

## Content

<b>CHAPTER 1 VLAN CONFIGURATION.....</b>	<b>1-1</b>
<b>1.1 COMMANDS FOR VLAN CONFIGURATION .....</b>	<b>1-1</b>
1.1.1 debug gvrp event .....	1-1
1.1.2 debug gvrp packet .....	1-1
1.1.3 dot1q-tunnel enable.....	1-2
1.1.4 dot1q-tunnel selective enable.....	1-2
1.1.5 dot1q-tunnel selective s-vlan.....	1-2
1.1.6 dot1q-tunnel tpid.....	1-2
1.1.7 garp timer join .....	1-2
1.1.8 garp timer leave.....	1-3
1.1.9 garp timer leaveAll .....	1-3
1.1.10 gvrp (Global).....	1-3
1.1.11 gvrp (Port) .....	1-4
1.1.12 no garp timer .....	1-4
1.1.13 name .....	1-4
1.1.14 private-vlan .....	1-5
1.1.15 private-vlan association .....	1-6
1.1.16 show dot1q-tunnel .....	1-6
1.1.17 show garp timer .....	1-6
1.1.18 show gvrp fsm information.....	1-7
1.1.19 show gvrp leaveAll fsm information .....	1-7
1.1.20 show gvrp leavetimer running information.....	1-8
1.1.21 show gvrp port-member .....	1-8
1.1.22 show gvrp port registerd vlan .....	1-9
1.1.23 show gvrp timer running information.....	1-9
1.1.24 show gvrp vlan registerd port .....	1-10
1.1.25 show vlan .....	1-10
1.1.26 show vlan-translation .....	1-11
1.1.27 switchport access vlan.....	1-11
1.1.28 switchport dot1q-tunnel.....	1-12
1.1.29 switchport forbidden vlan .....	1-12
1.1.30 switchport hybrid allowed vlan .....	1-12
1.1.31 switchport hybrid native vlan .....	1-13

<b>Commands for VLAN and MAC Address Configuration</b>	<b>Content</b>
1.1.32 switchport interface .....	1-14
1.1.33 switchport mode .....	1-14
1.1.34 switchport mode trunk allow-null .....	1-15
1.1.35 switchport trunk allowed vlan .....	1-15
1.1.36 switchport trunk native vlan .....	1-16
1.1.37 vlan .....	1-17
1.1.38 vlan internal .....	1-17
1.1.39 vlan ingress enable.....	1-17
1.1.40 vlan-translation .....	1-18
1.1.41 vlan-translation enable.....	1-18
1.1.42 vlan-translation miss drop.....	1-18

## **CHAPTER 2 COMMANDS FOR MAC ADDRESS TABLE**

<b>CONFIGURATION .....</b>	<b>2-1</b>
<b>2.1 COMMANDS FOR MAC ADDRESS TABLE CONFIGURATION.....</b>	<b>2-1</b>
2.1.1 clear mac-address-table dynamic .....	2-1
2.1.2 mac-address-table aging-time .....	2-1
2.1.3 mac-address-table static   static-multicast   blackhole .....	2-2
2.1.4 show mac-address-table .....	2-3
<b>2.2 COMMANDS FOR MAC ADDRESS BINDING CONFIGURATION .....</b>	<b>2-3</b>
2.2.1 clear port-security dynamic .....	2-3
2.2.2 mac-address-table periodic-monitor-time.....	2-4
2.2.3 mac-address-table trap enable .....	2-4
2.2.4 mac-address-table synchronizing enable .....	2-4
2.2.5 show port-security .....	2-5
2.2.6 show port-security address .....	2-6
2.2.7 show port-security interface.....	2-6
2.2.8 station-movement check.....	2-7
2.2.9 switchport port-security .....	2-7
2.2.10 switchport port-security convert.....	2-8
2.2.11 switchport port-security lock.....	2-8
2.2.12 switchport port-security mac-address .....	2-8
2.2.13 switchport port-security maximum.....	2-9
2.2.14 switchport port-security timeout.....	2-9
2.2.15 switchport port-security violation.....	2-10

# Chapter 1 VLAN Configuration

## 1.1 Commands for VLAN Configuration

### 1.1.1 debug gvrp event

**Command:** debug gvrp event interface (ethernet | port-channel ) IFNAME

no debug gvrp event interface (ethernet | port-channel ) IFNAME

**Function:** Enable/disable GVRP event debugging including the transfer of state machine and the expiration of timer.

**Parameters:** ethernet, physical port  
port-channel, aggregate port  
IFNAME, port name

**Command Mode:** Admin mode

**Default:** GVRP event debugging is disabled.

**Usage Guide:** Use this command to enable GVRP event debugging.

**Example:** Show GVRP event debugging.

```
Switch(config)#debug gvrp event interface ethernet 1/1
```

```
%Jan 16 02:25:14 2006 GVRP EVENT: LO -> VO , interface ethernet 1/1, vlan 100
```

```
%Jan 16 02:35:15 2006 GVRP EVENT: join timer expire, interface ethernet 1/1
```

### 1.1.2 debug gvrp packet

**Command:** debug gvrp packet (receive | send) interface (ethernet | port-channel )  
IFNAME

no debug gvrp packet (receive | send) interface (ethernet | port-channel  
) IFNAME

**Function:** Enable/disable GVRP packet debugging.

**Parameters:** receive, enabling the debugging of receiving GVRP packet  
send, enabling the debugging of sending GVRP packet  
ethernet, physical port  
port-channel, aggregate port  
IFNAME, port name

**Command Mode:** Admin mode

**Default:** GVRP packet debugging is disabled.

**Usage Guide:** Use this command to enable the debugging of GVRP packet.

**Example:** Show information of sending and receiving GVRP packet.

```
Switch(config)#debug gvrp packet receive interface ethernet 1/1
```

```
Receive packet, smac 00-21-27-aa-0f-46, dmac 01-80-C2-00-00-21,
```

```
length 90, protocol ID:1,attribute type:0x01,
```

Attribute Index	Length	Event	Value
-----	-----	-----	-----
1	10	joinIn	100
2	10	joinEmpty	140
3	10	leaveIn	150
4	10	leaveEmpty	180

### 1.1.3 dot1q-tunnel enable

This command is not supported by the switch.

### 1.1.4 dot1q-tunnel selective enable

This command is not supported by the switch.

### 1.1.5 dot1q-tunnel selective s-vlan

This command is not supported by the switch.

### 1.1.6 dot1q-tunnel tpid

This command is not supported by the switch.

### 1.1.7 garp timer join

**Command:** `garp timer join <200-500>`

**Function:** Set the value of garp join timer, note that the value of join timer must be less than half leave timer.

**Parameters:** <200-500>, the value of timer in millisecond

**Command Mode:** Global mode

**Default:** 200 ms.

**Usage Guide:** Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.

**Example:** Set the value of garp join timer as 200ms.

```
Switch(config)#garp timer join 200
```

## 1.1.8 garp timer leave

**Command:** `garp timer leave <500-1200>`

**Function:** Set the value of garp leave timer, note that the value of leave timer must be double of join timer and less than leaveAll timer.

**Parameters:** <500-1200>, the value of timer in millisecond

**Command Mode:** Global mode

**Default:** 600 ms.

**Usage Guide:** Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.

**Example:** Set the value of garp leave timer as 600ms.

```
Switch(config)#garp timer leave 600
```

## 1.1.9 garp timer leaveAll

**Command:** `garp timer leaveall <5000-60000>`

**Function:** Set the value of garp leaveAll timer, note that the value of leaveAll timer must be larger than leave timer.

**Parameters:** <5000-60000>, the value of timer in millisecond

**Command Mode:** Global mode

**Default:** 10000 ms.

**Usage Guide:** Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.

**Example:** Set the value of garp leaveAll as 20000ms.

```
Switch(config)#garp timer leaveall 20000
```

## 1.1.10 gvrp (Global)

**Command:** `gvrp`

`no gvrp`

**Function:** Enable/disable GVRP function globally.

**Parameters:** None.

**Command Mode:** Global mode

**Default:** Disabled.

**Usage Guide:** Enable GVRP function globally and only in this way GVRP module can work normally.

**Example:** Enable GVRP function globally.

```
Switch(config)#gvrp
```

## 1.1.11 gvrp (Port)

**Command:** gvrp

no gvrp

**Function:** Enable/disable GVRP function on port. Notice: although GVRP can be enabled on port when GVRP is not enabled globally, it will not take effect until global GVRP is enabled.

**Parameters:** None

**Command Mode:** Port mode

**Default:** Disabled

**Usage Guide:** GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port).

**Example:** Enable GVRP of port.

```
Switch(config-if-ethernet1/1)#gvrp
```

## 1.1.12 no garp timer

**Command:** no garp timer (join | leave | leaveall)

**Function:** Restore garp join | leave | leaveAll timer to the default value.

**Parameters:** join, join timer

leave, leave timer

leaveAll, leaveAll timer

**Command Mode:** Global mode

**Default:** 200 | 600 | 10000 milliseconds for join | leave | leaveall timer respectively.

**Usage Guide:** Check whether the default value satisfy the range. If so, modify the value of garp join | leave | leaveAll timer to the default value, otherwise return a configuration error.

**Example:** Restore garp timer to the default value.

```
Switch(config)#no garp timer leaveall
```

## 1.1.13 name

**Command:** name <vlan-name>

no name

**Function:** Specify a name, a descriptive string, for the VLAN; the no operation of the command will delete the name of the VLAN.

**Parameters:** <vlan-name> is the specified name string.

**Command Mode:** VLAN Configuration Mode.

**Default:** The default VLAN name is vlanXXX, where xxx is VID.

**Usage Guide:** The switch can specify names for different VLANs, making it easier for users to identify and manage VLANs.

**Examples:** Specify the name of VLAN100 as TestVlan.

```
Switch(Config-Vlan100)#name TestVlan
```

## 1.1.14 private-vlan

**Command:** `private-vlan {primary | isolated | community}`

`no private-vlan`

**Function:** Configure current VLAN to Private VLAN. The no command cancels the Private VLAN configuration.

**Parameter:** **primary** set current VLAN to Primary VLAN, **isolated** set current VLAN to Isolated VLAN, **community** set current VLAN to Community VLAN.

**Command Mode:** VLAN mode

**Default:** Private VLAN is not configured by default.

**Usage Guide:** There are three Private VLANs: **Primary** VLAN, **Isolated** VLAN and **Community** VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.

Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.

It is to be noted Private VLAN messages will not be transmitted by GVRP.

**Example:** Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types.

```
Switch(config)#vlan 100
```

```
Switch(Config-Vlan100)#private-vlan primary
```

Note:This will remove all the ports from vlan 100

```
Switch(Config-Vlan100)#exit
```

```
Switch(config)#vlan 200
```

```
Switch(Config-Vlan200)#private-vlan isolated
```

Note:This will remove all the ports from vlan 200

```
Switch(Config-Vlan200)#exit
```

```
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Note:This will remove all the ports from vlan 300
Switch(Config-Vlan300)#exit
```

## 1.1.15 private-vlan association

**Command:** `private-vlan association <secondary-vlan-list>`  
`no private-vlan association`

**Function:** Set Private VLAN association; the no command cancels Private VLAN association.

**Parameter:** `<secondary-vlan-list>` Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ';'.  
**Command mode:** VLAN Mode.

**Default:** There is no Private VLAN association by default.

**Usage Guide:** This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN.

Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

**Example:** Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

```
Switch(Config-Vlan100)#private-vlan association 200;300
```

## 1.1.16 show dot1q-tunnel

This command is not supported by the switch.

## 1.1.17 show garp timer

**Command:** `show garp timer (join | leave | leaveall )`

**Function:** Show the value of each timer. Note that the value is not the remaining time to run the timer but the initial value when enabling the timer.

**Parameters:** join, join timer  
leave, leave timer  
leaveAll, leaveAll timer

**Command Mode:** Admin mode

**Default:** 200|600|10000 milliseconds for join | leave | leaveAll timer respectively.

**Usage Guide:** Show the corresponding value of the timer specified in the command.

**Example:** Show the value of all garp timers currently.

Switch#show garp timer join

Garp join timer's value is 200(ms)

## 1.1.18 show gvrp fsm information

**Command:** show gvrp fsm information interface (ethernet | port-channel) IFNAME

**Function:** Show the current state of all registered machines and request state machines on specified or all ports.

**Parameters:** ethernet, physical port

port-channel, aggregate port

IFNAME, port name

**Command Mode:** Admin mode

**Default:** MT for registered machine and VO for request state machine.

**Usage Guide:** Show the corresponding state of all registered machines and request state machines.

**Example:** Show the state of all state machines.

Switch#show gvrp fsm information interface ethernet 1/1

VA: Very anxious Active member, AA: Anxious Active member, QA: Quiet Active member

VP: Very anxious Passive member, AP: Anxious Passive member, QP: Quiet Passive member

VO: Very anxious Observer, AO: Anxious Observer, QO: Quiet Observer

LA: Leaving Active member, LO: leaving Observer

Interface ethernet 1/1 gvrp fsm information:

Index	VLANID	Applicant	Registrar
1	100	VO	LV
2	300	VP	IN

## 1.1.19 show gvrp leaveAll fsm information

**Command:** show gvrp leaveall fsm information interface (ethernet | port-channel) IFNAME

**Function:** Show the state of leaveAll state machine on specified or all ports.

**Parameters:** ethernet, physical port

port-channel, aggregate port

IFNAME, port name

**Command Mode:** Admin mode

**Default:** Passive.

**Usage Guide:** Check the state of leaveAll state machine.

**Example:** Show the state of leaveAll state machine on port.

```
Switch#show gvrp leaveall fsm information interface ethernet 1/1
Interface      leaveAll fsm
-----      -
Ethernet1/1    passive
```

## 1.1.20 show gvrp leavetimer running information

**Command:** show gvrp leavetimer running information (vlan <1-4094> |) interface (Ethernet | port-channel |) IFNAME

**Function:** Show running of all leavetimer on current port.

**Parameters:** <1-4094>, VLAN tag  
Ethernet, physical port  
port-channel, aggregate port  
IFNAME, port name

**Command Mode:** Admin mode

**Default:** leavetimer is disabled.

**Usage Guide:** Show running state and expiration time of each leave timer.

**Example:** Show running state and expiration time of each leave timer on current port.

```
Switch#show gvrp leavetimer running information interface ethernet 1/1
VLANID      running state      expired time
-----      -
100          UP                 0.2 s
300          DOWN              non
```

## 1.1.21 show gvrp port-member

**Command:** show gvrp (active|) port-member

**Function:** Shows all ports with GVRP enabled. "active" means the port is in active state with GVRP enabled.

**Parameters:** active means the port is in active state

**Command Mode:** Admin mode

**Default:** GVRP is disabled on port.

**Usage Guide:** Show all ports (enable GVRP) saved in GVRP.

**Example:** Show all ports with GVRP enabled.

```
Switch#show gvrp port member
```

Ports which were enabled gvrp included:

Ethernet1/3 (T)	Ethernet1/4 (T)
Ethernet1/5 (T)	Ethernet1/6 (T)
Ethernet1/7 (T)	Ethernet1/8 (T)
Ethernet1/9 (T)	Ethernet1/10 (T)

## 1.1.22 show gvrp port registerd vlan

**Command:** show gvrp port (dynamic | static |) registerd vlan interface (Ethernet | port-channel |) IFNAME

**Function:** Show the dynamic or static registration VLANs on current port.

**Parameters:** dynamic, dynamic registration

static, static registration

Ethernet, physical port

port-channel, aggregate port

IFNAME, port name

**Command Mode:** Admin mode

**Default:** No dynamic or static registration VLANs on port.

**Usage Guide:** Show the corresponding VLANs of the registered machines by dynamic or static registration.

**Example:** Show all dynamic or static registration VLANs on current port.

```
Switch#show gvrp port registerd vlan interface ethernet 1/1
```

Current port dynamic registerd vlan included:

```
Vlan10    vlan20
```

```
Vlan40    vlan60
```

Current port static registerd vlan included:

```
Vlan10    vlan30
```

```
Vlan40    vlan200
```

## 1.1.23 show gvrp timer running information

**Command:** show gvrp timer (join | leaveall) running information interface (ethernet | port-channel |) IFNAME

**Function:** Show running of all join|leaveAll timer on current port.

**Parameters:** join, join timer

leaveall, leaveAll timer

ethernet, physical port

port-channel, aggregate port

IFNAME, port name

**Command Mode:** Admin mode

**Default:** Join timer is disabled and leaveAll timer is enabled.

**Usage Guide:** Check running state of join|leaveAll timer on port.

**Example:** Show running state and expiration time of each timer.

```
Switch(config)#show gvrp timer join running information interface ethernet 1/1
```

Current port's jointimer running state is: UP

Current port's jointimer expired time is: 0.2 s

## 1.1.24 show gvrp vlan registered port

**Command:** show gvrp vlan <1-4094> registered port

**Function:** Show the ports with specified VLAN registered.

**Parameters:** <1-4094>: VLAN tag

**Command Mode:** Admin mode

**Default:** No ports with specified VLAN registered.

**Usage Guide:** None.

**Example:** Show all ports with current VLAN registered.

```
Switch#show gvrp vlan 100 registered port
```

```
Ethernet1/3 (T)      Ethernet1/4 (T)
```

```
Ethernet1/5 (T)      Ethernet1/6 (T)
```

```
Ethernet1/7 (T)      Ethernet1/8 (T)
```

```
Ethernet1/9 (T)      Ethernet1/10 (T)
```

## 1.1.25 show vlan

**Command:** show vlan [brief | summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> | name <vlan-name>]]

**Function:** Display detailed information for all VLANs or specified VLAN.

**Parameter:** **brief** stands for brief information; **summary** for VLAN statistics; <vlan-id> for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; <vlan-name> is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.

**Command mode:** Admin Mode and Configuration Mode.

**Usage Guide:** If no <vlan-id> or <vlan-name> is specified, then information for all VLANs in the switch will be displayed.

**Example:** Display the status for the current VLAN; display statistics for the current VLAN.

```
Switch#show vlan
```

VLAN Name	Type	Media	Ports
-----------	------	-------	-------

```
-----
```

1	default	Static	ENET	Ethernet1/1	Ethernet1/2
				Ethernet1/3	Ethernet1/4
				Ethernet1/9	Ethernet1/10
				Ethernet1/11	Ethernet1/12
2	VLAN0002	Static	ENET	Ethernet1/5	Ethernet1/6
				Ethernet1/7	Ethernet1/8

Switch#show vlan summary  
The max. vlan entrys: 4094

Existing Vlan:  
Universal Vlan:  
1 12 13 15 16 22

Total Existing Vlan is:6

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN

## 1.1.26 show vlan-translation

This command is not supported by the switch.

## 1.1.27 switchport access vlan

**Command:** `switchport access vlan <vlan-id>`  
`no switchport access vlan`

**Function:** Add the current Access port to the specified VLAN. The “**no switchport access vlan**” command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

**Parameter:** `<vlan-id>` is the VID for the VLAN to be added the current port, valid range is 1 to 4094.

**Command mode:** Port Mode.

**Default:** All ports belong to VLAN1 by default.

**Usage Guide:** Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

**Example:** Add some Access port to VLAN100.

```
Switch(config)#interface ethernet 1/8
Switch(Config-If-Ethernet1/8)#switchport mode access
Switch(Config-If-Ethernet1/8)#switchport access vlan 100
Switch(Config-If-Ethernet1/8)#exit
```

## 1.1.28 switchport dot1q-tunnel

This command is not supported by this switch.

## 1.1.29 switchport forbidden vlan

**Command:** `switchport forbidden vlan {WORD | all | add WORD | except WORD | remove WORD}`

**no switchport forbidden vlan**

**Function:** Configure the forbidden vlan for a port. Note that this command can only be used to configure on trunk or hybrid ports and the port with GVRP not enabled. No command cancels the forbidden vlanlist for a port.

**Parameters:** WORD, add the vlanList as forbidden vlan and cover the previous configuration

all, set all VLANs as forbidden vlan

add WORD, add vlanList to the current forbidden vlanList

except WORD, set all VLANs as forbidden vlan except vlanList

remove WORD, remove vlan specified by vlanList from current forbidden

vlanList

**Command Mode:** Port mode

**Default:** Forbidden vlanList is empty

**Usage Guide:** Tag the corresponding position for forbidden vlanList and clear allow vlanList flags in ports. A port leaves these VLANs if it joins them statically, and it sends message to GVRP module to enable corresponding registered machine of the port to enter forbidden mode.

**Example:** Port quits the corresponding VLAN and the corresponding registered machine of GVRP to enter forbidden mode.

```
Switch(config-if-ethernet1/1)#switchport forbidden vlan all
```

## 1.1.30 switchport hybrid allowed vlan

**Command:** `switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag}`

**no switchport hybrid allowed vlan**

**Function:** Set hybrid port which allow the VLAN to pass with tag or untag method; the “**no switchport hybrid allowed vlan**” command restores the default setting.

**Parameter:** **WORD:** Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;

**all:** Set all VLANs to allowed vlan;

**add WORD:** Add vlanList to the existent allowed vlanList;

**except WORD:** Set all VLANs to allowed vlan except the configured vlanList;

**remove WORD:** Delete the specific VLAN of vlanList from the existent allow vlanList;

**tag:** Join the specific VLAN with tag mode;

**untag:** Join the specific VLAN with untag mode.

**Command mode:** Port Mode.

**Default:** Deny all VLAN traffic to pass.

**Usage Guide:** The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the previous.

**Example:** Set hybrid port allowed vlan 1, 3, 5-20 with untag mode and allow vlan 100; 300; 500-2000 with tag mode.

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

```
Switch(Config-If-Ethernet1/5)#switchport mode hybrid
```

```
Switch(Config-If-Ethernet1/5)#switchport hybrid allowed vlan 1;3;5-20 untag
```

```
Switch(Config-If-Ethernet1/5)#switchport hybrid allowed vlan 100; 300; 500-2000 tag
```

```
Switch(Config-If-Ethernet1/5)#exit
```

### 1.1.31 switchport hybrid native vlan

**Command:** `switchport hybrid native vlan <vlan-id>`

**no switchport hybrid native vlan**

**Function:** Set the PVID for Hybrid port; the “**no switchport hybrid native vlan**” command restores the default setting.

**Parameter:** **<vlan-id>** is the PVID of Hybrid port.

**Command mode:** Port Mode.

**Default:** The default PVID of Hybrid port is 1.

**Usage Guide:** When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

**Example:** Set the native vlan to 100 for a Hybrid port.

```
Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/5)#switchport hybrid native vlan 100
Switch(Config-If-Ethernet1/5)#exit
```

## 1.1.32 switchport interface

**Command:** `switchport interface [ethernet | portchannel] [<interface-name | interface-list>]`

`no switchport interface [ethernet | portchannel] [<interface-name | interface-list>]`

**Function:** Specify Ethernet port to VLAN; the no command deletes one or one set of ports from the specified VLAN.

**Parameter:** **ethernet** is the Ethernet port to be added. **portchannel** means that the port to be added is a link-aggregation port. **interface-name** port name, such as e1/1. If this option is selected, ethernet or portchannel should not be. **interface-list** is the port list to be added or deleted, “;” and “-” are supported, for example: ethernet1/1;3;4-7;8.

**Command mode:** VLAN Mode.

**Default:** A newly created VLAN contains no port by default.

**Usage Guide:** Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

**Example:** Assign Ethernet port 1, 3, 4-7, 8 of VLAN100.

```
Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8
```

## 1.1.33 switchport mode

**Command:** `switchport mode {trunk | access | hybrid}`

**Function:** Set the port in access mode, trunk mode or hybrid mode.

**Parameter:** **trunk** means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only; **hybrid** means the port allows the traffic of multi-VLANs to pass with tag or untag mode.

**Command mode:** Port Mode.

**Default:** The port is in Access mode by default.

**Usage Guide:** Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with

the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

**Example:** Set port 5 to trunk mode and port 8 to access mode, port 10 to hybrid mode.

```
Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#exit
Switch(config)#interface ethernet 1/8
Switch(Config-If-Ethernet1/8)#switchport mode access
Switch(Config-If-Ethernet1/8)#exit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/10)#exit
```

### 1.1.34 switchport mode trunk allow-null

**Command:** `switchport mode trunk allow-null`

**Function:** Add a port as trunk mode. When enabling GVRP, the mode that adds the ports with trunk mode to all VLANs is not appropriate. Therefore, add a port as trunk port and does not join any VLANs by default for enabling GVRP on trunk port is appropriate. It is recommended to configure a port as trunk with this command before enabling GVRP. This command can also be used when a port has been configured as trunk already, which equals to clearing allow-list and quits all VLANs.

**Parameters:** None

**Command Mode:** Port mode

**Default:** access mode.

**Usage Guide:** Configure the port as trunk, enable it to leave all VLANs and clear allow-list.

**Example:** `Switch(config-if-ethernet1/1)#switchport mode trunk allow-null`

### 1.1.35 switchport trunk allowed vlan

**Command:** `switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD}`

`no switchport trunk allowed vlan`

**Function:** Set trunk port to allow VLAN traffic; the “`no switchport trunk allowed vlan`” command restores the default setting.

**Parameter:** **WORD:** specified VLANs; keyword;

**all:** all VLANs, the range from 1 to 4094;

**add:** add assigned VLANs behind **allow vlan**;

**except:** all VLAN add to **allow vlan** except assigned VLANs;

**remove:** delete assigned **allow vlan** from **allow vlan** list.

**Command mode:** Port Mode.

**Default:** Trunk port allows all VLAN traffic by default.

**Usage Guide:** The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited.

**Example:** Set Trunk port to allow traffic of VLAN1, 3, 5-20.

```
Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet1/5)#exit
```

## 1.1.36 switchport trunk native vlan

**Command:** `switchport trunk native vlan <vlan-id>`

`no switchport trunk native vlan`

**Function:** Set the PVID for Trunk port; the “`no switchport trunk native vlan`” command restores the default setting.

**Parameter:** **<vlan-id>** is the PVID for Trunk port.

**Command mode:** Port Mode.

**Default:** The default PVID of Trunk port is 1.

**Usage Guide:** PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When an untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this commands for VLAN forwarding.

**Example:** Set the native VLAN for a Trunk port to 100.

```
Switch(config)#interface ethernet 1/5
Switch(Config-If-Ethernet1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet1/5)#exit
```

## 1.1.37 vlan

**Command:** vlan WORD

**no vlan** WORD

**Function:** Create VLANs and enter VLAN configuration mode. If using ';' and '-' connect with multi-VLANs, then only create these VLANs. If only existing VLAN, then enter VLAN configuration mode; if the VLAN is not exist, then create VLAN and enter VLAN configuration mode. In VLAN Mode, the user can set VLAN name and assign the switch ports to the VLAN. The no command deletes specified VLANs.

**Parameter:** WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ';' and '-'.

**Command mode:** Global Mode.

**Default:** Only VLAN1 is set by default.

**Usage Guide:** VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.

**Example:** Create VLAN100 and enter the configuration mode for VLAN 100.

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#
```

## 1.1.38 vlan internal

**Command:** vlan <2-4094> internal

**Function:** Specify the internal VLAN ID. After an ID is specified as the internal VLAN ID, it is not allowed to be used by other VLAN. Internal VLAN is only used to LOOPBACK interface and can not add physical port. New internal VLAN ID takes effect after save the configuration and reboot the switch.

**Parameter:** <vlan-id>: The ID is specified as internal VLAN ID, the range is 2 to 4094.

**Command mode:** Global Mode.

**Default:** 1006.

**Usage Guide:** Set 1006 as the default internal VLAN ID, the internal VLAN ID needs to be modified when the network set 1006 as VLAN ID. Internal VLAN ID must select an unused ID or else affect other VLAN. This command takes effect after save the configuration and reboot the switch.

**Example:** Set 100 as the internal VLAN ID.

```
Switch(config)#vlan 100 internal
```

## 1.1.39 vlan ingress enable

**Command:** `vlan ingress enable`

`no vlan ingress enable`

**Function:** Enable the VLAN ingress filtering for a port; the “`no vlan ingress enable`” command disables the ingress filtering.

**Command mode:** Global Mode

**Default:** Enable VLAN ingress filtering function.

**Usage Guide:** After VLAN ingress filtering is enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is the VLAN member port, or else drop the data.

**Example:** Disable VLAN ingress rules on the port.

```
Switch(config)#no vlan ingress enable
```

### 1.1.40 vlan-translation

This command is not supported by the switch.

### 1.1.41 vlan-translation enable

This command is not supported by the switch.

### 1.1.42 vlan-translation miss drop

This command is not supported by the switch.

# Chapter 2 Commands for MAC Address Table Configuration

## 2.1 Commands for MAC Address Table Configuration

### 2.1.1 clear mac-address-table dynamic

**Command:** clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>]  
[interface [ethernet | portchannel] <interface-name>]

**Function:** Clear the dynamic address table.

**Parameter:** <mac-addr>: MAC address will be deleted; <interface-name> the port name for forwarding the MAC packets; <vlan-id> VLAN ID.

**Command mode:** Admin mode.

**Usage Guide:** Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically.

**Example:** Delete all dynamic MAC.

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

### 2.1.2 mac-address-table aging-time

**Command:** mac-address-table aging-time <0 / aging-time>  
no mac-address-table aging-time

**Function:** Sets the aging-time for the dynamic entries of MAC address table.

**Parameter:** <aging-time> is the aging-time seconds, range from 10 to 1000000; 0 to disable aging.

**Command Mode:** Global Mode.

**Default:** Default aging-time is 300 seconds.

**Usage Guide:** If no destination address of the packets is same with the address entry in aging-time, the address entry will get aged. The user had better set the aging-time according to the network condition, it usually use the default value.

**Example:** Set the aging-time to 600 seconds.

```
Switch(config)#mac-address-table aging-time 600
```

## 2.1.3 mac-address-table static | static-multicast |

### blackhole

**Command:** `mac-address-table {static | static-multicast | blackhole} address <mac-addr> vlan <vlan-id> [interface ethernet <interface-name>] | [source | destination | both]`

`no mac-address-table {static | static-multicast | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface ethernet <interface-name>]`

**Function:** Add or modify static address entries, static multicast entries and filter address entries. The no command deletes the three entries.

**Parameter:** **static** is the static entries; **static-multicast** is the static multicast entries; **blackhole** is filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both. When choose the filter entries, blackhole address can't based on port, and not configure to interface; **dynamic** is dynamic address entries; **<mac-addr>** MAC address to be added or deleted; **<interface-name>** name of the port transmitting the MAC data packet; **<vlan-id>** is the vlan number. **source** is based on source address filter; **destination** is based on destination address filter; **both** is based on source address and destination address filter, the default is both.

**Command Mode:** Global Mode

**Default:** When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number.

**Usage Guide:** In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.

**no mac-address-table** command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except application, system entries. MAC address entries can be classified according to the different source, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically. STATIC is the static MAC address entries (including blackhole entries) added by user. APPLICATION is the static MAC address entries added by application protocol (such as dot1x, security port...). SYSTEM is the additive static MAC address entries according to VLAN interface. When adding STATIC entries, it can cover the conflictive DYNAMIC, except APPLICATION, SYSTEM entries.

After configure the static multicast MAC by this command, the multicast MAC traffic

will be forwarded to the specified port of the specified VLAN.

**Example:** Port 1/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.

```
Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/1
```

Configure a static multicast MAC 01-00-5e-00-00-01, the egress is ethernet 1/1.

```
Switch(config)#mac-address-table static-multicast address 01-00-5e-00-00-01 vlan 1 interface ethernet1/1
```

## 2.1.4 show mac-address-table

**Command:** `show mac-address-table [static | blackhole | multicast | aging-time <aging-time> | count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]`

**Function:** Show the current MAC table.

**Parameter:** **static** static entries; **blackhole** filter entries; **aging-time <aging-time>** address aging time; **count** entry's number, **multicast** multicast entries; **<mac-addr>** entry's MAC address; **<vlan-id>** entry's VLAN number; **<interface-name>** entry's interface name.

**Command mode:** Admin and Configuration Mode.

**Default:** MAC address table is not displayed by default.

**Usage guide:** This command can display various classes of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

**Example:** Display all the filter MAC address entries.

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

## 2.2 Commands for Mac Address Binding configuration

### 2.2.1 clear port-security dynamic

**Command:** `clear port-security dynamic [address <mac-addr> | interface <interface-id>]`

**Function:** Clear the Dynamic MAC addresses of the specified port.

**Command mode:** Admin Mode.

**Parameter:** **<mac-addr>** stands MAC address; **<interface-id>** for specified port number.

**Usage Guide:** The secure port must be locked before dynamic MAC clearing operation can be perform in specified port. If no ports and MAC are specified, then all dynamic MAC in all locked secure ports will be cleared; if only port but no MAC address is specified, then

all MAC addresses in the specified port will be cleared.

**Example:** Delete all dynamic MAC in port1.

```
Switch#clear port-security dynamic interface Ethernet 1/1
```

## 2.2.2 mac-address-table periodic-monitor-time

**Command:** `mac-address-table periodic-monitor-time <5-86400>`

**Function:** Set the MAC monitor interval to count the added and deleted MAC in time, and send out them with trap message.

**Parameter:** `<5-86400>`: the interval is 5 to 86400 seconds.

**Command mode:** Global Mode.

**Default:** 60 seconds.

**Usage Guide:** Associate this command with `mac-address-table synchronizing enable` command to use.

**Example:** Set the MAC monitor interval as 120 seconds.

```
Switch(Config)#mac-address-table periodic-monitor-time 120
```

## 2.2.3 mac-address-table trap enable

**Command:** `mac-address-table trap enable`

`no mac-address-table trap enable`

**Function:** Enable or disable mac notification trap passthrough.

**Parameter:** None.

**Command mode:** Port Mode.

**Default:** Disable.

**Usage Guide:** Enable `mac-address-table synchronizing` and global mac notification trap, then enable `mac-address-table mac trap` and mac notification trap in port mode. This command takes effect as subcommand of `mac-address-table synchronizing trap` command after enable global `mac-address-table synchronizing trap` only.

**Example:** Enable mac notification trap in port mode after the global mac notification trap is enabled.

```
Switch(config)#mac-address-table synchronizing enable
```

```
Switch(config-if-ethernet1/1)#mac-address-table trap enable
```

```
Switch(config-if-enternet1/1)#exit
```

```
Swtich(config-if-ethernet1/1)#
```

## 2.2.4 mac-address-table synchronizing enable

**Command: mac-address-table synchronizing enable**

**no mac-address-table synchronizing enable**

**Function:** Enable the monitor function for MAC, if a MAC is added or deleted, the system will report this monitored event; the no command will cancel this function.

**Parameter:** None.

**Command mode:** Global Mode.

**Default:** Disable.

**Usage Guide:** The user enables this function to obtain the status of the MAC changing or the accessed user.

**Example:** Enable the monitor function for MAC.

Switch(Config)#mac-address-table synchronizing enable

## 2.2.5 show port-security

**Command: show port-security**

**Function:** Display the secure MAC addresses of the port.

**Command mode:** Admin and Configuration Mode.

**Default:** The switch is not display port-security configuration.

**Usage Guide:** This command displays the secure port MAC address information.

**Example:**

Switch#show port-security

Security Port	MaxSecurity Addr (count)	CurrentAddr (count)	Security Action
Ethernet1/1	1	1	Protect
Ethernet1/3	10	1	Protect
Ethernet1/5	1	0	Protect

Max Addresses limit in System:128

Total Addresses in System:2

Displayed information	Explanation
Security Port	Is port enabled as a secure port.
MaxSecurityAddr	The maximum secure MAC address number set for the security port.
CurrentAddr	The current secure MAC address number of the security port.
Security Action	The violation mode of the port configuration.

Total Addresses in System	The current secure MAC address number of the system.
Max Addresses limit in System	The maximum secure MAC address number of the system.

## 2.2.6 show port-security address

**Command:** `show port-security address [interface <interface-id>]`

**Function:** Display the secure MAC addresses of the port.

**Command mode:** Admin and Configuration Mode.

**Parameter:** `<interface-id>` stands for the port to be displayed.

**Usage Guide:** This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed. The following is an example:

```
Switch#show port-security address interface ethernet 1/3
```

```
Security Mac Address Table
```

```
-----
```

Vlan	Mac Address	Type	Ports
1	0000.0000.1111	SecureConfigured	Ethernet1/1

```
-----
```

```
Total Addresses: 1
```

Displayed information	Explanation
Vlan	The VLAN ID for the secure MAC Address.
Mac Address	Secure MAC address.
Type	Secure MAC address type.
Ports	The port that the secure MAC address belongs to.
Total Addresses	Current secure MAC address number in the system.

## 2.2.7 show port-security interface

**Command:** `show port-security interface <interface-id>`

**Function:** Display the configuration of secure port.

**Command mode:** Admin and Configuration Mode.

**Parameter:** `<interface-id>` stands for the port to be displayed.

**Default:** Configuration of secure ports is not displayed by default.

**Usage Guide:** This command displays the detailed configuration information for the

secure port.

**Example:**

Switch#show port-security interface ethernet 1/1

Port Security: Enabled

Port status: Security Up

Violation mode: Protect

Maximum MAC Addresses: 1

Total MAC Addresses: 1

Configured MAC Addresses: 1

Lock Timer is ShutDown

Mac-Learning function is: Opened

Displayed information	Explanation
Port Security	Is port enabled as a secure port.
Port status	Port secure status.
Violation mode	Violation mode set for the port.
Maximum MAC Addresses	The maximum secure MAC address number set for the port.
Total MAC Addresses	Current secure MAC address number for the port.
Configured MAC Addresses	Current secure static MAC address number for the port.
Lock Timer	Whether locking timer (timer timeout) is enabled for the port.
Mac-Learning function	Whether the MAC address learning function is enabled.

## 2.2.8 station-movement check

This command is not supported by the switch.

## 2.2.9 switchport port-security

**Command:** switchport port security

**no switchport port security**

**Function:** Enable MAC address binding function for the port; the no command disables the MAC address binding function for the port.

**Command mode:** Port Mode.

**Default:** MAC address binding is not enabled by default.

**Usage Guide:** The MAC address binding function and Port Aggregation functions are mutually exclusive. Therefore, if MAC binding function for a port is to be enabled, the Port Aggregation functions must be disabled, and the port enabling MAC address binding must not be a Trunk port.

**Example:** Enable MAC address binding function for port 1.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port security
```

## 2.2.10 switchport port-security convert

**Command:** `switchport port-security convert`

**Function:** Converts dynamic secure MAC addresses learned by the port to static secure MAC addresses, and disables the MAC address learning function for the port.

**Command mode:** Port Mode.

**Usage Guide:** The port dynamic MAC convert command can only be executed after the secure port is locked. After this command has been executed, dynamic secure MAC addresses learned by the port will be converted to static secure MAC addresses. The command does not reserve the configuration.

**Example:** Converting MAC addresses in port 1 to static secure MAC addresses.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security convert
```

## 2.2.11 switchport port-security lock

**Command:** `switchport port-security lock`

`no switchport port-security lock`

**Function:** Lock the port. After the port is locked, the MAC-address learning function will be shut down; the no operation of this command will reset the MAC-address learning function.

**Command Mode:** Port Configuration Mode.

**Default:** Ports are unlocked.

**Usage Guide:** Ports can only be locked after the MAC-address binding function is enabled. When a port becomes locked, its MAC learning function will be disabled.

**Examples:** Lock port 1.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security lock
```

## 2.2.12 switchport port-security mac-address

**Command:** `switchport port-security mac-address <mac-address>`

`no switchport port-security mac-address <mac-address>`

**Function:** Add a static secure MAC address; the no command deletes a static secure MAC address.

**Command mode:** Port Mode.

**Parameters:** `<mac-address>` stands for the MAC address to be added or deleted.

**Usage Guide:** The MAC address binding function must be enabled before static secure MAC address can be added.

**Example:** Adding MAC 00-03-0F-FE-2E-D3 to port1.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security mac-address 00-03-0F-FE-2E-D3
```

## 2.2.13 switchport port-security maximum

**Command:** `switchport port-security maximum <value>`

`no switchport port-security maximum`

**Function:** Sets the maximum number of secure MAC addresses for a port; the no command restores the maximum secure address number of 1.

**Command mode:** Port Mode.

**Parameter:** `< value>` is the up limit for static secure MAC address, the valid range is 1 to 128.

**Default:** The default maximum port secure MAC address number is 1.

**Usage Guide:** The MAC address binding function must be enabled before maximum secure MAC address number can be set. If secure static MAC address number of the port is larger than the maximum secure MAC address number set, the setting fails; extra secure static MAC addresses must be deleted, so that the secure static MAC address number is no larger than the maximum secure MAC address number for the setting to be successful.

**Example:** Set the maximum secure MAC address number as 4 for port1.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security maximum 4
```

## 2.2.14 switchport port-security timeout

**Command:** `switchport port-security timeout <value>`

`no switchport port-security timeout`

**Function:** Set the timer for port locking; the no command restores the default setting.

**Parameter:** `<value>` is the timeout value, the valid range is 0 to 300s.

**Command mode:** Port Mode.

**Default:** Port locking timer is not enabled by default.

**Usage Guide:** The port locking timer function is a dynamic MAC address locking function. MAC address locking and conversion of dynamic MAC entries to secure address entries will be performed on locking timer timeout. The MAC address binding function must be enabled prior to running this command.

**Example:** Set port1 locking timer to 30 seconds.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security timeout 30
```

## 2.2.15 switchport port-security violation

**Command:** `switchport port-security violation {protect | shutdown} [recovery <30-3600>]`

**no switchport port-security violation**

**Function:** Configure the port violation mode. The `no` restores the violation mode to `protect`.

**Command Mode:** Port mode.

**Parameter:** `protect` refers to protect mode

**shutdown** refers to shutdown mode

**recovery:** configure the border port can be recovered automatically after implement shutdown violation operation

**<30-3600>:** the recovery time, do not recover it by default

**Default:** The port violation mode is `protect` by default.

**Usage Guide:** The port violation mode configuration is only available after the MAC address binding function is enabled. when the port secure MAC address exceeds the security MAC limit, if the violation mode is `protect`, the port only disable the dynamic MAC address learning function; while the port will be shut if at `shutdown` mode. Users can manually open the port with `no shutdown` command.

**Example:** Set the violation mode of port 1 to shutdown.

```
Switch(config)#interface Ethernet 1/1
```

```
Switch(Config-If-Ethernet1/1)#switchport port-security violation shutdown recovery 60
```