

# Layer-2 Modules Configuration Commands

# Table of Contents

Chapter 1 Physical Feature Configuration Commands .....	1
1.1 Interface Configuration Commands.....	1
1.1.1 speed.....	1
1.1.2 duplex.....	2
1.1.3 flow-control .....	2
Chapter 2 Port Protection and Security .....	4
2.1 Port Protection Commands .....	4
2.1.1 switchport protected .....	4
2.2 Port Security Commands.....	4
2.2.1 switchport port-security bind mac.....	5
2.2.2 switchport port-security bind ip.....	5
2.2.3 switchport port-security block mac .....	6
2.2.4 switchport port-security block ip .....	7
2.2.5 switchport port-security static mac-address .....	7
2.2.6 switchport port-security mode static .....	8
2.2.7 switchport port-security mode dynamic.....	9
2.2.8 switchport port-security dynamic maximum .....	9
Chapter 3 Control of Port Block and Storm .....	11
3.1 Configuration Commands of Port Block .....	11
3.1.1 switchport block.....	11
3.2 Storm Control Command.....	11
3.2.1 storm-control .....	12
Chapter 4 Port mirroring .....	13
4.1 Port Mirroring Configuration Commands.....	13
4.1.1 mirror .....	13
4.1.2 show mirror.....	13
Chapter 5 MAC Configuration.....	15
5.1 MAC Address Configuration Commands.....	15
5.1.1 mac address-table static .....	15
5.1.2 mac address-table aging-time .....	15
5.1.3 show mac address-table .....	16
5.1.4 clear mac address-table.....	17
Chapter 6 Layer-2 (L2) Tunnel Protocol Configuration.....	18
6.1 L2 Channel Configuration Commands .....	18
6.1.1 l2protocol-tunnel.....	18
6.2 L2 Tunnel Monitoring Commands.....	18
6.2.1 debug l2 l2protocol-tunnel .....	18
Chapter 7 VLAN Configuration Commands.....	20
7.1 VLAN Configuration Commands .....	20
7.1.1 vlan.....	20
7.1.2 name .....	21

---

7.1.3 switchport pvid.....	21
7.1.4 switchport mode.....	22
7.1.5 switchport trunk.....	23
7.1.6 show vlan.....	23
Chapter 8 STP Configuration Commands.....	26
8.1 SSTP Configuration Commands.....	26
8.1.1 spanning-tree.....	26
8.1.2 spanning-tree mode.....	26
8.1.3 spanning-tree sstp priority.....	27
8.1.4 spanning-tree sstp hello-time.....	28
8.1.5 spanning-tree sstp max-age.....	28
8.1.6 spanning-tree sstp forward-time.....	29
8.1.7 spanning-tree sstp cost.....	30
8.1.8 spanning-tree cost.....	30
8.1.9 spanning-tree sstp port-priority.....	31
8.1.10 spanning-tree port-priority.....	32
8.1.11 show spanning-tree.....	33
8.1.12 spanning-tree management trap.....	34
8.2 VLAN STP Configuration Commands.....	34
8.2.1 spanning-tree mode pvst.....	34
8.2.2 spanning-tree vlan.....	35
8.2.3 spanning-tree vlan priority.....	36
8.2.4 spanning-tree vlan forward-time.....	36
8.2.5 spanning-tree vlan max-age.....	37
8.2.6 spanning-tree vlan hello-time.....	38
8.2.7 spanning-tree vlan cost.....	39
8.2.8 spanning-tree vlan port-priority.....	39
8.2.9 show spanning-tree vlan.....	40
8.3 RSTP Configuration Commands.....	41
8.3.1 spanning-tree mode rstp.....	41
8.3.2 spanning-tree rstp forward-time.....	42
8.3.3 spanning-tree rstp hello-time.....	42
8.3.4 spanning-tree rstp max-age.....	43
8.3.5 spanning-tree rstp priority.....	44
8.3.6 spanning-tree rstp cost.....	44
8.3.7 spanning-tree rstp port-priority.....	45
8.3.8 spanning-tree rstp edge.....	46
8.3.9 spanning-tree rstp point-to-point.....	46
8.3.10 spanning-tree rstp migration-check.....	47
8.4 MSTP Configuration Commands.....	48
8.4.1 spanning-tree mode mstp.....	48
8.4.2 spanning-tree mstp name.....	48
8.4.3 spanning-tree mstp revision.....	49
8.4.4 spanning-tree mstp instance.....	49
8.4.5 spanning-tree mstp root.....	50
8.4.6 spanning-tree mstp priority.....	51

---

8.4.7 spanning-tree mstp hello-time.....	52
8.4.8 spanning-tree mstp forward-time.....	53
8.4.9 spanning-tree mstp max-age.....	53
8.4.10 spanning-tree mstp diameter.....	54
8.4.11 spanning-tree mstp max-hops.....	54
8.4.12 spanning-tree mstp port-priority.....	55
8.4.13 spanning-tree mstp cost.....	56
8.4.14 spanning-tree mstp edge.....	56
8.4.15 spanning-tree mstp point-to-point.....	57
8.4.16 spanning-tree mstp mst-compatible.....	58
8.4.17 spanning-tree mstp migration-check.....	58
8.4.18 show spanning-tree mstp.....	59
8.4.19 show spanning-tree mstp region.....	60
8.4.20 show spanning-tree mstp detail.....	61
8.4.21 show spanning-tree mstp interface.....	62
8.5 Optional STP Attribute Configuration Commands.....	64
8.5.1 spanning-tree portfast.....	64
8.5.2 spanning-tree bpduguard.....	65
8.5.3 spanning-tree bpdufilter.....	66
8.5.4 spanning-tree uplinkfast.....	66
8.5.5 spanning-tree backbonefast.....	67
8.5.6 spanning-tree guard.....	68
8.5.7 spanning-tree loopguard.....	68
8.5.8 spanning-tree fast-aging.....	69
8.5.9 spanning-tree fast-aging flush-fdb.....	70
Chapter 9 802.1x Configuration Commands.....	72
9.1 802.1x Configuration Commands.....	72
9.1.1 dot1x enable.....	72
9.1.2 dot1x port-control.....	73
9.1.3 dot1x multiple-hosts.....	74
9.1.4 dot1x default.....	75
9.1.5 dot1x max-req.....	75
9.1.6 dot1x reauth-max.....	76
9.1.7 dot1x re-authentication.....	76
9.1.8 dot1x timeout quiet-period.....	77
9.1.9 dot1x timeout re-authperiod.....	78
9.1.10 dot1x timeout tx-period.....	78
9.1.11 dot1x user-permit.....	79
9.1.12 dot1x authentication method.....	80
9.1.13 dot1x authen-type、dot1x authentication type.....	80
9.1.14 dot1x guest-vlan.....	81
9.1.15 dot1x guest-vlan id.....	82
9.1.16 aaa authentication dot1x.....	83
9.1.17 debug dot1x error.....	83
9.1.18 debug dot1x state.....	84
9.1.19 debug dot1x packet.....	84

9.1.20 show dot1x ..... 85

# Chapter 1 Physical Feature Configuration Commands

## 1.1 Interface Configuration Commands

The following are interface configuration commands:

- speed
- duplex
- flow-control

### 1.1.1 speed

Syntax

**speed {10 | 100 |1000 | auto }**

**no speed**

To set the speed of the interface, ran **speed {10| 100 | 1000 | auto}**.

Parameter

Parameter	Description
<b>10, 100,1000</b>	Sets the speed of a port to 10M, 100M or 1000M.
<b>auto</b>	Sets the speed of the interface to <b>auto</b> .

Default value

The speed of the electrical interface is auto, the speed of the 100M optical interface is 100M and the speed of the 1000M optical interface is 1000M.

Description

This command is configured in layer-2 interface configuration mode.

**Note:**

The speed of the optical interface is fixed. For example, the speeds of GBIC and GE-FX are 1000m, while the speed of FE-FX is 100M. If the **speed** command for an optical interface has the **auto** parameter, the optical interface has the automatic negotiation function, or the optical interface is mandatory and cannot be negotiated.

Example

The following example shows how to set the speed of interface switchFastEthernet4/1 to 100M:

```
Router_config# interface switchFastEthernet4/1
Router_config_sfe4/1# speed 100
```

### 1.1.2 duplex

#### Syntax

**duplex {auto / full / half }**

**no duplex**

To set the duplex mode of an interface, run **duplex {auto | full | half}**.

#### Parameter

Parameter	Description
<b>auto</b>	Automatic negotiation
<b>full</b>	Full duplex
<b>half</b>	Half duplex

#### Default value

The electrical interface is in automatic negotiation mode , while the optical interface is in full duplex mode.

#### Description

This command is configured in layer-2 interface configuration mode.

#### Note:

The duplex mode of the optical interface is fixed, that is, the duplex mode of all optical interfaces is the full duplex mode.

#### Example

The following example shows how to set interface switchFastEthernet4/1 to the full duplex mode.

```
Router_config# interface switchFastEthernet4/1
Router_config_sfe4/1# duplex full
```

### 1.1.3 flow-control

#### Syntax

**flow-control [on|off ]**

**no flow-control**

To configure flow control for an interface, run **flow-control{on | off}**.

#### Parameter

None

#### Default value

Disables the flow control function.

### Description

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows that the flow control function of the port is disabled.

```
Router_config_sfe4/1# no flow-control
```



## Chapter 2 Port Protection and Security

### 2.1 Port Protection Commands

Port protection configuration commands include:

- switchport protected

#### 2.1.1 switchport protected

Syntax

**[no] switchport protected**

To configure port protection and realize layer-2 isolation on an port, run this command.

Parameter

None

Default value

Port protection is not enabled on the switching port by default.

Description

When port protection is enabled, this port is isolated from other switching ports on layer 2.

This command is configured in layer-2 interface configuration mode.

Example

The following example shows how to enable port protection on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2#switchport protected
```

### 2.2 Port Security Commands

The port security commands include:

- switchport port-security bind mac
- switchport port-security bind ip
- switchport port-security block mac
- switchport port-security block ip
- switchport port-security static mac-address
- switchport port-security mode static
- switchport port-security mode dynamic
- switchport port-security dynamic maximum

## 2.2.1 switchport port-security bind mac

### Syntax

**[no]** switchport port-security bind mac *mac-address*

To bind a MAC address to a security port, run this command.

### Parameter

Parameter	Description
<i>mac-address</i>	Stands for the bound MAC address. Its format is H.H.H.

### Default value

No MAC address is bound to a switching port by default.

### Description

When a security port is bound to a MAC address, only those packets whose source MAC address is same to the bound MAC address can pass through this security port.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to bind an MAC address to port sfe4/2.

```
Router_config#int sfe4/2
```

```
Router_config_sfe4/2# switchport port-security bind mac 0000.0000.0001
```

## 2.2.2 switchport port-security bind ip

### Syntax

**[no]** switchport port-security bind ip *ip-address*

**[no]** switchport port-security bind ip *ip-address* mac *mac-address*

To bind IP to a security port, run **[no] switchport port-security bind ip *ip-address***.

At the same time the security port will be bound to an IP address and a MAC address.

### Parameter

Parameter	Description
<i>ip-address</i>	Stands for the bound IP address. Its format is A.B.C.D.
<i>mac-address</i>	Stands for the bound MAC address. Its format is H.H.H.

### Default value

No IP address is bound to a switching port by default.

### Description

When a security port is bound to an IP address, only those packets whose source IP address is same to the bound IP address can pass through this security port.

When a security port is bound to an IP address and a MAC address simultaneously, only those packets whose source IP/MAC address is same to the bound IP/MAC address can pass through this security port.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to bind an IP address to port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2# switchport port-security bind ip 192.2.2.1
Router_config_sfe4/2# switchport port-security bind ip 192.2.2.2 mac 0000.0000.0001
```

## 2.2.3 switchport port-security block mac

### Syntax

**[no]** switchport port-security block mac *mac-address*

To filter the MAC addresses on a security port, run this command.

### Parameter

Parameter	Description
<i>mac-address</i>	Stands for the filtered MAC address. Its format is H.H.H.

### Default value

No MAC address is filtered on a switching port by default.

### Description

When MAC filtration is filtered on a security port, only those packets whose source MAC address is same to the configured MAC address will be filtered and won't get through this port.

### Example

The following example shows how to set MAC filtration on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2# switchport port-security block mac 0000.0000.0001
```

## 2.2.4 switchport port-security block ip

### Syntax

**[no] switchport port-security block ip** *ip-address*

**[no] switchport port-security block ip** *ip-address mac* *mac-address*

To filter IP addresses on a security port, run **[no] switchport port-security block ip** *ip-address*.

At the same time the security port will filter IP addresses and MAC addresses.

### Parameter

Parameter	Description
<i>ip-address</i>	Stands for the IP address. Its format is A.B.C.D.
<i>mac-address</i>	Means a MAC address. Its format is H.H.H.

### Default value

No IP address is filtered on a switching port by default.

### Description

When IP filtration is filtered on a security port, only those packets whose source IP address is same to the configured IP address will be filtered and won't get through this port.

When IP filtration and MAC filtration are enabled on a security port, only those packets whose source IP/MAC addresses are same to the configured IP/MAC addresses will be filtered and won't get through this port.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to set IP filtration on port sfe4/2.

```
Router_config#int sfe4/2
```

```
Router_config_sfe4/2# switchport port-security block ip 192.2.2.1
```

```
Router_config_sfe4/2# switchport port-security block ip 192.2.2.2 mac 0000.0000.0001
```

## 2.2.5 switchport port-security static mac-address

### Syntax

**[no] switchport port-security static mac-address** *mac-address-value*

To configure the static MAC address table on a security port, run this command.

### Parameter

Parameter	Description
-----------	-------------

<i>mac-address-value</i>	Means an MAC address. Its format is H.H.H.
--------------------------	--

### Default value

None

### Description

After the static MAC address table of a security port is configured, the matched packets are allowed or forbidden to pass through this port according to the current security mode.

When this command is used along with **switchport port-security mode static accept**, only the packets whose source MAC addresses are in the static MAC address table can pass through the security port.

When this command is used along with **switchport port-security mode static reject**, only the packets whose source MAC addresses are in the static MAC address table are forbidden to pass through the security port.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to configure the static MAC address table of the security port on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2# switchport port-security static mac-address 0000.0000.0001
Router_config_sfe4/2# switchport port-security static mac-address 0000.0000.0002
```

## 2.2.6 switchport port-security mode static

### Syntax

**[no] switchport port-security mode static {accept|reject}**

To configure the static MAC table mode on a security port, run this command.

### Parameter

Parameter	Description
<b>accept</b>	Means that the packet whose source MAC address is in the static MAC address table is allowed to pass through.
<b>reject</b>	Means that the packet whose source MAC address is in the static MAC address table is forbidden to pass through.

### Default value

None

### Description

This command is used to allow or forbid those packets whose source MAC addresses are in the static MAC table to pass through the security port.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to enable the Allow mode of the static MAC table on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2#switchport port-security mode static accept
```

## 2.2.7 switchport port-security mode dynamic

### Syntax

**[no] switchport port-security mode dynamic**

To configure the dynamic mode of a security port, run this command.

### Parameter

None

### Default value

None

### Description

When the security port is set to the dynamic mode, the security port will learn a certain number of MAC addresses and then does not receive packets with other addresses. The maximum number of dynamic MAC addresses can be configured by **switchport port-security dynamic maximum**.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to configure the dynamic mode of security port on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2#switchport protected
```

## 2.2.8 switchport port-security dynamic maximum

### Syntax

**[no] switchport port-security dynamic maximum *number***

To configure the maximum number of learnable MAC addresses in dynamic security-port mode, run this command.

### Parameter

Parameter	Description
<i>number</i>	Means the maximum number of dynamic MAC addresses.

### Default value

1.

### Description

In the dynamic security port mode, this command can be used to set the maximum number of learnable MAC addresses.

This command is configured in layer-2 interface configuration mode.

### Example

The following example shows how to enable the maximum number of dynamic MAC addresses on port sfe4/2.

```
Router_config#int sfe4/2
```

```
Router_config_sfe4/2#switchport port-security dynamic maximum 10
```

## Chapter 3 Control of Port Block and Storm

### 3.1 Configuration Commands of Port Block

The following command is used for port block settings :

- switchport protected

#### 3.1.1 switchport block

Syntax

**[no] switchport block {unicast | multicast | broadcast}**

To configure an port not to forward a designated type of packets, run **switchport block {unicast / multicast / broadcast}**.

Parameter

Parameter	Description
<b>unicast</b>	Means that the unknown unicast frame is not forwarded on a port.
<b>multicast</b>	Means that the multicast frame is not forwarded on the port.
<b>broadcast</b>	Means that the broadcast frame is not forwarded on the port.

Default value

All packets can be forwarded by default.

Description

This command is configured in layer-2 interface configuration mode.

Example

The following example shows how to not forward unknown unicast frames on port sfe4/2.

```
Router_config#int sfe4/2
Router_config_sfe4/2#switchport block unicast
```

### 3.2 Storm Control Command

The storm control command is:

- storm-control



### 3.2.1 storm-control

#### Syntax

**[no] storm-control {broadcast | multicast | unicast} threshold *count***

To configure flow control for a port, run **storm-control {broadcast | multicast | unicast} threshold *count***.

#### Parameter

Parameter	Description
<b>broadcast   multicast   unicast</b>	Defines broadcast/multicast/unicast storm control.
<i>count</i>	Defines the flow percent of storm control on a port. That is, it defines the threshold flux of the storm.

#### Default value

The storm control function is disabled by default.

#### Description

This command is configured in layer-2 interface configuration mode.

#### Example

The following example shows how to set the control percentage of unicast frame storm on port *sfe4/2* to 20:

```
Router_config#int sfe4/2
Router_config_sfe4/2# storm-control unicast threshold 20
```

## Chapter 4 Port mirroring

### 4.1 Port Mirroring Configuration Commands

Port mirroring configuration commands include:

- mirror
- show mirror

#### 4.1.1 mirror

Syntax

**[no] mirror session *session\_number* {destination {interface *interface-id*} | source {interface *interface-id* [, | -] [**both** | **rx** | **tx**]}}**

To configure port mirroring, run **mirror session *session\_number* {destination {interface *interface-id*} {rspan *vid tpid*} | source {interface *interface-id* [, | -] [**rx** | **tx**]}}**.

Parameter

Parameter	Description
<i>session_number</i>	Number of port mirroring Value range: 1
<i>destination</i>	Information about destination port mirroring
<i>source</i>	Information about the mirrored port
<i>both</i>   <i>rx</i>   <i>tx</i>	Data flow that will be mirrored <b>rx</b> means that only the input data is mirrored; <b>tx</b> means that only the output data is mirrored; <b>both</b> means both the input data and the output data are mirrored.

Default value

None

Description

This command is configured in global configuration mode.

Example

The following example shows how to set port sfe4/2 to the output mirror of port sfe4/1.

```
Router_config# mirror session 1 destination interface sfe4/2
```

```
Router_config# mirror session 1 source interface sfe4/1 tx
```

#### 4.1.2 show mirror

Syntax

**show mirror** [session *session\_number*]

To display the information about port mirroring, run **show mirror [session session\_number]**.

#### Parameter

Parameter	Description
<i>session_number</i>	Number of port mirroring Value range: 1

#### Default value

None

#### Instruction

This command is used to display the information about port mirroring.

#### Example

The following example shows how to display the information about all port mirroring.

```
Switch# show mirror
Session 1
-----
Source Ports:
RX Only: Fe0/3
TX Only: None
Both: None
Source VLANs:
RX Only: None
TX Only: None
Both: None
```

## Chapter 5 MAC Configuration

### 5.1 MAC Address Configuration Commands

#### 5.1.1 mac address-table static

##### Syntax

**[no] mac address-table static** *mac-addr* vlan *vlan-id* interface *interface-id*

To add a static MAC address, run **mac address-table static** *mac-addr* vlan *vlan-id* **interface** *interface-id*. To cancel the static MAC address, run **no mac address-table static** *mac-addr* vlan *vlan-id* **interface** *interface-id*.

##### Parameter

Parameter	Description
<i>mac-addr</i>	Means an MAC address. Value range: H.H.H
<i>vlan-id</i>	A VLAN that the MAC address belongs to Value range: 1-4094
<i>interface-id</i>	Physical port that the MAC address belongs to

##### Default value

None

##### Instruction

This command is configured in global configuration mode.

##### Example

The following example shows how to bind MAC address 0004.5600.67ab to port sfe4/2 of VLAN1.

```
Router_config# mac address-table static 0004.5600.67ab vlan 1 interface sfe4/2
```

#### 5.1.2 mac address-table aging-time

##### Syntax

**mac address-table aging-time** [0 | 10-1000000]

To configure the aging time of the MAC address table, run the previous command.

##### Parameter

Parameter	Description
<b>0</b>	Means that the MAC address never ages.
<b>10-1000000</b>	Aging time of the MAC address whose unit is second

**Default value**

None

**Instruction**

This command is configured in global configuration mode.

**Example**

The following example shows how to set the aging time of the MAC address to 100 seconds.

```
Router_config# mac address-table aging-time 100
```

**5.1.3 show mac address-table****Syntax**

**show mac address-table** {dynamic [interface *interface-id* | vlan *vlan-id*] | static}

To display the MAC address table of the switch, run **show mac address-table {dynamic [interface *interface-id* | vlan *vlan-id*] | static}**.

**Parameter**

Parameter	Description
<b>dynamic</b>	Dynamically-learned MAC address table
<i>interface-id</i>	Name of an interface
<i>vlan-id</i>	Value range: 1-4094
<b>static</b>	Static MAC address table

**Default value**

None

**Instruction**

This command is used to display the MAC address table.

**Example**

The following example shows how to display all static MAC address tables.

```
Switch# show mac address-table static
```

```
Mac Address Table
```

```
-----
```

```
Vlan Mac Address Type Ports
```

```
-----
```

```
All 0000.0000.0001 STATIC CPU
```

```
All 0000.0000.0002 STATIC CPU
```

```
All 0000.0000.0003 STATIC CPU
```

```
All 0000.0000.0009 STATIC CPU
```

All 0000.0000.0012 STATIC CPU  
 All 0180.c200.000b STATIC CPU  
 All 0180.c200.000c STATIC CPU  
 All 0180.c200.000d STATIC CPU  
 All 0180.c200.0010 STATIC CPU

#### 5.1.4 clear mac address-table

##### Syntax

**clear mac address-table** dynamic [address *mac-addr* | interface *interface-id* | vlan *vlan-id*]

To delete a dynamic MAC address, run the previous command.

##### Parameter

Parameter	Description
dynamic	Means a dynamic MAC address.
<i>address mac-addr</i>	Means an MAC address. Value range: H.H.H
<i>interface-id</i>	Means a name of a L2 interface.
<i>vlan-id</i>	VLAN ID. Value range: 1-4094

##### Default value

None

##### Description

This command is used in EXEC mode.

##### Example

The following example shows how to clear all dynamically-learned MAC addresses on interface sfe4/2.

```
Switch# clear mac address-table dynamic interface sfe4/2
```

## Chapter 6 Layer-2 (L2) Tunnel Protocol Configuration

### 6.1 L2 Channel Configuration Commands

The following is a L2 tunnel monitoring command:

- `l2protocol-tunnel`

#### 6.1.1 `l2protocol-tunnel`

##### Syntax

**[no] l2protocol-tunnel [stp]**

To configure the layer-2 (L2) protocol tunnel, run the previous command.

##### Parameter

None

##### Default value

By default, the tunnel function of any L2 protocol is not enabled on the port of the switch.

When the tunnel function is enabled, the tunnel function of all supported L2 protocols is enabled if no specific L2 protocol is designated.

##### Description

Currently only STP supports the tunnel function in our switches.

##### Example

The following example shows how to enable the tunnel function of the STP (including STP/PVST) on interface **switchFastEthernet 4/1**.

```
Router_config#int switchFastEthernet 4/1
Router_config_sfe4/1#l2protocol-tunnel stp
```

### 6.2 L2 Tunnel Monitoring Commands

The following is a L2 tunnel monitoring command:

- `debug l2 l2protocol-tunnel`

#### 6.2.1 `debug l2 l2protocol-tunnel`

##### Syntax

**[no] debug l2 l2protocol-tunnel [error | packet]**

To set the debugging option of the L2 protocol tunnel, run the previous command.

Parameter

None

Default value

If a specific option is not designated, all debugging options of a L2 protocol tunnel are enabled by default.

Description

None

Example

The following example shows how to enable the tunnel function of the STP on interface f0/2.

```
Router_config#int f0/2
Router_config_f0/2#l2protocol-tunnel stp
```



## Chapter 7 VLAN Configuration Commands

### 7.1 VLAN Configuration Commands

The following are VLAN configuration commands:

- vlan
- name
- vlan access-map
- action
- match
- vlan filter
- switchport pvid
- switchport mode
- switchport trunk
- switchport trunk

#### 7.1.1 vlan

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

To add or delete VLAN, run **vlan** *vlan-id* or **no vlan** *vlan-id*.

##### Parameter

Parameter	Description
<i>vlan-id</i>	Defines the ID of the VLAN. Value range: 1-4094

##### Default value

None

##### Command mode

Global configuration mode

##### Instruction

After this command is run, the system enters the VLAN configuration mode and then you can modify some VLAN attributes.

##### Example

The following example shows how to add the VLAN whose ID is 200:

```
Router_config#
Router_config#vlan 2
Router_config_vlan_2#
```

### 7.1.2 name

**[no] name str**

To name a VLAN, run **name str**.

#### Parameter

Parameter	Description
<i>str</i>	Defines the name of the VLAN. Value range: 1-32 characters

#### Default value

The name of the default VLAN is **default**. Other VLANs are named as VLANxxxx (**xxxx** stands for a 4-bit ID).

#### Command mode

VLAN configuration mode

#### Instruction

This command can be used to modify the VLAN name to symbolize a specific VLAN.

#### Example

The following example shows how to set the name of VLAN200 to **main405**:

```
Router_config#
Router_config#
Router_config#vlan 200
Router_config_vlan_200#name ?
WORD The ascii name of VLAN(32bytes)
Router_config_vlan_200#name main405
```

### 7.1.3 switchport pvid

**switchport pvid vlan-id**

**no switchport pvid**

To configure VLAN of the access-mode port, run **switchport pvid vlan-id**.

#### Parameter

Parameter	Description
<i>vlan-id</i>	VLAN ID which the port belongs to, ranging between 1 and 4049 Value range: 1-4094

#### Default value

All ports belong to VLAN 1.

**Command mode**

Port configuration mode

**Instruction**

Before this command is configured, VLAN which PVID belongs to must exist. The port can be in access mode or relay mode.

**Example**

The following example shows how to set port **switchFastEthernet 4/1** to the access port of VLAN10:

```
Router_config#vlan10
Router_config#interface switchFastEthernet 4/1
Router_config_sfe4/1#switchport pvid 10
```

**7.1.4 switchport mode**

```
switchport mode {access | trunk | dot1q-tunnel tpid | dot1q-tunnel-uplink tpid | dot1q-translating-tunnel}
no switchport mode
```

To configure the mode of the port, run the previous command.

**Parameter**

Parameter	Description
<i>access</i>	Access mode
<i>trunk</i>	Relay mode

**Default value**

Access mode

**Command mode**

Port configuration mode

**Instruction**

The switch's port supports the following two modes: access mode and relay mode.

The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

The 802.1X standard does not support authentication on the trunk port. The reason is that the authentication object regulated in the standard is not the port. As to port multiplexing, if user authentication is approved in one VLAN, all other VLAN users who multiplex this port are also authorized correspondingly, therefore, the trunk port does not support authentication.

### 7.1.5 switchport trunk

**[no] switchport trunk** {*vlan-allowed* *vlan-list*} | {*vlan-untagged* *vlan-list*}

To configure the attributes of the relay port, run the previous command.

#### Parameter

Parameter	Description
<i>vlan-allowed</i>	VLAN ID which can be received and transmitted by the port Value range: 1-4094
<i>vlan-untagged</i>	Frame that will be transmitted without adding the VLAN tag Value range: 1-4094

#### Default value

The native VLAN ID of all relay ports is 1. The allowable value for all VLANs ranges between 1 and 4094.

#### Command mode

Port configuration mode

#### Instruction

No matter the port is in access mode or in relay mode, you can run this command on the port. However, the port is in relay mode when this command functions.

The **vlan-allowed** parameter is used to control the VLAN range of the port; the **vlan-untagged** parameter is used to control the transmission of the untagged VLAN packets from the port.

When the vlan list is used, you can add, remove or set the lists of the existing VLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan 5, vlan 7".

#### Example

The following example shows how to set the allowed VLAN range to 1-10.

```
Router_config_sfe4/1#switchport trunk vlan-allowed 1-10,20-30,55
Router_config_sfe4/1#switchport trunk vlan-untagged 2-1000
```

### 7.1.6 show vlan

**show vlan** [**access-map** | **filter** | **id** *vlan-id* | **interface** *intf-id* | **dot1q-tunnel** [**interface** *intf*]]

To display relative information about all VLANs, run the previous command.

#### Parameter

Parameter	Description
-----------	-------------

<b>access-map</b>	Displays all VLAN access lists.
<b>filter</b>	Displays all VLAN filters.
<i>id</i>	Displays the designated VLAN. Value range: 1-4094
<i>interface</i>	Displays the designated port.
<b>dot1q-tunnel</b> <b>[interface intf]</b>	Displays the global information and statistics information about Dot1Q tunnel, or displays the detailed information about Dot1Q tunnel of the designated port.

### Default value

None

### Command mode

EXEC mode

### Instruction

None

### Example

The following example shows how to display relative information about all VLANs.

```
Switch#sho vlan
VLAN Status Name      Ports
-----
1  Static  Default      F0/1, F0/2, F0/3, F0/4, F0/5, F0/6, F0/7, F0/8
                        F0/9, F0/10, F0/11, F0/12, F0/13, F0/14, F0/15
                        F0/16, F0/17, F0/18, F0/19, F0/20, F0/21, F0/22
                        F0/23, F0/24, G1/1, G2/1, P1
2  Static  VLAN0002     F0/3
3  Static  VLAN0003     F0/3
4  Static  VLAN0004     F0/3
5  Static  VLAN0005     F0/3
6  Static  VLAN0006     F0/3
```

The **status** parameter stands for the VLAN generation source; the **static** parameter means that VLAN is generated through configuration; the **dynamic** parameter means that VLAN is generated dynamically through the GVRP protocol.

The following example shows the detailed information about a VLAN:

```
Switch> show vlan id 1
VLAN id: 1, Name: default, TotalPorts:11
```

```
Ports      Attributes
-----
F0/1      Trunk,Untagged
F0/2      Access
F0/5      Trunk,Untagged
F0/7      Trunk,Tagged
F0/8      Trunk,Tagged
```

```
F0/9      Trunk,Tagged
F0/11     Access
F0/12     Access
F0/14     Trunk,Tagged
F0/15     Trunk,Tagged
F0/16     Trunk,Untagged
```

The following example shows relative information about a VLAN on a port:

Switch#sho vlan int f0/6

```
Interface      VLAN
Name           Property PVID Vlan-Map      uTagg-VLan-Map
-----
FastEthernet0/6  Trunk   1   3,5,7,9,11,13,15 none
                17,19
```

Switch#sho vlan int f0/7

```
Interface      VLAN
Name           Property PVID Vlan-Map      uTagg-VLan-Map
-----
FastEthernet0/7  Access  7   7             ----
```

The following example shows how to display the VLAN access table:

```
Switch#show vlan access-map
Vlan access-map "map_1" 10
Match clauses:
ip address: ip1
Action:
drop
Vlan access-map "map_1" 20
Match clauses:
mac address: mac1
Action:
forward
Vlan access-map "map_1" 30
Match clauses:
Action:
Drop
```

The following example shows how to display the VLAN filtration list:

```
Switch#show vlan filter
VLAN Map map_1 is filtering VLANs:
20-22
```

## Chapter 8 STP Configuration Commands

### 8.1 SSTP Configuration Commands

#### 8.1.1 spanning-tree

##### Syntax

**spanning-tree**

**no spanning-tree**

To enable the default STP mode, run **spanning-tree**; to disable the STP, run **no spanning-tree**.

##### Parameter

None

##### Default value

RSTP is enabled by default.

##### Instruction

None

##### Command mode

Global configuration mode

Physical interface configuration mode or aggregation port configuration mode

##### Example

None

#### 8.1.2 spanning-tree mode

##### Syntax

**spanning-tree mode {rstp|sstp}**

**no spanning-tree mode**

To configure the spanning-tree operation mode, run **spanning-tree mode {rstp|sstp}**.  
To forbid STP running, run **no spanning-tree mode**.

##### Parameter

Parameter	Description
<b>rstp</b>	Starts the RSTP mode.

<b>sstp</b>	Starts the SSTP mode.
-------------	-----------------------

#### Default value

SSTP 或 RSTP

#### Instruction

None

#### Command mode

Global configuration mode

#### Example

The following example shows how to enable the SSTP mode.

```
Router_config# spanning-tree mode sstp
Router_config#
```

### 8.1.3 spanning-tree sstp priority

#### Syntax

(1) **spanning-tree sstp priority** *value*

**no spanning-tree sstp priority**

To configure the SSTP priority value, run **spanning-tree sstp priority** *value*. To resume the default value of the SSTP priority value, run **no spanning-tree sstp priority**.

#### Parameter

Parameter	Description
<i>value</i>	Priority value Value range: 0-61440

#### Default value

32768

#### Description

When setting the priority value, you can make the switch as the root of the whole network spanning tree. The configuration value takes 4096 as a step and its value is the multiple of 4096. The configurable values are 0, 4096, 8192, 3\*4096, 4\*4096,..... and 15\*4096.

#### Command mode

Global configuration mode



## Example

The following example shows how to set the priority level of SSTP to 4096.

```
Router_config# spanning-tree sstp priority 4096
Router_config#
```

### 8.1.4 spanning-tree sstp hello-time

#### Syntax

**spanning-tree sstp hello-time** *time*

**no spanning-tree sstp hello-time**

To configure the transmission interval of SSTP packets, run **spanning-tree sstp hello-time** *time*. To resume the default transmission interval, run **no spanning-tree sstp hello-time**.

#### Parameter

Parameter	Description
<i>time</i>	Updates the interval. Range: 1-10 seconds

#### Default value

4s

#### Instruction

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

#### Command mode

Global configuration mode

#### Example

The following example shows how to configure the transmission interval of BPDU of SSTP to 8 seconds.

```
Router_config# spanning-tree sstp hello-time 8
Router_config#
```

### 8.1.5 spanning-tree sstp max-age

#### Syntax

**spanning-tree sstp max-age** *time*

**no spanning-tree sstp max-age**

To configure the maximum lifespan of the SSTP BPDU, run **spanning-tree sstp max-age** *time*. To resume the default interval time, run **no spanning-tree sstp max-age**.

## Parameter

Parameter	Description
<i>seconds</i>	Means the maximum lifespan of BPDU. Range: 6-40 seconds

## Default value

20s

## Instruction

None

## Command mode

Global configuration mode

## Example

The following example shows how to configure the maximum lifespan of SSTP to 24 seconds.

```
Router_config# spanning-tree sstp max-age 24
Router_config#
```

## 8.1.6 spanning-tree sstp forward-time

## Syntax

**spanning-tree sstp forward-time** *time*

**no spanning-tree sstp forward-time**

To configure the forwarding delay, run **spanning-tree sstp forward-time** *time*. To resume the default forwarding delay, run **no spanning-tree sstp forward-time**.

## Parameter

Parameter	Description
<i>time</i>	Time of the forwarding delay Value range: 4-30 seconds

## Default value

15 seconds

## Instruction

None

## Command mode

Global configuration mode

## Example

The following example shows how to configure the forwarding delay of SSTP to 20 seconds.

```
Router_config# spanning-tree sstp forward-delay 20
Router_config#
```

## 8.1.7 spanning-tree sstp cost

## Syntax

**spanning-tree sstp cost *value***

**no spanning-tree sstp cost**

To configure the path cost of a port in SSTP mode, run **spanning-tree sstp cost *value***. To resume the default path cost, run **no spanning-tree sstp cost**.

## Parameter

Parameter	Description
<i>value</i>	Value of the path cost Value range: 1-200000000

## Default value

The value of the path cost of the 10M Ethernet is 100.

+The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

## Instruction

None

## Command mode

Port configuration mode

## Example

The following example shows how to set the path cost of port **switchFastEthernet 4/1** to 100 in SSTP mode.

```
Router_config_sfe4/1#spanning-tree sstp cost 100
Router_config_sfe4/1#
```

## 8.1.8 spanning-tree cost

## Syntax

**spanning-tree cost *value***

**no spanning-tree cost**

To configure the path cost of a port in all STP mode, run **spanning-tree cost *value***. To resume the default path cost, run **no spanning-tree cost**.

## Parameter

Parameter	Description
<i>value</i>	Value of the path cost of a port Value range: 1-200000000

## Default value

The default value depends on the rate of each port in all STP mode.

## Instruction

The results of this command validates in all STP modes. In VLAN-based STP mode, the path cost of a port will be updated in all VLAN spanning trees; In MSTP mode, the path cost of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, After you run **spanning-tree sstp cost 100** and **spanning-tree cost 110**, the path cost of the port is still 100 in SSTP mode.

## Command mode

Port configuration mode

## Example

The following example shows how to set the path cost of port **switchFastEthernet 4/1** to 24:

```
Router_config_sfe4/1# spanning-tree cost 24
Router_config_sfe4/1#
```

## 8.1.9 spanning-tree sstp port-priority

## Syntax

**spanning-tree sstp port-priority *value***

**no spanning-tree sstp port-priority**

To configure the priority value of a port in SSTP mode, run **spanning-tree sstp port-priority *value***. To resume the default value of the priority value, run **no spanning-tree sstp port-priority**.

## Parameter

Parameter	Description
<i>value</i>	Priority level of a port Value range: 0-255

**Default value**

128 (0x80)

**Instruction**

The value of the priority level of a port must be the multiple of 16.

**Command mode**

Port configuration mode

**Example**

The following example shows how to set the priority level of port **switchFastEthernet 4/1** to 32:

```
Router_config_sfe4/1# spanning-tree sstp port-priority 32
Router_config_sfe4/1#
```

**8.1.10 spanning-tree port-priority****Syntax****spanning-tree port-priority *value*****no spanning-tree port-priority**

To configure the priority level of a port in all STP modes, run **spanning-tree port-priority *value***. To resume the default priority level, run **spanning-tree port-priority**.

**Parameter**

Parameter	Description
<i>value</i>	Means the priority level of a port. Value range: 0-255 Step: 16

**Default value**

The default value of the priority level of a port is 128 in all modes.

**Instruction**

The results of this command validates in all STP modes. In VLAN-based STP mode, the priority level of a port will be updated in all VLAN spanning trees; In MSTP mode, the priority level of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, After you run **spanning-tree sstp port-priority 100** and **spanning-tree port-priority 110**, the port-priority of the port is still 100 in SSTP mode.

**Command mode**

Port configuration mode

## Example

The following example shows how to set the priority level of port switchFastEthernet 4/1 to 16 in all STP modes.

```
Router_config_sfe4/1#spanning-tree port-priority 16
Router_config_sfe4/1#
```

## 8.1.11 show spanning-tree

### Syntax

**show spanning-tree** [**detail** | **interface** *intf-i*]

To display the spanning-tree information, run the previous command.

### Parameter

Parameter	Description
<i>intf-i</i>	Name of the port, such as F0/10 and G1/1

### Default value

None

### Description

This command is used to display the state of the spanning tree.

### Command mode

Port configuration mode

### Example

```
Router_config#show span

Spanning tree enabled protocol SSTP

SSTP
  Root ID      This bridge is the root

  Bridge ID    Priority          32768
              Address          00E0.0F64.8365
              Hello/MaxAge/FwdDly 4/20/15(s)

Intf   Port ID          Designated          Port ID
Name   Pri.Nbr Role Sts Cost   Bridge ID          Pri.Nbr Cost
-----
F0/47  128.47  Desg LIS 12        32768 00E0.0F64.8365 128.47  0

Router_config#
```

### 8.1.12 spanning-tree management trap

#### Syntax

**spanning-tree management trap [ newroot | topologychange ]**

To enable STP Trap, run the above-mentioned command.

#### Parameter

Parameter	Description
newroot	Stands for the newRoot trap type.
topologychange	Stands for the topologyChange trap type.

#### Default value

None

#### Description

This command is used to enable STP Trap.

#### Command mode

Global configuration mode

#### Example

None

## 8.2 VLAN STP Configuration Commands

#### Note:

S2116, S2448, S3448, S6508 and S8500 support the modes in which the spanning tree cases are based on VLAN. Please refer to related device models and corresponding software version documents.

### 8.2.1 spanning-tree mode pvst

#### Syntax

**spanning-tree mode pvst**

**no spanning-tree mode**

To enable VLAN-based STP mode, run **spanning-tree mode pvst**. To disable all STP modes, run **no spanning-tree mode**.

#### Parameter

None

**Default value**

The default STP mode is SSTP or RSTP.

**Instruction**

None

**Example**

The following example shows how to enable PVST on the switch.

```
Router_config# spanning-tree mode pvst
Router_config#
```

**8.2.2 spanning-tree vlan****Syntax**

**spanning-tree vlan** *vlan-list*

**no spanning-tree vlan** *vlan-list*

To designate VLAN to distribute the STP case, run **spanning-tree vlan *vlan-list***. To cancel the spanning tree of the designated VLAN, run **no spanning-tree vlan *vlan-list***.

**Parameter**

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15

**Default value**

By default, the switch creates the first 30 VLAN STP cases.

Other VLANs are automatically added to the STP forbidden list.

**Instruction**

None

**Command mode**

Global configuration mode

**Example**

The following example shows how to cancel the spanning tree of VLAN 10, 11, 15-19 and then how to distribute the spanning trees to VLAN 40-50.

```
Router_config#no spanning-tree vlan 10,11,15-19
Router_config#spanning-tree vlan 40-50
Router_config#
```



### 8.2.3 spanning-tree vlan priority

#### Syntax

**spanning-tree vlan *vlan-list* priority *value***

**no spanning-tree vlan *vlan-list* priority**

To designate the priority level of the bridge of the VLAN STP, run **spanning-tree vlan *vlan-list* priority *value***.

#### Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the priority level, ranging between 0 and 61400 (step: 4096)

#### Default value

By default, the priority level of the bridge of each VLAN spanning tree is 32768 plus the VLAN number.

#### Instruction

None

#### Command mode

Global configuration mode

#### Example

The following example shows how to set the priority levels of the bridges of VLAN1-3, 5-10 to 4096.

```
Router_config#spanning-tree vlan 1-3,5-10 priority 4096
Router_config#
```

### 8.2.4 spanning-tree vlan forward-time

#### Syntax

**spanning-tree vlan *vlan-list* forward-time *value***

**no spanning-tree vlan *vlan-list* forward-time**

To set the Forward Delay parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan *vlan-list* forward-time *value***.

#### Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15

<i>value</i>	Value of the forward-delay parameter Value range: 4-30 seconds Default value: 15 seconds
--------------	--

**Default value**

The value of the **forward-delay** parameter of all VLANs is 15 seconds.

**Instruction**

None

**Command mode**

Global configuration mode

**Example**

The following example shows how to set the **forward delay** parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Router_config#spanning-tree vlan 1-3,5-10 forward-time 19
Router_config
```

**8.2.5 spanning-tree vlan max-age****Syntax**

**spanning-tree vlan *vlan-list* max-age *value***

**no spanning-tree vlan *vlan-list* max-age**

To set the **Max Age** parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan *vlan-list* max age *value***. To resume the default value, run **no spanning-tree vlan *vlan-list* max age**.

**Parameter**

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the <b>max-age</b> parameter Value range: 6-40 seconds Default value: 20 seconds

**Default value**

The default value of the **max-age** parameter for all VLANs is 20 seconds.

**Instruction**

None

## Command mode

Global configuration mode

## Example

The following example shows how to set the **max age** parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Router_config#spanning-tree vlan 1-3,5-10 max-age 19
Router_config
```

## 8.2.6 spanning-tree vlan hello-time

### Syntax

**spanning-tree vlan** *vlan-list* **hello-time** *value*

**no spanning-tree vlan** *vlan-list* **hello-time**

To set the **hello time** parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan *vlan-list* hello time *value***. To resume the default value, run **no spanning-tree vlan *vlan-list* hello time**.

### Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the <b>hello time</b> parameter Value range: 1-10 seconds Default value: 4 seconds

### Default value

The default value of the **Hello-Time** parameter for all VLANs is 4 seconds.

### Instruction

None

## Command mode

Global configuration mode

## Example

The following example shows how to set the **Hello Time** parameter of VLAN 1-3, 5-10 to 9 seconds.

```
Router_config#spanning-tree vlan 1-3,5-10 hello-time 9
Router_config
```

## 8.2.7 spanning-tree vlan cost

### Syntax

**spanning-tree vlan *vlan-list* cost *value***

**no spanning-tree vlan *vlan-list* cost**

To set the path cost of the spanning tree in the designated VLAN, run **spanning-tree vlan *vlan-list* cost *value***. To resume the default value, run **no spanning-tree vlan *vlan-list* cost**.

### Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Path cost of a port, which ranges between 1 and 200,000,000

### Default value

The path cost of a port depends on the port rate.

The value of the path cost of the 10M Ethernet is 100.

+The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

### Instruction

None

### Command mode

Port configuration mode

### Example

The following example shows how to set the path cost of port switchFastEthernet 4/10 VLANs 1, 2, 3, 5, 6, 7, 8, 9, 10 to 100.

```
Router_config_sfe4/10)#spanning-tree vlan 1-3,5-10 cost 100
```

```
Router_config_sfe4/10)
```

## 8.2.8 spanning-tree vlan port-priority

### Syntax

**spanning-tree vlan *vlan-list* port-priority *value***

**no spanning-tree vlan *vlan-list* port-priority**

To set the priority level of the spanning tree in the designated VLAN, run **spanning-tree vlan *vlan-list* port-priority *value***. To resume the default value, run **no spanning-tree vlan *vlan-list* port-priority**.

## Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Priority level of a port, which ranges between 0 and 255 and whose step is 16

## Default value

128

## Instruction

None

## Command mode

Port configuration mode

## Example

The following example shows how to set the priority level of port switchFastEthernet 4/1 VLAN1-3,5-10 to 32.

```
Router_config_sfe4/1#spanning-tree vlan 1-3,5-10 port-priority 32
```

## 8.2.9 show spanning-tree vlan

## Syntax

**show spanning-tree vlan *vlan-list* [ **detail** ]**

To check the state of the spanning tree in the designated VLAN, run the previous command:

## Parameter

Parameter	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>detail</i>	Displays the detailed information about the state of the spanning tree.

## Default value

None

## Instruction

None

## Command mode

None

## Example

The following example shows how to check the spanning tree of VLAN 1-2.

```
Router_config#show spanning-tree vlan 1-2
```

```
Spanning tree enabled protocol PVST
```

```
VLAN0001
```

```
Root ID      This bridge is the root
```

```
Bridge ID    Priority          4097
             Address          00E0.0F64.8365
             Hello/MaxAge/FwdDly  4/20/15(s)
```

Intf Name	Port ID Pri.Nbr	Role	Sts	Cost	Designated Bridge ID	Port ID Pri.Nbr	Cost
F0/47	128.47	Desg	FWD	12	4097 00E0.0F64.8365	128.47	0

```
VLAN0002
```

```
Root ID      This bridge is the root
```

```
Bridge ID    Priority          4098
             Address          00E0.0F64.8365
             Hello/MaxAge/FwdDly  4/20/15(s)
```

Intf Name	Port ID Pri.Nbr	Role	Sts	Cost	Designated Bridge ID	Port ID Pri.Nbr	Cost
F0/47	128.47	Desg	FWD	12	4098 00E0.0F64.8365	128.47	0

```
Router_config#
```

## 8.3 RSTP Configuration Commands

### 8.3.1 spanning-tree mode rstp

## Syntax

```
spanning-tree mode rstp
```

```
no spanning-tree mode
```

To enable the RSTP function, run **spanning-tree mode rstp**. To disable the STP, run **no spanning-tree mode**.

## Parameter

None

## Default value

RSTP is running.

## Instruction

None

## Example

The following example shows how to enable RSTP on the switch.

```
Router_config# spanning-tree mode rstp
Router_config#
```

## 8.3.2 spanning-tree rstp forward-time

## Syntax

**spanning-tree rstp forward-time** *time*

**no spanning-tree rstp forward-time**

To configure the forwarding delay of RSTP, run **spanning-tree rstp forward-time** *time*. To resume the default forwarding delay of RSTP, run **no spanning-tree rstp forward-time**.

## Parameter

Parameter	Description
<i>time</i>	Time of the forwarding delay Range: 4-30 seconds

## Default value

15 seconds

## Instruction

None

## Example

The following example shows how to set the forwarding delay of RSTP to 20 seconds.

```
Router_config# spanning-tree rstp forward-time 20
Router_config#
```

## 8.3.3 spanning-tree rstp hello-time

## Syntax

**spanning-tree rstp hello-time** *time*

**no spanning-tree rstp hello-time**

To configure the update interval of RSTP, run **spanning-tree rstp hello-time *time***. To resume the default update interval of RSTP, run **no spanning-tree rstp hello-time**.

#### Parameter

Parameter	Description
<i>time</i>	Updates the interval. Range: 1-10 seconds

#### Default value

4 seconds

#### Instruction

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

#### Example

The following example shows how to set the update interval of RSTP to 8 seconds.

```
Router_config# spanning-tree rstp hello-time 8
Router_config#
```

### 8.3.4 spanning-tree rstp max-age

#### Syntax

**spanning-tree rstp max-age *time***

**no spanning-tree rstp max-age**

To configure the maximum lifespan of the RSTP BPDU, run **spanning-tree rstp max-age *time***. To resume the default interval time, run **no spanning-tree rstp max-age**.

#### Parameter

Parameter	Description
<i>time</i>	Maximum interval of the lifespan Range: 6-40 seconds

#### Default value

20 seconds

#### Instruction

None



## Example

The following example shows how to set the maximum lifespan of RSTP to 24 seconds.

```
Router_config# spanning-tree rstp max-age 24
Router_config#
```

### 8.3.5 spanning-tree rstp priority

#### Syntax

**spanning-tree rstp priority** *value*

**no spanning-tree rstp priority**

To configure the RSTP priority value, run **spanning-tree rstp priority** *value*. To resume the default value of the RSTP priority value, run **no spanning-tree rstp priority**.

#### Parameter

Parameter	Description
<i>value</i>	Priority level of the bridge Value range: 0-61440 Step: 4096

#### Default value

32768

#### Instruction

None

#### Example

The following example shows how to set the bridge priority of RSTP to 4096.

```
Router_config# spanning-tree rstp priority 4096
Router_config#
```

### 8.3.6 spanning-tree rstp cost

#### Syntax

**spanning-tree rstp cost** *value*

**no spanning-tree rstp cost**

To configure the path cost of a port, run **spanning-tree rstp cost** *value*. To resume the default value, run **no spanning-tree rstp cost**.

#### Parameter

Parameter	Description
-----------	-------------

<i>value</i>	Value of the path cost Value range: 1-200000000
--------------	---

#### Default value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

#### Instruction

None

#### Example

The following example shows how to set the path cost of port **switchFastEthernet 4/1** to 24:

```
Router_config_sfe4/1# spanning-tree rstp cost 24
```

### 8.3.7 spanning-tree rstp port-priority

#### Syntax

**spanning-tree rstp port-priority** *value*

**no spanning-tree rstp port-priority**

To configure the priority level of a port, run **spanning-tree rstp port-priority** *value*. To resume the default value, run **no spanning-tree rstp port-priority**.

#### Parameter

Parameter	Description
<i>value</i>	Priority level of a port Value range: 0-255 Step: 16

#### Default value

128

#### Instruction

None

#### Example

The following example shows how to set the priority level of port **switchFastEthernet 4/1** to 24:

```
switch(config_f0/0)# spanning-tree rstp port-priority 24
switch(config_f0/0)#
```

### 8.3.8 spanning-tree rstp edge

#### Syntax

**spanning-tree rstp edge [ force-true | force-false | auto ]**

To set the edge of a port to **force-true**, **force-false** or **auto**, run this command.

#### Parameter

Parameter	Description
<i>force-true</i>	Sets the edge port to be forcedly effective.
<i>force-false</i>	Sets the edge port to be forcedly ineffective.
<i>auto</i>	Sets the edge port to be automatic check (default).

#### Default value

None

#### Instruction

This command is used only in switches that support IEEE 802.1D 2004 RSTP.

#### Command mode

Port configuration mode

#### Example

None

### 8.3.9 spanning-tree rstp point-to-point

#### Syntax

**spanning-tree rstp point-to-point [ force-true | force-false | auto ]**

To set the point-to-point connection of a port to **force-true**, **force-false** or **auto**, run this command.

#### Parameter

Parameter	Description
<i>force-true</i>	Sets the point-to-point connection to be forcedly effective.
<i>force-false</i>	Sets the point-to-point connection to be forcedly ineffective.
<i>auto</i>	Sets the point-to-point connection to be automatic check (default).

**Default value**

None

**Instruction**

This command is used only in switches that support IEEE 802.1D 2004 RSTP.

**Command mode**

Port configuration mode

**Example**

None

### 8.3.10 spanning-tree rstp migration-check

**Syntax**

**spanning-tree rstp migration-check**

To restart checking protocol transfer of RSTP, run the previous command.

**Parameter**

None

**Default value**

None

**Instruction**

This command is used to restart the protocol transfer check on a port and to change the port in STP-compatible mode to the RSTP mode, enabling RSTP BPDU to be transmitted.

This command is used only in switches that support IEEE 802.1D 2004 RSTP.

**Command mode**

Global or port configuration mode

**Example**

The following example shows how to check protocol transfer on port switchFastEthernet 4/10.

```
Router_config_sfe4/10)#spanning-tree rstp migration-check
Router_config_sfe4/10)
```

## 8.4 MSTP Configuration Commands

### 8.4.1 spanning-tree mode mstp

#### Syntax

**spanning-tree mode mstp**

**no spanning-tree mode**

To set the operation mode of the spanning tree to MSTP, run **spanning-tree mode mstp**. To stop running STP, run **no spanning-tree mode**.

#### Parameter

None

#### Default value

MSTP is shut down, while SSTP or RSTP is running.

#### Instruction

None

#### Example

The following example shows how to enable MSTP on a switch.

```
Router_config# spanning-tree mode mstp
Router_config#
```

### 8.4.2 spanning-tree mstp name

#### Syntax

**spanning-tree mstp name *string***

**no spanning-tree mstp name**

To configure the MSTP name, run **spanning-tree mstp name *string***. To resume the default name, run **no spanning-tree mstp name**.

#### Parameter

Parameter	Description
string	A character string to configure the name, which contains up to 32 characters and is capital sensitive. Its default value is the MAC address of a switch.

#### Default value

Its default value is the MAC address of a switch.

## Instruction

None

## Example

The following example shows how to set the name of MSTP for a switch to **reg-01**.

```
Router_config# spanning-tree mstp name reg-01
Router_config#
```

## 8.4.3 spanning-tree mstp revision

## Syntax

**spanning-tree mstp revision** *value*

**no spanning-tree mstp revision**

To configure the MSTP revision number, run **spanning-tree mstp revision** *value*. To resume the default revision number, run **no spanning-tree mstp revision**.

## Parameter

Parameter	Description
<i>value</i>	Revision number, which ranges between 0 and 65535 and whose default value is 0

## Default value

The default value of the revision number is 0.

## Instruction

None

## Example

The following example shows how to set the revision number of MSTP to 100.

```
Router_config# spanning-tree mstp revision 100
Router_config#
```

## 8.4.4 spanning-tree mstp instance

## Syntax

**spanning-tree mstp instance** *instance-id* **vlan** *vlan-list*

**no spanning-tree mstp instance** *instance-id*

To map VLAN to MSTI, run **spanning-tree mstp instance** *instance-id* **vlan** *vlan-list*. To remap VLAN to CIST, run **no spanning-tree mstp instance** *instance-id*.

## Parameter

Parameter	Description
<i>instance-id</i>	Instance ID of the spanning-tree, which stands for an MSTI Value range: 1-15
<i>vlan-list</i>	A VLAN list which is mapped to a spanning tree Value range: 1-4094

## Default value

All VLANs are mapped to CIST (MST00).

## Instruction

Instance ID is an independent value which stands for an STP instance.

The **vlan-list** parameter can stand for a VLAN group, such as VLANs 1,2 and3, VLANs 1-5 or VLANs 1,2,5-10.

## Example

The following example shows how to map VLAN1 to STP instance 1, and VLANs 5, 7, 10-20 to STP instance 2 and then remap these VLANs to MST00.

```
Router_config# spanning-tree mstp instance 1 vlan 2
Router_config# spanning-tree mstp instance 2 vlan 5,7,10-20
Router_config# no spanning-tree mstp instance 2
```

## 8.4.5 spanning-tree mstp root

## Syntax

**spanning-tree mstp *instance-id* root {primary | secondary}**

[ **diameter *net-diameter* [ hello-time *seconds* ] ]**

**no spanning-tree mstp root**

To set a designated STP instance to a primary or secondary root, run **spanning-tree mstp *instance-id* root {primary | secondary}**. To resume the default value of the bridge priority of an STP instance, run **no spanning-tree mstp root**.

The **diameter** command and the **hello time** command are allowed to modify the network diameter and the **hello-time** parameter.

## Parameter

Parameter	Description
<i>instance-id</i>	Number of the STP instance, which ranges between 0 and 15
<i>primary</i>	Sets an STP instance to a primary root.
<i>secondary</i>	Sets an STP instance to a secondary root.
<i>net-diameter</i>	An optional parameter which presents the network diameter

	When <b>instance-id</b> is 0, <b>net-diameter</b> ranges between 2 and 7.
<i>seconds</i>	An optional parameter standing for the value of the <b>Hello Time</b> parameter, which ranges between 1 and 10 seconds

### Default value

The default value of the bridge priority for all STP instances is 32768. The network diameter is 7, while Hello Time is 2 seconds.

### Instruction

The **diameter** command and the **hello-time** command validate only when the **instance-id** parameter is 0.

In general, after the command to set the primary root is executed, the protocol automatically check the bridge ID of the current network's root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance. If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as the secondary root.

### Example

The following example shows how to set a switch to the primary root in CIST, and how to recalculate the time parameter of STP through **diameter 3** and **hello-time 3**, and then set the switch to the secondary root in MST01.

```
Router_config# spanning-tree mstp 0 root primary diameter 3 hello-time 3
Router_config# spanning-tree mstp 1 root secondary
```

## 8.4.6 spanning-tree mstp priority

### Syntax

**spanning-tree mstp** *instance-id* **priority** *value*

**no spanning-tree mstp priority**

To configure the value of the bridge priority of a designated STP instance, run **spanning-tree mstp** *instance-id* **priority** *value*. To resume the default value of the bridge priority, run **no spanning-tree mstp priority**.

### Parameter

Parameter	Description
<i>instance-id</i>	Number of the STP instance, which ranges between 0 and 15
<i>value</i>	Value of the bridge priority, which can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672,



32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
---

#### Default value

The default value of the bridge priority for all STP instances is 32768.

#### Instruction

The priority values in each STP instance are independent and can be configured independently.

#### Example

The following example shows how to set the priority values of a switch in CIST and MST01 to 4096 and 8192 respectively.

```
Router_config# spanning-tree mstp 0 priority 4096
Router_config# spanning-tree mstp 1 priority 8192
```

### 8.4.7 spanning-tree mstp hello-time

#### Syntax

**spanning-tree mstp hello-time** *seconds*

**no spanning-tree mstp hello-time**

To configure the Hello Time of MSTP, run **spanning-tree mstp hello-time seconds**. To resume the default value of the Hello Time of MSTP, run **no spanning-tree mstp hello-time**.

#### Parameter

Parameter	Description
seconds	Value range: 1-10 seconds Default value: 2 seconds

#### Default value

2 seconds

#### Instruction

None

#### Example

The following example shows how to set the Hello Time parameter of MSTP to **10**.

```
Router_config# spanning-tree mstp hello-time 10
Router_config# no spanning-tree mstp hello-time
```

## 8.4.8 spanning-tree mstp forward-time

### Syntax

**spanning-tree mstp forward-time** *seconds*

**no spanning-tree mstp forward-time**

To configure the **forward delay** parameter of MSTP, run **spanning-tree mstp forward-time *seconds***. To resume the default value of the **forward delay** parameter of MSTP, run **no spanning-tree mstp forward-time**.

### Parameter

Parameter	Description
seconds	Value range: 4-30 seconds Default value: 15 seconds

### Default value

15 seconds

### Instruction

None

### Example

The following example shows how to set the **Forward Delay** parameter of MSTP to **10**.

```
Router_config# spanning-tree mstp forward-time 10
```

```
Router_config# no spanning-tree mstp forward-time
```

## 8.4.9 spanning-tree mstp max-age

### Syntax

**spanning-tree mstp max-age** *seconds*

**no spanning-tree mstp max-age**

To configure the **max age** parameter of MSTP, run **spanning-tree mstp max-age *seconds***. To resume the default value of the **forward delay** parameter of MSTP, run **no spanning-tree mstp max-age**.

### Parameter

Parameter	Description
seconds	Value range: 6-40 seconds Default value: 20 seconds

### Default value

20 seconds

## Instruction

None

## Example

The following example shows how to set the **max age** parameter of MSTP to **10**.

```
Router_config# spanning-tree mstp max-age 10
Router_config# no spanning-tree mstp max-age
```

## 8.4.10 spanning-tree mstp diameter

## Syntax

**spanning-tree mstp diameter** *net-diameter*

**no spanning-tree mstp diameter**

To configure the network diameter of MSTP, run **spanning-tree mstp diameter** *net-diameter*. To resume the default value of the network diameter, run **no spanning-tree mstp diameter**.

## Parameter

Parameter	Description
net-diameter	Value range: 2-7 Default value: 7

## Default value

The default value of the network diameter is 7.

## Instruction

The **net-diameter** parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved. The **net-diameter** parameter is effective only to CIST. After configuration, the three time parameters of STP are automatically updated to a prior value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the reasonability of the time parameter.

## Example

The following example shows how to set the network diameter of MSTP to 5 and then resume its default value.

```
Router_config# spanning-tree mstp diameter 5
Router_config# no spanning-tree mstp diameter
```

## 8.4.11 spanning-tree mstp max-hops

## Syntax

**spanning-tree mstp max-hops** *hop-count*

**no spanning-tree mstp max-hops**

To set the maximum hops of MSTP BPDU, run **spanning-tree mstp max-hops *hop-count***. To resume the default settings, run **no spanning-tree mstp max-hops**.

## Parameter

Parameter	Description
hop-count	Value range: 1-40 Default value: 20

## Default value

The default value of the maximum hops is 20.

## Instruction

None

## Example

The following example shows how to set the maximum hops of MSTP BPDU to **5** and then resume the default value.

```
Router_config# spanning-tree mstp max-hops 5
Router_config# no spanning-tree mstp max-hops
```

## 8.4.12 spanning-tree mstp port-priority

## Syntax

**spanning-tree mstp *instance-id* port-priority *value***

**no spanning-tree *instance-id* port-priority**

To configure the port priority in the designated spanning-tree instance, run **spanning-tree mstp *instance-id* port-priority *value***. To resume the port priority to the default settings, run **no spanning-tree mstp *instance-id* port-priority**.

## Parameter

Parameter	Description
instance-id	ID of the STP instance, which ranges between 0 and 15
value	Value of the port priority, which can be one of the following values 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240.

## Default value

The port priority in all STP instances is 128 by default.

## Instruction

None

## Example

The following example shows how to set the priority value of port switchFastEthernet 4/1 in CIST to **16** and then resume the default value.

```
Router_config_sfe4/1# spanning-tree mstp 0 port-priority 16
Router_config_sfe4/1# no spanning-tree mstp 0 port-priority
```

## 8.4.13 spanning-tree mstp cost

## Syntax

**spanning-tree mstp** *instance-id* **cost** value

**no spanning-tree mstp** *instance-id* **cost**

To set the path cost of the spanning tree in the designated STP instance, run **spanning-tree mstp** *instance-id* **cost** *value*. To resume the default value, run **no spanning-tree mstp** *instance-id* **cost**.

## Parameter

Parameter	Description
instance-id	ID of the STP instance, which ranges between 0 and 15
value	Path cost of a port, which ranges between 1 and 200,000,000

## Default value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

## Instruction

None

## Example

The following example shows how to set the path cost of port switchFastEthernet 4/1 to 200 in CIST.

```
Router_config_sfe4/1# spanning-tree mstp 0 cost 200
Router_config_sfe4/1#
```

## 8.4.14 spanning-tree mstp edge

## Syntax

**spanning-tree mstp edge** { **force-true** | **force-false** | **auto** }

**no spanning-tree mstp edge**

To configure the MSTP edge of a port, run **spanning-tree mstp edge { force-true | force-false | auto }**. To resume the connection type to be automatic check, run **no spanning-tree mstp edge**.

## Parameter

Parameter	Description
force-true	Set a port forcedly to be an edge port.
force-false	Set a port forcedly to be not an edge port.
auto	Checks the edge automatically (default).

## Default value

MSTP will automatically check the edge port by default.

## Instruction

None

## Example

None

## 8.4.15 spanning-tree mstp point-to-point

## Syntax

**spanning-tree mstp point-to-point { force-true | force-false | auto }**

**no spanning-tree mstp point-to-point**

To configure the connection type of a port, run **spanning-tree mstp point-to-point { force-true | force-false | auto }**. To resume the connection type to **auto-check**, run **no spanning-tree mstp point-to-point**.

## Parameter

Parameter	Description
force-true	Sets the port connection mode to <b>point-to-point</b> .
force-false	Sets the port connection mode to <b>sharing</b> .
auto	Sets the port connection mode to <b>auto-check</b> (the default mode).

## Default value

MSTP will automatically check the port connection mode by default.

**Instruction**

None

**Example**

The following example shows how to set the connection mode of port switchFastEthernet 4//1 to **sharing**.

```
Router_config_sfe4/1# spanning-tree mstp point-to-point force-false
Router_config_sfe4/1#
```

**8.4.16 spanning-tree mstp mst-compatible****Syntax****spanning-tree mstp mst-compatible****no spanning-tree mstp mst-compatible**

To activate the MST-compatible mode, run **spanning-tree mstp mst-compatible**. To shut down the MST-compatible mode, run **no spanning-tree mstp mst-compatible**.

**Parameter**

None

**Default value**

The compatible mode is not activated by default and the switch cannot establish an area with other switches which transmit BPDU in compatible mode.

**Instruction**

After the compatible mode is enabled, you are recommended to set a connected switch which runs other MSTP to the root of CIST, securing that the switch can enter the compatible mode through receiving packets.

**Example**

The following example shows how to activate the MST-compatible mode of a switch in global configuration mode.

```
Router_config#spanning-tree mstp mst-compatible
```

**8.4.17 spanning-tree mstp migration-check****Syntax****spanning-tree mstp migration-check**

To remove the STP information which is checked on a port and then restart the protocol transform process, run the previous command.

**Parameter**

None

**Default value**

None

**Instruction**

This command validates both in global configuration mode and in port configuration mode.

**Example**

The following example shows how to conduct the protocol transfer check on all ports and then conduct the second protocol transfer check on port switchFastEthernet 4//1.

```
Router_config# spanning-tree mstp migration-check
Router_config# interface f 0/1
Router_config_sfe4/1# spanning-tree mstp migration-check
```

**8.4.18 show spanning-tree mstp****Syntax**

**show spanning-tree mstp [ instance *instance-id* ]**

To browse the MSTP information, run **show spanning-tree mstp [instance *instance-id*]**. If the **instance** parameter is not in the command syntax, the information about all spanning-tree instances will be displayed.

**Parameter**

Parameter	Description
instance-id	ID of the STP instance, which ranges between 0 and 15

**Default value**

None

**Instruction**

This command can be used in monitoring mode, global configuration mode or port mode.

**Example**

The following example shows how to browse all spanning-tree instances. MST00 stands for CIST, while Type stands for the connection type of the corresponding port.

```
Switch#show spanning-tree mstp
```

```
MST00      Vlans Mapped: 1,4-4094
Bridge     Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0)
Root       This bridge is the CIST and regional root
Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times Hello Time 2, Forward Delay 15, Max Age 20
```



Interface	Role	Sts	Cost	Pri.	Nbr	Type
F0/1	Desg	FWD	200000	128.1		P2p
F0/3	Back	BLK	200000	128.3		P2p
F0/47	Desg	FWD	200000	128.47		Edge

  

MST01	Vlans Mapped: 2					
Bridge	Address	00E0.0F64.8365	Priority	32769	(32768 mst-id 1)	
Root	This bridge for MST01					

  

Interface	Role	Sts	Cost	Pri.	Nbr	Type
F0/1	Desg	FWD	200000	128.1		P2p

  

MST02	Vlans Mapped: 3					
Bridge	Address	00E0.0F64.8365	Priority	32770	(32768 mst-id 2)	
Root	This bridge for MST02					

  

Interface	Role	Sts	Cost	Pri.	Nbr	Type
F0/1	Desg	FWD	200000	128.1		P2p

#### 8.4.19 show spanning-tree mstp region

##### Syntax

##### **show spanning-tree mstp region**

To browse the area configuration information about MSTP, run the previous command.

##### Parameter

None

##### Default value

None

##### Instruction

None

##### Example

In the following example, MST Config Table is to display the relationship between VLAN and spanning-tree instance.

```
Router_config# show spanning-tree mstp region
```

```
MST Region:
```

```
  Name: [reg01]
```

```
  Revision:[0]
```

```
MST Config Table:
```

```
  Instance    VLAN IDs
```

```
-----
```

```

0    1,4-4094
1    2
2    3

```

#### 8.4.20 show spanning-tree mstp detail

##### Syntax

##### **show spanning-tree mstp detail**

To browse the detailed information about MSTP, run the previous command.

##### Parameter

None

##### Default value

None

##### Instruction

None

##### Example

The following example shows how to browse the detailed information about MSTP, which includes the port connection types and the configuration of optional attributes.

```
Switch#show spanning-tree mstp detail
```

```

MST00      Vlans Mapped: 1,4-4094
Bridge      Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0)
Root        This bridge is the CIST and regional root
Configured  Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times  Hello Time 2, Forward Delay 15, Max Age 20

FastEthernet0/1 of MST00 is designated forwarding
Port Info      Port ID 128.1      Priority 128      Cost 200000
Designated Root      Address 00E0.0F64.8365 Priority 32768 Cost 0
CIST Regional Root    Address 00E0.0F64.8365 Priority 32768 Cost 0
Designated Bridge     Address 00E0.0F64.8365 Priority 32768 Port ID 128.1
Edge Port:  disabled                               Link Type: point-to-point (auto)
Bpdu Guard: disabled (default)                     Root Guard: disabled (default)
Loop Guard: disabled (default)

Timers:  message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
Bpdu sent 335, received 5

FastEthernet0/3 of MST00 is backup blocking
Port Info      Port ID 128.3      Priority 128      Cost 200000
Designated Root      Address 00E0.0F64.8365 Priority 32768 Cost 0
CIST Regional Root    Address 00E0.0F64.8365 Priority 32768 Cost 0
Designated Bridge     Address 00E0.0F64.8365 Priority 32768 Port ID 128.1
Edge Port:  disabled                               Link Type: point-to-point (auto)
Bpdu Guard: disabled (default)                     Root Guard: disabled (default)

```

Loop Guard: disabled (default)  
 Timers: message expires in 5 sec, forward delay 15 sec, up time 662 sec  
 Number of transitions to forwarding state: 0  
 Bpdu sent 5, received 335

FastEthernet0/47 of MST00 is designated forwarding  
 Port Info Port ID 128.47 Priority 128 Cost 200000  
 Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0  
 CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0  
 Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.47  
 Edge Port: enabled (auto) Link Type: point-to-point (auto)  
 Bpdu Guard: disabled (default) Root Guard: disabled (default)  
 Loop Guard: disabled (default)  
 Timers: message expires in 0 sec, forward delay 0 sec, up time 1485 sec  
 Number of transitions to forwarding state: 1  
 Bpdu sent 744, received 0

MST01 Vlans Mapped: 2  
 Bridge Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1)  
 Root This bridge for MST01

FastEthernet0/1 of MST01 is designated forwarding  
 Port Info Port ID 128.1 Priority 128 Cost 200000  
 Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0  
 Designated Bridge Address 00E0.0F64.8365 Priority 32769 Port ID 128.1  
 Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec  
 Number of transitions to forwarding state: 1  
 MST Config Message transmitted 335, received 0

MST02 Vlans Mapped: 3  
 Bridge Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2)  
 Root This bridge for MST02

FastEthernet0/1 of MST02 is designated forwarding  
 Port Info Port ID 128.1 Priority 128 Cost 200000  
 Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0  
 Designated Bridge Address 00E0.0F64.8365 Priority 32770 Port ID 128.1  
 Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec  
 Number of transitions to forwarding state: 1  
 MST Config Message transmitted 335, received 0

#### 8.4.21 show spanning-tree mstp interface

##### Syntax

**show spanning-tree mstp interface *interface-id***

To browse the information about a port under MSTP, run the previous command.

##### Parameter

Parameter	Description
interface-id	Name of an interface, such as f0/1 and fastEthernet0/3

**Default value**

None

**Instruction**

None

**Example**

The following example shows how to browse the information about interface f0/1.

```
Switch#show spanning-tree mstp interface f0/1
```

```
FastEthernet0/1 of MST00 is designated forwarding
```

```
Port Info          Port ID 128.1          Priority 128    Cost 200000
Designated Root    Address 00E0.0F64.8365 Priority 32768  Cost 0
CIST Regional Root Address 00E0.0F64.8365 Priority 32768  Cost 0
Designated Bridge  Address 00E0.0F64.8365 Priority 32768  Port ID 128.1
Edge Port:         disabled                Link Type:     point-to-point (auto)
Bpdu Guard:        disabled (default)      Root Guard:    disabled (default)
Loop Guard:         disabled (default)
Timers:            message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
Bpdu sent 430, received 5
```

```
FastEthernet0/1 of MST01 is designated forwarding
```

```
Port Info          Port ID 128.1          Priority 128    Cost 200000
Designated Root    Address 00E0.0F64.8365 Priority 32769  Cost 0
Desingated Bridge  Address 00E0.0F64.8365 Priority 32769  Port ID 128.1
Timers:            message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0
```

```
FastEthernet0/1 of MST02 is designated forwarding
```

```
Port Info          Port ID 128.1          Priority 128    Cost 200000
Designated Root    Address 00E0.0F64.8365 Priority 32770  Cost 0
Desingated Bridge  Address 00E0.0F64.8365 Priority 32770  Port ID 128.1
Timers:            message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0
```

```
Instance Role Sts Cost      Pri.Nbr Vlans Mapped
-----
0      Desg FWD 200000  128.1  1,4-4094
1      Desg FWD 200000  128.1  2
2      Desg FWD 200000  128.1  3show spanning-tree mstp protocol-migration
```

**Syntax****show spanning-tree mstp protocol-migration**

To browse the protocol transfer information on an interface under MSTP, run the previous command.

## Parameter

None

## Default value

None

## Instruction

None

## Example

The following example shows how to browse the information about protocol transfer on an interface. In the following example, interface f0/2 is running in 802.1D STP mode.

```
Switch#show spanning-tree mstp protocol-migration
```

```
MSTP Port Protocol Migration
```

Interface	Protocol	Info
F0/2	802.1D	

## 8.5 Optional STP Attribute Configuration Commands

### 8.5.1 spanning-tree portfast

## Syntax

**spanning-tree portfast** {bpdufilter default | bpduguard default | default}

**no spanning-tree portfast** {bpdufilter default | bpduguard default | default}

To configure the portfast attribute in global configuration mode, run **spanning-tree portfast {bpdufilter default | bpduguard default | default}**. To cancel this attribute in global configuration mode, run **no spanning-tree portfast {bpdufilter default | bpduguard default | default}**.

**spanning-tree portfast** [disable | trunk]

**no spanning-tree portfast**

To configure the portfast attribute in port configuration mode, run **spanning-tree portfast [disable | trunk ]**. To cancel this attribute in port configuration mode, run **no spanning-tree portfast**.

## Parameter

Parameter	Description
bpdufilter default	Starts the BPDU filtration.
bpduguard default	Starts the BPDU protection.

default	Means the default mode.
---------	-------------------------

### Default value

This function is not enabled by default.

### Description

The portfast attribute enables a port in SSTP/PVST mode to promptly enter the forwarding state without state change. This configuration invalidates in RSTP/MSTP mode.

After the portfast attribute is configured, it need be protected through BPDU Guard configuration or BPDU Filter configuration.

### Command mode

Global or port configuration mode

### Example

The following example shows how to enable the portfast attribute in global configuration mode.

```
Router_config# spanning-tree portfast default
Router_config#
```

The following example shows how to enable the attributes of port f0/0:

```
Switch(config_f0/0)# spanning-tree portfast
Switch(config_f0/0)#
```

## 8.5.2 spanning-tree bpduguard

### Syntax

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

**no spanning-tree bpduguard**

To configure BPDU Guard, run **spanning-tree bpduguard {disable | enable}**. To cancel BPDU Guard, run **no spanning-tree bpduguard**.

### Parameter

None

### Default value

This function is not enabled by default.

### Instruction

In SSTP/PVST mode, if a port that has the BPDU Guard function and the Portfast function configured receives BPDU, this port will be mandatorily shut down. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

**Command mode**

Port configuration mode

**Example**

The following example shows how to enable BPDU protection on port f0/0.

```
Switch(config_f0/0)# spanning-tree bpduguard enable
Switch(config_f0/0)#
```

**8.5.3 spanning-tree bpdufilter****Syntax**

**spanning-tree bpdufilter {disable | enable}**

**no spanning-tree bpdufilter**

To configure the BPDU filtration, run **spanning-tree bpdufilter {disable | enable}**. To cancel the BPDU filtration, run **no spanning-tree bpdufilter**.

**Parameter**

None

**Default value**

This function is not enabled by default.

**Description**

In SSTP/PVST mode, a port which has the BPDU Filter function and the Port Fast function configured receives BPDU, the BPDU Filter attribute and the Port Fast attribute are automatically shut down. In this case, the port resumes to be a normal port which first enters the listening state, the learning state and then the forwarding state.

This function invalidates in RSTP/MSTP mode.

**Command mode**

Port configuration mode

**Example**

The following example shows how to enable BPDU filtration on port f0/0.

```
Switch(config_f0/0)# spanning-tree bpdufilter enable
Switch(config_f0/0)#
```

**8.5.4 spanning-tree uplinkfast****Syntax**

**spanning-tree uplinkfast [max-update-rate pkts-per-second]**

**no spanning-tree uplinkfast [max-update-rate]**

To configure the uplinkfast function, run **spanning-tree uplinkfast [max-update-rate pkts-per-second]**. To cancel the uplinkfast function, run **no spanning-tree uplinkfast [max-update-rate]**.

#### Parameter

None

#### Default value

This function is not enabled by default.

#### Instruction

The UplinkFast function validates only in SSTP/PVST mode.

#### Command mode

Global configuration mode

#### Example

The following example shows how to enable the UplinkFast attribute.

```
Router_config# spanning-tree uplinkfast
Router_config#
```

### 8.5.5 spanning-tree backbonefast

#### Syntax

**spanning-tree backbonefast**

**no spanning-tree backbonefast**

To configure the backbonefast function, run **spanning-tree backbonefast**. To cancel the backbonefast function, run **no spanning-tree backbonefast**.

#### Parameter

None

#### Default value

This function is not enabled by default.

#### Instruction

The backbonefast function validates only in SSTP/PVST mode.

#### Command mode

Global configuration mode

#### Example

The following example shows how to enable the backbonefast function:



```
Router_config# spanning-tree backbonefast
Router_config#
```

### 8.5.6 spanning-tree guard

#### Syntax

**spanning-tree guard** {loop | none | root}

**no spanning-tree guard**

To configure the Port Guard function, run **spanning-tree guard** {**loop** | **none** | **root**}. To cancel this function, run **no spanning-tree guard**.

#### Parameter

Parameter	Description
<i>loop</i>	Guard loop Range: 1-0*fe
<i>none</i>	Guard none Range: 48 bits
<i>root</i>	Guard root

#### Default value

This protection function is not enabled.

#### Instruction

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the port cannot receive BPDU continuously.

#### Command mode

Port configuration mode

#### Example

The following example shows how to prevent port f0/0 from being the root:

```
Switch(config_f0/0)# spanning-tree guard root
Switch(config_f0/0)#
```

### 8.5.7 spanning-tree loopguard

#### Syntax

**spanning-tree loopguard** default

To configure the guard loop in global configuration mode, run **spanning-tree loopguard default**. To cancel the guard loop in global configuration mode, run **no spanning-tree loopguard default**.

Parameter

None

Default value

None

Description

None

Command mode

Global configuration mode

Example

The following example shows how to enable the loopguard function.

```
Router_config# spanning-tree loopguard default
Router_config#
```

### 8.5.8 spanning-tree fast-aging

Syntax

**spanning-tree fast-aging**

**no spanning-tree fast-aging**

The two commands above are used to enable or disable the fast aging mechanism of the address table.

**spanning-tree fast-aging protection**

**no spanning-tree fast-aging protection**

The two commands above are used to enable or disable the protection of fast aging of the address table.

**spanning-tree fast-aging protection time *value***

**no spanning-tree fast-aging protection time**

The two commands above are used to configure the time of aging protection of the address table.

Parameter

Parameter	Description
<i>value</i>	Stands for the aging protection time. 10-60 seconds (15 seconds by default)

#### Default value

Fast aging is enabled by default. However protection is not enabled by default.

#### Description

switches of version 2.0.1M and the previous versions, and hi-end switches of version 4.0.00 and the previous versions do not support the aging protection of the address table.

#### Command mode

Global configuration mode

#### Example

The following example shows how to enable fast aging protection and set the protection time to 30 seconds.

```
Router_config#spanning-tree fast-aging protection
Router_config#spanning-tree fast-aging protection time 30
```

### 8.5.9 spanning-tree fast-aging flush-fdb

#### Syntax

**spanning-tree fast-aging flush-fdb**  
**no spanning-tree fast-aging flush-fdb**

To enable or disable FDB-Flush, run the previous commands.

#### Parameter

None

#### Default value

There is no default settings.

#### Description

**Please configure this command under the guide of technical engineers.**

switches of version 2.0.1M and the previous versions, and hi-end switches of version 4.0.00 and the previous versions do not support the aging protection of the address table.

FDB-Flush is independent of fast aging. FDB-Flush can be configured while **no spanning-tree fast-aging** is configured. Fast aging protection is invalid to FDB-Flush.

#### Command mode

Global configuration mode

## Example

The following example shows how to disable fast aging and enable FDB-Flush.

```
Router_config#no spanning-tree fast-aging
Router_config#spanning-tree fast-aging flush-fdb
```

## Chapter 9 802.1x Configuration Commands

### 9.1 802.1x Configuration Commands

The following commands are used to configure 802.1x:

- dot1x enable
- dot1x port-control
- dot1x multiple-hosts
- dot1x default
- dot1x max-req
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x user-permit
- dot1x authentication method
- dot1x accounting enable
- dot1x accounting method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

#### 9.1.1 dot1x enable

Syntax

```
dot1x enable  
no dot1x enable
```

Parameter

None

## Default value

None

## Instruction

If the 802.1x function is not enabled, you cannot start it on an interface. If the 802.1x function is forbidden, all interfaces have no the 802.1x function, and at the same time, all 802.1x packets will not be received by CPU but can be forwarded in VLAN like normal multicast packets.

## Command mode

Global configuration mode

## Example

The following example shows how to enable dot1x.

```
Router_config#dot1x enable
```

```
Router_config#
```

## 9.1.2 dot1x port-control

## Syntax

**dot1x port-control {*auto*|*force-authorized*|*force-unauthorized*}**

**no dot1x port-control**

## Parameter

Parameter	Description
<b>auto</b>	Enables the 802.1x authentication mode.
<b>force-authorized</b>	Cancels the 802.1x authentication.
<b>force-unauthorized</b>	Sets the interface to <b>unauthorized</b> mandatorily.

## Default value

force-authorized

## Instruction

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the **auto** command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or listening port.

## Command mode

Port configuration mode

## Example

The following example shows how to enable 802.1x on interface f0/24.

```
Switch(config_f0/24)# dot1x port-control auto
Switch(config_f0/24)#
```

The following example shows how to firstly set interface f0/23 to the VLAN backbone and then enable 802.1x.

```
Switch(config_f0/23)#switchport mode trunk
Switch(config_f0/23)#dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(f0/23)
Switch(config_f0/23)#
```

### 9.1.3 dot1x multiple-hosts

#### Syntax

```
dot1x multiple-hosts
no dot1x multiple-hosts
```

#### Parameter

None

#### Default value

The 802.1x multi-client authentication is disabled.

#### Instruction

The 802.1x authentication is mainly for the single host user. At this time, the switch allows only one user to conduct the authentication and the access control. However, sometimes the port may connect multiple hosts through 802.1x-unsupported switching device, such as switch 1108. In order to make these hosts' users access successfully, you can enable the multi-host port access function.

After an interface is configured to 802.1x multi-client authentication, the switch will perform authentication to different host users. If the authentication passes, the switch allows these hosts to access through the switch itself.

#### Command mode

Port configuration mode

#### Example

The following example shows how to enable multi-client interface authentication on interface f0/24.

```
Switch(config_f0/24)# dot1x multiple-hosts
Switch(config_f0/24)#
```

### 9.1.4 dot1x default

Syntax

**dot1x default**

Parameter

None

Default value

None

Instruction

This command is used to resume all global configurations to the default settings.

Command mode

Global configuration mode

Example

The following example shows how to resume all dot1x configuration parameters to their default values.

```
Router_config#dot1x default
Router_config#
```

### 9.1.5 dot1x max-req

Syntax

**dot1x max-req** *count*  
**no dot1x max-req**

Parameter

Parameter	Description
<i>count</i>	Maximum times of identity authentication requests, ranging between 1 and 10

Default value

2

Instruction

You can modify the maximum times of ID authentication request according to different network environments, ensuring that the authentication between the client and the authentication server passes.



## Command mode

Global configuration mode

## Example

The following example shows how to configure the maximum times of dot1x identity authentication request to **4**.

```
Router_config#dot1x max-req 4
Router_config#
```

### 9.1.6 dot1x reauth-max

#### Syntax

**dot1x reauth-max** *count*  
**no dot1x reauth-max**

#### Parameter

Parameter	Description
<i>count</i>	Maximum authentication re-try times, ranging between 1 and 10

#### Default value

4

#### Instruction

This command is used to set the authentication retry times. If the retry times exceeds the maximum retry times and the client has no response, the authentication is mounted.

## Command mode

Global configuration mode

## Example

The following example shows how to configure the maximum times of dot1x identity authentication request to **5**.

```
Router_config#dot1x reauth-max 5
Router_config#
```

### 9.1.7 dot1x re-authentication

#### Syntax

**dot1x re-authentication**  
**no dot1x re-authentication**

## Parameter

None

## Default value

None

## Instruction

After an interface passes authentication, the interface will still perform authentication to hosts in a certain period. You can run **dot1x timeout re-autjperiod** to configure the period.

## Command mode

Global configuration mode

## Example

The following example shows how to enable the re-authentication function.

```
Router_config#dot1x re-authentication
Router_config#
```

## 9.1.8 dot1x timeout quiet-period

## Syntax

```
dot1x timeout quiet-period time
no dot1x timeout quiet-period
```

## Parameter

Parameter	Description
<i>time</i>	Period for restarting dot1x authentication, ranging between 0 and 65535 seconds

## Default value

60s

## Instruction

There is a certain period when the switch cannot perform any authentication after the previous authentication fails.

## Command mode

Global configuration mode

## Example

The following example shows how to set the value of **quiet-period** to 40.

```
Router_config#dot1x timeout quiet-period 40
Router_config#
```

### 9.1.9 dot1x timeout re-authperiod

#### Syntax

```
dot1x timeout re-authperiod time
no dot1x timeout re-authperiod
```

#### Parameter

Parameter	Description
<i>time</i>	dot1x re-authentication period, ranging between 1 and 4294967295s

#### Default value

3600s

#### Instruction

This command validates only when the re-authentication function is enabled.

#### Command mode

Global configuration mode

#### Example

The following example shows how to set the dot1x re-authentication period to 7200 seconds.

```
Router_config# dot1x timeout re-authperiod 7200
Router_config#
```

### 9.1.10 dot1x timeout tx-period

#### Syntax

```
dot1x timeout tx-period time
no dot1x timeout tx-period
```

#### Parameter

Parameter	Description
<i>time</i>	Time which ranges between 1 and 65535 seconds

#### Default value

30s

**Instruction**

This command is used to set the client's authentication request response interval. If the interval is exceeded, the switch would retransmit the authentication request.

**Command mode**

Global configuration mode

**Example**

The following example shows how to set the transmission frequency to 24.

```
Switch(config_f0/0)# dot1x timeout tx-period 24
Switch(config_f0/0)#
```

**9.1.11 dot1x user-permit****Syntax**

```
dot1x user-permit xxx yyy zzz
no dot1x user-permit
```

**Parameter**

Parameter	Description
xxx	A user name
yyy	A user name
zzz	A user name

**Default value**

No user is bound and all users would pass.

**Instruction**

This command can be used to bind users on an interface. Each interface can be bound to up to eight users. When the 802.1x authentication is enabled, the authentication is performed only to those bound users. However, to those unbound users, the authentication must fail.

**Command mode**

Port configuration mode

**Example**

The following example shows how to bind users a, b, c and d on interface switchFastEthernet 4/1.

```
Router_config_sfe4/1# dot1x user-permit a b c d
Router_config_sfe4/1#
```

### 9.1.12 dot1x authentication method

#### Syntax

**dot1x authentication method xxx**  
**no dot1x authentication method**

#### Parameter

Parameter	Description
xxx	Method name

#### Default value

Default method

#### Instruction

This command is used to configure the authentication method which must be one of authentication methods provided by AAA. One interface only uses one authentication method. When AAA performs authentication to the 802.1x user, AAA would select the configured authentication method to perform the authentication.

#### Command mode

Port configuration mode

#### Example

The following example shows how to set the authentication method on interface switchFastEthernet 4/1 to **abcd** which applies the local username for authentication and that on interface f0/2 to **efgh** which applies the remote radius authentication.

```
Router_config #aaa authentication dot1x abcd local
Router_config #aaa authentication dot1x efgh group radius
Router_config #int switchFastEthernet 4/1
Router_config_sfe4/1# dot1x authentication method abcd
Router_config_sfe4/1# int switchFastEthernet 4/2
Router_config_sfe4//2)# dot1x authentication method efgh
```

### 9.1.13 dot1x authen-type、 dot1x authentication type

#### Syntax

**dot1x authen-type {chap|eap}**  
**no dot1x authen-type**

To configure the dot1x authentication type in global configuration mode, run **dot1x authen-type**; to resume the default settings in global configuration mode, run **no dot1x authen-type**.

**dot1x authentication type {chap|eap}**  
**no dot1x authentication type**

To configure the dot1x authentication type on an interface, run **dot1x authentication type**; to resume the default settings on an interface, run **no dot1x authentication type**.

#### Parameter

None

#### Default value

The default dot1x authentication type is **chap**.

The default dot1x authentication type in global configuration mode is also used applied by default in interface configuration mode.

#### Instruction

This command is used to configure the authentication class, while the authentication class decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

#### Command mode

Interface or global configuration mode

#### Example

The following example shows how to set the authentication type on interface switchFastEthernet 4/1 to **chap** and the global authentication type to **eap**.

```
Router_config #dot1x authen-type eap
Router_config #int switchFastEthernet 4/1
Router_config_sfe4/1# dot1x authentication type chap
```

### 9.1.14 dot1x guest-vlan

#### Syntax

**dot1x guest-vlan**

**no dot1x guest-vlan**

To enable the guest-vlan function of dot1x in global configuration mode, run **dot1x guest-vlan**. To disable the guest-vlan function of dot1x in global configuration mode, run **no dot1x guest-vlan**.

#### Parameter

None

#### Default value

The guest-vlan function of dot1x is shut down in global configuration mode by default.

### Instruction

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the **dot1x guest-vlan id** command.

### Command mode

Global configuration mode

### Example

The following example shows how to enable the guest-vlan function in global configuration mode.

```
Router_config #dot1x guest-vlan
```

## 9.1.15 dot1x guest-vlan id

### Syntax

**dot1x guest-vlan id**

**no dot1x guest-vlan**

To configure the value of **dot1x guest-vlan id** on an interface, run **dot1x guest-vlan id**; to resume the default value **0**, run **no dot1x guest-vlan**.

### Parameter

ID: stands for the value of guest vlan, which can be any vlan ID configured in the system.

### Default value

0

### Instruction

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the **dot1x guest-vlan id** command.

### Command mode

Port configuration mode

### Example

The following example shows how to configure the guest-vlan id in port configuration commands.

```
Switch(config_if) #dot1x guest-vlan 2
```

## 9.1.16 aaa authentication dot1x

## Syntax

```

aaa authentication dot1x {default} method1 [method2...]
no aaa authentication dot1x {default} method1 [method2...]

```

## Parameter

Parameter	Description
<b>default</b>	Uses the following method when a user is authenticated.
<i>method1</i> [ <i>method2...</i> ]	enable 、 group radius、 line、 local、 local-case、 none

## Default value

There is no authentication.

## Instruction

The **method** parameter provides a series of methods to authenticate the password of the client host. You'd better adopt the radius as the AAA authentication mode of 802.1x. You can also use the local configuration data for authentication, such as user password saved in the local configuration.

## Command mode

Global configuration mode

## Example

The following example shows how to configure the dot1x authentication method to **radius**.

```

Router_config#aaa authentication dot1x default group radius
Router_config#

```

## 9.1.17 debug dot1x error

## Syntax

```

debug dot1x error

```

## Parameter

None

## Default value

None



## Instruction

This command is used to export all error information occurred during dot1x running. The error information can help locating the errors.

## 9.1.18 debug dot1x state

## Syntax

**debug dot1x state**

## Parameter

None

## Default value

None

## Instruction

The following shows the format of information output:

```
2003-3-18 17:40:09 802.1x:AuthSM(F0/10) state Connecting-> Authenticating, event rxRespId
```

```
2003-3-18 17:40:09 802.1x:F0/10 Create user for Enter authentication
```

```
2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Idle-> Response, event authStart
```

```
2003-3-18 17:40:09 802.1x:F0/10 user "myname" denied, Authentication Force Failed
```

```
2003-3-18 17:40:09 802.1x:F0/10 Authentication Fail
```

```
2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Response-> Fail, event aFail
```

## 9.1.19 debug dot1x packet

## Syntax

**debug dot1x packet**

## Parameter

None

## Default value

*None*

## Instruction

```
2003-3-18 17:40:09 802.1x:F0/10 Tx --> Supplicant(0008.74bb.d21f)
```

```
EAPOL ver:01, type:00, len:5
```

```
EAP code:01, id:03, type:01, len:5
```

```
00
```

```
2003-3-18 17:40:09 802.1x:F0/10 Rx <-- Supplicant(0008.74bb.d21f)
```

```
EAPOL ver:01, type:00, len:10
```

```
EAP code:02, id:03, type:01, len:10
62 64 63 6f 6d a5
```

### 9.1.20 show dot1x

#### Syntax

**show dot1x** [interface *intf-id*]

To display the 802.1x configuration information, run the previous command.

#### Parameter

Parameter	Description
<i>intf-id</i>	Stands for a specific physical interface.

#### Default value

None

#### Instruction

This command is used to display the 802.1x configuration information.

#### Command mode

EXEC

#### Example

The following example shows how to configure **dot1x port-control auto** on interface f0/10.

```
Router_config#sho dot1x
802.1X Parameters
reAuthen      No
reAuth-Period 3
quiet-Period  10
Tx-Period     30
Supp-timeout  30
Server-timeout 30
reAuth-max    4
max-request   2
authen-type   Eap
IEEE 802.1x on port F0/10 enabled
Authorized      Yes
Authen Type     Eap
Authen Method   default
Permit Users    All Users
Multiple Hosts  Disallowed
Supplicant      aaa(0008.74bb.d21f)
Current Identifier 21
Authenticator State Machine
State           Authenticated
```

Reauth Count	0
Backend State Machine	
State	Idle
Request Count	0
Identifier (Server)	20
Port Timer Machine	
Auth Tx While Time	16
Backend While Time	16
reAuth Wait Time	3
Hold Wait Time	0