

# Port Security

Ethernet Switch

ZyNOS 4.0

## Support Notes

Version 4.0

July 2011



## Port Security Overview

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. See Chapter 10 on page 105 for information on configuring static MAC address forwarding.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. By default, MAC address learning is still enabled even though the port security is not activated.

Functionally the Switch allows for three possible outcomes with port security. You can configure the ports to:

- Forward all packets and learn all MAC addresses.
- Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Drop all packets from unknown MAC addresses and learn a limited number of MAC addresses.

## Port Security Setup

Click “Advanced Application” >” Port Security” in the navigation panel to display the screen as shown.

**Port Security** [VLAN MAC Address Limit](#)

**MAC Freeze :**

Port List

**Port Security :**

Active

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>

## VLAN MAC Address Limit

Use this screen to set the MAC address learning limit on per-port and per-VLAN basis. Click “VLAN MAC Address Limit” in the “Advanced Application” > “Port Security” screen to display the screen as shown.

The screenshot shows the "VLAN MAC Address Limit" configuration page under the "Port Security" section. The page has a title bar with "VLAN MAC Address Limit" and "Port Security". Below the title bar, there are four input fields: "Active" (checkbox), "Port" (text box), "VID" (text box), and "Limit Number" (text box). Below these fields are three buttons: "Add", "Cancel", and "Clear". At the bottom of the page, there is a table with the following headers: "Index", "Active", "Port", "VID", "Limit Number", and "Delete". Below the table are two buttons: "Delete" and "Cancel".

## Scenario

### Port Security Example 1

The following example demonstrates the various settings and results associated with different port security configurations. Ports 1 to 5 are configured to:

- Port 1 - Forward all packets and learn all MAC addresses.
- Port 2 - Forward all packets and learn all MAC addresses.
- Port 3 - Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Port 4 - Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Port 5 - Drop all packets from unknown MAC addresses but forward packets from up to 100 learned MAC addresses.

**Port Security**

MAC Freeze :

Port List

Port Security :

Active

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	100
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

PORT	SETTINGS			RESULT
	ACTIVATE PORT SECURITY	ACTIVATE ADDRESS LEARNING	LIMIT NO. OF LEARNED MAC ADDRESSES	
1		X	0 (disables limits)	Forward all packets, learn all MAC addresses.
2	X	X	0 (disables limits)	Forward all packets, learn all MAC addresses.
3	X		0 (disables limits)	Drop all packets from unknown MAC addresses, do not learn MAC addresses.
4	X		100	Drop all packets from unknown MAC addresses, do not learn MAC addresses.
5	X	X	100	Drop packets from unknown MAC addresses, learn up to 100 MAC addresses.

## Port Security Example 2

The following example demonstrates the various settings and results associated with different port security configurations. Ports configured to:

- Port 2 - Port 2 can only learn 3 MAC address in the Vlan which VID is 2.
- Port 4 - Port 4 can only learn 5 MAC address in the Vlan which VID is 4

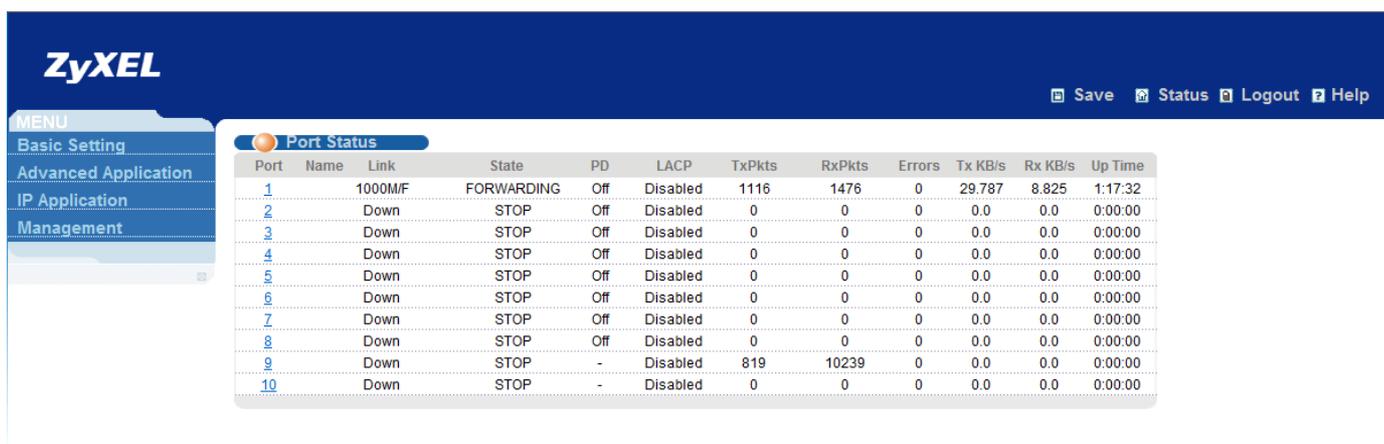
**VLAN MAC Address Limit**
Port Security

Active	<input checked="" type="checkbox"/>
Port	<input type="text" value="2"/>
VID	<input type="text" value="2"/>
Limit Number	<input type="text" value="3"/>

Index	Active	Port	VID	Limit Number	Delete
1	Yes	2	2	3	<input type="checkbox"/>
2	Yes	4	4	5	<input type="checkbox"/>

## Configuration ZyXEL switch using the Web GUI

1. Connect the MGMT port to a PC or Notebook with the RJ45 Cable.
2. By default, the MGMT IP address of the out-band port is 192.168.0.1/24
3. Set your NIC to 192.168.0.100/24
4. Open an Internet browser (e.g. IE) and enter <http://192.168.0.1> into the URL field.
5. By default, the username for the administrator is “admin” and the password is “1234”.
6. After successfully logging in you will see a screen similar to the one below.



7. To enter the “Port Security” page, click “Advanced Application” “Port Security”

## Configuration ZyXEL switch using the CLI

### Port Security Example 1

```

vlan 1 name 1
  normal ""
  fixed 1-10
  forbidden ""
    
```

```
untagged 1-10
ip address inband-default 192.168.1.1 255.255.255.0
exit
ip address 192.168.0.1 255.255.255.0
port-security
port-security 2
port-security 3
port-security 4
port-security 5
port-security 2 learn inactive
port-security 3
port-security 4 address-limit 100
port-security 5 learn inactive
port-security 5 address-limit 100
```

## Port Security Example 2

```
vlan 1 name 1
normal ""
fixed 1-10
forbidden ""
untagged 1-10
ip address inband-default 192.168.1.1 255.255.255.0
exit
ip address 192.168.0.1 255.255.255.0
port-security
port-security 2
port-security 3
port-security 4
port-security 5
port-security 2 vlan 2 address-limit 3
port-security 4 vlan 4 address-limit 5
```