1 MSTP Commands

Command	Function
bpdu src-mac-check	Enable the bridge protocol data unit (BPDU) source MAC address check on an interface.
bridge-frame forwarding protocol bpdu	Enable BPDU transparent transmission.
clear spanning-tree counters	Clear statistics on sent and received STP packets.
clear spanning-tree detected-protocols	Clear the original protocol and force the device to migrate to the RSTP protocol.
clear spanning-tree mst topochange record	Clear STP topology change information.
instance	Create/enter an instance and move a VLAN from the original instance to the instance.
l2protocol-tunnel stp	Enable the global STP BPDU tunnel function.
l2protocol-tunnel stp enable	Enable the STP BPDU tunnel function on an interface.
l2protocol-tunnel stp tunnel-dmac	Configure the tunnel address for transmitting STP BPDUs from a customer network.
name	Configure a name for an MST region.
revision	Configure a revision number for an MST region.
show l2protocol-tunnel stp	Display the configuration of a BPDU tunnel.
show spanning-tree	Display the global spanning tree configuration and status information.
show spanning-tree interface	Display the spanning tree configuration and status information of an interface.
show spanning-tree mst	Display the MST region configuration.
show spanning-tree mst topochange record	Display spanning tree topology change records.
spanning-tree	Enable the STP function or configure STP global time parameters.
spanning-tree autoedge	Enable the autoedge function on a designated port.
spanning-tree bpdufilter	Enable the BPDU filter function on an interface so that the interface neither sends nor receives BPDUs,

	but works in forwarding state.
spanning-tree bpduguard	Enable or disable the BPDU guard function on an interface so that the interface enters error-disabled state when receiving a BPDU.
spanning-tree compatible enable	Enable the spanning tree compatibility mode on an interface.
spanning-tree guard loop	Enable the loop guard function on an interface.
spanning-tree guard none	Disable the guard function on an interface.
spanning-tree guard root	Enable the root guard function on an interface.
spanning-tree ignore tc	Enable the TC filter function on an interface so that the interface diffuses only TC packets generated by itself and does not diffuse received TC packets.
spanning-tree link-type	Forcibly set the connection type of an interface to point-to-point or shared.
spanning-tree loopguard default	Enable the global loop guard function.
spanning-tree mode	Set the spanning tree mode to STP, RSTP, or MSTP.
spanning-tree mst configuration	Enter the MST configuration mode.
spanning-tree mst cost	Configure a port path cost.
spanning-tree mst port-priority	Configure a port priority.
spanning-tree mst priority	Configure a bridge priority.
spanning-tree pathcost method	Configure the method of calculating the default port path cost.
spanning-tree portfast	Configure an interface as an edge port and enable the interface to rapidly enter forwarding state.
spanning-tree portfast bpdufilter default	Enable the global BPDU filter function.
spanning-tree portfast bpduguard default	Enable the global BPDU guard function.
spanning-tree portfast default	Configure all interfaces as edge ports and enable them to rapidly enter forwarding state.
spanning-tree reset	Restore spanning tree parameters to default values.
spanning-tree tc-guard	Enable the TC guard function on an interface.
spanning-tree tc-protection	Enable the global TC protection function.
spanning-tree tc-protection tc-guard	Enable the global TC guard function.

1.1 bpdu src-mac-check

Function

Run the **bpdu src-mac-check** command to enable the bridge protocol data unit (BPDU) source MAC address check on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The BPDU source MAC address check function is disabled on an interface by default.

Syntax

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

default bpdu src-mac-check

Parameter Description

H.H.H: Source MAC address to be matched by BPDUs.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

The Spanning Tree protocol (STP) functions available in interface configuration mode can be configured and take effect only on L2 switching ports. Otherwise, the configuration will fail. If an interface is not an L2 switching port, run the **switchport** command to convert it into an L2 switching port.

If the peer device connects to the local device in a point-to-point manner and the MAC address of the peer device is certain, the BPDU source MAC address check function can be configured on the local device. After this function is enabled, the device receives only BPDU frames matching the designated source MAC address and discards all the other BPDU frames. In addition, when the device encounters BPDU packet attacks, illegitimate BPDU packets can be identified and discarded to prevent the Multiple Spanning Tree Protocol (MSTP) function failure due to the attacks.

Only one BPDU source MAC check address can be configured for one interface.

Examples

The following example enables the BPDU source MAC address check function on port TenGigabitEthernet t 0/1 to receive only BPDU frames whose source MAC address is 00d0.f800.1e2f.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# bpdu src-mac-check 00d0.f800.1e2f
```

Notifications

N/A

Common Errors

An interface is not configured as an L2 switching port, and as a result, the BPDU source MAC address check function fails to be configured.

Platform Description

N/A

Related Commands

N/A

1.2 bridge-frame forwarding protocol bpdu

Function

Run the **bridge-frame forwarding protocol bpdu** command to enable BPDU transparent transmission.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

BPDU transparent transmission is disabled by default.

Syntax

bridge-frame forwarding protocol bpdu

no bridge-frame forwarding protocol bpdu

default bridge-frame forwarding protocol bpdu

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

IEEE 802.1Q uses the destination MAC address (0180.c200.0000) of BPDUs as the reserved address. When a device supporting IEEE 802.1Q receives a frame with the destination address of 0180.c200.0000, it recognizes the frame as a BPDU and will not forward it.

However, in the actual network deployment, some BPDU frames need to be transparently transmitted by devices. For example, STP is disabled on device A but enabled on devices B and C that are connected through device A. In this case, device A needs to transparently transmit BPDU frames so that devices B and C can normally perform STP calculation.

BPDU transparent transmission takes effect only when STP is disabled. When STP is enabled on a device, the device will not transparently transmit BPDU frames.

Examples

The following example enables the BPDU transparent transmission function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# bridge-frame forwarding protocol bpdu
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 clear spanning-tree counters

Function

Run the **clear spanning-tree counters** command to clear statistics on sent and received STP packets.

Syntax

clear spanning-tree counters [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Clears statistics on STP packets sent and received by this specified interface.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

This command is used to clear statistics on sent and received STP packets.

Examples

The following example clears statistics on sent and received STP packets.

```
Hostname> enable
Hostname# clear spanning-tree counters
```

The following example clears statistics on STP packets sent and received by interface TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear spanning-tree counters interface tenGigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

-
-
-
- **show spanning-tree**

1.4 clear spanning-tree detected-protocols

Function

Run the **clear spanning-tree detected-protocols** command to clear the original protocol and force the device to migrate to the RSTP protocol.

Syntax

clear spanning-tree detected-protocols [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies an interface.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

When finding that the peer device supports the Rapid Spanning Tree Protocol (RSTP), the administrator can configure this command to force all interfaces to send RSTP BPDUs and check the version of received BPDU frames so that the two interconnected devices migrate to RSTP. This function is also called protocol migration.

Examples

The following example clears the original protocol and forces the device to migrate to RSTP.

```
Hostname> enable
Hostname# clear spanning-tree detected-protocols
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 clear spanning-tree mst topochange record

Function

Run the **clear spanning-tree mst topochange record** command to clear STP topology change information.

Syntax

clear spanning-tree mst *instance-id* **topochange record**

Parameter Description

instance-id: Instance ID. The value range is from 0 to 64. Only instance **0** is valid for STP and RSTP.

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the spanning tree topology change records, clears the topology change information of STP instance **0**, and then displays the spanning tree topology change records again.

```
Hostname> enable
Hostname# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time                Interface            Old status    New status    Type
2013.5.1 4:18:46    TE0/6                Learning      Forwarding    Normal
Hostname# clear spanning-tree mst 0 topochange record
Hostname# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst topochange record**

1.6 instance

Function

Run the **instance** command to create/enter an instance and move a VLAN from the original instance to the instance.

Run the **no** form of this command to delete an instance (not instance **0**) or move a VLAN in an instance (not instance **0**) to instance **0**.

Run the **default** form of this command to delete an instance (not instance **0**) and move all the VLANs in the instance (not instance **0**) to instance **0**.

Only instance **0** exists and all VLANs belong to instance **0** by default.

Syntax

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

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

default instance *instance-id*

Parameter Description

instance-id: Instance ID. The value range is from 0 to 64.

vlan *vlan-range*: Indicates the VLAN list. The value range of a VLAN ID is from 1 to 4094. The VLAN list can contain one or more VLANs. You can separate VLAN IDs by commas (,) or connect continuous VLAN IDs by using a hyphen (-).

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

If a device has a small physical memory (such as 64 MB), creating 64 instances may result in memory insufficiency when devices are stacked. You are advised to control the number of created instances in the case of stacking.

Instance **0** can be neither created nor deleted. Custom instances 1–64 can be created and deleted. You cannot delete VLANs from instance **0** but can delete those from custom instances. Deleting a VLAN from a custom instance will move the VLAN to instance **0**.

In the **instance** *instance-id* **vlan** *vlan-range* command, the value range of *instance-id* is from 0 to 64.

In the **no instance** *instance-id* [**vlan** *vlan-range*] and **default instance** *instance-id* commands, the value of *instance-id* cannot be **0** and its value range is from 1 to 64.

The **no instance** *instance-id* command (without the **vlan** *vlan-range* parameter) command has the same function as the **default instance** *instance-id* command, that is, delete an instance (not instance **0**) and move all the VLANs in the instance (not instance **0**) to instance **0**.

The **no instance** *instance-id* **vlan** *vlan-range* command (carrying the **vlan** *vlan-range* parameter) can move a VLAN in an instance (not instance **0**) to instance **0**. If there are multiple VLANs in the specified instance, you

can carry the **vlan** *vlan-range* parameter in this command to move the specified VLANs to instance **0**. Moving all VLANs in an instance to instance **0** will delete the instance.

Examples

The following example enters the MST configuration mode, moves VLAN 3 and VLANs 5–10 to instance **1**, and displays the multiple spanning tree (MST) region configuration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 3, 5-10
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      :
Revision : 0
Instance  Vlans Mapped
--------  ----------------
0         1-2,4,11-4094
1         3,5-10
```

The following example moves VLAN 3 from instance **1** to instance **0**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# no instance 1 vlan 3
```

The following example deletes instance **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# no instance 1
```

Notifications

When you move a VLAN to an instance, the following notification will be displayed:

```
%Warning:you must create vlans before configuring instance-vlan relationship.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **name**
- **revision**
- **show spanning-tree mst**

1.7 l2protocol-tunnel stp

Function

Run the **l2protocol-tunnel stp** command to enable the global STP BPDU tunnel function.

Run the **no** form of this command to disable this feature.

The global STP BPDU tunnel function is disabled by default.

Syntax

l2protocol-tunnel stp

no l2protocol-tunnel stp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

In 802.1Q in 802.1Q (QinQ) application, after the STP BPDU tunnel function is enabled, STP packets from the customer network can be transparently transmitted through tunnels of the service provider network. In this way, the STP calculations of the customer network and service provider network are performed separately without mutual interference. 01D0.f800.0005 is the default BPDU tunnel address.

The STP BPDU tunnel function needs to be enabled in both global configuration mode and interface configuration mode so that STP packets can be transparently transmitted through tunnels.

Examples

The following example enables the STP BPDU tunnel function in both global configuration mode and interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# l2protocol-tunnel stp enable
Hostname(config-if-TenGigabitEthernet 0/1)# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp enable**
- **l2protocol-tunnel stp tunnel-dmac**
- **show l2protocol-tunnel stp**

1.8 l2protocol-tunnel stp enable

Function

Run the **l2protocol-tunnel stp enable** command to enable the STP BPDU tunnel function on an interface.

Run the **no** form of this command to disable this feature.

The STP BPDU tunnel function is disabled on an interface by default.

Syntax

l2protocol-tunnel stp enable

no l2protocol-tunnel stp enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In QinQ application, after the STP BPDU tunnel function is enabled, STP packets from the customer network can be transparently transmitted through tunnels of the service provider network. In this way, the STP calculations of the customer network and service provider network are performed separately without mutual interference. 01D0.f800.0005 is the default BPDU tunnel address.

The STP BPDU tunnel function needs to be enabled in both global configuration mode and interface configuration mode so that STP packets can be transparently transmitted through tunnels.

Examples

The following example enables the STP BPDU tunnel function in both global configuration mode and interface configuration mode.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# l2protocol-tunnel stp
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode dot1q-tunnel
Hostname(config-if-TenGigabitEthernet 0/1)# l2protocol-tunnel stp enable
Hostname(config-if-TenGigabitEthernet 0/1)# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp tunnel-dmac**
- **show l2protocol-tunnel stp**

1.9 l2protocol-tunnel stp tunnel-dmac

Function

Run the **l2protocol-tunnel stp tunnel-dmac** command to configure the tunnel address for transmitting STP BPDUs from a customer network.

Run the **no** form of this command to remove this configuration.

The default tunnel address for transmitting STP BPDUs from a customer network is 01d0.f800.0005.

Syntax

l2protocol-tunnel stp tunnel-dmac *mac-address*

no l2protocol-tunnel stp tunnel-dmac

Parameter Description

mac-address: Tunnel address for transmitting STP BPDUs from a customer network. The value range is 01d0.f800.0005 (default), 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

After an STP packet from a customer network is transmitted to a provider edge (PE) of a service provider network, the PE changes the destination MAC address of the packet from the BPDU dedicated address (0180.c200.0000) to the tunnel address (01d0.f800.0005 by default) and forwards the packet in the service provider network. When the packet reaches a PE at the other end, the PE restores the destination MAC address of the packet from the tunnel address (01d0.f800.0005 by default) to the BPDU dedicated address (0180.c200.0000) and forwards the packet to the peer customer network. The BPDU tunnel function is used to transmit STP packets from a customer network through tunnels in a service provider network so that STP calculations of the customer network and service provider network are performed separately without mutual interference.

Examples

The following example sets the tunnel address for transmitting STP BPDUs from a customer network to 011a.a900.0005.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

Notifications

When the configured tunnel address for transmitting STP BPDUs from a customer network is not within the above range, the following notification will be displayed:

```
Optional at the following addresses: 01d0.f800.0005, 011a.a900.0005,
010f.e200.0003 or 0100.0ccd.cdd0-d2.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp enable**
- **show l2protocol-tunnel stp**

1.10 name

Function

Run the **name** command to configure a name for an MST region.

Run the **no** form of this command to remove this configuration.

The default name of an MST region is an empty string.

Syntax

name *name*

no name

Parameter Description

name: Name of an MST region. The value is a string of up to 32 bytes.

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

The **show spanning-tree mst configuration** command is used to display information about the current MST region, including the name of the MST region.

Examples

The following example enters the MST configuration mode and sets the name of an MST region to Region 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# name region1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **revision**
- **show spanning-tree mst**

1.11 revision

Function

Run the **revision** command to configure a revision number for an MST region.

Run the **no** form of this command to remove this configuration.

The default revision number of an MST region is **0**.

Syntax

revision *version*

no revision

Parameter Description

version: Revision number of an MST region. The value range is from 0 to 65535.

Command Modes

MST configuration mode

Default Level

15

Usage Guidelines

The **show spanning-tree mst configuration** command is used to display information about the current MST region, including the revision number of the MST region.

Examples

The following example enters the MST configuration mode and sets the revision number of an MST region to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# revision 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **name**
- **show spanning-tree mst**

1.12 show l2protocol-tunnel stp

Function

Run the **show l2protocol-tunnel stp** command to display the configuration of a BPDU tunnel.

Syntax

show l2protocol-tunnel stp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the configuration of a BPDU tunnel.

```
Hostname> enable
Hostname# show l2protocol-tunnel stp
L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address:011a.a900.0005
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Table 1-1Output Fields of the show l2protocol-tunnel stp Command

Field	Description
L2protocol-tunnel	Whether the L2 protocol tunnel function is enabled ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
L2protocol-tunnel destination mac address	MAC address of the L2 protocol tunnel
TenGigabitEthernet 0/1 l2protocol-tunnel stp enable	Port with the L2 protocol tunnel function enabled

Notifications

N/A

Platform Description

N/A

Related Commands

- **l2protocol-tunnel stp**
- **l2protocol-tunnel stp enable**
- **l2protocol-tunnel stp tunnel-dmac**

1.13 show spanning-tree

Function

Run the **show spanning-tree** command to display the global spanning tree configuration and status information.

Syntax

show spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **mst** *instance-id* | **pathcost method** | **tx-hold-count**]

show spanning-tree [**counters** | **inconsistentports** | **summary**]

show spanning-tree [**v-stp information**]

Parameter Description

forward-time: Displays the port status change interval (**Bridge Forward Delay**).

hello-time: Displays the interval for periodically sending BPDUs (**Bridge Hello Time**).

max-age: Displays the maximum timeout time of a BPDU (**Bridge Max Age**).

mst *instance-id*: Displays the global spanning tree configuration of a specified instance.

max-hops: Specifies the maximum hop count of BPDUs.

pathcost method: Displays the path cost calculation method.

tx-hold-count: Displays the maximum number of BPDUs that can be sent per second.

counters: Displays statistics on sent and received STP packets.

inconsistentports: Displays ports blocked due to root guard or loop guard.

summary: Displays the spanning tree topology and port forwarding status.

v-stp information: Displays information about the V-STP function.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

Packets with the timeout time out of **max-age** will be discarded.

Forward-time indicates the interval for STP to transition from the listening state to the learning state or from the learning state to the forwarding state. After port role election is complete, a port waits for twice the period of **Forward Delay** before entering the forwarding state.

The restrictive relationship among the values of **forward-time, hello-time, and max-age** is as follows: 2 × (**Hello Time** + 1s) ≤ **Max Age** ≤ 2 × (**Forward Delay** – 1s). The values must meet this condition. Otherwise, the topology may be unstable.

A device selects an interface with the minimum sum of root path costs as the root port. Configuring **pathcost method** (the default value is **long**) will affect the port path cost and further affect the topology of the entire network.

The **show spanning-tree** command displays spanning tree information only after the **spanning-tree** command is run to enable STP.

Examples

The following example displays the global spanning tree configuration. All information will be displayed if no parameter is carried in the command. If parameters [**forward-time** | **hello-time** | **max-age** | **max-hops** | **mst** *instance-id* | **pathcost method** | **tx-hold-count**] are carried, specified global configuration will be displayed.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree
Hostname(config)# show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef  : Disabled

###### mst 0 vlans map : ALL
BridgeAddr : 00d0.f822.4444
Priority: 32768
TimeSinceTopologyChange : 3d:20h:16m:49s
TopologyChanges : 0
DesignatedRoot : 32768.00d0.f822.4444
RootCost : 0
RootPort : 0
CistRegionRoot : 32768.00d0.f822.4444
CistPathCost : 0
```

The following example displays the interval for sending STP BPDUs after the **hello-time** parameter is carried in the command.

```
Hostname> enable
Hostname# show spanning-tree hello-time
BridgeHelloTime :2
```

The following example displays global spanning tree configuration of instance **0** after the **mst** *instance-id* parameter is carried in the command.

```
Hostname# show spanning-tree mst 0
```

```
###### MST 0 vlans mapped : ALL
BridgeAddr : 00d0.f822.4444
Priority: 32768
TimeSinceTopologyChange : 3d:21h:7m:35s
TopologyChanges : 0
DesignatedRoot : 32768.00d0.f822.4444
RootCost : 0
RootPort : 0
CistRegionRoot : 32768.00d0.f822.4444
CistPathCost : 0
```

Table 1-1Output Fields of the show spanning-tree Command

Field	Description
StpVersion	STP version ● MSTP ● RSTP ● STP
SysStpStatus	STP status ● ENABLED ● DISABLED
Max Age	Aging time of STP BPDUs. The default value is **20**.
Hello Time	Interval for STP to send two adjacent BPDUs. The default value is **2**.
Forward Delay	Duration of STP in the listening and learning states. The default value is **15**.
BridgeMaxAge	Aging time of BPDUs on this device. The default value is **20**.
BridgeHelloTime	Interval for the device to send two adjacent BPDUs. The default value is **2**.
BridgeForwardDelay	Duration of STP in the listening and learning states on this device. The default value is **15**.
MaxHops	Maximum hop count of BPDUs. The default value is **20**.
PathCostMethod	Path cost calculation method ● **long**: Uses the path cost specified in IEEE 802.1t. ● **long standard**: Calculates the cost value by using a formula according to IEEE 802.1t. ● **short**: Uses the path cost specified in IEEE 802.1d.
TxHoldCount	Maximum number of BPDUs that can be sent per second
BPDUGuard	Status of the global BPDU guard function ● Enabled ● Disabled

Field	Description
BPDUFilter	Status of the global BPDU filter function ● Enabled ● Disabled
LoopGuardDef	Status of the global loop guard function ● Enabled ● Disabled
BridgeAddr	Bridge address of the device
Priority	Bridge priority of the device
TimeSinceTopologyChange	Time that has elapsed since the last topology change, in the format of "d:h:m:s", that is, "day:hour:minute:second".
TopologyChanges	Number of topology change times
DesignatedRoot	ID of a designated bridge
RootCost	Root path cost
RootPort	Root port
CistRegionRoot	Bridge ID of a region root
CistPathCost	Path cost from the region root to CIST root

The following example displays ports that are blocked due to root guard or loop guard.

```
Hostname> enable
Hostname# show spanning-tree inconsistentports
Name                 Interface              Inconsistent
-------------------- ---------------------- ------------------

Current Number of Inconsistent ports    :   0
```

Table 1-2Output Fields of the show spanning-tree Command

Field	Description
Name	Name
Port	Port name
Inconsistent	Blocking status
Current Number of Inconsistent ports	Number of ports that are blocked due to root guard or loop guard

The following example displays statistics on sent and received STP packets.

```
Hostname> enable
Hostname# show spanning-tree counters
---------------------- STP BPDU count ----------------------
 Port                            Receive          Send
 TenGigabitEthernet 0/1               0             122594

------------------------ STP TC or TCN count -------------------------
 MSTID      Port                              Receive      Send
 0           TenGigabitEthernet 0/1               0            0
```

Table 1-3Output Fields of the show spanning-tree Command

Field	Description
Port	Port ID
Receive	Number of packets received by the port
Send	Number of packets sent by the port
MSTID	Spanning tree instance ID

The following example displays the spanning tree topology and port forwarding status.

```
Hostname> enable
Hostname # show spanning-tree summary
Spanning tree enabled protocol stp
  Root ID    Priority    0
             Address     00d0.f822.3344
             this bridge is root
             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    0
             Address     00d0.f822.3344
             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Te0/2            Desg FWD 20000      128      False    P2p
Te0/1            Desg FWD 20000      128      False    P2p
```

Table 1-4Output Fields of the show spanning-tree Command

Field	Description
Root ID	Spanning tree information of the root device recognized by the local device
Bridge ID	Spanning tree information of the local device
Priority	Bridge priority

Field	Description
Address	Device MAC address
Hello Time	Interval for sending two adjacent BPDUs
Forward Delay	Duration of STP in the listening and learning states
Max Age	Aging time of BPDUs
Port	STP port
Role	Port role
Sts	Port status
Cost	Port path cost
Prio	Port priority
OperEdge	Edge port attribute ● **True**: Edge port ● **False**: Non-edge port
Type	Port connection status ● **P2p**: Point-to-point connection ● **Shared**: Shared connection

The following example displays V-STP information.

```
Hostname> enable
Hostname# show spanning-tree v-stp information
V-STP status                  : disable
Local bridge mac              : 00d0.f822.4444
Selected bridge mac           : 0000.0000.0000
Peerlink Port                 : Virtual-port
Calculate Virtual Index     : 4095
Mlag Remote device connected : N
MST 0 Root Port          : None
```

Table 1-5Output Fields of the show spanning-tree Command

Field	Description
V-STP status	V-STP status ● enable ● disable
Local bridge mac	MAC address of the local bridge
Selected bridge mac	MAC address of the selected bridge
Peerlink Port	Peerlink port of an M-LAG group

Field	Description
Calculate Virtual Index	Calculated virtual index
Mlag Remote device connected	Connection status of the M-LAG remote device ● **Y**: Connected ● **N**: Disconnected
MST 0 Root Port	Root port of instance **0**

Notifications

If the global spanning tree configuration is queried when STP is disabled, the following notification will be displayed:

```
No spanning tree instance exists.
```

Platform Description

N/A

Related Commands

- **spanning-tree**
- **spanning-tree pathcost method**

1.14 show spanning-tree interface

Function

Run the **show spanning-tree interface** command to display the spanning tree configuration and status information of an interface.

Syntax

show spanning-tree [**mst** *instance-id*] **interface** *interface-type interface-number* [**bpdufilter** | **bpduguard** | **link-type** | **portfast**]

show spanning-tree [**mst** *instance-id*] *port-index*

Parameter Description

mst *instance-id*: Displays the configuration and status information of an interface in a specified instance.

interface *interface-type interface-number*: Displays the spanning tree configuration and status information of an interface by interface type and interface number (for example, TenGigabitEthernet 0/1).

port-index: Displays the spanning tree configuration and status information of an interface by interface number (for example, 1). The value range is from 0 to 65535. The actual value cannot exceed the maximum port ID. TenGigabitEthernet 0/1 is 1 and *port-index* of port TenGigabitEthernet 0/2 is 2.

bpdufilter: Displays whether the BPDU filter function is enabled on an interface.

bpduguard: Displays whether the BPDU guard is enabled on an interface.

link-type: Displays the connection type of an interface.

portfast: Displays whether the fast forwarding function is enabled on an interface and whether the interface is an edge port.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

For an interface in up state, you can run the **show spanning-tree interface** *interface-type interface-number* command without any parameter to display all characteristic states of the interface. For an interface in down state, the above command cannot display all characteristic states but you can run the [**bpdufilter** | **bpduguard** | **link-type** | **portfast**] command with parameters contained in the command to display required information.

Examples

The following example displays the statuses of interfaces TenGigabitEthernet 0/1 and TenGigabitEthernet 0/2.

```
Hostname> enable
Hostname(config)# show interface description
Interface                  Status   Administrative Description
------------------------ -------- -------------- -----------
TenGigabitEthernet 0/1        up       up
TenGigabitEthernet 0/2        down     up
Hostname(config)# exit
```

The following example displays the spanning tree configuration of port TenGigabitEthernet 0/1 (the port status is up).

```
Hostname# show spanning-tree interface tenGigabitEthernet 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : None

###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
```

```
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
```

The following example displays the spanning tree configuration of port TenGigabitEthernet 0/2 (the port status is down).

```
Hostname# show spanning-tree interface tenGigabitEthernet 0/2
no spanning tree info available for TenGigabitEthernet 0/2.
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 bpdufilter
PortBPDUFilter : Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 portfast
PortAdminPortFast :Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 bpduguard
PortBPDUGuard : Disabled
Hostname# show spanning-tree interface tenGigabitEthernet 0/2 link-type
PortAdminLinkType : auto
```

Table 1-1Output Fields of the show spanning-tree interface Command

Field	Description
PortAdminPortFast	Whether a fast forwarding port is configured
PortOperPortFast	Whether the port is in fast forwarding state
PortAdminAutoEdge	Whether an autoedge port is configured
PortOperAutoEdge	Whether the port is in autoedge state
PortAdminLinkType	Link type configured for the port
PortOperLinkType	Actual link type of the port
PortBPDUGuard	Status of the BPDU guard function of the port
PortBPDUFilter	Status of the BPDU filter function of the port
PortGuardmode	Port guard mode
MST *instance-id* vlans mapped	VLAN list mapped to an instance
PortState	Port forwarding status in an instance
PortPriority	Port priority in an instance
PortDesignatedRoot	Designated root bridge of the port in an instance
PortDesignatedCost	External root path cost of the port in an instance
PortDesignatedBridge	Designated bridge of the port in an instance
PortDesignatedPortPriority	Priority of the designated port in an instance

Field	Description
PortDesignatedPort	Designated port in an instance
PortForwardTransitions	Number of times that the port transitions to the forwarding state in an instance
PortAdminPathCost	Path cost configured for the port in an instance
PortOperPathCost	Actual path cost of the port in an instance
Inconsistent states	Root or loop inconsistent state of the port in an instance
PortRole	Port role

Notifications

When you view all spanning tree information of a port in down state, the following notification will be displayed:

```
no spanning tree info available for TenGigabitEthernet 0/2.
```

When you enter a value in the range of 0 to 65535 but beyond the port ID in the *port-index* parameter, the following notification will be displayed:

```
no spanning tree info available for the interface.
```

Platform Description

N/A

Related Commands

- **spanning-tree autoedge**
- **spanning-tree bpdufilter**
- **spanning-tree bpduguard**
- **spanning-tree link-type**
- **spanning-tree portfast**

1.15 show spanning-tree mst

Function

Run the **show spanning-tree mst** command to display the MST region configuration.

Syntax

show spanning-tree mst configuration

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays the MST region configuration before an instance is configured.

```
Hostname> enable
Hostname# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name     :
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0        : ALL
------------------------------------------------------
```

The following example displays the MST region configuration after VLAN 1 is added to instance 1.

```
Hostname> enable
Hostname# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name     : test
Revision : 0
Instance  Vlans Mapped
--------  ---------------
0        : 2-4094
1        : 1
------------------------
```

Table 1-1 Output Fields of the show spanning-tree mst Command

Field	Description
Multi spanning tree protocol	Whether MSTP is enabled
Name	Name of an MST region
Revision	Version of the MST region
Instance Vlans Mapped	Mapping between instances and VLANs

Notifications

N/A

Platform Description

N/A

Related Commands

- instance
- name
- revision
- spanning-tree
- spanning-tree mst configuration
- spanning-tree mst cost
- spanning-tree mst port-priority
- spanning-tree mst priority

1.16 show spanning-tree mst topochange record

Function

Run the **show spanning-tree mst topochange record** command to display spanning tree topology change records.

Syntax

show spanning-tree mst *instance-id* **topochange record**

Parameter Description

instance-id: ID of a specified instance whose spanning tree topology changes need to be displayed. The value range is from 0 to 64. Instance **0** exists by default and instances 1–64 can be customized.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display topology changes of an interface by instance, including the interface experiencing a status change, status change time, old status, new status, and cause for the status change.

Examples

The following example displays the spanning tree topology change records of instance 0.

```
Hostname> enable
Hostname# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time                 Interface          Old status    New status    Type
2013.5.1 4:18:46      Te0/1              Learning      Forwarding    Normal
```

Table 1-1Output Fields of the show spanning-tree mst topochange record Command

Field	Description
Time	Topology change time of an interface
Port	Interface experiencing the topology change
Old status	Old spanning tree status of the interface ● **Discarding**: Discarded state ● **Learning**: Learning state ● **Forwarding**: Forwarding state
New status	New spanning tree status of the interface ● **Discarding**: Discarded state ● **Learning**: Learning state ● **Forwarding**: Forwarding state
Type	Cause for the topology change of the interface. The possible causes are as follows: ● **Normal**: Normal status change of the interface, for example, status change when the interface is up/down. ● **LoopGuard Block**: The interface enters blocking state due to loop inconsistency. ● **RootGuard Block**: The interface enters blocking state due to root inconsistency. ● **Inferior Block**: The interface enters blocking state because it receives a BPDU of a lower priority. ● **LoopGuard Unblock**: The interface recovers from loop inconsistency and enters forwarding state. ● **RootGuard Unblock**: The interface recovers from root inconsistency and enters forwarding state. ● **Inferior Unblock**: The interface does not receive BPDUs of a lower priority and enters forwarding state.

Notifications

When a specified instance does not have topology change, the following notification will be displayed ([dec] indicates the instance ID):

```
%There's no topology change information has been record on mst [ dec ].
```

Platform Description

N/A

Related Commands

- clear spanning-tree mst topochange record

1.17 spanning-tree

Function

Run the **spanning-tree** command to enable the STP function or configure STP global time parameters.

Run the **no** form of this command to disable this feature or remove this configuration.

Run the **default** form of this command to restore the default configuration.

The STP function is enabled by default.

The STP function is disabled by default.

Syntax

spanning-tree [**forward-time** *forward* | **hello-time** *hello* | **max-age** *age* | **max-hops** *hop-count* | **timer-factor** *factor* | **tx-hold-count** *count*]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count**]

default spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count** }

spanning-tree [**forward-time** *forward* | **hello-time** *hello* | **max-age** *age* | **max-hops** *hop-count* | **tx-hold-count** *count*]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count**]

default spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **tx-hold-count** }

Parameter Description

forward-time *forward*: Specifies the port status change interval, in seconds. After port role election is complete, STP waits for twice the period of **Forward Delay** before entering the forwarding state, that is, the interval for STP to transition from listening state to learning state and from learning state to forwarding state. The value range is from 4 to 30. The default value is **15**.

hello-time *hello*: Specifies the interval for the device to periodically send BPDUs, in seconds. The value range is from 1 to 10. The default value is **2**.

max-age *age*: Specifies the maximum timeout time of BPDUs, in seconds. Packets beyond **max age** will be discarded. The value range is from 6 to 40. The default value is **20**.

max-hops *hop-count*: Specifies the maximum hop count of BPDU frames of all MSTIs, that is, the number of devices that BPDUs of MSTIs can pass through before the BPDUs are discarded. The value range is from 1 to 40, and the default value is **20**.

tx-hold-count *count*: Configures the maximum number of BPDUs that can be sent per second. The value range is from 1 to 10, and the default value is **3**.

timer-factor *factor*: Configures the packet receiving timeout factor. Timeout time = Timeout factor (indicated by *factor*) × Hello Time. If a device fails to receive a BPDU from the upstream device within the timeout time, it re-calculates the spanning tree. The value range is from 1 to 30, and the default value is **20**.

timer-factor *factor*: Configures the packet receiving timeout factor. The timeout time is calculated as follows: Timeout time = Timeout factor (indicated by *factor*) × Hello Time. If a device fails to receive a BPDU from the upstream device within the timeout time, it re-calculates the spanning tree. The value range is from 1 to 30, and the default value is **3**.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The restrictive relationship among the values of **forward-time, hello-time, and max-age** is as follows: 2 × (**Hello Time** + 1s) ≤ **Max Age** ≤ 2 × (**Forward Delay** – 1s). The values must meet this condition. Otherwise, the topology may be unstable.

In an MST region, the BPDU sent by the root bridge contains the **Hot Count** field. The BPDU hop count decreases by 1 each time the BPDU passes through one device from the root bridge till the hop count becomes 0, indicating that the BPDU will be discarded by the receiving device due to timeout. In general, the default value of **max-hops** does not need to be changed for a network with the scale less than 20 hops, but needs to be changed to match the actual network situation when the network scale is greater than 20 hops. Changing the maximum hop count will affect all instances.

You can run the **show spanning-tree** command to display the STP global configuration.

Examples

The following example enables the MSTP function and sets **Forward Delay** to 10s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree
Hostname(config)# spanning-tree forward-time 10
```

The following example sets the maximum number of BPDUs that can be sent per second to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tx-hold-count 5
```

The following example sets the timeout factor to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#spanning-tree timer-factor ?
  <1-30>  Range of timer factor  (default value: 3)
Hostname(config)# spanning-tree timer-factor 4
```

The following example sets the maximum hop count of BPDUs to 30 for all instances on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree max-hops 30
```

Notifications

When the **spanning-tree** command is configured to enable the STP protocol, the following notification will be displayed:

```
Enable spanning-tree.
```

STP and the Transparent Interconnection of Lots of Links (TRILL) protocol of data centers are mutually exclusive. When STP is enabled after TRILL is enabled, the following notification will be displayed:

```
% Error! You must disable TRILL first.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show spanning-tree

1.18 spanning-tree autoedge

Function

Run the **spanning-tree autoedge** command to enable the autoedge function on a designated port.

Run the **spanning-tree autoedge disabled** command to disable this feature.

The autoedge function of a designated port is enabled by default.

Syntax

spanning-tree autoedge [**disabled**]

Parameter Description

disabled: Disables the autoedge function of an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In a spanning tree topology, each LAN connects to the root bridge through a designated port of the upstream node. After this command is configured, if a designated port fails to receive a BPDU from the downstream port within a period of time (3s), it deems that the device connected to this port is a terminal, automatically deems itself as an edge port, and enters forwarding state. If receiving a BPDU, the port identified as an edge port will be automatically identified as a non-edge port.

Caution

The autoedge function can be enabled only on designated ports.

RSTP and MSTP support the autoedge function but STP does not support the function.

If BPDU filter has been enabled on a port, the port directly enters forwarding state and is not automatically identified as an edge port.

You can run the **show spanning-tree interface** *interface-type interface-number* command to display the spanning tree configuration of an interface. When the value of the **PortAdminAutoEdge** field is **Enabled**, this function is enabled. The value **Disabled** indicates that this function is disabled.

Examples

The following example disables the autoedge function of port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree autoedge disabled
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**

1.19 spanning-tree bpdufilter

Function

Run the **spanning-tree bpdufilter** command to enable the BPDU filter function on an interface so that the interface neither sends nor receives BPDUs, but works in forwarding state.

Run the **spanning-tree bpdufilter disabled** command to disable this feature.

The BPDU filter function is disabled on an interface by default.

Syntax

spanning-tree bpdufilter { **enabled | disabled** }

Parameter Description

enabled: Enables the BPDU filter function on an interface.

disabled: Disables the BPDU filter function on an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

BPDU filter is a method of preventing BPDU attacks. When BPDU filter is enabled, a port neither sends nor receives BPDUs, but directly enters forwarding state. If a port receives a BPDU, it transitions to disabled state and the BPDU filter function automatically fails.

BPDU filter can be enabled globally or on interfaces.

- The **spanning-tree portfast bpdufilter default** command is used to enable the global BPDU filter function. The global BPDU filter function takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with the port fast configuration, the port fast configuration prevails.
- The **spanning-tree bpdufilter enabled** command is used to enable the BPDU filter function on an interface. The function takes effect on the interface regardless of whether the interface is an edge port.

Note

In general, when a port running STP transitions from listening state to learning state and then to forwarding state, it needs to wait for twice the period of **Forward-Delay** (2 × 15 = 30s by default). If a device port directly connects to a network terminal, you can enable the BPDU filter function to enable the port to work in forwarding state.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpdufilter** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the BPDU filter function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree bpdufilter enabled
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**
- **spanning-tree portfast bpdufilter default**

1.20 spanning-tree bpduguard

Function

Run the **spanning-tree bpduguard** command to enable or disable the BPDU guard function on an interface so that the interface enters error-disabled state when receiving a BPDU.

The BPDU guard function is disabled on an interface by default.

Syntax

spanning-tree bpduguard { **enable** | **disabled** }

Parameter Description

enable: Enables the BPDU guard function on an interface.

disabled: Disables the BPDU guard function on an interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

If a user illegally connects to a network device to an interface, to which a terminal should be connected, the network device may send BPDUs, causing a network topology change. If an interface with BPDU guard enabled receives a BPDU, it starts the BPDU guard mechanism, enters the error-disabled state, and is disabled, indicating that a network exception occurs.

An interface in error-disabled state can be restored automatically or manually. The **errdisable recovery** [**interval** *seconds*] command is used to configure the interval for automatically restoring a port from error-disabled state, in seconds. The value range is from 30 to 86400. The **errdisable recovery** command is used to manually restore a port from error-disabled state.

BPDU guard can be enabled globally or on interfaces.

- The **spanning-tree portfast bpduguard default** command is used to enable global BPDU guard, which takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with port fast configuration, the port fast configuration prevails.
- The **spanning-tree bpduguard enable** command is used to enable BPDU guard, which takes effect on interfaces regardless of whether they are edge ports.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpduguard** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the BPDU guard function on port TenGigabitEthernet 0/1 and sets the auto-recovery time to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree bpduguard enable
Hostname(config-if-TenGigabitEthernet 0/1)# errdisable recovery interval 60
```

Notifications

When an interface with BPDU guard enabled receives a BPDU, the following notification will be displayed ([char] indicates the interface name):

```
SPANTREE-BLOCK_BPDUGUARD: Received BPDU on port [ char ] with BPDU Guard enabled.
Disabling port.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **errdisable recovery** (interface/Ethernet interface)
- **show spanning-tree interface**
- **spanning-tree portfast bpduguard default**

1.21 spanning-tree compatible enable

Function

Run the **spanning-tree compatible enable** command to enable the spanning tree compatibility mode on an interface.

Run the **no** form of this command to disable this feature.

The spanning tree compatibility mode is enabled on an interface by default.

The spanning tree compatibility mode is disabled on an interface by default.

Syntax

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

After the spanning tree compatibility mode is enabled on an interface, STP calculates whether the interface participates in the calculation of a specified instance based on the VLAN, to which the interface belongs, and the mapping between the VLAN and the instance. When the interface sends a BPDU, only the MSTI configuration message of the instance calculated by the interface, is carried to ensure compatibility with other devices.

For example, instances 1 and 2 exist on a device. Port GigabitEthernet 0/1 belongs only to VLAN 10, and VLAN 10 belongs to instance 1. If the spanning tree compatibility mode is enabled on port GigabitEthernet 0/1, the BPDU sent by port GigabitEthernet 0/1 carries only information of instance 0 (the port participates in calculation of this instance by default) and instance 1, with no information of instance 2.

Examples

The following example creates instance 1 and instance 2, associates instance 1 with VLAN 10 and instance 2 with VLAN 20, adds port TenGigabitEthernet 0/1 to VLAN 10, enables the spanning tree compatibility mode on port TenGigabitEthernet 0/1, and adds port TenGigabitEthernet 0/2 to VLAN 20. After configuration, BPDUs sent by port TenGigabitEthernet 0/1 will not carry information about instance 2 and port TenGigabitEthernet 0/2 will not participate in the spanning tree calculation of instance 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 10
Hostname(config-mst)# instance 2 vlan 20
Hostname(config-mst)# exit
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# switchport mode access
Hostname(config-if-TenGigabitEthernet 0/1)# switchport access vlan 10
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree compatible enable
Hostname(config-if-TenGigabitEthernet 0/1)# exit
Hostname(config)# interface Gigabitethernet 0/2
Hostname(config-if-TenGigabitEthernet 0/2)# switchport
Hostname(config-if-GTenGigabitEthernet 0/2)# switchport mode access
Hostname(config-if-TenGigabitEthernet 0/2)# switchport access vlan 20
Hostname(config-if-TenGigabitEthernet 0/2)# spanning-tree compatible enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree mst configuration**

1.22 spanning-tree guard loop

Function

Run the **spanning-tree guard loop** command to enable the loop guard function on an interface.

Run the **no** function to disable this feature.

The loop guard function is disabled on an interface by default.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

The root port or backup port of a non-root bridge may fail to receive BPDUs due to the unidirectional link failure, and the root port becomes a designated port and enters forwarding state. As a result, loops occur in the network. To prevent this situation, you can configure loop guard on a non-root bridge.

After loop guard is enabled, when the root port or backup port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives a BPDU for spanning tree calculation.

Loop guard can be enabled globally or on interfaces.

- The **spanning-tree loopguard default** command is used to globally enable the loop guard function on all interfaces.
- The **spanning-tree guard loop** command is used to enable the loop guard function on an interface.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the loop guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-GTenGigabitEthernet 0/1)# spanning-tree guard loop
```

Notifications

When loop guard is configured after root guard is configured, the following notification will be displayed ([chars] indicates the interface name):

```
SPANTREE-ROOTGUARD_CONFIG_CHANGE: Root Guard disabled on port [ chars ].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- spanning-tree loopguard default

1.23 spanning-tree guard none

Function

Run the **spanning-tree guard none** command to disable the guard function on an interface.

Run the **no** form of this command to remove this configuration.

There is no interference in the guard function of an interface by default.

Syntax

spanning-tree guard none

no spanning-tree guard none

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

When an interface is blocked due to root guard, you can manually restore the port to the normal state by using two methods:

- Run the **no spanning-tree guard root** command to disable the root guard function on the interface.
- Run the **spanning-tree guard none** command to disable the guard function on the interface.

Examples

The following example disables the guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree guard none
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- spanning-tree guard root

1.24 spanning-tree guard root

Function

Run the **spanning-tree guard root** command to enable the root guard function on an interface.

Run the **no** form of this command to disable the root guard function on an interface.

The root guard function is disabled on an interface by default.

Syntax

spanning-tree guard root

no spanning-tree guard root

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the network design, the root bridge and backup root bridge are usually classified into the same region. Designated ports on a root bridge may receive configuration BPDUs with a higher priority due to a misconfiguration or malicious attacks, and the root bridge loses the current root bridge role. As a result, an incorrect network topology change is incurred. To prevent this situation, you can configure the root guard function on designated ports of the root bridge.

After the root guard function is enabled, the device ports are designated ports on all instances. If a port receives a high-priority BPDU, the port enters blocking state due to root-inconsistent. If the port fails to receive a high-priority BPDU within a period of time, it returns to the normal state.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the root guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree guard root
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree guard loop**
- **spanning-tree guard none**

1.25 spanning-tree ignore tc

Function

Run the **spanning-tree ignore tc** command to enable the TC filter function on an interface so that the interface diffuses only TC packets generated by itself and does not diffuse received TC packets.

Run the **no** function to disable this feature.

The TC filter function is disabled on an interface by default.

Syntax

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies

the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.
- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the TC filter function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree ignore tc
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree tc-guard**
- **spanning-tree tc-protection**
- **spanning-tree tc-protection tc-guard**

1.26 spanning-tree link-type

Function

Run the **spanning-tree link-type** command to forcibly set the connection type of an interface to point-to-point or shared.

Run the **no** form of this command to restore the default configuration.

The default connection type of an interface is auto mode. If an interface works in full-duplex mode, the connection type is point-to-point. If an interface works in half-duplex mode, the connection type is shared.

Syntax

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

no spanning-tree link-type

Parameter Description

point-to-point: Forcibly sets the connection type of an interface to point-to-point.

shared: Forcibly sets the connection type of an interface to shared.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

A designated port of RSTP can perform a Proposal/Agreement handshake with the connected bridge and rapidly enter forwarding state, to implement fast convergence. In this way, the port does not need to wait for twice the period of **Forward Delay** before entering forwarding state. Only interfaces using the point-to-point connection support fast convergence via handshake. You are advised to configure the point-to-point connection for devices, so as to give full play to the devices. If the connection type is not configured, the device automatically sets the port connection type based on the port duplex status.

You can run the **show spanning-tree interface** *interface-type interface-number* **link-type** command to display the spanning tree configuration of an interface. When the **PortAdminLinkType** field is set to **Auto**, the connection type of an interface is auto mode. The value **point-to-point** indicates that the connection type of an interface is forcibly set to point-to-point, and **shared** indicates that the connection type of an interface is forcibly set to non-point-to-point.

Examples

The following example forcibly sets the connection type of port TenGigabitEthernet 0/1 to point-to-point.

```
Hostname> enable
Hostname# show spanning-tree interface gtenGigabitEthernet 0/1 link-type
PortAdminLinkType : auto
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
```

```
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree link-type point-to-
point
Hostname(config-if-TenGigabitEthernet 0/1)# end
Hostname# show spanning-tree interface tenGigabitEthernet 0/1 link-type
PortAdminLinkType : point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**

1.27 spanning-tree loopguard default

Function

Run the **spanning-tree loopguard default** command to enable the global loop guard function.

Run the **no** form of this command to restore the default configuration.

The global loop guard function is disabled by default.

Syntax

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The root port or backup port of a non-root bridge may fail to receive BPDUs due to the unidirectional link failure, and the root port becomes a designated port and enters forwarding state. As a result, loops occur in the network. To prevent this situation, you can configure loop guard on a non-root bridge.

After loop guard is enabled, when the root port or backup port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives a BPDU for spanning tree calculation.

Loop guard can be enabled globally or on interfaces.

- The **spanning-tree loopguard default** command is used to globally enable the loop guard function on all interfaces.
- The **spanning-tree guard loop** command is used to enable the loop guard function on an interface.

Loop guard and root guard are mutually exclusive on an interface and they cannot take effect at the same time.

Examples

The following example enables the global loop guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree loopguard default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree guard loop**

1.28 spanning-tree mode

Function

Run the **spanning-tree mode** command to set the spanning tree mode to STP, RSTP, or MSTP.

Run the **no** form of this command to restore the default configuration.

The default spanning tree mode is MSTP.

Syntax

spanning-tree mode { **mstp** | **rstp** | **stp** }

no spanning-tree mode

Parameter Description

mstp: Indicates the Multiple Spanning Tree Protocol (IEEE 802.1s).

rstp: Indicates the Rapid Spanning Tree Protocol (IEEE 802.1w).

stp: Indicates the Spanning Tree Protocol (IEEE 802.1d).

Command Modes

Global configuration mode

Usage Guidelines

However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Orion devices, run this command to switch the spanning tree mode to a lower version to ensure compatibility.

Caution

- When you switch from the MSTP mode to RSTP or STP mode, all information about MST regions will be cleared.
- The spanning tree mode switching will cause the spanning tree recalculation.

You can run the **show spanning-tree** command to display the spanning tree configuration.

Default Level

15

Examples

The following example switches the spanning tree mode to STP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mode stp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show spanning-tree

1.29 spanning-tree mst configuration

Function

Run the **spanning-tree mst configuration** command to enter the MST configuration mode.

Run the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to enable the MSTP protocol. Devices that have the same configuration name, revision number, and instance mappings constitute an MST region. Configuration names, revision numbers, and instance mappings are recorded in the **MST CFG ID** field of MST BPDUs and they can be configured.

- Configuration name: Identifies an MST region. The value is a string of up to 32 characters and the default value is empty.
- Revision number: Identifies an MST region. The value is a 2-byte non-negative integer and the default value is **0**.
- Instance mapping: Indicates mappings between instances and VLANs. One MST region can contain multiple MSTIs. Instance **0** exists by default and instances 1–64 can be created. This device supports VLANs 1–4094. VLANs belong to instance **0** except those that have been assigned to instances.

MST regions are independent of each other. If a port on a device receives a BPDU with **MST CFG ID** same as that of the MST BPDU of the device, the device deems that the peer device and the device belong to the same MST region. Otherwise, the device deems that the peer device belongs to a different MST region. The load sharing advantage of MSTP can be reflected only after multiple devices are configured to the same MST region. Therefore, MST regions need to be properly divided and devices in the same MST region need to have the same **MST CFG ID**.

Examples

The following example enters the MST configuration mode, configures an MST region named region1, configures instance 1 to include VLAN 3 and VLANs 5–10, and displays the MST region configuration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst configuration
Hostname(config-mst)# instance 1 vlan 3, 5-10
Hostname(config-mst)# name region1
Hostname(config-mst)# revision 1
Hostname(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name     : region1
Revision : 1
Instance  Vlans Mapped
--------  ---------------
0        1-2,4,11-4094
1        3,5-10
---------------------------
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **instance**
- **name**
- **revision**
- **show spanning-tree mst**

1.30 spanning-tree mst cost

Function

Run the **spanning-tree mst cost** command to configure a port path cost.

Run the **no** command to restore the default configuration.

A device automatically calculates the port path cost based on the link rate of an interface by default.

Syntax

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] **cost**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the port path cost can be configured based on this instance. The value range is from 0 to 64, and the default value is **0**.

cost *cost*: Specifies the port path cost. The value range is from 1 to 200000000. The port path cost is automatically calculated based on the link rate of an interface in accordance with IEEE 802.1t Long by default. For example, as shown in 1.33 Table 1-1, the path cost of an interface with the rate of 1000 Mbps is 20,000, the path cost of an interface with the rate of 100 Mbps is 200,000, and the path cost of an interface with the rate of 10 Mbps is 2,000,000.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

The root path cost is the sum of path costs of all ports in the path from a device to the root. When the administrator needs to control the spanning tree topology, the port path cost can be modified to affect the root path cost value.

You can run the **show spanning-tree mst interface** *interface-type interface-number* command to verify the above configuration.

Examples

The following example sets the port path cost of port TenGigabitEthernet 0/1 to 400 in instance 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree mst 3 cost 400
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.31 spanning-tree mst port-priority

Function

Run the **spanning-tree mst port-priority** command to configure a port priority.

Run the **no** form of this command to restore the default configuration.

The default port priority is 128.

Syntax

spanning-tree [**mst** *instance-id*] **port-priority** *port-priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the instance-based port priority can be configured. The value range is from 0 to 64, and the default value is **0**.

port-priority *port-priority*: Specifies the port priority. The value range is multiples of 16, that is, 0, 16, 32, 48, 64, 80, 96, 112, 128 (default value), 144, 160, 176, 192, 208, 224, and 240, totaling 16 integers.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

A port ID consists of two bytes, with the first byte of *port-priority* and the second byte of port ID.

When the administrator needs to control the spanning tree topology, he can configure *port-priority* to change the port ID.

You can run the **show spanning-tree mst interface** *interface-type interface-number* command to verify the above configuration.

Examples

The following example sets the port priority of port TenGigabitEthernet 0/1 in instance 20 to 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree mst 20 port-priority 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.32 spanning-tree mst priority

Function

Run the **spanning-tree mst priority** command to configure a bridge priority.

Run the **no** command to restore the default configuration.

The default bridge priority is **32768**.

Syntax

spanning-tree [**mst** *instance-id*] **priority** *priority*

no spanning-tree [**mst** *instance-id*] **priority**

Parameter Description

mst *instance-id*: Specifies the ID of an instance so that the bridge priority can be configured based on this instance. The value range is from 0 to 64, and the default value is **0**.

priority *priority*: Specifies the bridge priority. The value range is multiples of 4096, that is, 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768 (default value), 36864, 40960, 45056, 49152, 53248, 57344, and 61440, totaling 16 integers.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

In the spanning tree calculation, devices elect roles by comparing elements in the priority vector <root ID, root path cost, bridge ID, port ID>. A smaller value indicates a higher priority. The devices compare the root ID (bridge ID of each device initially) to elect the root bridge. All ports on the root bridge are designated ports. On a non-root bridge, the device elects the root port by comparing elements in the priority vector. On a network segment that directly connects two ports, the designated port is elected by comparing elements in the priority vector. Finally, non-designated ports are blocked.

A bridge ID consists of eight bytes, with the first two bytes of the bridge priority (indicated by *priority*) and the last six bytes used for the MAC address of the bridge.

When the administrator needs to control the spanning tree topology, *priority* can be changed to change the bridge ID.

After running the **spanning-tree** command to enable STP, you can run the **show spanning-tree** and **show spanning-tree summary** commands to verify the above configuration.

Examples

The following example sets the bridge priority of instance 20 to 8192 in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree mst 20 priority 8192
```

Notifications

When the configured bridge priority is not a multiple of 4096, the following notification will be displayed:

```
bridge priority must be IN increments of 4096
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree mst**

1.33 spanning-tree pathcost method

Function

Run the **spanning-tree pathcost method** command to configure the method of calculating the default port path cost.

Run the **no** form of this command to restore the default configuration.

The port path cost is calculated according to IEEE 802.1t Long by default.

Syntax

spanning-tree pathcost method { **long** | **long standard** | **short** }

no spanning-tree pathcost method

Parameter Description

long: Sets and calculates the port path cost according to IEEE 802.1t Long.

long standard: Sets and calculates the port path cost according to IEEE 802.1t Long Standard.

short: Sets and calculates the port path cost according to IEEE 802.1d Short.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

The methods of calculating the default port path costs specified in standards are listed in Table 1-1. Be sure to adopt a consistent port path cost standard for the entire network.

IEEE 802.1d Short: The range of the port path cost is from 1 to 65535. Aggregate port cost = Physical port cost × 95%.

IEEE 802.1t Long: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost × 95%.

IEEE 802.1t Long Standard: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost/Linkupcnt. At this moment, the cost value of the aggregate port will change with the number of member ports, which will lead to the network topology change. For configurations of aggregate ports and the Link Aggregation Control Protocol (LACP), see *Link Aggregation Port*.

- When an aggregate port is a static aggregate port, **Linkupcnt** refers to the number of member ports in Link Up state.
- When an aggregate port is an LACP aggregate port, **Linkupcnt** refers to the number of member ports participating in the aggregate port data forwarding.
- When no member port of an aggregate port is in Link Up state or forwarding data, the value of **Linkupcnt** is **1**.

Table 1-1Port Path Costs Calculated Based on the Link Rate

Port Rate	Port	IEEE 802.1d Short	IEEE 802.1t Long	IEEE 802.1t Long Standard
10 Mbps	Common port	100	2000000	2000000
	Aggregate port	95	1900000	2000000/Linkupcnt
100 Mbps	Common port	19	200000	200000
	Aggregate port	18	190000	200000/Linkupcnt
1000 Mbps	Common port	4	20000	20000
	Aggregate port	3	19000	20000/Linkupcnt
10000 Mbps	Common port	2	2000	2000
	Aggregate port	1	1900	20000/Linkupcnt

You can run the **show spanning-tree pathcost method** command to display the configuration.

Examples

The following example sets the port path cost calculation method to **Long Standard**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree pathcost method long standard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show spanning-tree

1.34 spanning-tree portfast

Function

Run the **spanning-tree portfast** command to configure an interface as an edge port and enable the interface to rapidly enter forwarding state.

Run the **spanning-tree portfast disabled** command to remove this configuration.

Interfaces are non-edge ports by default.

Syntax

spanning-tree portfast

spanning-tree portfast disabled

Parameter Description

disabled: Restores an interface to a non-edge port and disables the fast forwarding function of the interface.

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

If you are sure that a device interface is directly connected to a network terminal, you can manually configure the interface as an edge port. An edge port can enter forwarding state rapidly without waiting for twice the period of **Forward Delay**. The global BPDU guard and BPDU filter functions take effect only on edge ports.

- The **spanning-tree portfast default** command is used to configure the port fast attribute for all interfaces.
- The **spanning-tree portfast** command is used to configure the port fast attribute for a specific interface.

You can run the **show spanning-tree interface** *interface-type interface-number* **portfast** command to display the spanning tree configuration of an interface. If the value of the **PortAdminPortFast** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example configures port TenGigabitEthernet 0/1 as an edge port and enables the port to rapidly enter forwarding state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
```

Notifications

When an interface is manually configured as an edge port, the following notification will be displayed:

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

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree interface**
- **spanning-tree portfast default**

1.35 spanning-tree portfast bpdufilter default

Function

Run the **spanning-tree portfast bpdufilter default** command to enable the global BPDU filter function.

Run the **no** form of this command to disable the global BPDU filter function.

The global BPDU filter function is disabled by default.

Syntax

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

BPDU filter is a method of preventing BPDU attacks. When BPDU filter is enabled, a port neither sends nor receives BPDUs, but directly enters forwarding state. If a port receives a BPDU, it transitions to disabled state and the BPDU filter function automatically fails.

BPDU filter can be enabled globally or on interfaces.

- The **spanning-tree portfast bpdufilter default** command is used to enable the global BPDU filter function. The global BPDU filter function takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When

the autoedge function conflicts with the port fast configuration, the port fast configuration prevails.

- The **spanning-tree bpdufilter enabled** command is used to enable the BPDU filter function on an interface. The function takes effect on the interface regardless of whether the interface is an edge port.

Note

In general, when a port running STP transitions from listening state to learning state and then to forwarding state, it needs to wait for twice the period of **Forward-Delay** (2 × 15 = 30s by default). If a device port directly connects to a network terminal, you can enable the BPDU filter function to enable the port to work in forwarding state.

You can run the **show spanning-tree** command to display the configuration.

Examples

The following example enables the global BPDU filter function and configures port TenGigabitEthernet 0/1 as an edge port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree portfast bpdufilter default
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**
- **spanning-tree bpdufilter**
- **spanning-tree portfast**

1.36 spanning-tree portfast bpduguard default

Function

Run the **spanning-tree portfast bpduguard default** command to enable the global BPDU guard function.

Run the **no** form of this command to disable this feature.

The global BPDU guard function is disabled by default.

Syntax

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If a user illegally connects to a network device to an interface, to which a terminal should be connected, the network device may send BPDUs, causing a network topology change. If an interface with BPDU guard enabled receives a BPDU, it starts the BPDU guard mechanism, enters error-disabled state, and is disabled, indicating that an error occurs. An interface in error-disabled state can be restored automatically or manually. You can run the **errdisable recovery** [**interval** *seconds*] command to configure the interval for automatically restoring a port, in seconds. The value range is from 30 to 86400. If the command carries no parameter, the port needs to be manually restored.

BPDU guard can be enabled globally or on interfaces.

- The **spanning-tree portfast bpduguard default** command is used to enable global BPDU guard, which takes effect only on edge ports. Edge ports can be automatically identified by the system, and you can also run the **spanning-tree portfast** command to configure edge ports. When the autoedge function conflicts with port fast configuration, the port fast configuration prevails.
- The **spanning-tree bpduguard enabled** command is used to enable BPDU guard, which takes effect on interfaces regardless of whether they are edge ports.

You can run the **show spanning-tree interface** *interface-type interface-number* **bpduguard** command to display the spanning tree configuration of an interface. If the value of the **PortBPDUFilter** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example enables the global BPDU guard function, configures port TenGigabitEthernet 0/1 as an edge port, and sets the auto-recovery time to 60s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree portfast bpduguard default
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree portfast
Hostname(config-if-TenGigabitEthernet 0/1)# errdisable recovery interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show spanning-tree**
- **spanning-tree bpduguard**
- **spanning-tree portfast**

1.37 spanning-tree portfast default

Function

Run the **spanning-tree portfast default** command to configure all interfaces as edge ports and enable them to rapidly enter forwarding state.

Run the **no** form of this command to remove this configuration.

All interfaces are non-edge ports by default.

Syntax

spanning-tree portfast default

no spanning-tree portfast default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If you are sure that a device interface is directly connected to a network terminal, you can manually configure the interface as an edge port. An edge port can enter forwarding state rapidly without waiting for twice the period of **Forward Delay**. The global BPDU guard and BPDU filter functions take effect only on edge ports.

- The **spanning-tree portfast default** command is used to configure the port fast attribute for all interfaces.
- The **spanning-tree portfast** command is used to configure the port fast attribute for a specific interface.

You can run the **show spanning-tree interface** *interface-type interface-number* **portfast** command to display the spanning tree configuration of an interface. If the value of the **PortAdminPortFast** field is **Enabled**, this function is enabled, and the value **Disabled** indicates that this function is disabled.

Examples

The following example configures all interfaces as edge ports and enables them to rapidly enter forwarding state.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# spanning-tree portfast default
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- spanning-tree portfast

1.38 spanning-tree reset

Function

Run the **spanning-tree reset** command to restore spanning tree parameters to default values.

Syntax

spanning-tree reset

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command does not have the **no** form.

When STP is enabled, configuring the **spanning-tree reset** command cannot restore STP to the default disabled state.

Examples

The following example restores all spanning tree parameters to default values.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree reset
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 spanning-tree tc-guard

Function

Run the **spanning-tree tc-guard** command to enable the TC guard function on an interface.

Run the **no** form of this command to disable this feature.

The TC guard function is disabled on an interface by default.

Syntax

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.
- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively

control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.

- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the TC guard function on port TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# switchport
Hostname(config-if-TenGigabitEthernet 0/1)# spanning-tree tc-guard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree ignore tc**
- **spanning-tree tc-protection**
- **spanning-tree tc-protection tc-guard**

1.40 spanning-tree tc-protection

Function

Run the **spanning-tree tc-protection** command to enable the global TC protection function.

Run the **no** form of this command to disable this feature.

TC protection is disabled by default.

Syntax

spanning-tree tc-protection

no spanning-tree tc-protection

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.
- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the global TC protection function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tc-protection
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- spanning-tree ignore tc
- spanning-tree tc-guard
- spanning-tree tc-protection tc-guard

1.41 spanning-tree tc-protection tc-guard

Function

Run the **spanning-tree tc-protection tc-guard** command to enable the global TC guard function.

Run the **no** form of this command to disable this feature.

The global TC guard function is disabled by default.

Syntax

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

TC diffusion: When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU) to notify the upstream device of the spanning tree change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root bridge receives the BPDU. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned. If a device encounters TC packet attacks, it frequently performs the deletion operation, which occupies excessive device resources. After TC packet attacks are diffused to the whole network, the performance of devices throughout the network will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection: This function restricts a device to perform only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TCN BPDU is received in this period. If the device receives TCN BPDUs in this period, it performs another deletion operation after the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries. TC protection can be enabled or disabled only globally.

- TC guard: After TC guard is configured on a port, the port will neither diffuse TC packets generated by itself in the case of a topology change nor diffuse received downstream TC packets. TC guard can effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by the access device flapping. TC guard can be enabled or disabled globally or on interfaces.
- TC filter: TC guard blocks the diffusion of TC packets. When a topology change occurs, the device does not clear dynamic MAC addresses learned by interfaces, which may result in data forwarding errors. Hence, the TC filter function emerges. After TC filter is enabled on an interface, the interface does not process received downstream TC packets but processes only TC packets generated by itself due to topology changes. This function solves the problem of core route interruption caused by frequent up/down state switching of edge ports. It also ensures that core routing entries are updated in time when a topology change occurs. TC filter can be enabled or disabled only on interfaces.

Examples

The following example enables the global TC guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# spanning-tree tc-protection tc-guard
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **spanning-tree ignore tc**
- **spanning-tree tc-guard**
- **spanning-tree tc-protection**