Port-based VLAN

Ethernet Switch

ZyNOS 4.0

Support Notes

Version 4.00

Nov 2011

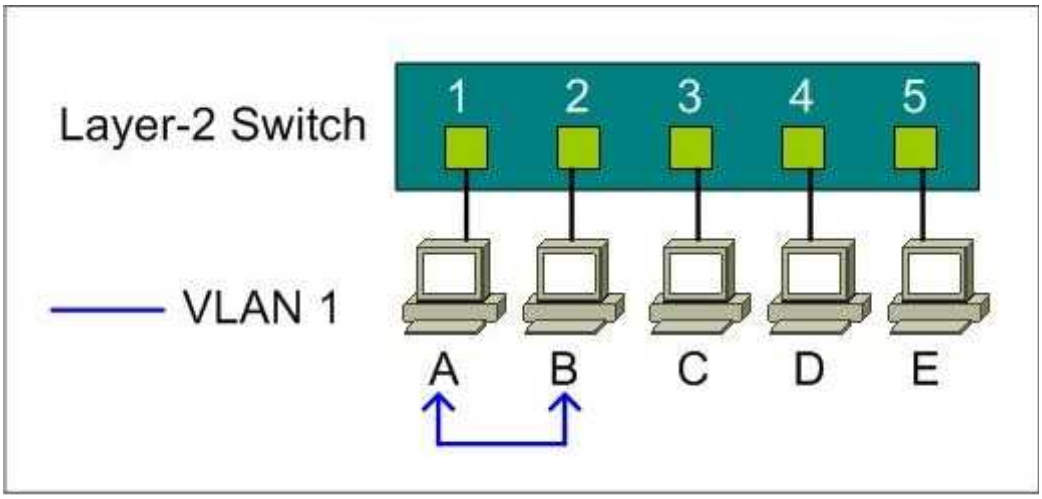
All contents copyright (c) 2011 ZyXEL Communications Corporation

- **Port-based VLAN**

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. You must define outgoing ports allowed for each port when using port-based VLANs. Note that VLAN only governs the outgoing traffic, in other words, it is unidirectional. Therefore, if you wish to allow two subscriber ports to talk to each other, e.g., between conference rooms in a hotel, you must define the egress (outgoing port) for both ports. An egress port is an outgoing port, that is, a port through which a data packet leaves.

There are 5 hosts (Host A, B, C, D and E) connected to a 5-port layer-2 switch which supports port-based VLAN.

Case 1: Host A and Host B can talk to each other, because they are in the same VLAN group. But Host A and Host B can't talk to Host C, D, and E.



Port-based VLAN definition:

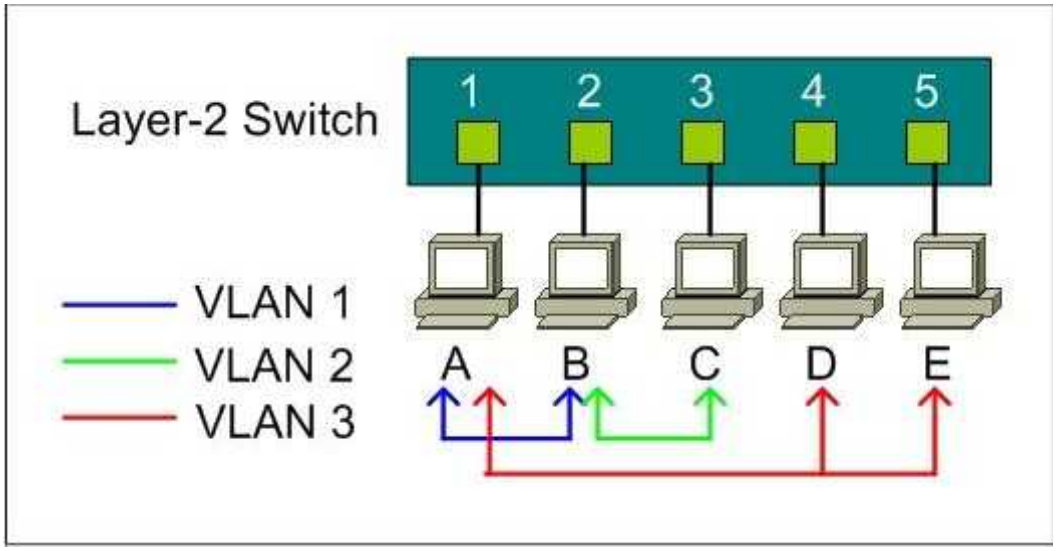
- Egress port for port 1: port 2
- Egress port for port 2: port 1

Case 2: There are 3 VLAN groups in the physical network. Host A and Host B can talk to each other; they are in the same VLAN group 1. Host B and Host C are in VLAN group 2. Host A, Host D and Host E are in VLAN group 3.

All contents copyright (c) 2011 ZyXEL Communications Corporation

All contents copyright (c) 2011 ZyXEL Communications Corporation.

All contents copyright (c) 2011 ZyXEL Communications Corporation



Port-based VLAN definition:

- Egress port for port 1: port 2, port 4, port 5
- Egress port for port 2: port 1, port 3
- Egress port for port 3: port 2
- Egress port for port 4: port 1, port 5
- Egress port for port 5: port 1, port 4

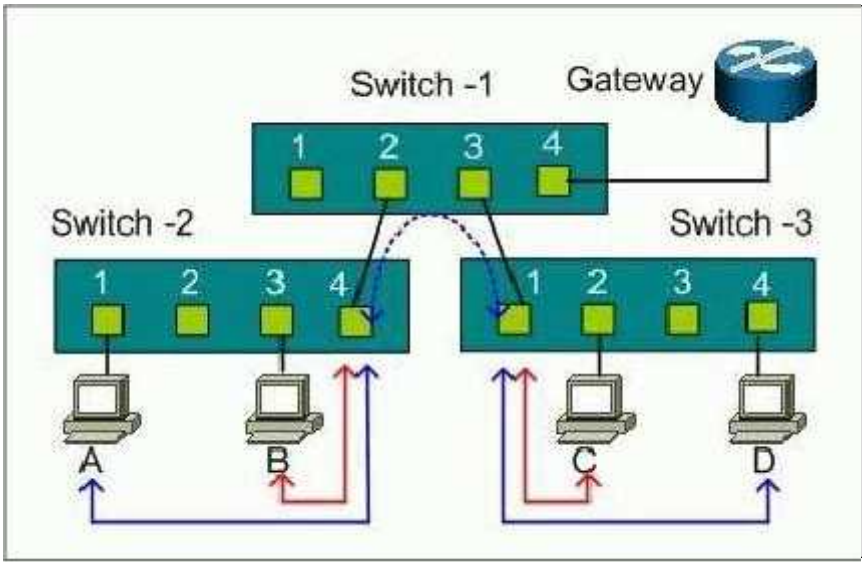
- ## Port-based VLAN across different switch

Port-based VLAN is specific only to the switch on which it was created. Definitely, Port-based VLAN can't spread across multiple switches. As the following network diagram shows, in most MTU cases, for the sake of security, subscribers are isolated from each other except from the gateway. There are two switches, Switch-2 and Switch-3, support port-based VLAN and uplink to a
non-port-based VLAN switch, Switch-1.

All contents copyright (c) 2011 ZyXEL Communications Corporation

All contents copyright (c) 2011 ZyXEL Communications Corporation.

All contents copyright (c) 2011 ZyXEL Communications Corporation



For Switch-2, port 1, port 2, and port 3 are allowed to communicate back and forth with uplink port 4, but not with the other ports.

- Switch-2 VLAN 1 member port: port 1 and port 4
- Switch-2 VLAN 2 member port: port 2 and port 4
- Switch-2 VLAN 3 member port: port 3 and port 4

For Switch-3, port 2, port 3, and port 4 are allowed to communicate back and forth with uplink port 1, but not with the other ports.

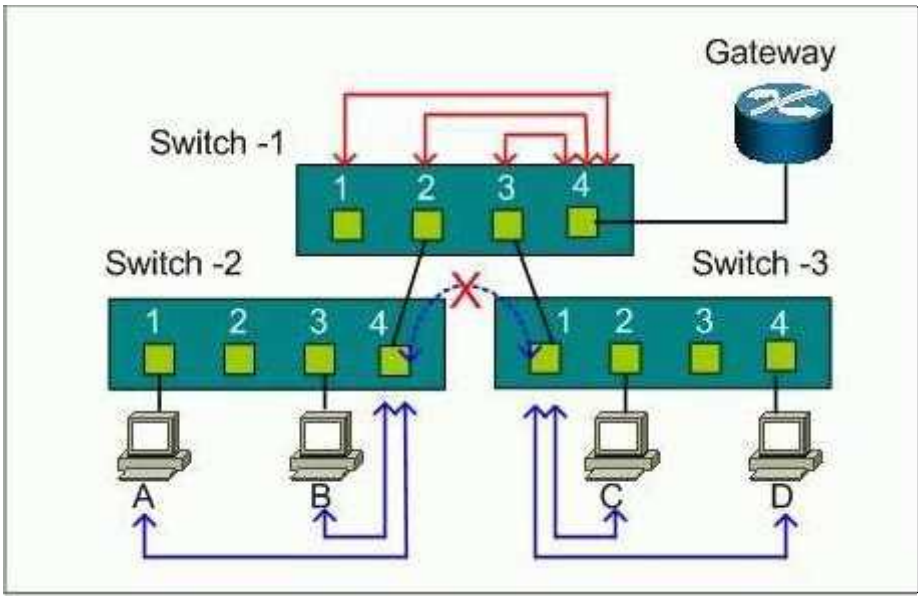
- Switch-3 VLAN 1 member port: port 2 and port 1
- Switch-3 VLAN 2 member port: port 3 and port 1
- Switch-2 VLAN 3 member port: port 4 and port 1

Host A can't talk to Host B due to the port-based VLAN in Switch-2, and Host C can't talk to Host D due to the port-based VLAN in Switch-3. But both Switch-2 and Switch-3 have an uplink to the non VLAN Switch-1. Host A and Host B will talk to Host C and Host D via the non VLAN switch because port-based VLAN can't spread across different switches.
To achieve the security between different switches, you must put another port-based VLAN switch for the uplink. Each port on the uplink switch also should be separated into different VLAN, except for the port to the gateway. So subscribers only can talk to the gateway for Internet access but can not communicate with each other.

All contents copyright (c) 2011 ZyXEL Communications Corporation

All contents copyright (c) 2011 ZyXEL Communications Corporation.

All contents copyright (c) 2011 ZyXEL Communications Corporation



For Switch-1, port 1, port2, and port 3 are allowed to communicate back and forth with uplink port 4, but not with the other ports.

- Switch-1 VLAN 1 member port: port 1 and port 4
- Switch-1 VLAN 2 member port: port 2 and port 4
- Switch-1 VLAN 3 member port: port 3 and port 4

How to configure Port-Based VLAN

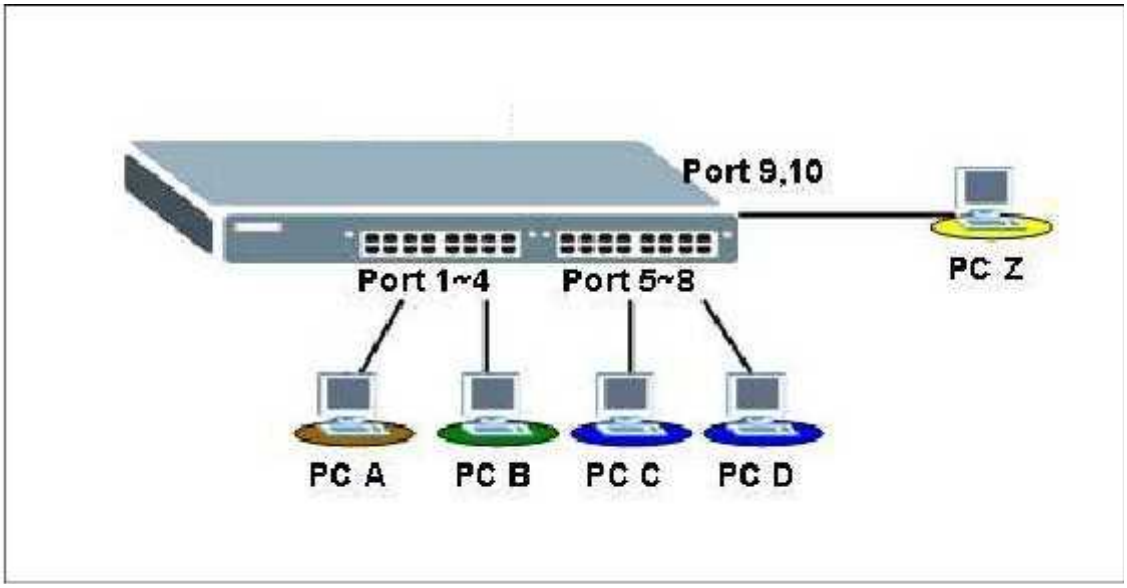
Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

All contents copyright (c) 2011 ZyXEL Communications Corporation

All contents copyright (c) 2011 ZyXEL Communications Corporation.

All contents copyright (c) 2011 ZyXEL Communications Corporation

Scenario



In this scenario, Port Based VLAN is used to separate one physical Switch into two smaller logical Switches. Ports 1~4 and 9, 10 are in one group and Ports
5~10 are in another group. Port-based VLANs are specific only to the switch on which they have been created.

All contents copyright (c) 2011 ZyXEL Communications Corporation

All contents copyright (c) 2011 ZyXEL Communications Corporation.

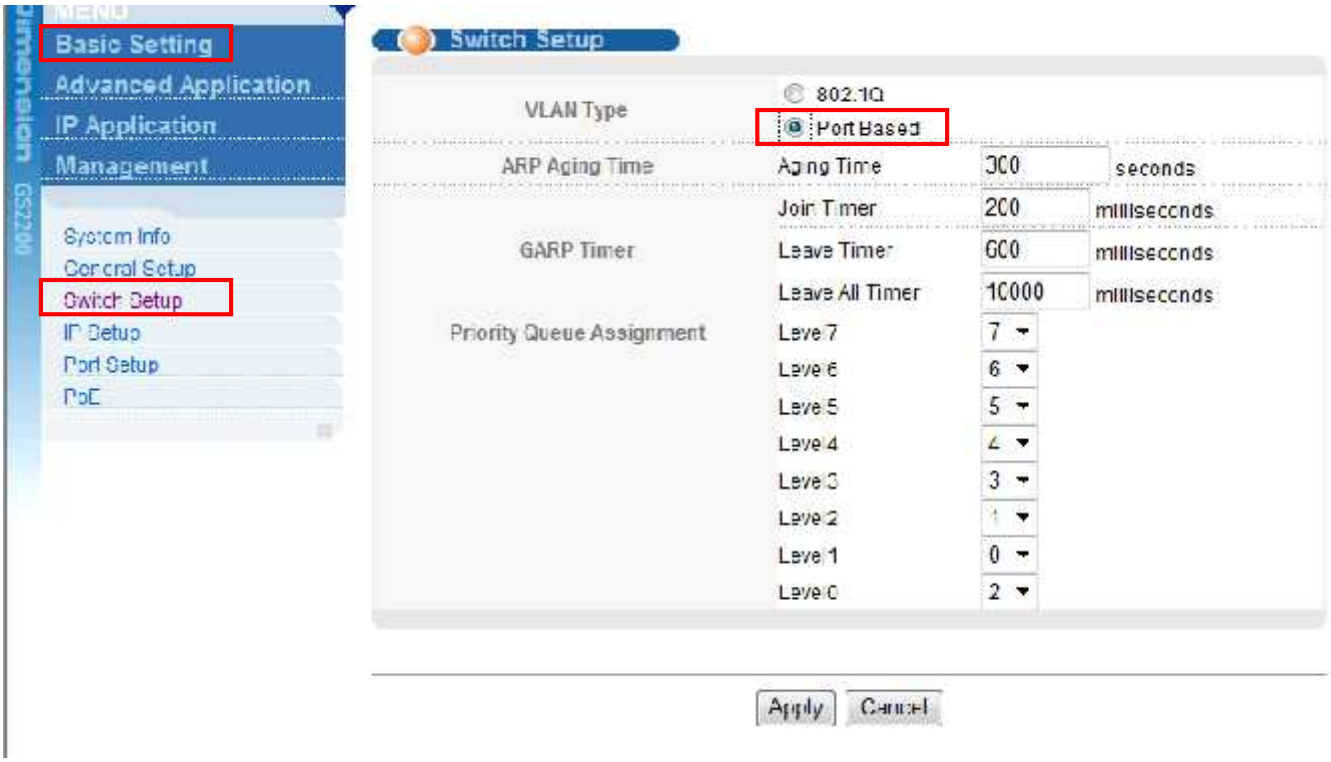
All contents copyright (c) 2011 ZyXEL Communications Corporation

Configuring your Switch to fulfill this scenario (GUI)

1. Connect a PC or Notebook to the port 1 with using the RJ45 Cable.
2. By default, the MGMT IP on every port is 192.168.1.1/24
3. Set your NIC to 192.168.1.2/24
4. Open an Internet browser such as IE and enter http://192.168.1.1 in the URL.
5. By default, you will need to put "admin" as the username and "1234" as the password.
6. After you login successfully, you will see a screen similar to the one below.

7. First, we need to tell the Switch to run VLAN as port based instead of 802.1q based. In order to do so, click on the "Basic Setting", then click "Switch Setup"; in the right side of the screen select the VLAN Type "Port Based" instead of "802.1Q", and click "Apply". Click "Save" to save the changes.

All contents copyright (c) 2011 ZyXEL Communications Corporation



8. Now, you need to tell the Switch how you are going to separate the physical Switch into small logical Switches. Click "Advanced Application" then "VLAN". In the right side of the screen, check the boxes as you need. In this case, we need to put ports 1~4 and ports 9, 10 in a group in order for them to communicate in both ways. We put port 5~10 in another group so that these two groups cannot talk with each other. Here we also logically define Port 9 and Port 10 as the uplink ports. Therefore, both groups can pass data to Port 9 and Port
10. In other words, these two ports belong to both groups at the same time. Check whether your setting looks like the one below.

All contents copyright (c) 2011 ZyXEL Communications Corporation

9. Finally, you can now verify the results. If everything works fine, PC A can ping PC B and PC Z. But it cannot ping PC C or PC D. It should work vice versa at the same time too.
10. For example,
    PC A: 192.168.1.4/24
    PC B: 192.168.1.5/24
    PC C: 192.168.1.6/24
    PC D: 192.168.1.7/24
    PC Z: 192.168.1.99/24
11. PING PC B from PC A (Should work)

All contents copyright (c) 2011 ZyXEL Communications Corporation

```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=12ms TTL=254
Reply from 192.168.1.5: bytes=32 time=6ms TTL=254
Reply from 192.168.1.5: bytes=32 time=7ms TTL=254
Reply from 192.168.1.5: bytes=32 time=6ms TTL=254

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 7ms
```

12. PING PC Z from PC A (Should work)

```
C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

Reply from 192.168.1.99: bytes=32 time=15ms TTL=254
Reply from 192.168.1.99: bytes=32 time=6ms TTL=254
Reply from 192.168.1.99: bytes=32 time=6ms TTL=254
Reply from 192.168.1.99: bytes=32 time=7ms TTL=254

Ping statistics for 192.168.1.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 15ms, Average = 8ms
```

13. PING PC C from PC A (Should NOT work)

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


All contents copyright (c) 2011 ZyXEL Communications Corporation

Configuring your Switch to fulfill this scenario (CLI)

1. Connect your PC or Notebook to the Switch Console port.
2. Open your Terminal program.(e.g. Hyper Terminal in Windows System)
3. Make sure that your port settings are
   bps:9600
   Data bits:8
   Parity: None
   Stop bits:1
   Flow control: None:
4. After you are connected successfully, enter the correct user name and the password.
5. Put "config" to go into the configuration mode.
6. Issue the following commands to setup Port Based VLAN on your Switch in this scenario.

```
vlan-type port-based
interface port-channel 1
  no egress set 5-8
exit
interface port-channel 2
  no egress set 5-8
exit
interface port-channel 3
  no egress set 5-8
exit
interface port-channel 4
  no egress set 5-8
exit
interface port-channel 5
  no egress set 1-4
exit
interface port-channel 6
  no egress set 1-4
exit
interface port-channel 7
  no egress set 1-4
exit
interface port-channel 8
  no egress set 1-4
exit
```

7. When all of the above is done, do not forget to put the "write memory" command under the enable mode to save your configuration.

All contents copyright (c) 2011 ZyXEL Communications Corporation