure a port as a promiscuous private VLAN port and the port is a Switched Port Analyzer (SPAN) destination the port becomes inactive,

You must have already configured the private VLANs, including associating the primary and secondary VLANs. See See the private-vlan command for more information on promiscuous ports and the **private-vlan association** command for more information on associating private VLANs.

As with all Layer 2 trunk ports, you must configure the allowed VLANs, the native VLAN, and whether you want tagging on the private VLAN promisucous trunk port. See the **switchport private-vlan trunk allowed vlan**, **switchport private-vlan trunk native vlan** and **switchport private-vlan trunk native vlan tag** commands to set these paramters.

This command does not require a license.

Examples

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

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

Related Commands

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

switchport mode private-vlan trunk secondary

To set the interface type to be a Layer 2 isolated trunk port for a private VLAN, use the **switchport mode private-vlan trunk secondary** command.

switchport mode private-vlan trunk secondary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Note See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide* for more information on trunk interfaces.

You must first use the **switchport** command on the interface before you can use the **switchport mode private-vlan trunk secondary** command. To return to the default Layer 3 port mode, enter the no **switchport** command. You can only make private VLAN isolated ports trunk ports; you cannot make private VLAN community ports trunk ports.

Beginning with Cisco Release 5.0(2) for the Cisco Nexus 7000 Series devices, you can configure private VLAN isolated trunk ports to carry traffic for multiple isolated VLANs and their associated primary VLANs. Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two isolated VLANs that are associated with the same primary VLAN into a private VLAN isolated trunk port.

You can map 16 pairs of primary and secondary VLANs to a private VLAN isolated trunk port.

You must associate the primary and secondary isolated VLANs before the pair you map to an isolated trunk port can become operational.

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

This command does not require a license.

Examples

This example shows how to set a port to be an isolated trunk port for private VLANs:

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

Related Commands

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

switchport private-vlan association trunk

To add private VLANs, associated isolated VLANs, and primary VLANs to a private VLAN isolated trunk port, use the command. To remove the private VLAN association from the port, use the **no** form of this command.

switchport private-vlan *primary-vlan-id secondary-vlan-id***association trunk**

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

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
secondary-vlan-id	Number of the isolated VLAN of the private VLAN relationship. **Note** You cannot add a community VLAN to an isolated trunk port.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must have configured the interface using the **switchport mode private-vlan trunk secondary** command before this command becomes operational.

You use the command to add private VLANs, isolated VLANs, and their associated primary VLANs to the isolated trunk port. In this way, the isolated trunk port can carry multiple private VLANs. You can add up to 16 pairs of isolated and primary VLANs to each isolated trunk port. You must associate the private VLANs by entering the **private-vlan association** command before this command becomes operational.

Note Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two isolated VLANs that are associated with the same primary VLAN into a private VLAN isolated trunk port.

Delete associations by doing the following:

- Enter the **no** form of this command to delete a Private VLAN associations, both primary and secondary VLANs.

- Enter the **no** form of the command with the *primary-vlan-id* argument to delete a secondary VLANs and their associated primary VLANs.
- Enter the **no** form of the command and the *primary-vlan-id* and *secondary-vlan-id* arguments to delete a specified primary and secondary associated private VLANs.

This command does not require a license.

Examples

This example shows how to add isolated VLAN 200 and its associated primary VLAN 100 to a private VLAN isolated trunk port:

```
switch(config-if)# 100 200
switch(config-if)#
```

Related Commands

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

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.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

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.

This command does not require a license.

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
switch(config-if)#
```

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

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

Related Commands

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

switchport private-vlan mapping

To define the private VLAN association for a promiscuous port or a promiscuous trunk 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 [**trunk** *primary-vlan-id* **remove** *secondary-vlan-list*]

no switchport private-vlan mapping [**trunk** *primary-vlan-id* **remove** *secondary-vlan-list*]

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
add	Associates the secondary VLANs to the primary VLAN.
secondary-vlan-list	Number of the secondary VLAN of the private VLAN relationship.
remove	Clears the association between the secondary VLANs and the primary VLAN.
trunk	Associates the primary and secondary VLANs of more than one private VLAN to the interface.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.
4.2(1)	The promiscuous trunk interface functionality was added.

Usage Guidelines

You configure the promiscuous trunk mode on the interface to allow that interface to carry traffic for multiple private VLANs. You can map a maximum of 16 private VLAN primary and secondary pairs on each promiscuous trunk port.

On a promiscuous trunk port, you must enter this command separately for each primary VLAN. You enter the primary VLAN value and then add or remove those secondary associated VLANs that you want. To map another primary VLAN, you must re-enter the command with the new primary VLAN value and then add or remove its associated VLANs as you want.

Note The association between the primary and secondary VLANs for all the private VLANs you want to add to this interface must be operational.

There is no run-time effect on the port unless it is in private VLAN-promiscuous mode or promiscuous trunk mode. If the port is in private VLAN-promiscuous mode or promiscuous trunk 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.

This command does not require a license.

Examples

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

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

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

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

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

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

This example shows how to add multiple private VLANs to the promiscuous trunk port; this example adds 5 private VLAN pairs:

```
switch(config-if)# switchport private-vlan mapping trunk 2 add 3-5
switch(config-if)# switchport private-vlan mapping trunk 4 add 5,8
switch(config-if)#
```

Related Commands

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

switchport private-vlan mapping trunk

To add or remove private VLAN pairs to the private VLAN promiscuous trunk port, use the **switchport private-vlan** mapping trunk command. To remove private VLAN mappings from the promiscuous trunk interface, use the **no** form of this command.

switchport private-vlan mapping trunk *primary-vlan* {**add** *secondary-vlan-list*| **remove** *secondary-vlan-list*}

no switchport private-vlan mapping trunk [*primary-vlan* [*secondary-vlan-list*]]

Syntax Description

primary-vlan	ID of the primary VLAN that you are adding to the private VLAN promiscuous trunk port.
add	Adds the secondary VLAN of the primary VLAN to the promiscuous trunk port.
secondary-vlan-list	ID of the secondary VLANs that you are adding to the promiscuous trunk port.
remove	Removes the secondary VLAN of the primary VLAN to the promiscuous trunk port.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must have configured the interface by using the **switchport mode private-vlan trunk promiscuous** command before this command becomes operational.

You use the **switchport private-vlan mapping trunk** command to add private VLANs, primary VLANs, and specified associated secondary VLANs to the promiscuous trunk port. In this way, the promiscuous trunk port can carry multiple private VLANs as well as normal VLANs. The secondary VLAN can be either an isolated or community VLAN. The private VLAN mapping between primary and secondary VLANs must be operational (see the **private-vlan mapping** command). You can add up to 16 pairs of isolated and primary VLANs to each isolated trunk port.

You must reenter the command for each primary VLAN that you are working with.

When you are using the **no** form of this command, the following guidelines apply:

- If you do not specify any primary VLANs, the system removes all the private VLANs on this interface.
- If you specify only the primary VLAN, the system removes that primary VLAN and all secondary VLANs associated with that primary VLAN on this interface.
- If you specify the primary VLAN and specific secondary VLANs, the system removes only those specified private VLAN pairs from this interface.

Note You must configure this interface as a VLAN interface if you want Layer 3 communication on this port.

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

This command does not require a license.

Examples

This example shows how to map two primary VLANs and selected associated secondary VLANs to the promiscuous trunk interface:

```
switch
(config-if)#
switchport
private-vlan mapping trunk 200 add 3,5
switch
(config-if)#
switchport
private-vlan mapping trunk 100 add 10
switch
(config-if)#
```

Related Commands

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

switchport private-vlan trunk allow vlan

To set the list of allowed VLANs on the private VLAN promiscuous trunking interface, use the **switchport private-vlan trunk allowed vlan** command. To allow *no* VLANs on the trunking interface, use the **no** form of this command.

switchport trunk allowed vlan {*vlan-list*| **all**| **none**| [**add**| **except**| **remove** *vlan-list*]}

no switchport trunk allowed vlan

Syntax Description

vlan-list	Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094.
all	Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode.
none	Blocks all VLANs transmitting through this interface in tagged format when in trunking mode.
add	*(Optional)* Adds the defined list of VLANs to those currently set instead of replacing the list.
except	*(Optional)* Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values.
remove	*(Optional)* Removes the defined list of VLANs from those currently set instead of replacing the list.

Command Default

No VLANs

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Private VLAN promiscuous trunk ports carry traffic for multiple private primary VLANs as well as for normal VLANs.

When you map the private primary and secondary VLANs to the promiscuous trunk port using the command **switchport private vlan mapping** command, the system automatically puts all the primary VLANs into the allowed VLAN list for this port. These ports can carry traffic for a maximum of 16 private VLAN primary and secondary VLANs.

You can enter the **switchport trunk allowed vlan** command on interfaces where the Switched Port Analyzer (SPAN) destination port is either a trunk or an access port.

If you remove the native VLAN from a trunk, the trunk interface continues to send and receive management traffic in that VLAN.

This command does not require a license.

Examples

This example shows how to add a series of consecutive VLANs to the list of allowed VLANs on a private VLAN promiscuous trunking port:

```
switch(config-if)# switchport private-vlan trunk allowed vlan add 4-6
switch(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport private-vlan trunk allowed vlan

To add allowed VLANs to the private VLAN promiscuous and isolated trunk ports, use the **switchport private-vlan** trunk allowed vlan command. To remove VLANs from the promiscuous and isolated trunk interfaces, use the **no** form of this command.

switchport private-vlan trunk allowed vlan {**add** *vlan-list*| **all**| **except** *vlan-list*| **none**| **remove** *vlan-list*}

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

Syntax Description

add	Adds a defined list of VLANs on the private VLAN promiscuous and isolated trunk ports. The default value is no VLANs allowed. **Note** You must configure at least the native VLAN as allowed on this interface, even if you are using the default native VLAN 1.
vlan-list	Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 3968 and 4048 to 4093.
all	Adds all VLANs to the private VLAN.
except	Allows all VLANs to transmit through this interface in tagged format except the specified values.
none	Blocks all VLANs transmitting through this interface in tagged format.
remove	Removes the defined list of VLANs from those VLANs currently set.

Command Default

Empty; no VLANs are allowed on the private VLAN promiscuous and isolated trunk ports by default.

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must have configured the interface by using either the **switchport mode private-vlan trunk secondary** or the **switchport mode private-vlan trunk promiscuous** command for this command to become operational.

When you map the private primary and secondary private VLANs to the isolated and promiscuous trunk ports, the system automatically adds all the primary VLANs into the list of allowed VLANs for this interface.

Note Ensure that the native VLAN is on the allowed VLANs on this interface. By default, these interfaces do not allow any traffic. So, even if you are using the default VLAN 1 as the native VLAN, you must configure that VLAN as allowed or you will not pass traffic.

This command does not require a license.

Examples

This example shows how to configure the native default VLAN 1 to be allowed on a private VLAN promiscuous or isolated trunk port:

```
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays information about interfaces.

switchport private-vlan trunk native vlan

To assign the native VLAN ID to a private VLAN promiscuous trunk interface, use the **switchport private-vlan trunk native vlan** command. To return the native VLAN ID to the default native VLAN, use the **no** form of this command.

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Syntax Description

vlan-id	Native VLAN for the private VLAN promiscuous trunk port in 802.1Q trunking mode. The range of valid values is from 1 to 4094, except the internally reserved VLANs 3968 to 4047 and 4094. The default v

Command Default

VLAN 1

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Private VLAN trunk ports carry traffic for multiple private primary VLANs, as well as normal VLANs.

If you are using a private VLAN as the native VLAN, you must enter a primary VLAN value. If you enter a secondary VLAN as a value here, the system rejects the command.

Note See the **switchport private-vlan trunk native vlan tag** command for more information about configuring the native VLAN for 802,1Q private VLAN promiscuous trunk ports.

This command does not require a license.

Examples

This example shows how to configure the native VLAN for a private VLAN promiscuous trunk interface:

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

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport private-vlan trunk native vlan tag

To enable dot1q (IEEE 802.1Q) tagging for the native VLAN in a private VLAN promiscuous trunk port, use the **switchport private-vlan trunk native vlan tag** command. To return to the default where no packets are tagged in the native VLAN in a trunk, use the **no** form of this command.

switchport private-vlan trunk native vlan tag

no switchport private-vlan trunk native vlan tag

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Typically, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN and allows all untagged traffic and control traffic to transit the switch. Packets that enter the switch with 802.1Q tags that match the native VLAN ID value are similarly stripped of tagging. If you choose to maintain the tagging on the native VLAN and drop untagged traffic on the private VLAN promiscuous trunk port, enter the **switchport private-vlan trunk native vlan tag** command.

Use the **switchport private-vlan trunk native vlan tag** command to configure the switch to tag the traffic received on the native VLAN and to admit only 802.1Q-tagged frame, dropping any untagged traffic, including untagged traffic in the native VLAN. Control traffic continues to be accepted untagged on the native VLAN on a trunked port, even when the **switchport private-vlan trunk native vlan tag** command is enabled.

Use this command to enable the tagging behavior on all native VLANs on all private VLAN promiscuous trunked ports on the switch.

Note If you enable 802.1Q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure 802.1Q tagging on each switch.

This command does not require a license.

Examples

This example shows how to enable tagging for all VLANs on all private VLAN promiscuous trunk ports on the switch:

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

Related Commands

Command	Description
show vlan dot1q tag native	Displays native VLAN-tagging information.

switchport trunk pruning vlan

To configure pruning eligibility on trunk ports, use the **switchport trunk pruning vlan** command.

switchport trunk pruning vlan [**add**| **except**| **none**| **remove**] *vlan-id*

Syntax Description

add	(Optional) Adds a VLAN to the current list.
except	(Optional) Specifies all VLANs except a particular VLAN.
none	(Optional) Specifies no VLANs.
remove	(Optional) Removes the VLANs from the current list.
vlan-id	VLAN ID. The range is from 2 to 1001.

Command Default

None

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a VLAN to the current list:

```
switch(config-if)# switchport trunk pruning vlan add 20
switch(config-if)#
```

This example shows how to remove a VLAN from the current list:

```
switch(config-if)# switchport trunk pruning vlan remove 12
switch(config-if)#
```

Related Commands

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

system vlan long-name

To enable VLAN long-names, use the system vlan long-name command. To disable this feature, use the no form of this command.

system vlan long-name

no system vlan long-name

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

To enable the system vlan long-name command, set the VLAN Trunking Protocol (VTP) to the transparent or off mode. This command allows you to configure VLAN names greater than 32 and less than or equal to 128 characters.

The VTP mode changes to off if the VLAN long-name are enabled instead of the default server. This situation is true even when a private VLAN or VLANs from 1002 to 1005 are present.

This command does not require a license.

Examples

This example shows how to enable long VLAN long names:

```
switch# config t
sqitch(config)# system vlan long-name
switch(config)#
```

Related Commands

Command	Description
show run vlan	Displays information about the run VLAN usage.

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 start-*vlan-id* **reserve**

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

Syntax Description

start-*vlan-id*	Starting VLAN ID. 128 VLANS are reserved starting from the start VLAN ID. For example, if you specify the starting VLAN ID as 0, the reserved VLAN range is from 0 to 127.

Command Default

3968–4096

Command Modes

Any command mode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you configure the system reserved VLAN range, all configuration on the VLANs that fall under the reserved VLAN range are deleted.

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

This command does not require a license.

Examples

This example shows how to configure a reserved VLAN range:

```
switch# system vlan 2000 reserve
This will delete all configs on vlans 2000-2127. Continue anyway? [no]
switch#
```

This example shows how to remove the reserved VLAN configuration:

```
switch# no system vlan 2000 reserve
This will delete all configs on vlans 2000-2127. Continue anyway? [no]
switch#
```

Related Commands

Command	Description
write erase	Reverts to the default reserved VLAN range.
show system vlan reserved	Displays information about the reserved VLAN usage.

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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelin

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

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.

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

This command does not require a license.

Examples

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

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

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 bpduguard default command.

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
6.2(10)	Updated the usage guidelines for the command.
4.0	This command was introduced.

Usage Guidelines

BPDU Guard prevents a port from receiving BPDUs. If the port still receives a BPDU, the BPDU packet is dropped.

Note In Cisco NX-OS Release 6.2(10) and later releases, the port will be error disabled when an invalid BPDU is received and BPDU Guard is enabled on the port.

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 device 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 bpduguard default for more information on the global command for BPDU Guard**. However, w**hen you enable this command on an *interface* , it applies to that interface *regardless* of the spanning tree port type. For a trunk port, configure an allowed VLAN list using the **switchport trunk allowed vlan** *vlan-list* command.

This command has three states:

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

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

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
spanning-tree port type edge bpduguard default	Enables BPDU Guard by default on all spanning tree edge ports.
show spanning-tree summary	Displays information about the spanning tree state.

spanning-tree bridge assurance

To enable Bridge Assurance on the device, 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use this command to enable Bridge Assurance on the device.

Bridge Assurance is active only on spanning tree network interfaces. To configure an interface as a spanning tree network interface, use either the spanning-tree port type networkcommand or the spanning-tree port type network default command.

Note Bridge Assurance works only on point-to-point links. You must configure this feature on both ends of the link.

When Bridge Assurance is enabled on network ports, all ports send bridge protocol data units (BPDUs). When a Bridge Assurance-enabled network port does not receive any BPDUs for a specified period, that interface moves into the blocking state. After the network port receives a BPDU again, the port begins its normal spanning tree transitions.

An interface that is connected to a Layer 2 host and misconfigured as a spanning tree network port moves into the blocking state.

Note Bridge Assurance is configured globally only.

This command does not require a license.

Examples

This example shows how to enable Bridge Assurance on the device:

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

Related Commands

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

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 (see spanning-tree cost, on page 87 for the values).

Command Default

auto

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 spanning-tree cost, on page 87).

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*, note that higher values 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 port channel bundle is considered a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.

Note Use this command to set the port cost for Rapid Per VLAN Spanning Tree Plus (PVST+). Use the **spanning-tree mst cost** command to set the port cost for Multiple Spanning Tree (MST).

This command does not require a license.

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 2/0
switch(config-if)# spanning-tree cost 250
switch(config-if)#
```

Related Commands

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

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**| **root**| **none**}

no spanning-tree guard

Syntax Description

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

Command Default

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to enable Root Guard:

```
switch(config-if)# spanning-tree guard root
switch(config-if)#
```

Related Commands

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