

OLT-1308/OLT-1308H

Standalone Managed Layer-2 GEAPON switch

Support Notes

Version1.0
Nov. 2006



Switch Management and Maintenance	3
Firmware Upgrade	3
Using the Web Configurator	3
Using the Console Port:.....	4
Using FTP:.....	4
Restore a Configuration File	4
Using the Web Configurator:	4
Using the Console Port:.....	5
Using FTP:.....	5
Backing Up a Configuration File	6
Using the Web Configurator:	6
Using the Console Port:.....	6
Using FTP:.....	7
Load Factory Defaults.....	7
Using the Web Configurator:	7
Using the Console Port:.....	8
General Networking	8
DHCP Relay Option 82 Application.....	8
Setting up a DHCP Relay Option 82 Environment.....	9
Separating a physical network into multiple virtual networks	23
What is Virtual LAN?.....	23
VLAN Overview	23
Port-based VLAN.....	24
Port-based VLAN across multiple switches	26
How to configure Port-Based VLAN	27
What is IEEE 802.1Q Tag-based VLAN?	32
How 802.1Q VLAN works	33
Connecting Two Switches using VLAN.....	36
Setting up VLAN Trunking	39
VLAN Stacking Overview.....	41
Configuring Switch A, E, F and H Using the Web Configurator	43
Configuring Switch B Using the Web Configurator	44
Configuring Switch C Using the Web Configurator	47
Configuring Switch D Using the Web Configurator	50
Configuring Switch G Using the Web Configurator.....	53
Network Scenario.....	57
Configuring Switches A, E, F and H Using the CLI	57
Configuring Switch B Using the CLI.....	58
Configuring Switch C via CLI	59
Configuring Switch D Using the CLI	60
IP Multicasting	62
Configuring IGMP snooping in your switch	62
Configuration of IGMP snooping by web	63
Configuration of IGMP and IGMP snooping by CLI	64
Overview of MVR.....	65
MVR Mode.....	66

Operation Mode	67
Scenario of MVR	67
Ringing a network by building redundant links and connections between Switch	81
What is Spanning Tree Protocol?	81
Spanning Tree Overview	81
How STP Works	82
How STP works	84
Switching security	86
MAC freeze	86
Setting up 802.1x Radius Authentication.	88
Port Authentication: RADIUS Setup	88
RADIUS Server Setup	89
Create User Account	89
Supplicant Setup (Windows XP).....	90
Classifier & Policy rule setup on your Switch	92
Classifier Configuration.....	93
Policy Rule Configuration	94
Centralized Management.....	96
Introduction to SNMPc and NetAtlas.....	96
SNMPc Overview	97
EMS Overview	97
Cluster Management Overview.....	105
How Cluster Management works.....	105
Configuring Cluster Management.....	106
FAQ	110
What are the default IP parameter settings?	110
What is the default login Name and Password to log into the Web Configurator?	110
How to access my SWITCH through the console port?.....	110
What is default login password for console, telnet, and FTP login?....	110
How to change the password?	110
How to access the Command Line Interface (CLI)?	111
If I have forgotten the password, how to reset the password to the default setting?	111
How to configure the IP address?.....	112
Is Online Help available on the Web Configurator?	112
How to restart device from the Web Configurator?.....	112
How to check the current running firmware version?	113
Is the mini GBIC transceiver hot-swappable?.....	113
What is "Dual-Personality interface" on a VDSL Switch?	113
Can I enable IGMP snooping on the Switch which is acting as an IGMP Router?.....	113
Can I enable MVR and IGMP snooping at the same time?	113

Switch Management and Maintenance

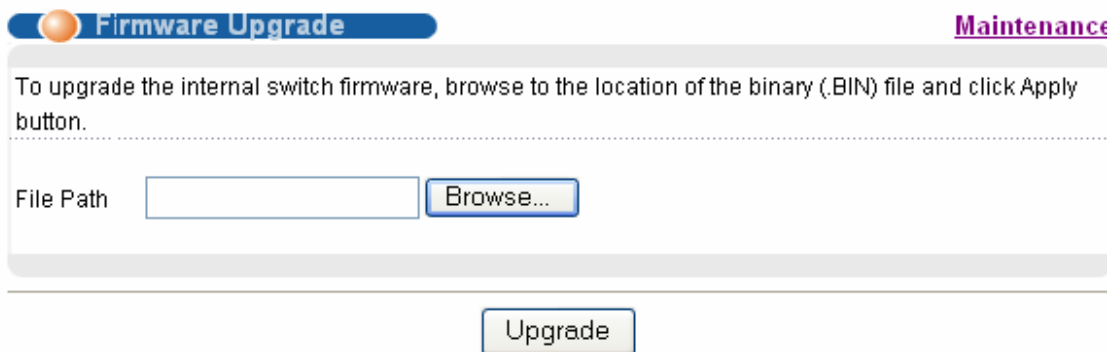
Firmware Upgrade

Using the Web Configurator

1. Download (and unzipped) the correct model firmware to your computer.
2. Click Management > Maintenance in the navigator panel to display the following screen.



3. Click the "Click Here" link for Firmware Upgrade to display the following screen.



4. In the File Path field, click Browse to locate the firmware file.
5. Click Upgrade to start the firmware upgrade process.

Using the Console Port:

1. Download (and unzipped) the correct model firmware to your computer.
2. Connect to the console port and launch a Terminal Emulation software
3. Restart the switch to enter the debug mode via the terminal.
4. Enter "ATUR".
5. Use the X-modem protocol to transfer (Send File) the firmware.
6. Enter "ATGO" to restart the switch after the file transfer is complete and the firmware upgrade process is done.

Using FTP:

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your computer to log into switch. (From the command prompt, type "ftp <Switch IP>").
3. Press [ENTER] when prompted for a user name.
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter "bin" to set the transfer mode to binary.
6. Use "put" to transfer the firmware from the computer to the switch, for example: "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the switch and renames it to "ras".
7. Enter "bye" to log out from the switch.

Restore a Configuration File

Using the Web Configurator:

1. Click Management > Maintenance in the navigator panel to display the following screen.



2. Click the “Click Here” link for Restore Configuration to display the following screen.

Restore Configuration Maintenance

To restore the device's configuration from a file, browse to the location of the configuration file and click Restore button.

File Path

3. In the File Path field, click Browse to locate the firmware file.
4. Click Restore to start restoring configuration.

Using the Console Port:

1. Connect to the console port and launch Terminal Emulation software.
2. Restart the switch to enter the debug mode via the terminal.
3. Enter “ATLC”
4. Use X-modem protocol to transfer (Send File) the configuration file (with a .rom file extension).
5. Enter “ATGO” to restart the switch after file transfer and the configuration restore processes are complete.

Using FTP:

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your computer to log into the switch. (From the command prompt, type “ftp <Switch IP>”.
3. Press [ENTER] when prompted for a user name
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter “bin” to set the transfer mode to binary.
6. Use “put” to transfer the configuration file from the computer to the switch, for example: “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the switch and renames it to “rom-0”.
7. Enter “bye” to log out from the switch.

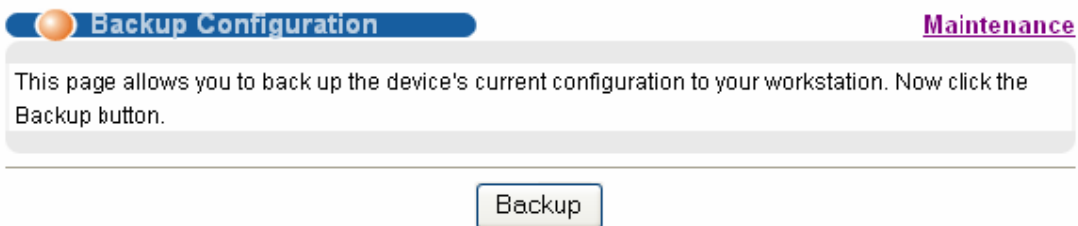
Backing Up a Configuration File

Using the Web Configurator:

1. Click Management > Maintenance in the navigator panel to display the following screen.



2. Click the “Click Here” link for Backup Configuration to display the following screen.



3. Click Backup to display the File Download dialog. Then, click Save to back up the configuration text file to a location you specify on your computer.

Using the Console Port:

1. Connect to the console port and launch a Terminal Emulation software.
2. Restart the switch to enter the debug mode via the terminal.
3. Enter “ATTD”.
4. Use X-modem protocol to transfer (Receive File) the configuration file (with a .rom file extension).
5. Enter “ATGO” to restart the switch after file transfer and the configuration backup processes are complete.

Using FTP:

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your PC to log into the switch. (From the command prompt, type "ftp <Switch IP>")
3. Press [ENTER] when prompted for a user name
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter "bin" to set the transfer mode to binary.
6. Use "get" to transfer the configuration file from the switch to your computer, for example: "get rom-0 config.rom" transfers the configuration file on the switch (rom-0) to your computer and renames it "config.rom".
7. Enter "bye" to log out from the switch.

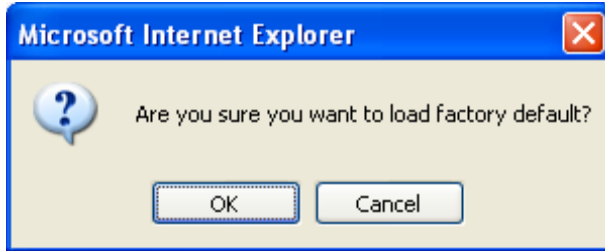
Load Factory Defaults

Using the Web Configurator:

1. Click Management > Maintenance in the navigation panel to display the following screen.



2. Click "Click Here" link for Load Factory Default.
3. A dialog box pops up with the "Are you sure you want to load factory defaults?" prompt.



4. Click OK.
5. Click OK again to start the configuration reset process. After it is complete, the device automatically restarts.
6. Please note that the IP address of the switch is now 192.168.1.1.

Using the Console Port:

1. Connect to the console port and open the Terminal Emulation Software.
2. Enter the administrator login password to log into the CLI. Enter "erase run" to load the factory default configuration.

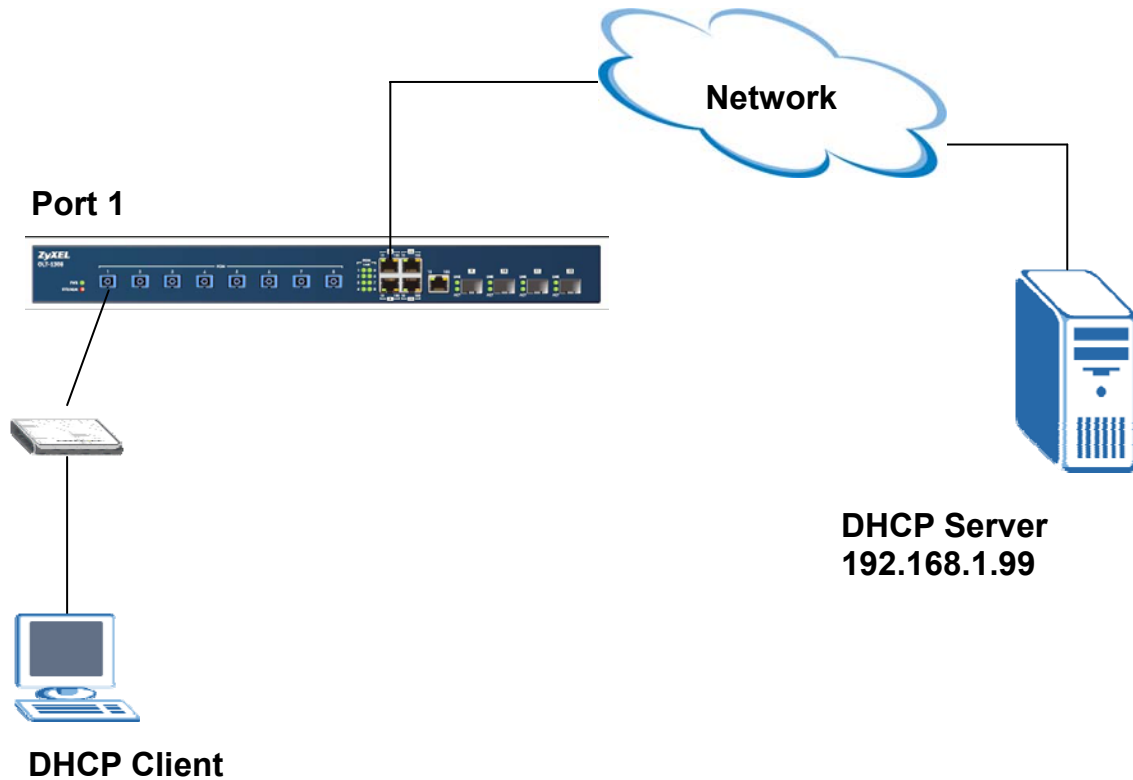
General Networking

DHCP Relay Option 82 Application

ISP may want to limit the number of IP address or provide some specific client IP addresses based on the switch ports, VLAN ID and option 82 string.

They can easily achieve this with the DHCP Relay Option 82 feature and a DHCP server that supports Option 82.

The following figure shows a network example.



Setting up a DHCP Relay Option 82 Environment

In this example, we will show you how to configure DHCP relay settings to allow a computer to obtain a specific IP address from a DHCP server based on the VDSL port, VLAN ID and the Option82 string.

In this network environment, we will use a OLT-1308 series with a computer connected to a CPE to the first VDSL port. The Option82 string is set to "OLT-1308".

The IP address of the DHCP server (IP Commander at 192.168.1.99) and it is to assign client IP addresses of 192.168.1.201 and 192.168.1.203 for VLAN ID 1 with Option82 string of "OLT-1308".

1. Switch settings

In the web configurator, click **Routing Protocol > DHCP Relay** in the navigation panel to display the **DHCP Relay** screen as shown. Enable the DHCP relay feature and the Option 82 function. Click **Information** to set "OLT-1308" as the Option 82 string. The **Information** field is READ ONLY here and it is the same as the host name of the switch you configured.

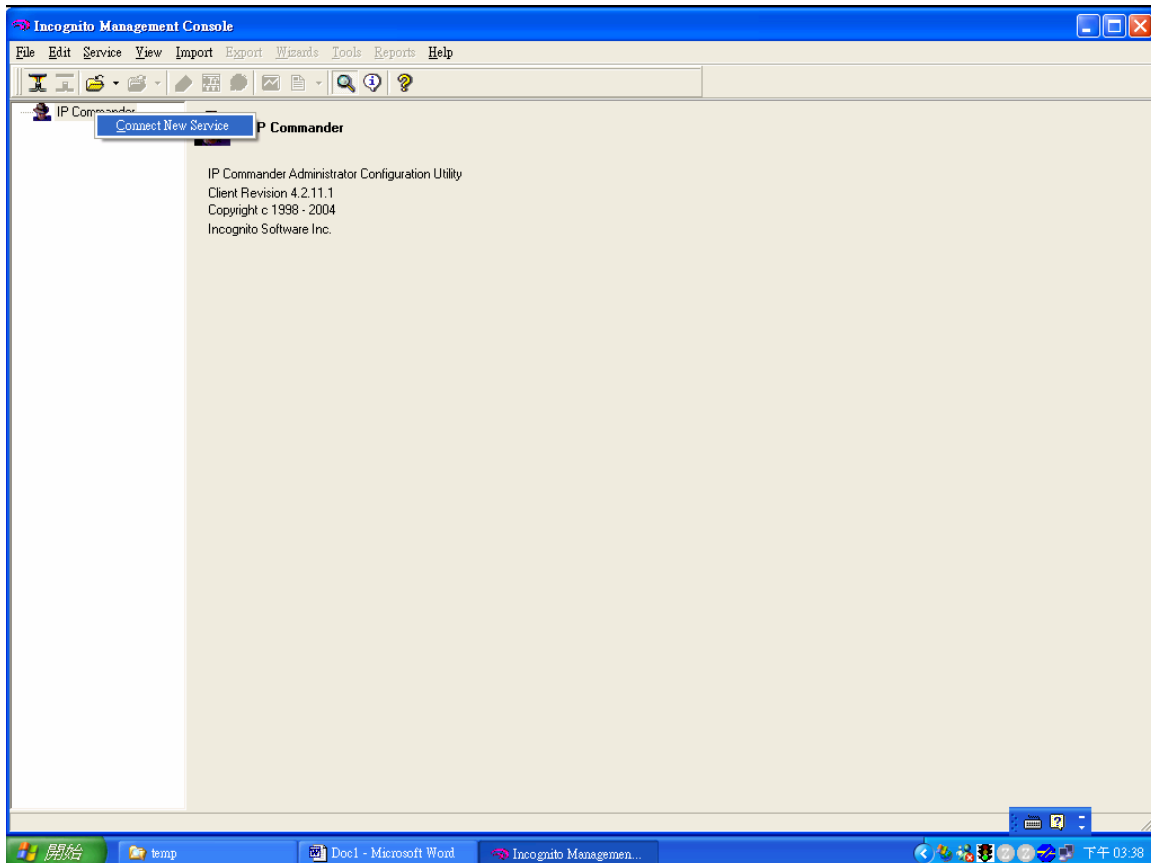
DHCP Relay	
Active	<input checked="" type="checkbox"/>
Remote DHCP Server 1	192.168.1.99
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	<input checked="" type="checkbox"/> Option 82
Information	<input checked="" type="checkbox"/> OLT-1308

Apply Cancel

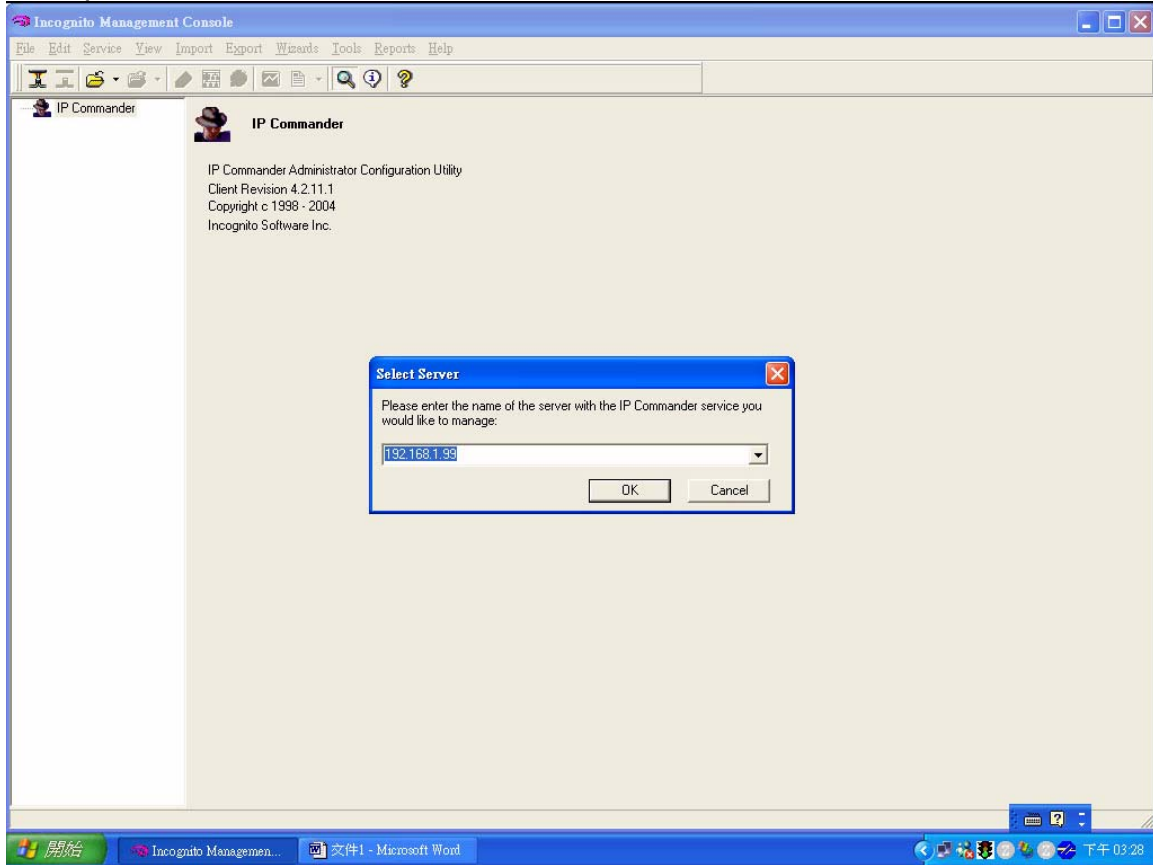
Next connect a computer to the Ethernet port of the CPE to the 1st VDSL port. Refer to the previous application for more information.

2. IP Commander setup

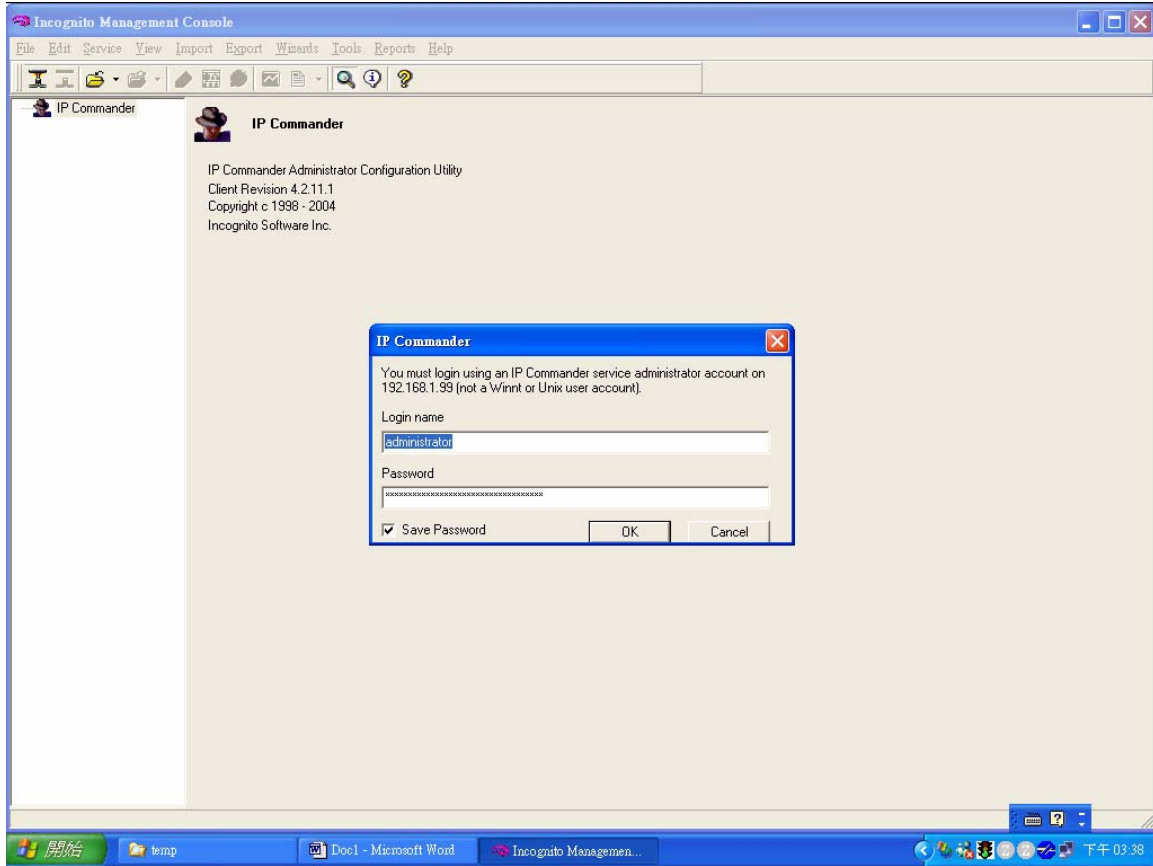
Launch IP Commander and right-click **IP Commander** and click **Connect New Server**.



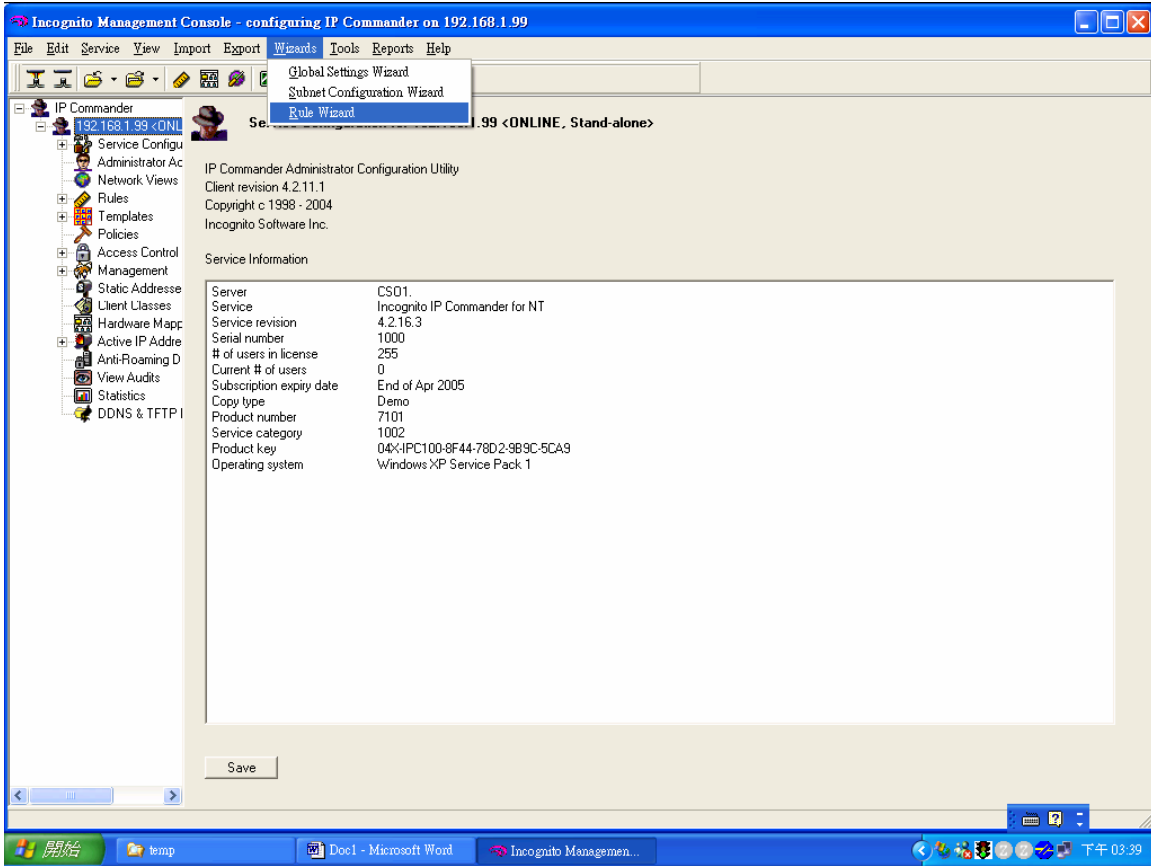
Enter the IP address or domain name for the DHCP server and click **OK**. For this example, we enter 192.168.1.99 for the IP address.



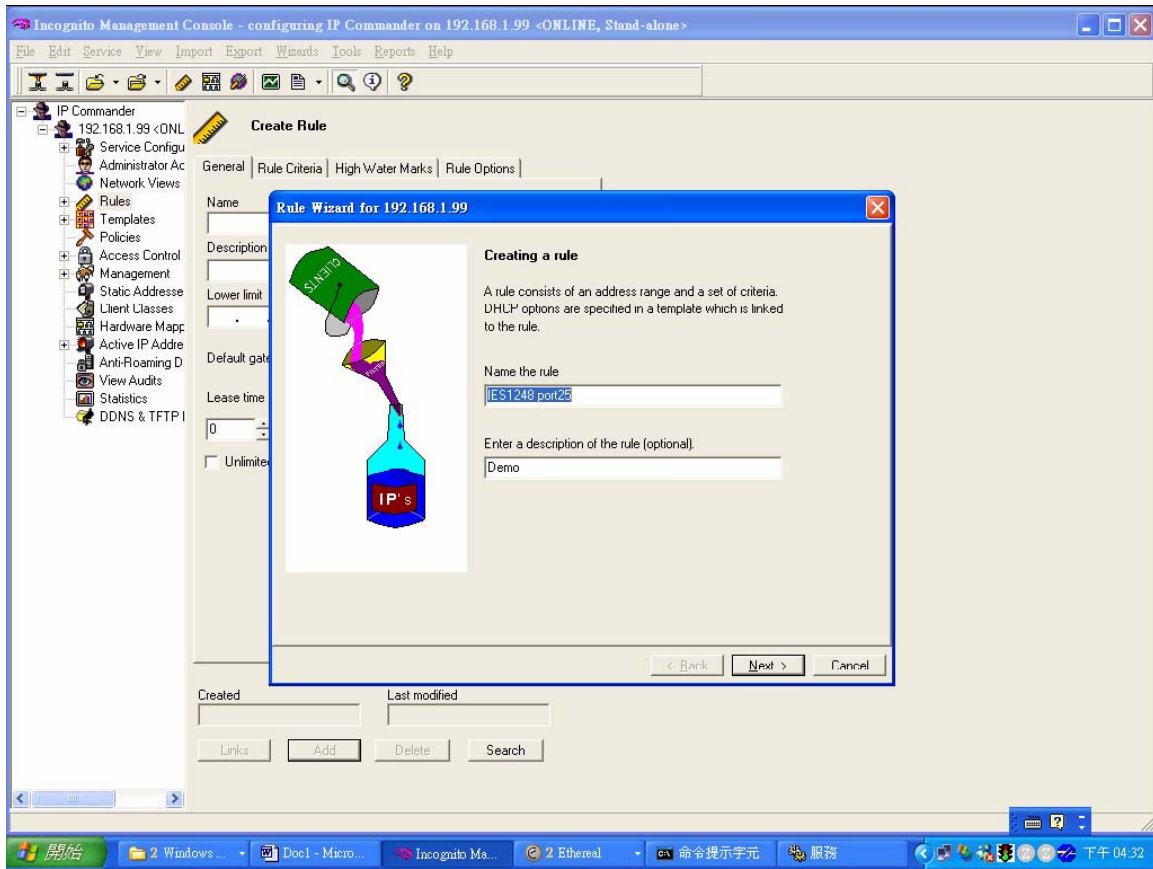
Enter the user name and password. The default user name is “administrator” and password is “incognito”.



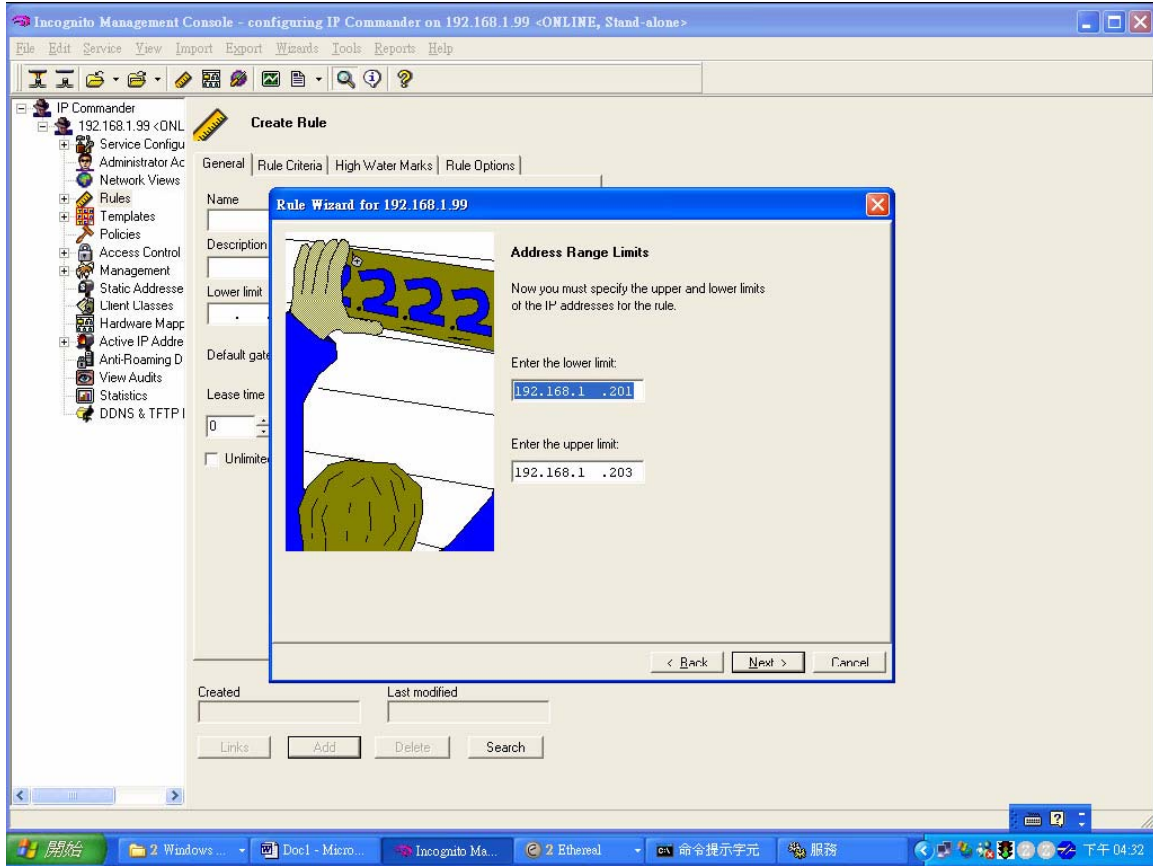
A screen displays. Make sure that the status of your DHCP is **online**. On the top menu, click **Wizard > Rule Wizard**.



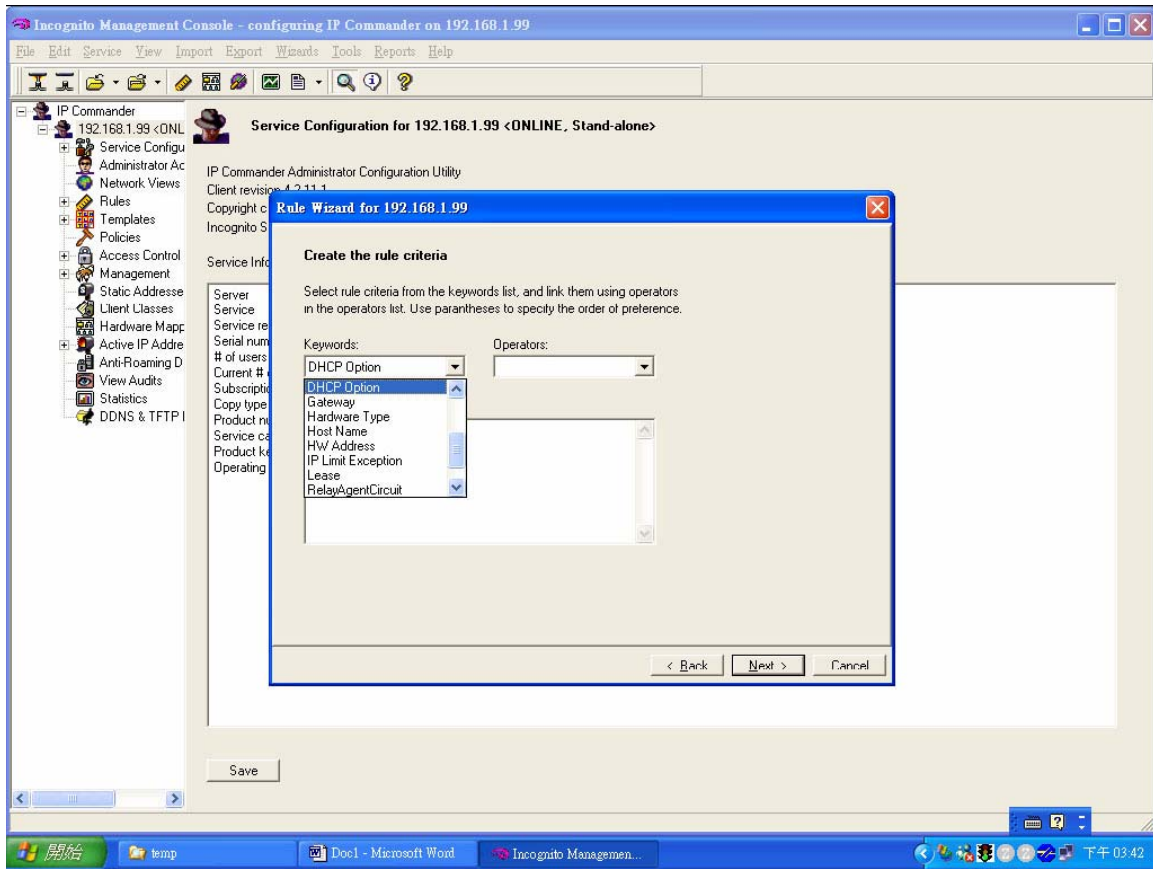
Enter a name and description for the new rule.



Specify one or a range of IP addresses for this rule. In this example, we configure an IP pool from 192.168.1.201 to 192.168.1.203.

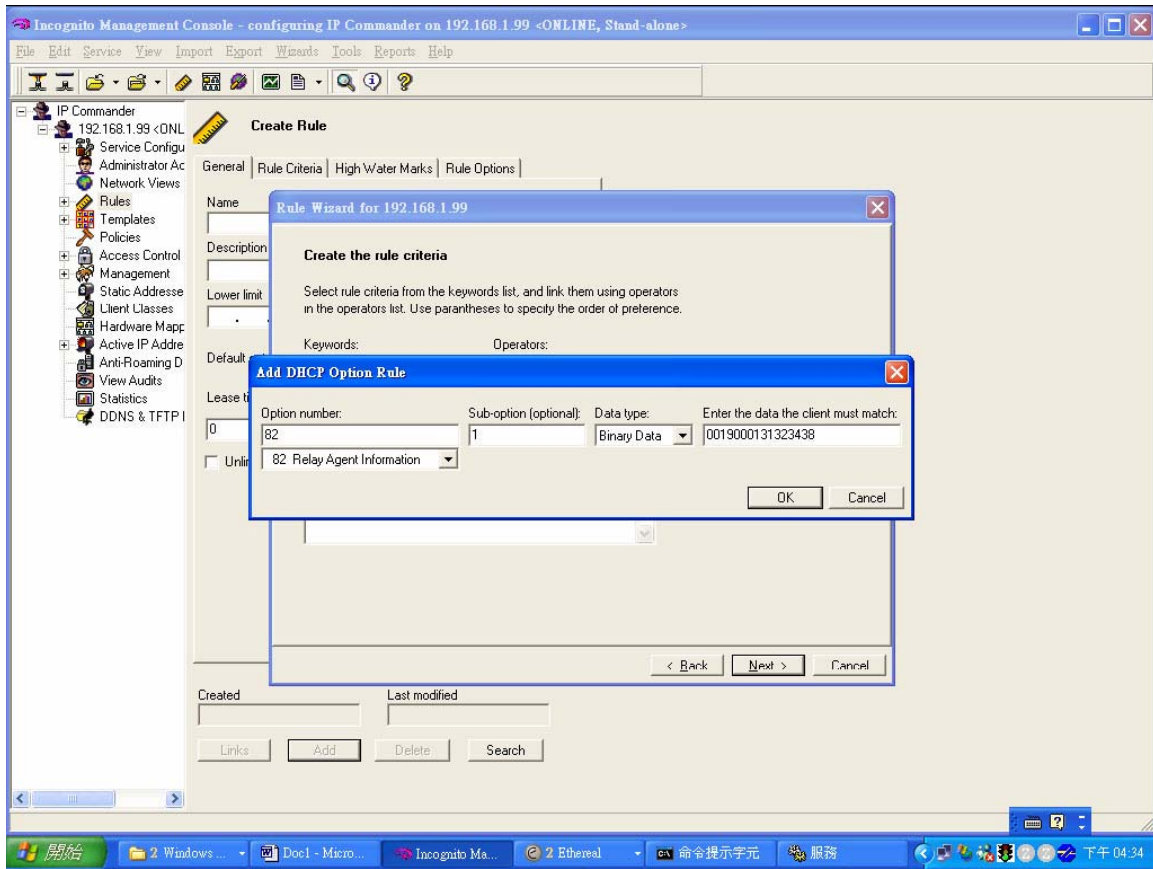


Next select **DHCP Option** in the Keywords field.

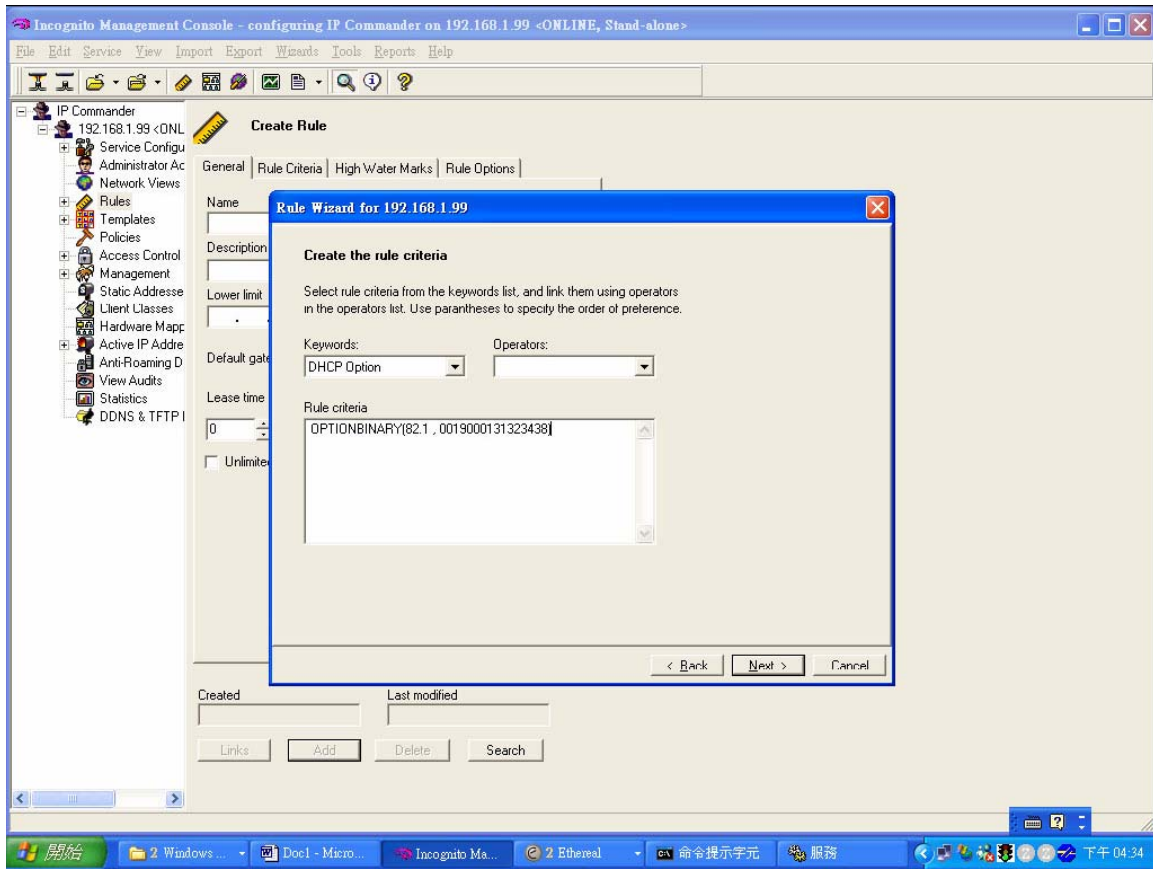


An Add DHCP Option Rule screen displays.

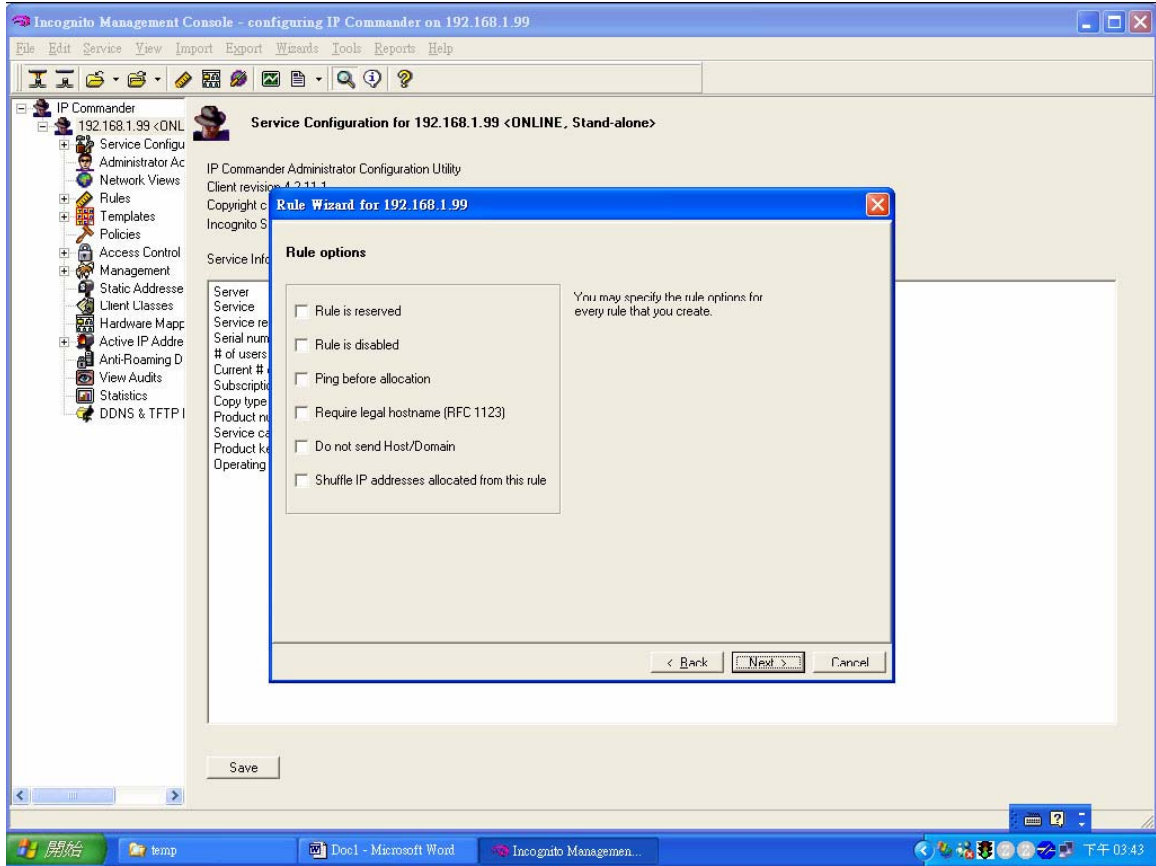
Select **Option 82 Relay Agent Information**, set sub-option 1 and use binary data. For port 1, VLAN 1 with option82 string of "OLT-1308", enter "0019000147532d33303132" as the key value and click **OK**. Note that the first two bytes define the port number, the second two bytes is the VLAN ID and the rest of the bytes are the Option 82 string.



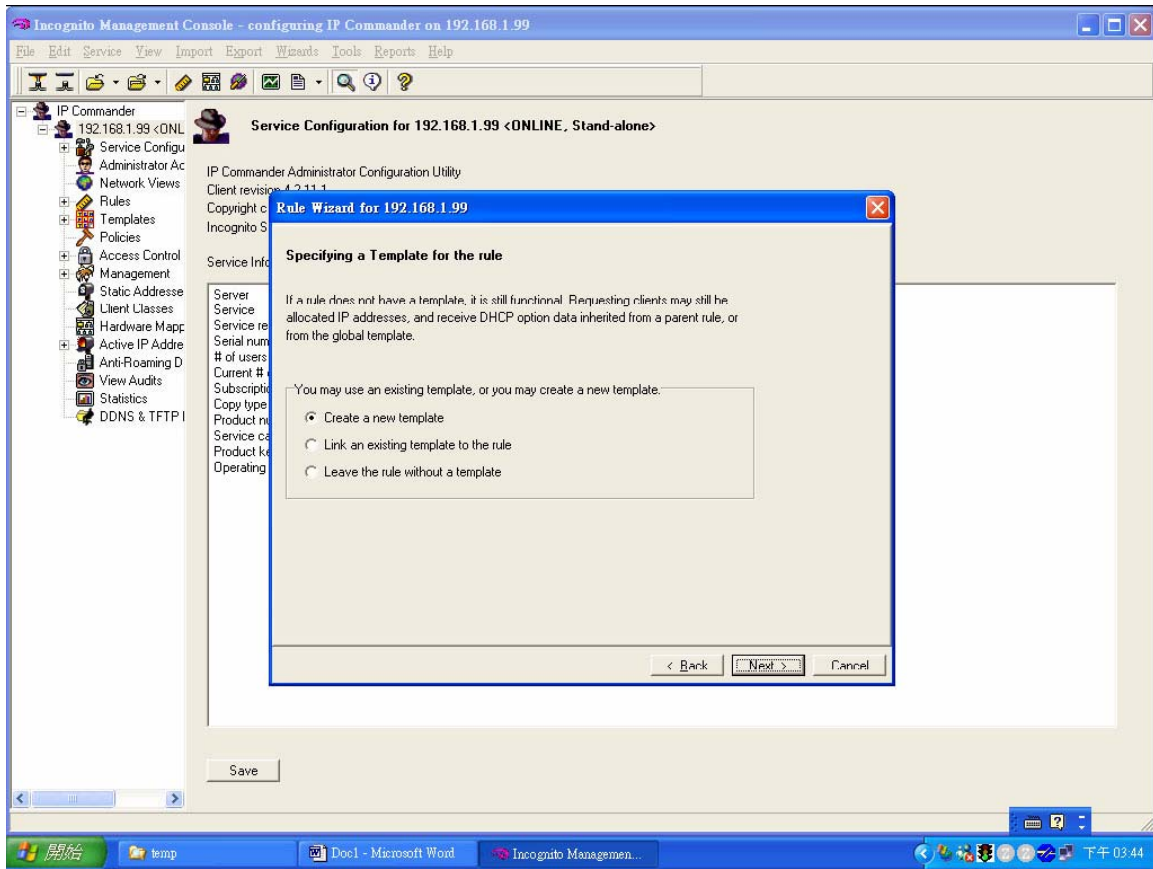
After setting the fields, you should see the following screen.



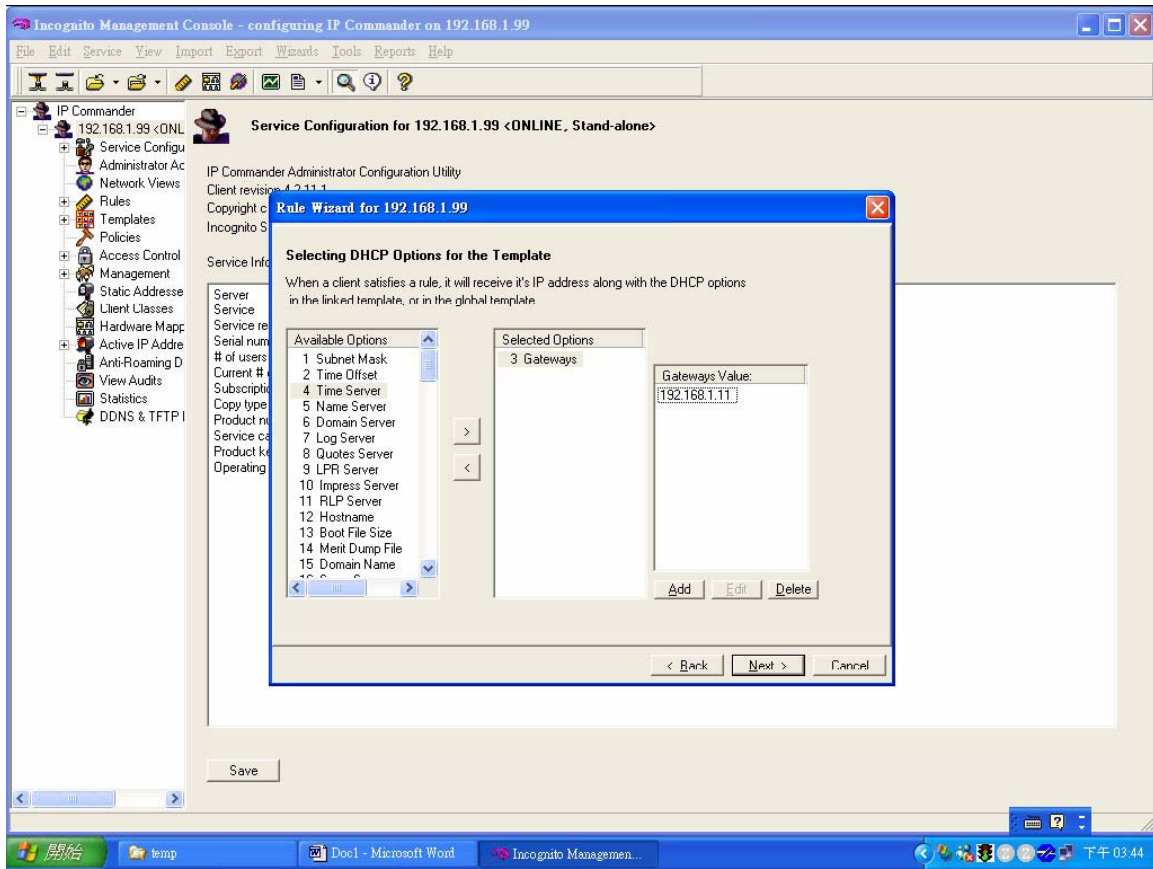
Click **Next** in the screen that displays.



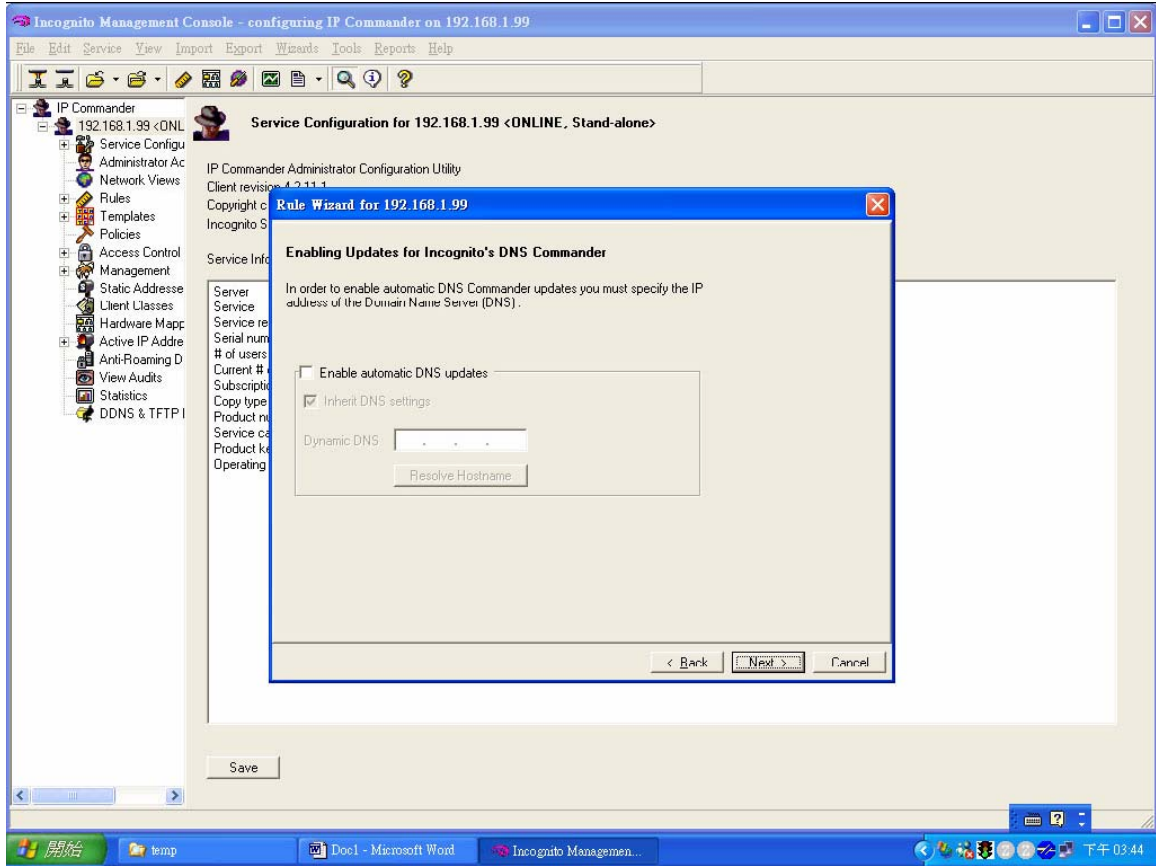
Optionally, you can create a new DHCP template with information such as gateway, DNS server, etc.



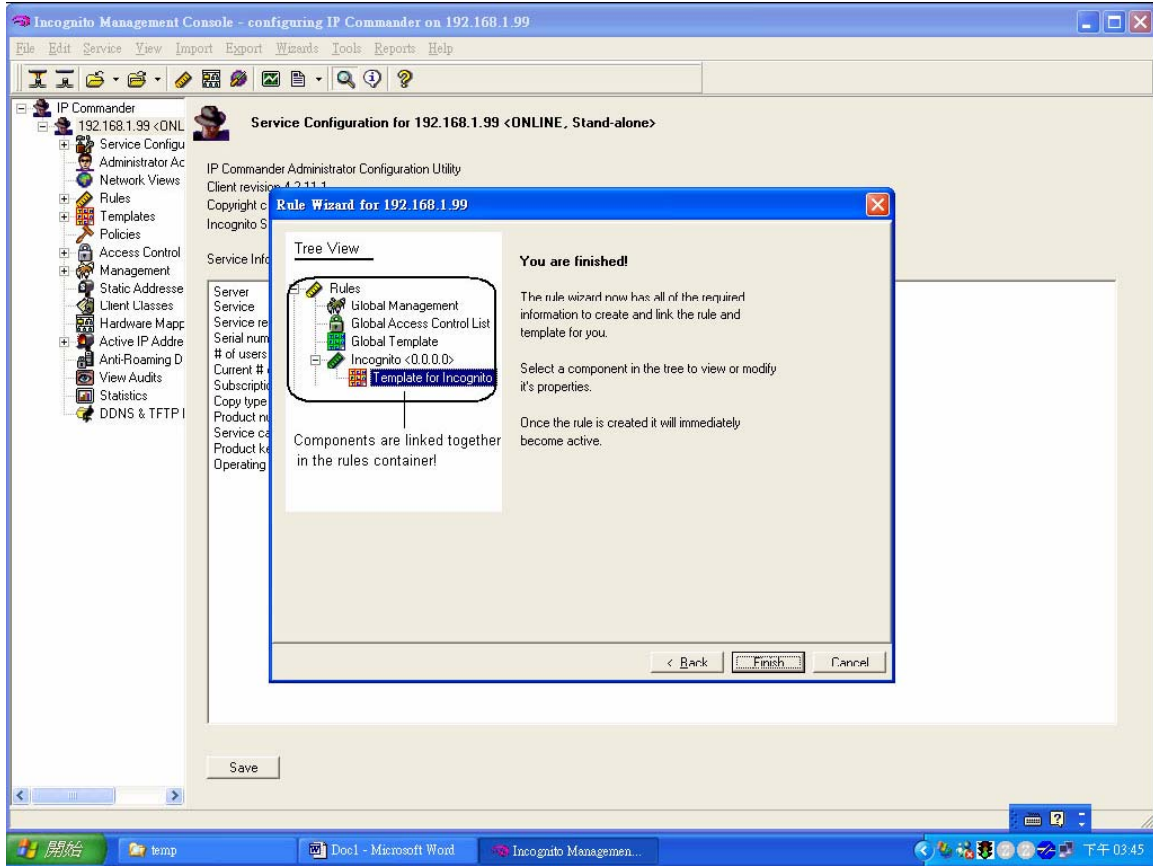
Here, enter "192.168.1.1" as gateway IP address for DHCP clients.



You can choose to enable DDNS service on the DHCP server.



Click Finish to complete the rule creation.



After the DHCP server configuration, your computer should be able to get an IP address of 192.168.1.201 when a DHCP request is sent.

Separating a physical network into multiple virtual networks

What is Virtual LAN?

VLAN Overview

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned

into multiple logical networks. Stations on a logical network belong to a group known as the VLAN Group. A station can belong to more than one group. Stations in the same VLAN group can communicate with each other. With VLAN, a station cannot directly communicate with stations that are not in the same VLAN group(s); the traffic must first go through a router.

In GePON applications, VLAN is vital in providing isolation and security among subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN. Thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. A VLAN group is a broadcast domain. In traditional Layer-2 switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

There are two VLAN implementations: Port-based VLAN and IEEE 802.1q Tagged VLAN. OLT-1308 supports both VLAN implementations. The major difference between both VLAN implementations is that Tagged VLAN can cross Layer-2 switches but Port-based VLAN cannot.

Port-based VLAN

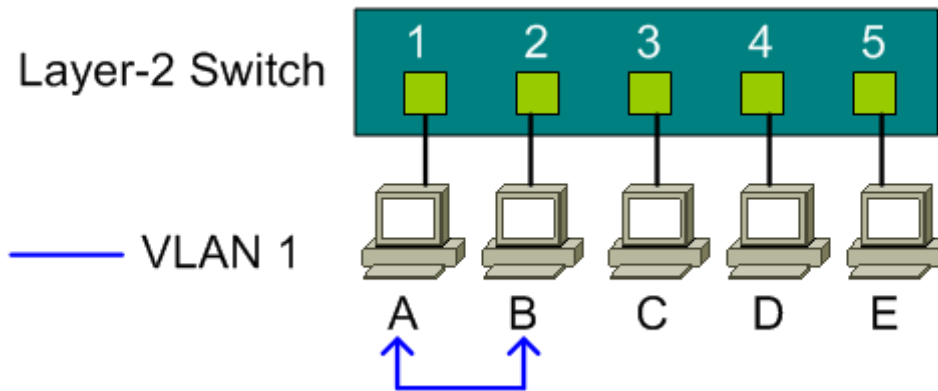
Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. You must define outgoing ports allowed for each port when using port-based VLANs. Note that VLAN only governs the outgoing traffic. In the other word, it is unidirectional.

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.

In the following figure, five hosts (A, B, C, D and E) are connected to a 5-port layer-2 switch which supported port-based VLAN.

Case 1:

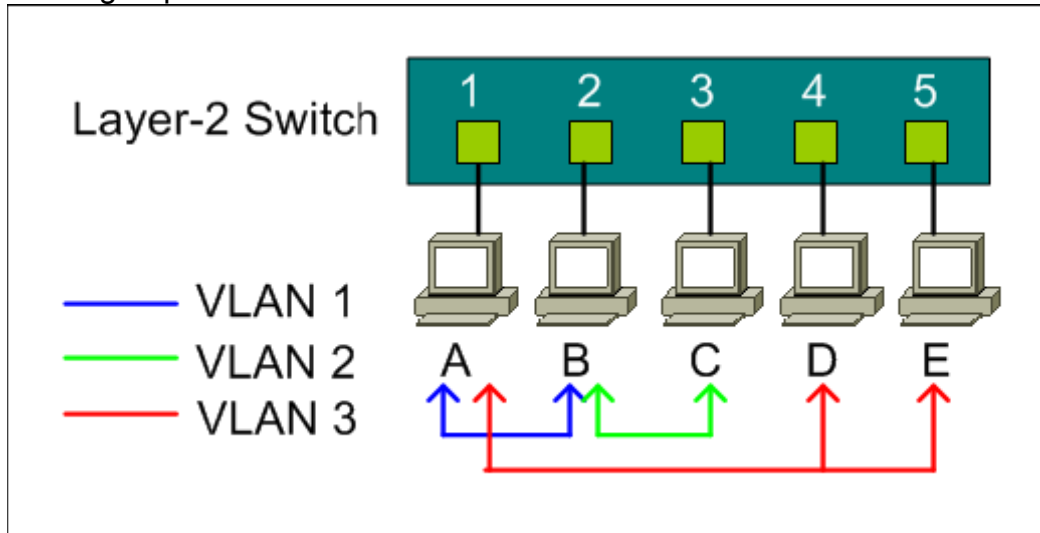
Hosts A and B can communicate with each other, because they are in the same VLAN group. But Hosts A and B cannot communicate with Hosts C, D, and E.

**Port-based VLAN definition:**

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

Case 2:

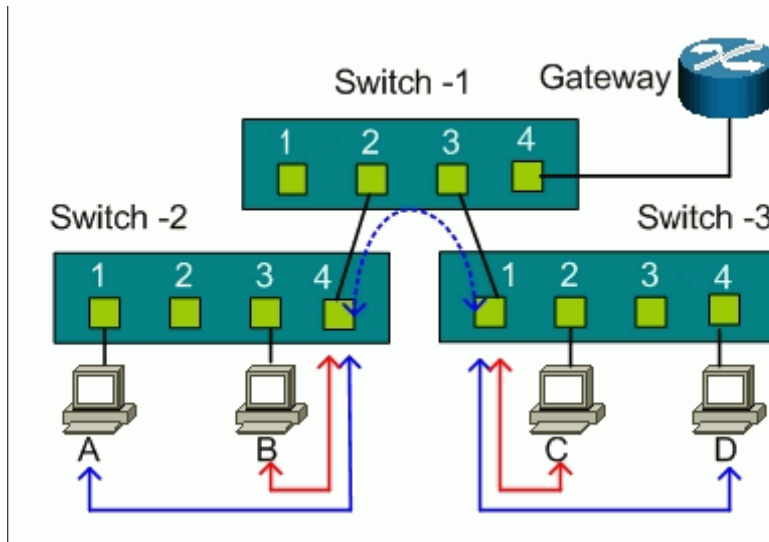
In this network example, there are three VLAN groups in the physical network. Hosts A and B can communicate with each other since they are in the same VLAN group (VLAN 1). Hosts B and C are in VLAN group 2. Hosts A, D and E are in VLAN group 3.

**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 multiple switches

Port-based VLAN is specific only to the switch on which it was created. Thus, port-based VLAN cannot cross multiple switches. The following figure shows an MTU network example. For network security, subscribers are isolated from each other except for the gateway. There are two switches, Switch-2 and Switch-3, that support port-based VLAN and an uplink to a non-port-based VLAN switch, Switch-1.



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

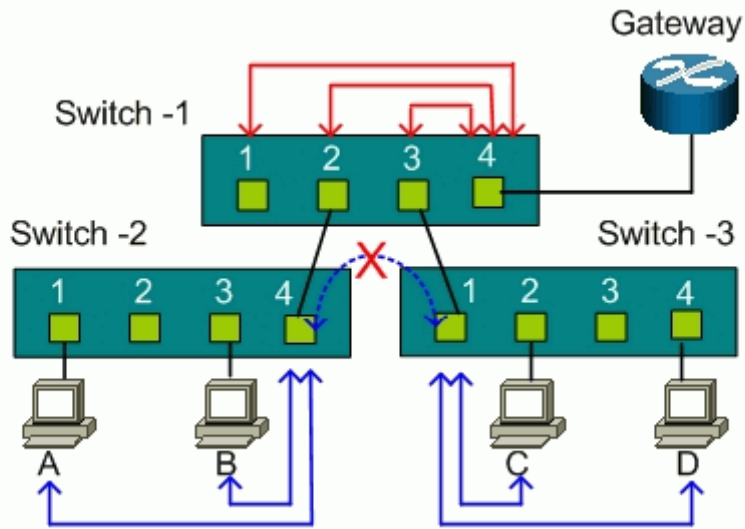
- Switch-2 VLAN 1 member port: port 1 and port 4
- Switch-2 VLAN 2 member port: port 2 and port 4
- Switch-2 VLAN 3 member port: port 3 and port 4

For Switch-3, ports 2, 3, and 4 are allowed to communicate with uplink port 1, but not with 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 cannot communicate with Host B due to the port-based VLAN implementation on Switch-2. Host C cannot communicate with Host D due to the port-based VLAN implementation on Switch-3. However, the uplink ports on both Switch-2 and Switch-3 connect to the non-VLAN Switch-1. Hosts A and B is able to communicate with Hosts C and D through the non-VLAN switch because port-based VLAN cannot cross multiple switches.

To provide security between switches, you must install another port-based VLAN switch for the uplink. Each port on the uplink switch also should be separated into different VLANs, except for the port connection to the gateway. So subscribers can only connect to the gateway for Internet access but not communicate with each other.

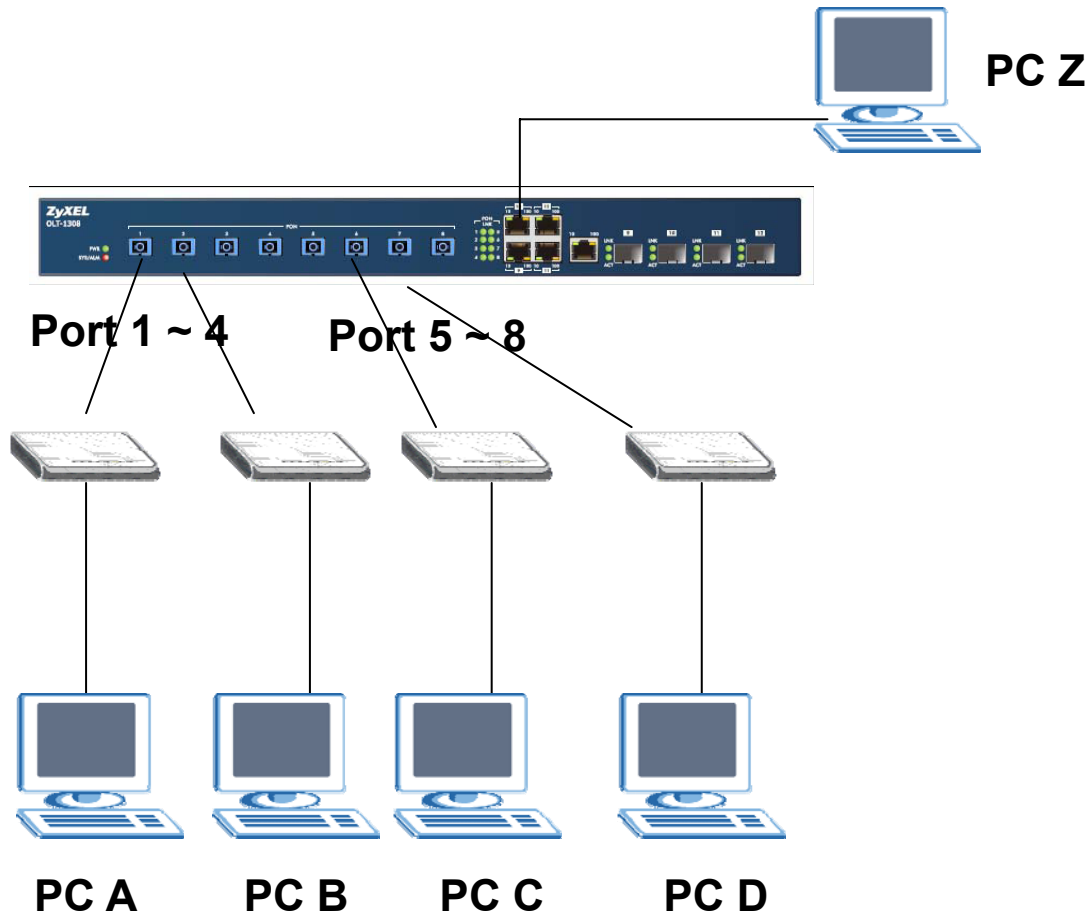


For Switch-1, ports 1, 2, and 3 are allowed to communicate with uplink port 4, but not with other ports.

- 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.



In this scenario, Port Based VLAN is used to separate one physical switch into two smaller logical switches. Ports 1~4 and 17, 18 belong to the same VLAN group, and ports 5~8 are in another group. Port-based VLANs are specific only to the switch on which they were created.

Configuring the Switch Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect a computer to the management port on the switch.
2. By default the management IP address of the switch is 192.168.0.1/24
3. Set the IP settings on your computer to 192.168.0.2/24
4. Open a web browser such as IE and enter <http://192.168.0.1> as the URL.
5. When prompted, enter “admin” as the username and “1234” as the password.
6. After you have logged in successfully, the main web configurator screen displays.

ZyXEL Status

System Up Time : 0:10:54

Port	OLT	Number of LLID	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1	Down	0	0	0	0	0.0	0.0	0:00:00
2	Down	0	0	0	0	0.0	0.0	0:00:00
3	Down	0	0	0	0	0.0	0.0	0:00:00
4	Down	0	0	0	0	0.0	0.0	0:00:00
5	Down	0	0	0	0	0.0	0.0	0:00:00
6	Down	0	0	0	0	0.0	0.0	0:00:00
7	Down	0	0	0	0	0.0	0.0	0:00:00
8	Down	0	0	0	0	0.0	0.0	0:00:00

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
9	1000MF SFP	FORWARDING	Disabled	0	0	0	0.0	0.0	0:00:17
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Poll Interval(s): 40 [Set Interval] [Stop]

Port: ALL [Clear Counter]

7. First, set the switch to use port based VLAN. Click **Basic Setting > Switch Setup** in the navigation panel and select “Port Based” in the VLAN Type field. Click **Apply** to save your changes.

ZyXEL Switch Setup

VLAN Type: 802.1Q Port Based

Bridge Control Protocol Transparency: Active

MAC Address Learning: Aging Time: 300 seconds

Join Timer: 200 milliseconds

GARP Timer: Leave Timer: 600 milliseconds

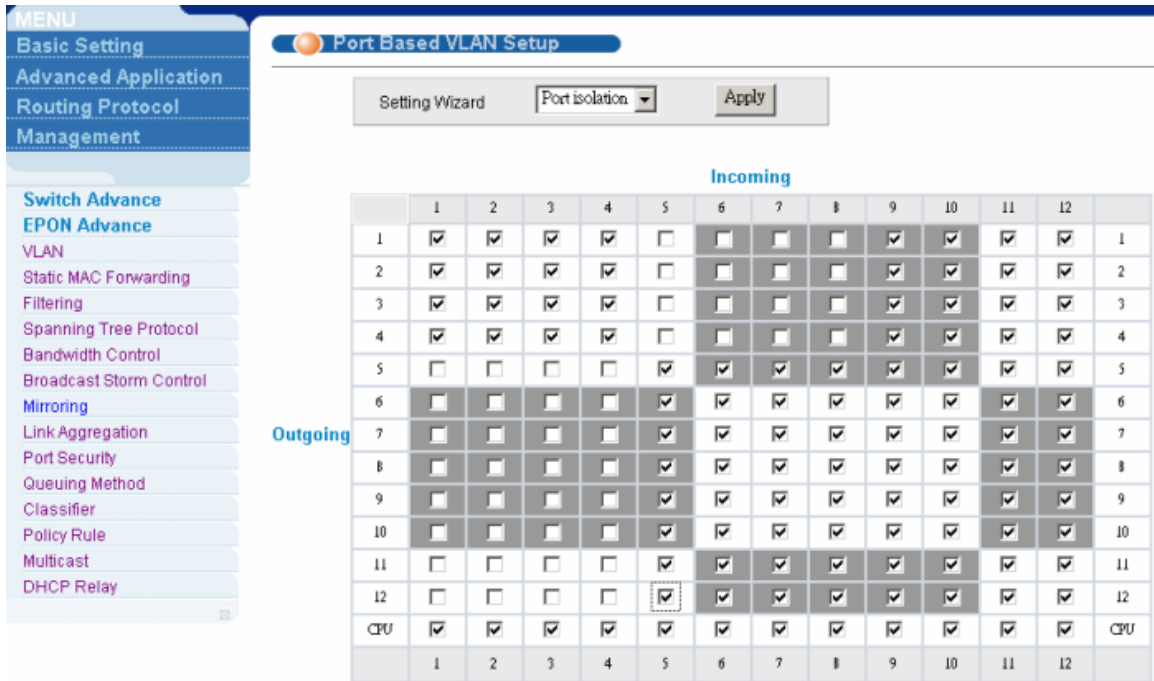
Leave All Timer: 10000 milliseconds

Priority Queue Assignment:

- Priority7: 7
- Priority6: 6
- Priority5: 5
- Priority4: 4
- Priority3: 3
- Priority2: 1
- Priority1: 0
- Priority0: 2

8. Next create logical partitions on the switch. Click **Advanced Application > VLAN** in the navigation panel and select the ports to belong to the VLAN. For this example, select ports 1~4 and 17, 18 to belong to a VLAN so they can communicate with each other.

Although ports 5~8 are in another group, both groups cannot communicate with each other. Here we also defined ports 17 and 18 as the uplink ports. Therefore, both groups can pass data to ports 17 and 18. In another word, these two ports belong to both VLAN groups at the same time. The configuration screen should look similar to the screen as shown.



9. Finally, verify the settings. If you have configured the VLAN settings properly, PC A can ping PC B and PC Z but not PC C or PC D and vice versa.

- 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 (successful reply messages)

```
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 (successful reply messages)

```
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 (not successful with request timed out message)

```
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),
```

Configuring the Switch Using the CLI

1. Connect your computer to the console port on the switch
2. Open your Terminal program (for example, Hyper Terminal in Windows System).
3. Make sure the console connection settings are configured as listed below.
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you can connect successfully, enter the user name and password.
5. Enter "en" or "enable" to go into the privileged mode. Enter "config" to go into the configuration mode.
6. Enter the following commands to configure Port Based VLAN on your Switch in this network example.

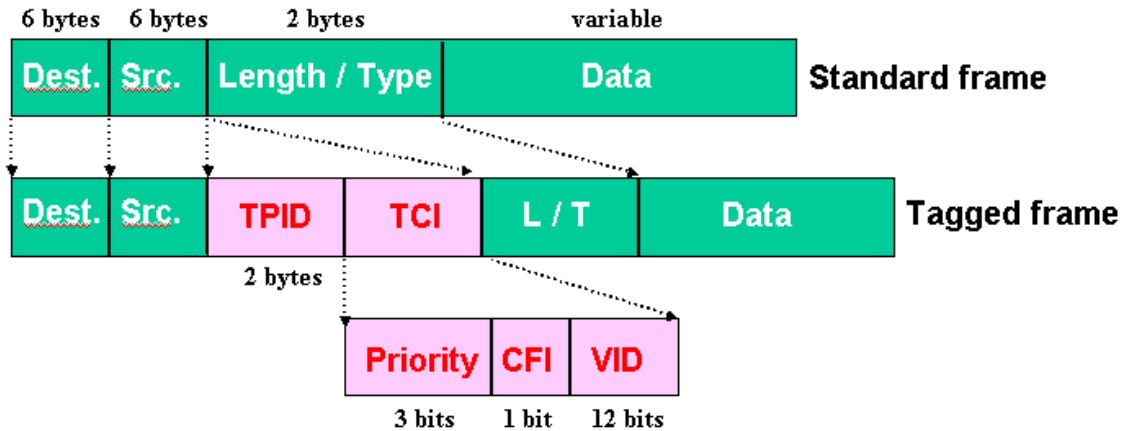

```
CAWINNT\system32\cmd.exe - telnet 192.168.0.1
write                               Write memory
OLT-1308# v1
Invalid input: v1
OLT-1308# config
OLT-1308(config)#
OLT-1308(config)# vlan-type port-bas
Invalid input: vlan-type port-bas
OLT-1308(config)# vlan-type port-based
OLT-1308(config)# vlan-type port-based interface port-chan
Invalid input: vlan-type port-based interface port-chan
OLT-1308(config)# vlan-type port-based interface port-channel 1 no egress set 58
OLT-1308(config)# vlan-type port-based interface port-channel 2 no egress set 58
OLT-1308(config)# vlan-type port-based interface port-channel 3 no egress set 58
OLT-1308(config)# vlan-type port-based interface port-channel 4 no egress set 58
OLT-1308(config)# vlan-type port-based interface port-channel 5 no egress set 14
OLT-1308(config)# vlan-type port-based interface port-channel 6 no egress set 14
OLT-1308(config)# vlan-type port-based interface port-channel 7 no egress set 14
OLT-1308(config)# vlan-type port-based interface port-channel 8 no egress set 14
OLT-1308(config)#
```

7. After entering the commands, use the “write memory” command under the enable mode to save your configuration.

What is IEEE 802.1Q Tag-based VLAN?

Tag-based VLAN Overview

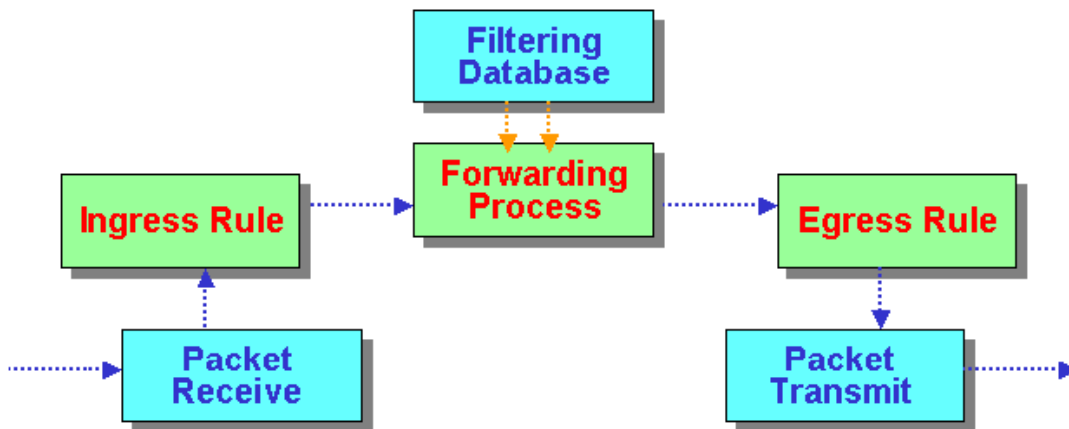
In the IEEE 802.1Q standard, Tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLANs can be created statically by an administrator or dynamically through GVRP. The **VLAN ID** associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).



- **TPID:** TPID has a defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the IEEE 802.1Q / 802.1P tag.
- **Priority:** The first three bits of the TCI define user priority, giving eight (2^3) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VID:** VLAN ID is the identification of the VLAN, which is used by the standard 802.1Q. It is 12 bits long and allows the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.
- Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame.

How 802.1Q VLAN works

Based on the VID information in the tag, the switch forwards and filters frames on the ports. Ports with the same VID can communicate with each other. IEEE 802.1Q VLAN function defines three tasks: Ingress Process, Forwarding Process and Egress Process.



1. Ingress Process:

Each port is capable of passing tagged or untagged frames. Ingress Process identifies if the incoming frames contain a tag, and classifies the incoming frames belonging to a VLAN. Each port has its own Ingress rule. If an Ingress rule accepts tagged frames only, the switch will drop all incoming non-tagged frames on the port. If an Ingress rule accepts all frame types, the switch allow both incoming tagged and untagged frames on the port.

When a tagged frame is received on a port, it carries a tag header that has an explicit VID. Ingress Process directly passes the tagged frame to Forwarding Process.

An untagged frame does not carry any VID to which it belongs. When an untagged frame is received, Ingress Process inserts a tag contained the PVID into the untagged frame. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.



After Ingress Process, all frames have a 4-bytes tag and VID information, and they are transitioned into Forwarding Process.

2. Forwarding Process:

The Forwarding Process makes forwarding decisions on the received frames

based on the Filtering Database. If you want to allow tagged frames to be forwarded to a certain port, this port must be the egress port of this VID. The egress port is an outgoing port for the specified VLAN, that is, frames with a specified VID tag can go through this port. Filtering Database stores and organizes VLAN registration information useful for switching frames to and from switch ports. It consists of static registration entries (Static VLAN or SVLAN table) and dynamic registration entries (Dynamic VLAN or DVLAN table). SVLAN table is manually added and maintained by the administrator. DVLAN table is automatically learned via GVRP protocol, and can't be created or updated by the administrator.

VLAN entries in Filtering Database have the following information:

1. **VID:** VLAN ID
2. **Port:** The switch port number
3. **Ad Control:** Registration administration control. There are 3 types of ad control, including **forbidden** registration, **fixed** registration and **normal** registration.
 - **Forbidden** registration: This port is forbidden to be the egress port of the specified VID.
 - **Fixed** registration: While ad control is fixed registration, it means this is a static registration entry. This port is the egress port of the specified VID (a member port of the specified VLAN). Frames with the specified VID tag can go through this port.
 - **Normal** registration: While ad control is normal registration, it means this is a dynamic registration entry. The forwarding decision is depended on the Dynamic VLAN table.
4. **Egress tag Control:** This information is used for Egress Process. The value may be tagged or untagged. If the value is tagged, outgoing frames on the egress port is tagged. If the value is untagged, the tag will be removed before a frame leaves the egress port.

VID	Port	Ad Control	Tag Control
10	1	Forbidden	Tag
10	2	Fixed	Tag
10	3	Normal	UnTag
20	1	Fixed	Tag
20	5	Fixed	UnTag

Filtering Database

VID	Egress Port
10	1
10	2
20	3

Dynamic VLAN (DVLAN) table

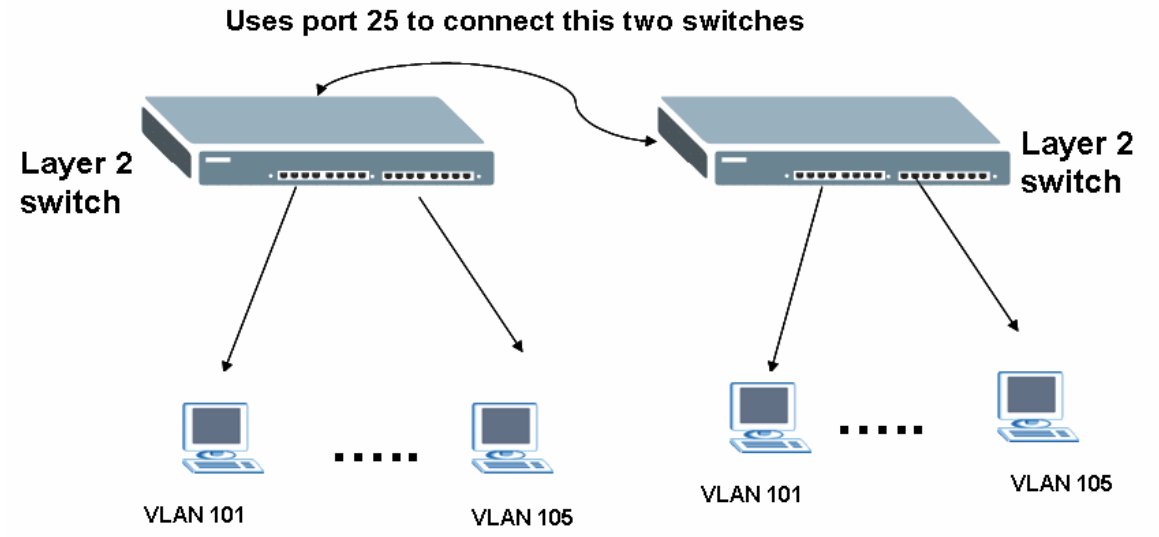
3. Egress Process:

The Egress Process decides if the outgoing frames is to be sent tagged or untagged. The Egress Process refers to the egress tag control information in Filtering Database. If the value is tagged, outgoing frames on the egress port is tagged. If the value is untagged, the tag will be removed before a frame leaves the egress port.

Connecting Two Switches using VLAN

This example shows you how to configure VLAN settings on two layer 2 switches which are connected using the trunk port. There are five VLANs on the first switch and seven VLANs on the second switch. The trunk port is port 25 on both switches. VLANs are configured on the switches but how to configure port 25 as the trunk port on both switches?

The following figure shows this network example.



The VLAN configurations on the two switches are as follows:

VLAN 2, 3, 4, 5, 6, 7, 8 on switch A

VLAN 2, 3, 4, 5, 6 on switch B

1. VLAN Configuration on switch A

Index	VID	2	4	6	8	10	12	14	16	18	20	22	24	26	ElapsedTime	Status
		1	3	5	7	9	11	13	15	17	19	21	23	25		
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	0:01:49	Static
		U	U	U	U	U	U	U	U	U	U	U	U	U		
2	101	U	-	-	-	-	-	-	-	-	-	-	-	-	0:01:49	Static
		U	U	-	-	-	-	-	-	-	-	-	-	-		
3	102	-	U	U	-	-	-	-	-	-	-	-	-	-	0:01:49	Static
		-	-	U	-	-	-	-	-	-	-	-	-	-		
4	103	-	-	-	U	U	-	-	-	-	-	-	-	-	0:01:49	Static
		-	-	-	U	U	-	-	-	-	-	-	-	-		
5	104	-	-	-	-	-	-	-	-	-	-	-	U	-	0:01:49	Static
		-	-	-	-	-	-	-	-	-	-	-	U	-		
6	105	-	-	-	-	-	U	U	-	-	-	-	-	-	0:01:49	Static
		-	-	-	-	-	U	U	-	-	-	-	-	-		
7	106	-	-	-	-	-	-	-	U	-	-	-	-	-	0:01:49	Static
		-	-	-	-	-	-	-	U	U	-	-	-	-		
8	107	-	-	-	-	-	-	-	-	U	U	-	-	-	0:01:48	Static
		-	-	-	-	-	-	-	-	-	U	U	-	-		

2. VLAN Configuration on switch B

Number Of VLAN = 6

Index	VID	Port Number														Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24	26			
1	1	1	3	5	7	9	11	13	15	17	19	21	23	25	0:02:25	Static	
		U	U	U	U	U	U	U	U	U	U	U	U	U			
2	101	U	U	-	-	-	-	-	-	-	-	-	-	-	0:02:25	Static	
		U	U	U	-	-	-	-	-	-	-	-	-	-			
3	102	-	-	U	U	U	-	-	-	-	-	-	-	-	0:02:25	Static	
		-	-	-	U	U	-	-	-	-	-	-	-	-			
4	103	-	-	-	-	-	U	U	-	-	-	-	-	-	0:02:25	Static	
		-	-	-	-	-	U	U	-	-	-	-	-	-			
5	104	-	-	-	-	-	-	-	U	U	-	-	-	-	0:02:25	Static	
		-	-	-	-	-	-	-	U	U	-	-	-	-			
6	105	-	-	-	-	-	-	-	-	-	U	U	-	-	0:02:25	Static	
		-	-	-	-	-	-	-	-	-	U	U	U	-			

Answer:

 In switch A, add port 25 in each VLAN
 VID:101 (port 1,2,3,"25 TAG")
 VID:102 (port 4,5,6,,"25 TAG")
 VID:103 (port 7,8,9,10,"25 TAG")
 VID:104 (port 23,24,"25 TAG")
 VID:105 (port 11,12,13,14,"25 TAG")
 VID:106 (port 15,16,17,"25 TAG")
 VID:107 (port 18,19,20,21,"25 TAG")

In switch B, add port 25 in each VLAN
 VID:101 (port 1,2,3,,4,"25 TAG")
 VID:102 (port 6,7,8,9,10,"25 TAG")
 VID:103 (port 11,12,13,14,"25 TAG")
 VID:104 (port 15,16,17,18,"25 TAG")
 VID:105 (port 19,20,21,23,22"25 TAG)

Clients in the same VLAN on both switches can communicate with each other.

PVID:

Set PVID on switch A

- Port 1, 2, 3 : **101**
- Port 4, 5, 6 : **102**
- Port 7, 8, 9, 10 : **103**
- Port 23, 24: **104**
- Port 11, 12, 13, 14: **105**
- Port 15, 16, 17: **106**
- Port 18, 19, 20, 21: **107**
- port 25: PVID=any

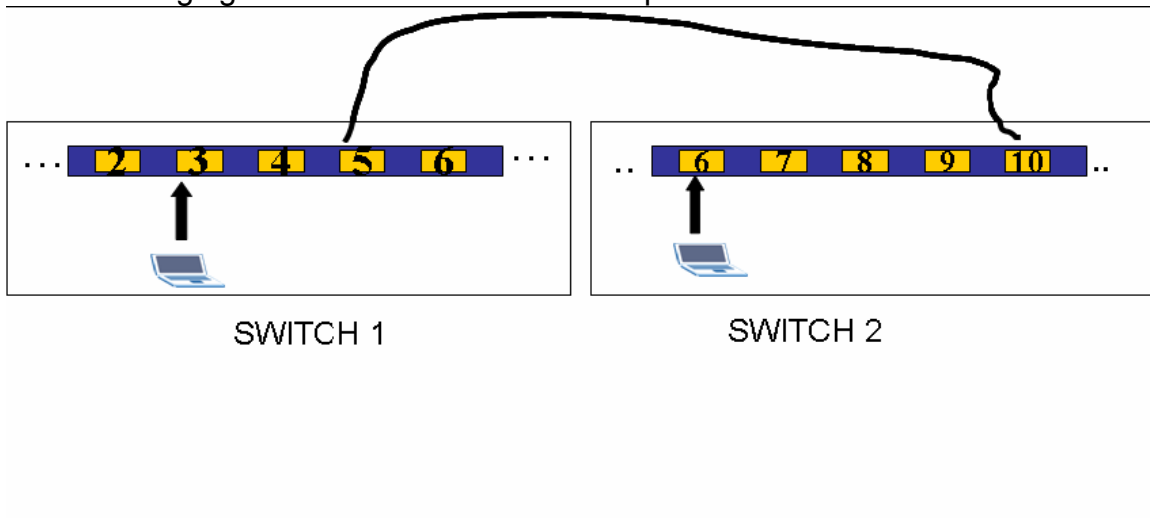
🕒 Set PVID on switch B:

- Port 1, 2, 3, 4 : **101**

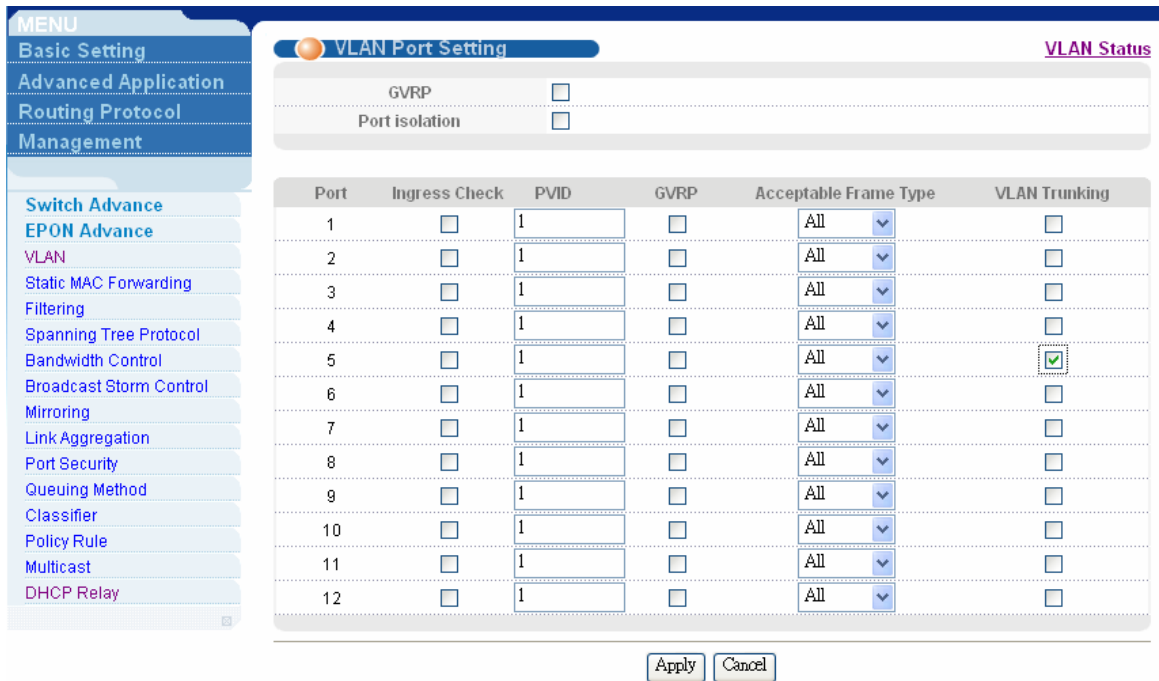
Port 6, 7, 8, 9, 10, : **102**
Port 11, 12, 13, 14, : **103**
Port 15, 16, 17, 18: **104**
Port 19, 20, 21, 22, 23: **105**
Port 25:PVID=any

Setting up VLAN Trunking

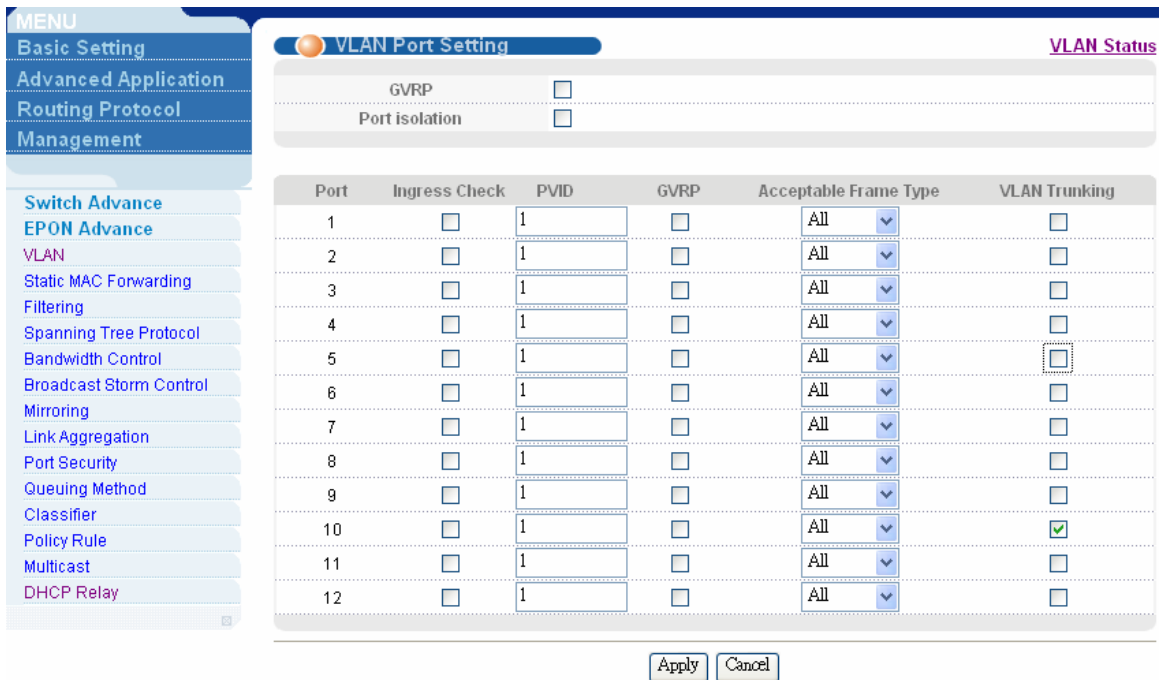
With the benefit of deploying VLAN trunking, you can connect two switches through a port that is configured as the VLAN trunking port. VLAN tagged frames from PC1 connected to switch 1 can reach PC 2 connected to switch 2 through the VLAN trunking port. In this example, port 5 on switch 1 is configured as the VLAN Trunking port while on switch 2, port 10 is the VLAN Trunking port. The following figure shows the network example.



The configuration screen for switch 1 is shown as follows.



The configuration screen for switch 2 is shown as follows.

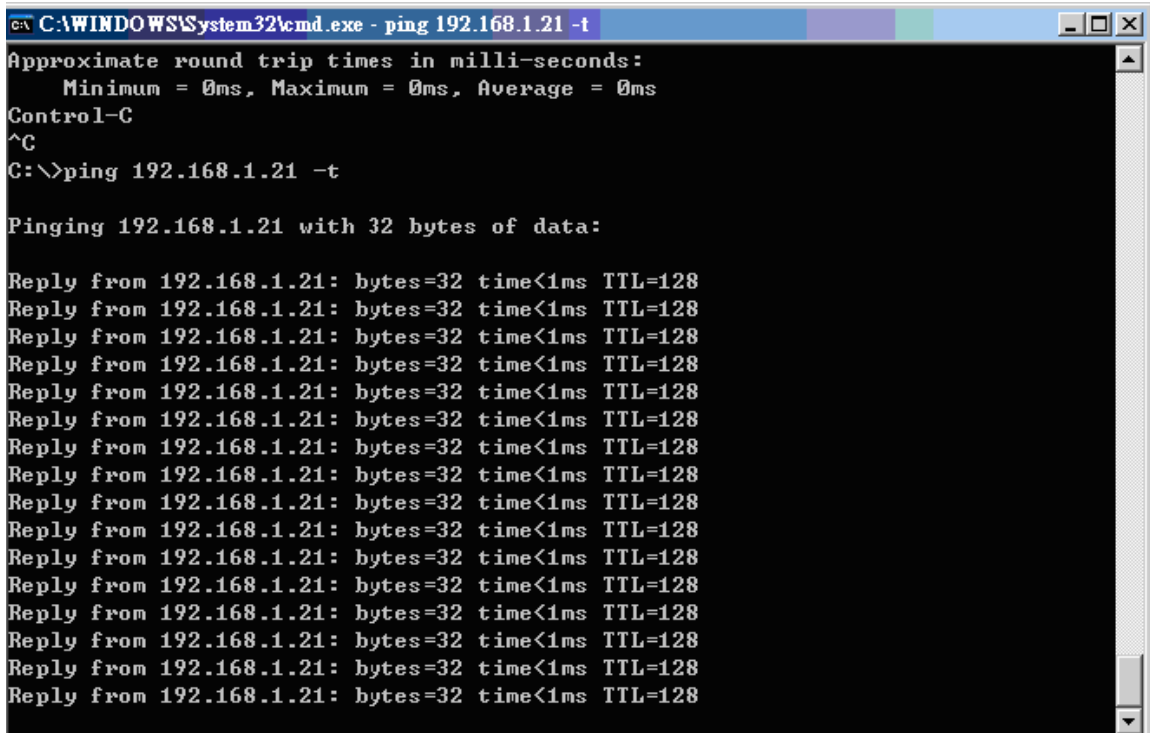


In the switch 1, we set port 2 as VLAN 2 untag
 In the switch 2, we set port 6 as VLAN 2 untag.

The switch 1 IP address: 192.168.1.31

The switch 2 IP address: 192.168.1.21

After the configuration, you can see that PC 1 connected to port 2 on switch 1 can still ping PC 2 connected to port 6 on switch 2.



```
C:\WINDOWS\System32\cmd.exe - ping 192.168.1.21 -t
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>ping 192.168.1.21 -t

Pinging 192.168.1.21 with 32 bytes of data:

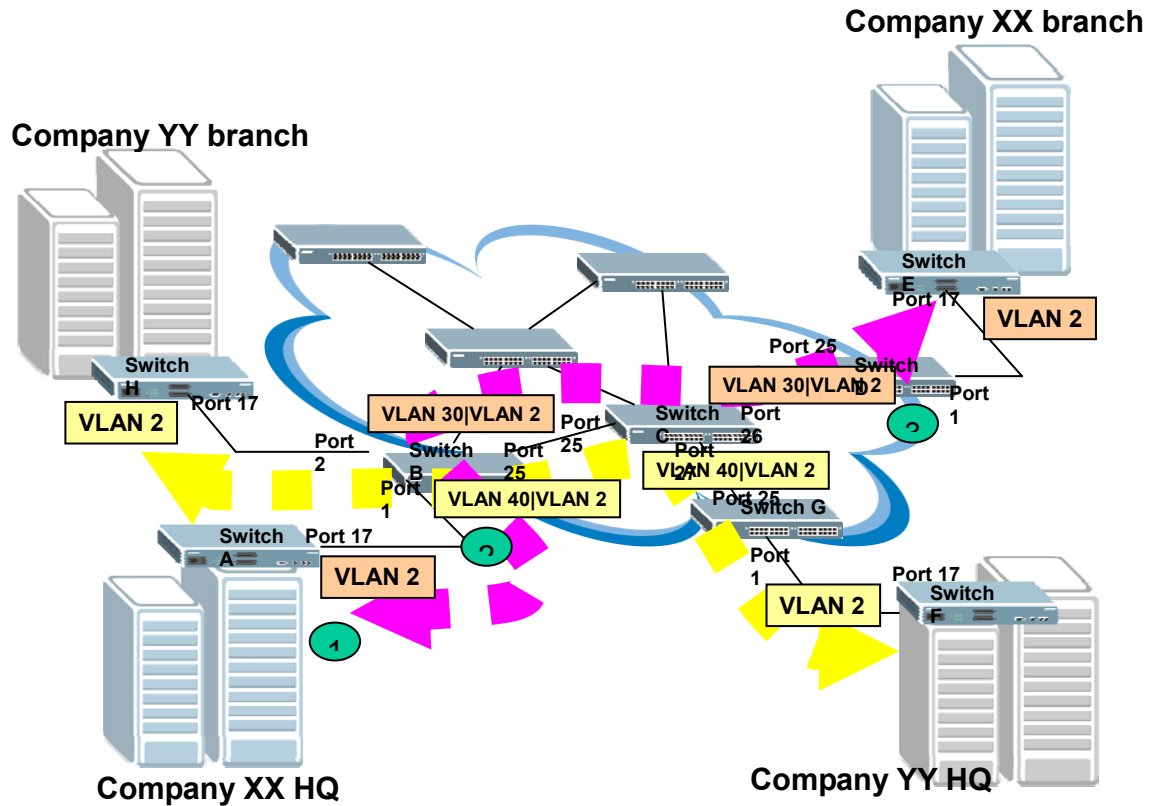
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
```

VLAN Stacking Overview

VLAN stacking allows a carrier to offer multiple virtual LANs over a single circuit. In essence, the carrier creates an Ethernet VPN to tunnel customer VLANs across its WAN. Thus it helps to avoid name conflicts among customers of multiple service providers who connect to the same carrier.

VLAN stacking works by assigning two VLAN IDs to each frame header. One is a "backbone" VLAN ID used by the service provider, the other (up to 4,096 unique 802.1Q VLAN tags) is used by the customers.

The following figure shows a network example.



In this example, company XX and company YY both subscribe to the same ISP for Internet service. Both companies have an internal VLAN group with VID 1. In order to prevent VLAN-tagged packets between these two companies from transmitting to each other's network, VLAN stacking is implemented in the ISP's network. The ISP assigns a service provider VID for each company- company XX is assigned an SP VID of 30 and company YY is assigned an SP VID of 40.

The following shows the packet flow between **Company XX HQ and its branch office.**

Company XX HQ → Switch A → Switch B → Switch C → Switch D → Company XX Branch Office.

In this case, VLAN Stacking is enabled on access ports 11 and 12 on Switch B. An SP tag is appended for ingress traffic and the appended SP tagged is removed during egress. VLAN Stacking is also enabled on the tunnel port on switches B (port 10), C, and D. Static VLAN Tx tagging must be DISABLED for the port which is set as a Normal or Access Port. Static VLAN Tx Tagging MUST be enabled on a port set as the Tunnel port.

The following shows the packet flow between **Company YY HQ and its branch office.**

Company YY HQ → Switch F → Switch G → Switch C → Switch B → Switch H

→ **Company YY Branch Office.**

VLAN Stacking is enabled on access port 10 on Switch G. An SP tag is appended on the ingress traffic and the SP tag is removed during egress. VLAN Stacking is enabled on a Tunnel port on switches G (port 9), C, and B.

From Switch A to Switch H

Switch A:

Enabled VLAN, VLAN1 and egress tagging on Port 17
Port 1 is connected to another access switch in a building.
Port 17 is connected to port 11 on Switch B

Switch B:

Enabled VLAN Stacking and STP
Port 1 is connected to port 17 on Switch A
Port 2 is connected to port 17 on Switch H
Port 25 is connected to port 25 Switch C

Switch C:

Enabled VLAN Stacking and STP
Port 27 is connected to port 25 on Switch G
Port 26 is connected to port 25 on Switch D
Port 25 is connected to port 25 on Switch B

Switch D:

Enabled VLAN Stacking
Port 1 is connected to port 17 on Switch E
Port 25 is connected to port 26 on Switch C

Switch E:

Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 1 on Switch D

Switch F:

Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 1 on Switch G

Switch G:

Enabled VLAN Stacking
Port 1 is connected to port 17 on Switch F
Port 25 is connected to port 27 on Switch C

Switch H:

Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 2 on Switch B

Configuring Switch A, E, F and H Using the Web Configurator

On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to

make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.

*By default all the ports in VLAN 1 are untagged during Egress.

Configuring Switch B Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter <http://192.168.0.1> as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

ZyXEL Status Logout Help

MENU
Basic Setting
Advanced Application
Routing Protocol
Management

Status
System Up Time : 29:10:27

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Ti
1	100M/F	FORWARDING	Disabled	6199	2356	0	0.0	0.0	2:13
2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00

Poll Interval(s) 40 Set Interval Stop

Port ALL Clear Counter

© Copyright 1995-2004 by ZyXEL Communica

7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status VLAN Port Setting Static VLAN

The Number Of VLAN = 1

Index	VID	Port Number														Elapsed Time	Sta
		2	4	6	8	10	12	14	16	18	20	22	24	26	28		
1	1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	0:00:20	Sta
		U	U	U	U	U	U	U	U	U	U	U	U	U	U		

Poll Interval(s) 40 Set Interval Stop

Change Pages Previous Page Next Page

© Copyright 1995-2004 by ZyXEL Communio

8. Create a VLAN with a VID of 30. Select **Fixed** and un-select **Tx Tagging** for port 1. For port 25, select both **Fixed** and **Tx Tagging**.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

Static VLAN VLAN Status

ACTIVE

Name VLAN30

VLAN Group ID 30

Port	Control	Tagging
1	Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden <input type="radio"/>	<input type="checkbox"/> Tx Tagging
2	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
3	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
4	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
5	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
6	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
7	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
8	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
9	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
10	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
11	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
12	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
13	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
14	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging
15	Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/>	<input checked="" type="checkbox"/> Tx Tagging

© Copyright 1995-2004 by ZyXEL Communio

9. Create another VLAN with a VID of 40. Select **Fixed** and un-select **Tx Tagging**

for port 2.

10. For port 12, select both **Fixed** and **Tx Tagging**. The **VLAN Status** screen should display as shown.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status
 The Number Of VLAN = 3

[VLAN Port Setting](#) [Static VLAN](#)

Index	VID	Port Number																												Elapsed Time	Stat
		2	4	6	8	10	12	14	16	18	20	22	24	26	28	1	3	5	7	9	11	13	15	17	19	21	23	25	27		
1	1	U	U	U	U	U	U	U	U	J	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:35	Sta	
		U	U	U	U	U	U	U	U	J	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U			
2	30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:00:34	Sta	
		U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	T	-				
3	40	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:00:34	Sta	
		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	T	-				

Poll Interval(s)

Change Pages

© Copyright 1995-2004 by ZyXEL Communica

11. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.

The screenshot shows the ZyXEL web configurator interface for VLAN Stacking. The 'Active' checkbox is checked, and the SPVID is set to 0x8100 (Hex). Below this, a table lists the configuration for ports 1 through 12. Ports 1 and 2 are highlighted with a red box, indicating they are the access ports for the VLAN stacking configuration.

Port	Role	SPVID	Priority
1	Access Port	30	0
2	Access Port	40	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0
9	Access Port	1	0
10	Access Port	1	0
11	Access Port	1	0
12	Access Port	1	0

13. To enable VLAN stacking, select **Active**. Set ports 1 and 2 as the access port and enter the corresponding SPVIDs as shown in the figure above.

25 Tunnel Port 1 0

14. Set port 25 as the “Tunnel Port” and leave the SPVID field to the default setting.

15. You have finished setting Switch B for VLAN stacking for this network example.

Configuring Switch C Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter <http://192.168.0.1> as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

Status
 System Up Time : 29:10:27

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Ti
1	100MF	FORWARDING	Disabled	6199	2356	0	0.0	0.0	2:13
2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00

Poll Interval(s)

Port

© Copyright 1995-2004 by ZyXEL Communica

7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status VLAN Port Setting **Static VLAN**
 The Number Of VLAN = 1

Index	VID	Port Number																Elapsed Time	Sta
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:20	Sta	
		U	U	U	U	U	U	U	U	U	U	U	U	U	U				

Poll Interval(s)

Change Pages

© Copyright 1995-2004 by ZyXEL Communica

Follow the steps in the previous section to configure VLANs 30 and 40 of which

ports 9, 10 and 11 are members. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.

The screenshot shows the ZyXEL web interface for VLAN Status. The navigation menu on the left includes: MENU, Basic Setting, Advanced Application, Routing Protocol, Management, VLAN, Static MAC Forwarding, Filtering, Spanning Tree Protocol, Bandwidth Control, Broadcast Storm Control, Mirroring, Link Aggregation, Port Authentication, Port Security, Access Control, Queuing Method, Classifier, Policy Rule, VLAN Stacking, Multicast, DHCP Relay, and DiffServ.

The main content area displays the following information:

- VLAN Status** (The Number Of VLAN = 3)
- Links for [VLAN Port Setting](#) and [Static VLAN](#).
- A table showing VLAN configurations:

Index	VID	Port Number																Elapsed Time	Stat
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	0:00:04	Sta		
		U	U	U	U	U	U	U	U	U	U	U	U	U	U				
2	30	-	-	-	-	-	-	-	-	-	-	-	-	T	-	0:00:04	Sta		
		-	-	-	-	-	-	-	-	-	-	-	-	T	T				
3	40	-	-	-	-	-	-	-	-	-	-	-	-	T	-	0:00:04	Sta		
		-	-	-	-	-	-	-	-	-	-	-	-	T	T				

At the bottom of the screen, there are controls for Poll Interval(s) set to 40, with buttons for Set Interval, Stop, Previous Page, and Next Page.

© Copyright 1995-2004 by ZyXEL Communic

11. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.

ZyXEL Status Logout Help

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management

VLAN Stacking

Active

SP VID Others (Hex)

Port	Role	SPVID	Priority
1	Access Port	1	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0
9	Access Port	1	0
10	Access Port	1	0
11	Access Port	1	0
12	Access Port	1	0

© Copyright 1995-2004 by ZyXEL Communica

Set ports 25, 26 and 27 as the “Tunnel Ports” and leave the SPVID fields to the default settings.

25	Tunnel Port	1	0
26	Tunnel Port	1	0
27	Tunnel Port	1	0

9. You have finished setting Switch C for VLAN stacking for this network example.

Configuring Switch D Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter <http://192.168.0.1> as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

Status
 System Up Time : 29:10:27

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Ti
1	100MF	FORWARDING	Disabled	6199	2356	0	0.0	0.0	2:13
2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00

Poll Interval(s) 40 Set Interval Stop
 Port ALL Clear Counter

© Copyright 1995-2004 by ZyXEL Communio

7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status
 The Number Of VLAN = 1

VLAN Port Setting Static VLAN

Index	VID	Port Number																Elapsed Time	Sta
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:20	Sta
		U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U		

Poll Interval(s) 40 Set Interval Stop
 Change Pages Previous Page Next Page

© Copyright 1995-2004 by ZyXEL Communio

Follow the steps in the previous section to configure VLAN 30 of which ports 1 and 12 are members. Since port 1 is an Access Port, un-select the **Tx Tagging** field. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.

The screenshot shows the ZyXEL web interface for VLAN configuration. The left navigation menu includes: MENU, Basic Setting, Advanced Application, Routing Protocol, Management, VLAN, Static MAC Forwarding, Filtering, Spanning Tree Protocol, Bandwidth Control, Broadcast Storm Control, Mirroring, Link Aggregation, Port Authentication, Port Security, Access Control, Queuing Method, Classifier, Policy Rule, VLAN Stacking, Multicast, DHCP Relay, and DiffServ.

The main content area displays 'VLAN Status' with 'The Number Of VLAN = 2'. It includes links for 'VLAN Port Setting' and 'Static VLAN'. A table shows the status of two VLANs:

Index	VID	Port Number														Elapsed Time	Sta
		2	4	6	8	10	12	14	16	18	20	22	24	26	28		
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:06	Sta
		U	U	U	U	U	U	U	U	U	U	U	U	U	U		
2	30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:00:06	Sta
		U	-	-	-	-	-	-	-	-	-	-	-	T	-		

Below the table, there are control elements: 'Poll Interval(s)' set to 40, 'Set Interval' and 'Stop' buttons, and 'Change Pages' with 'Previous Page' and 'Next Page' buttons.

© Copyright 1995-2004 by ZyXEL Communica

8. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.

ZyXEL Status Logout Help

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management

VLAN Stacking

Active

SP TPID 0x8100 Others (Hex)

Port	Role	SPVID	Priority
1	Access Port	30	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0
9	Access Port	1	0
10	Access Port	1	0
11	Access Port	1	0
12	Access Port	1	0

© Copyright 1999-2004 by ZyXEL Communica

To enable VLAN stacking, select **Active**. Set port 25 as the tunnel port and leave the SPVID field to the default settings.

25	Tunnel Port	1	0
----	-------------	---	---

9. You have finished setting Switch D for VLAN stacking for this network example.

Configuring Switch G Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter <http://192.168.0.1> as the URL.
5. A login screen displays. Enter "admin" (the default) as the username and "1234" (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

Status
 System Up Time : 29:10:27

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Ti
1	100MF	FORWARDING	Disabled	6199	2356	0	0.0	0.0	2:13
2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00

Poll Interval(s) 40 Set Interval Stop
 Port ALL Clear Counter

© Copyright 1995-2004 by ZyXEL Communio

7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status
 The Number Of VLAN = 1

VLAN Port Setting Static VLAN

Index	VID	Port Number														Elapsed Time	Sta		
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:20	Sta

Poll Interval(s) 40 Set Interval Stop
 Change Pages Previous Page Next Page

© Copyright 1995-2004 by ZyXEL Communio

Follow the steps in the previous section to configure VLAN 40 of which ports 1 and 12 are members. Since port 12 is a TunnelPort, select the **Tx Tagging** field. For the Access Port (port 1), un-select the **Tx Tagging** field. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management
 VLAN
 Static MAC Forwarding
 Filtering
 Spanning Tree Protocol
 Bandwidth Control
 Broadcast Storm Control
 Mirroring
 Link Aggregation
 Port Authentication
 Port Security
 Access Control
 Queuing Method
 Classifier
 Policy Rule
 VLAN Stacking
 Multicast
 DHCP Relay
 DiffServ

VLAN Status VLAN Port Setting Static VLAN
 The Number Of VLAN = 2

Index	VID	Port Number																Elapsed Time	Sta
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:10	Sta		
		U	U	U	U	U	U	U	U	U	U	U	U	U	U				
2	40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:00:09	Sta		
		U	-	-	-	-	-	-	-	-	-	-	-	T	-				

Poll Interval(s) Set Interval Stop
 Change Pages Previous Page Next Page

© Copyright 1996-2004 by ZyXEL Commun

8. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.

ZyXEL Status Logout Help

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management
- VLAN
 - Static MAC Forwarding
 - Filtering
 - Spanning Tree Protocol
 - Bandwidth Control
 - Broadcast Storm Control
 - Mirroring
 - Link Aggregation
 - Port Authentication
 - Port Security
 - Access Control
 - Queueing Method
 - Classifier
 - Policy Rule
 - VLAN Stacking
 - Multicast
 - DHCP Relay
 - DiffServ

VLAN Stacking

Active

SP VID: 0x8100 (Hex) Others (Hex)

Port	Role	SPVID	Priority
1	Access Port	40	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0
9	Access Port	1	0
10	Access Port	1	0
11	Access Port	1	0
12	Access Port	1	0

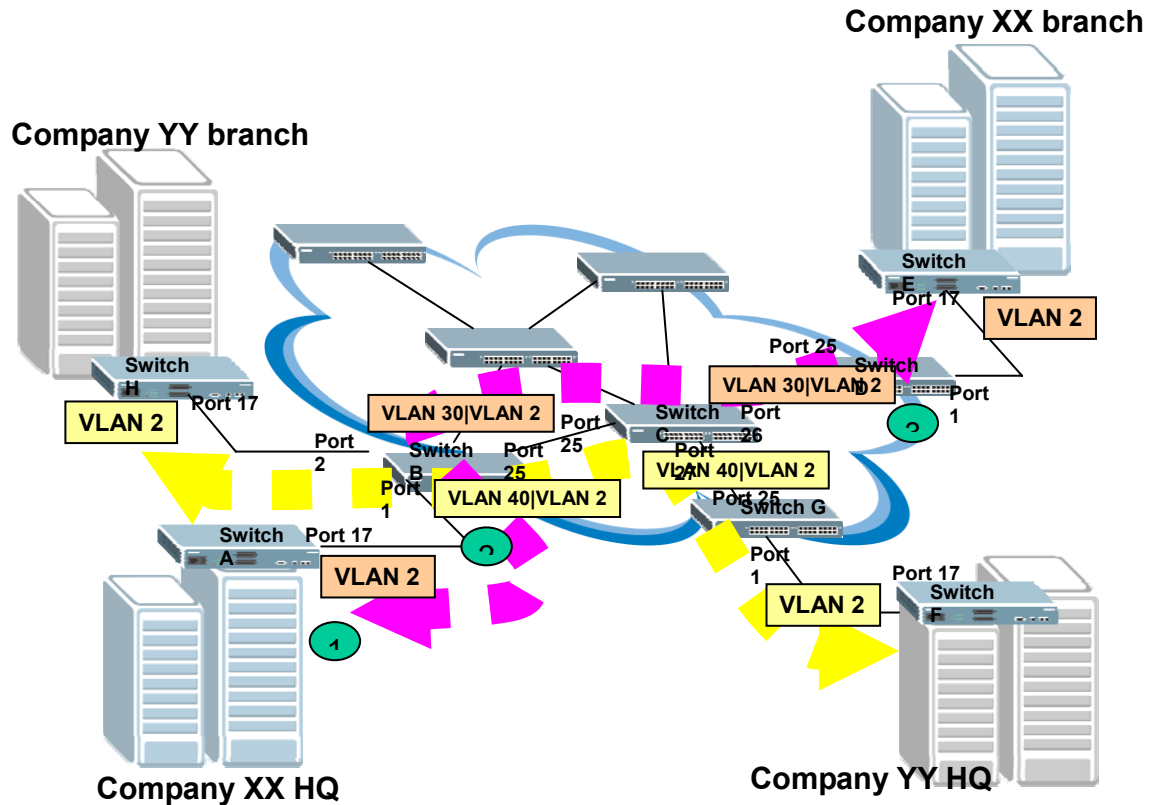
© Copyright 1995-2004 by ZyXEL Communio

To enable VLAN stacking, select **Active**. Set port 25 as the tunnel port and leave the SPVID field to the default settings.

25 Tunnel Port 1 0

9. You have finished setting Switch G for VLAN stacking for this network example.

Network Scenario



Configuring Switches A, E, F and H Using the CLI

On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.

*By default all the ports in VLAN 1 are untagged during Egress.

1. On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.

*By default all the ports in VLAN 1 are untagged during Egress.

2. Connect your computer to the console port on the switch.
3. Open a Terminal program (for example Hyper Terminal in Windows)
4. Configure the console port settings as shown next.

Bps: 9600

Data bits: 8

Parity: None

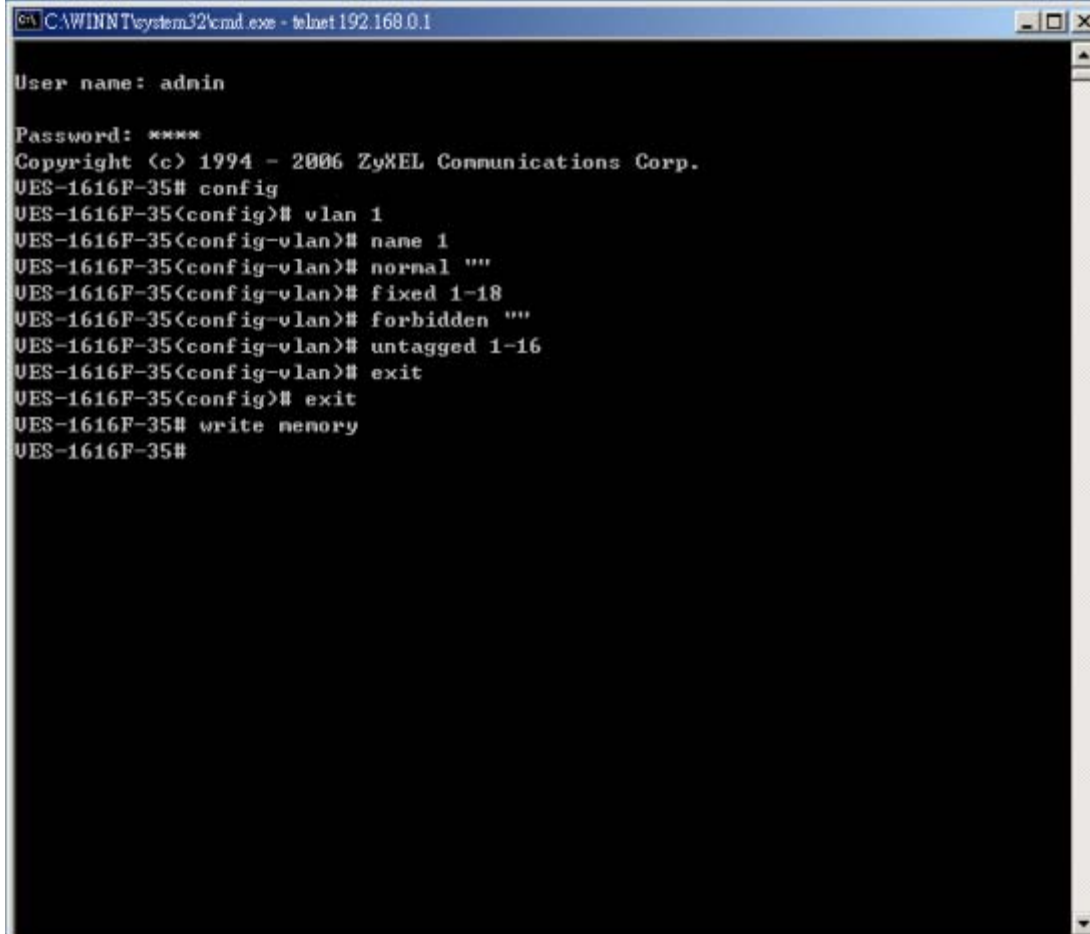
Stop bits: 1

Flow control: None:

5. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).

6. Enter “config” to go into the configuration mode.

7. Enter the commands as shown in the screen to configure VLAN 1 on switches A, E, F and H for this network scenario. (Port 17 will be tagged during Egress)

A screenshot of a terminal window titled "CAWINNT\system32\cmd.exe - telnet 192.168.0.1". The terminal shows the following text:

```
User name: admin
Password: ****
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
UES-1616F-35# config
UES-1616F-35(config)# vlan 1
UES-1616F-35(config-vlan)# name 1
UES-1616F-35(config-vlan)# normal ""
UES-1616F-35(config-vlan)# fixed 1-18
UES-1616F-35(config-vlan)# forbidden ""
UES-1616F-35(config-vlan)# untagged 1-16
UES-1616F-35(config-vlan)# exit
UES-1616F-35(config)# exit
UES-1616F-35# write memory
UES-1616F-35#
```

8. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch B Using the CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next.

Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:

4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
5. Enter “config” to go into the configuration mode.
6. Enter the commands as shown in the screen to configure VLAN Stacking on switch B for this network scenario.

```
vlan 30
name VLAN30
normal 2-24,26-28
fixed 1,25
forbidden ""
untagged 1
exit
```

```
vlan 40
name VLAN40
normal 1,3-24,26-28
fixed 2,25
forbidden ""
untagged 2
exit
```

```
interface port-channel 1
vlan-stacking SPVID 30
exit
```

```
interface port-channel 2
vlan-stacking SPVID 40
exit
```

```
interface port-channel 25
vlan-stacking role tunnel
exit
```

```
vlan-stacking
```

7. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch C via CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next

Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:

4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).

5. Enter “config” to go into the configuration mode.
 6. Enter the commands as shown in the screen to configure VLAN Stacking on switch C for this network scenario.
-

```
vlan 30
name VLAN30
normal 1-24,28
fixed 25-27
forbidden ""
untagged ""
exit

vlan 40
name VLAN40
normal 1-24,28
fixed 25-27
forbidden ""
untagged ""
exit

interface port-channel 25
vlan-stacking role tunnel
exit

interface port channel 26
vlan-stacking role tunnel
exit

interface port-channel 27
vlan-stacking role tunnel
exit

vlan-stacking
```

7. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch D Using the CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
5. Enter “config” to go into the configuration mode.
6. Enter the commands as shown in the screen to configure VLAN Stacking on switch D for this network scenario.

```
vlan 40
name VLAN40
normal 2-24,26-28
fixed 1,25
forbidden ""
untagged 1
exit

interface port-channel 1
vlan-stacking SPVID 40
exit

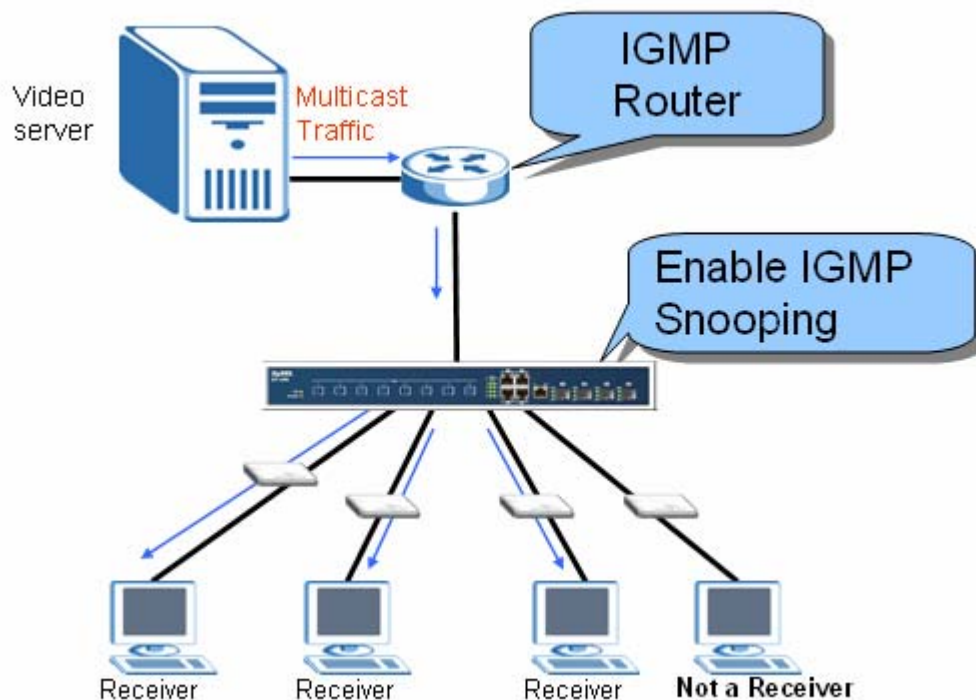
interface port-channel 25
vlan-stacking role tunnel
exit

vlan-stacking
```

6. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

IP Multicasting

Configuring IGMP snooping in your switch

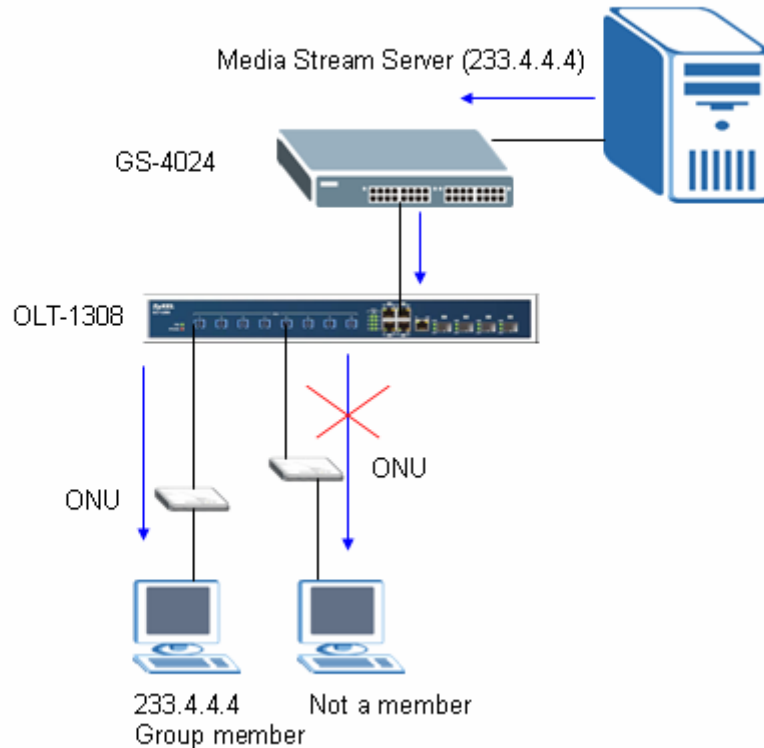


IGMP snooping is designed for scenarios with multicast traffic. It operates on the underlying IGMP mechanism where a layer two switch passively listens to the IGMP Query, Report and Leave (IGMP version 2) packets transmitted between the IGMP router and clients and collects passing IGMP messages. After that, the switch records the message's group registration information, and configures the multicasting information accordingly. If the multicast group information is unknown (not recorded on the switch), the switch discards that multicast traffic. Only the registered clients that join the group will receive multicast stream from the IGMP router. Thus this significantly reduces the multicast traffic forwarded down to the clients. Another advantage of IGMP snooping is to allow the intermediate switch to learn

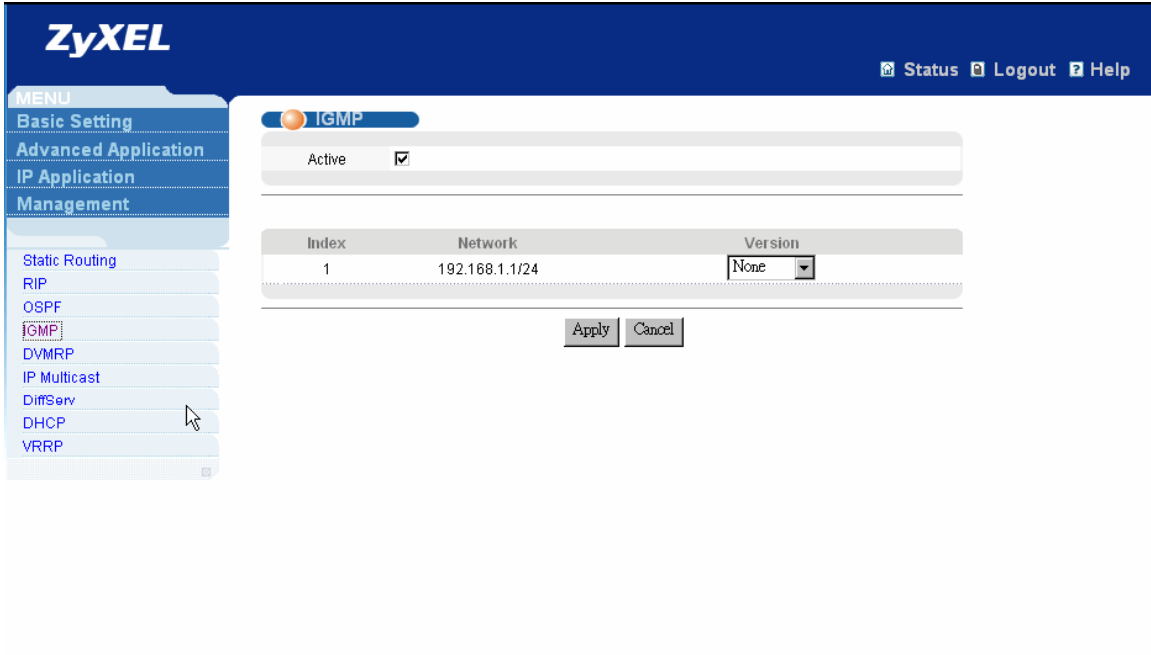
multicast group information without manually configuring switches.

Configuration of IGMP snooping by web

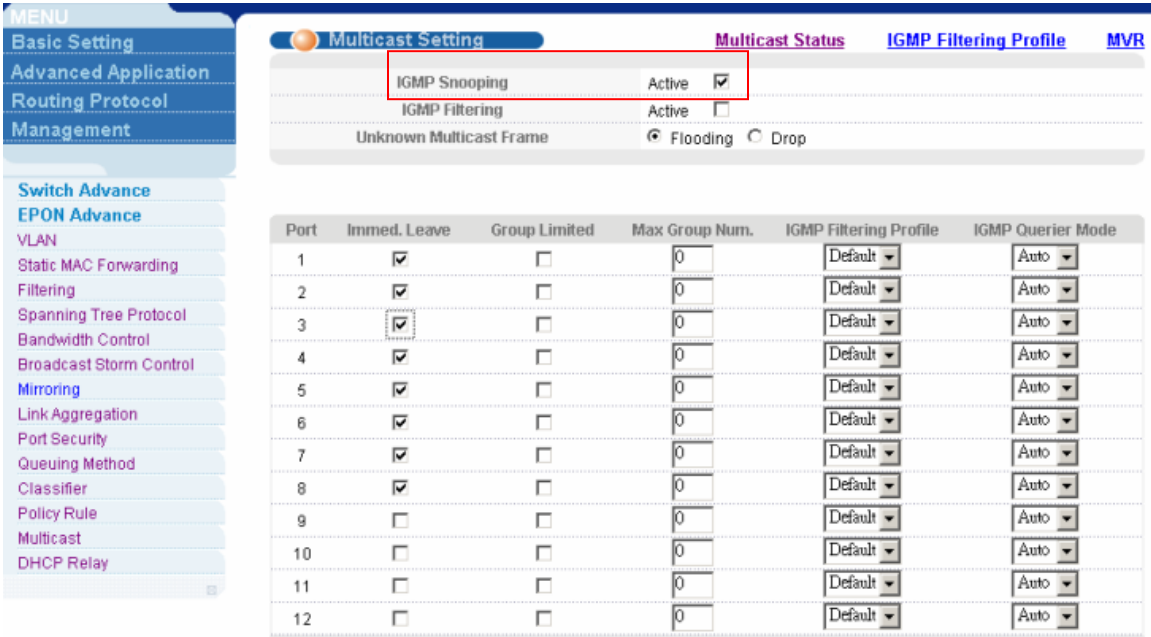
In this example, we enable the IGMP function on the GS-4024 (an IGMP router) to connect to a multimedia server. Also, we enable IGMP snooping function on the OLT-1308 the multimedia clients are connect to.



1. In GS-4024, click the **IP Application**, select **IGMP** where, IGMP function can be enabled and we can select either IGMP-v1 or IGMP-v2.



2. In the VDSL Switch, click **Advanced Application > Multicast > Multicast Setting** and then **IGMP Snooping** where we can enable IGMP snooping function with WEB-GUI.



Configuration of IGMP and IGMP snooping by CLI

1. Enable IGMP function in GS-4024
 In the configure mode
 GS-4024(config)# **router igmp**

2. Enable IGMP snooping in VDSL switch

In the configure mode of CLI,

OLT-1308(config)# **igmp-snooping**

3. Display the IGMP Status

In the exec mode of CLI

OLT-1308# **show multicast**

4. Display the IGMP snooping Status

In the exec mode of CLI

OLT-1308# **show igmp-snooping**

Note: One thing needs to be mentioned is that in the IGMP router, we do not need to enable IGMP snooping function.

Overview of MVR

MVR refers to Multicast VLAN Registration that enables a media server to transmit multicast stream in a single multicast VLAN while clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intending to join or leave the multicast group simply send the IGMP Join/leave message to a receiver port. The receiver port belonging to one of the multicast groups can receive multicast stream from media server. In the Figure 1, without support of MVR, the Multicast stream from the media server and the subscriber must reside in the same VLAN. For each VLAN, A media server is required to transmit multicast stream once and totally, media server transmits 6 times. In the Figure 2, on the contrary, with MVR, a media server is required to transmit multicast traffic to clients in different VLANs at once.

Figure 1

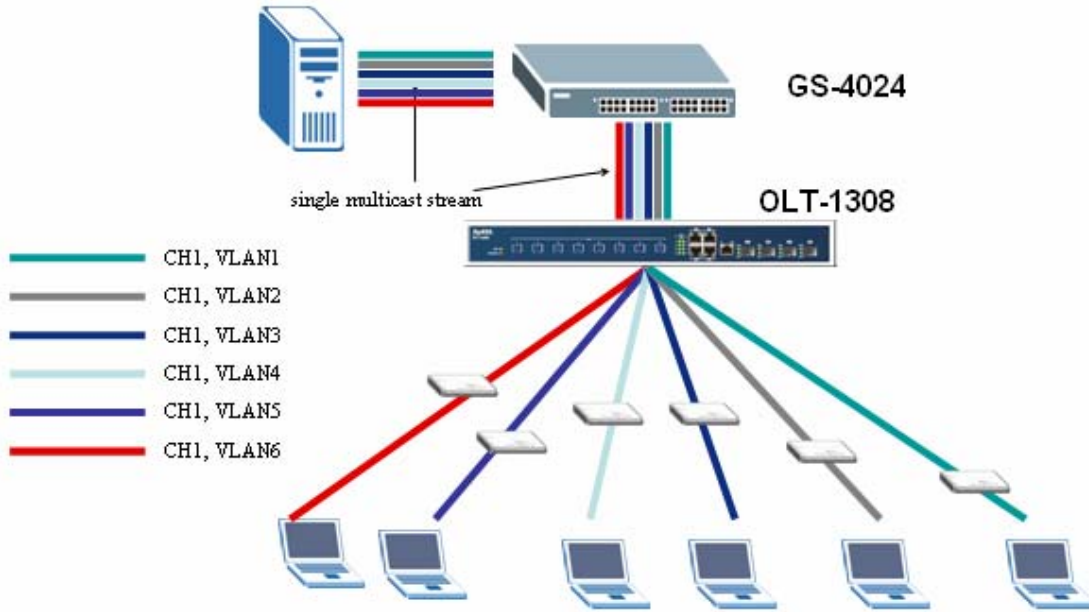
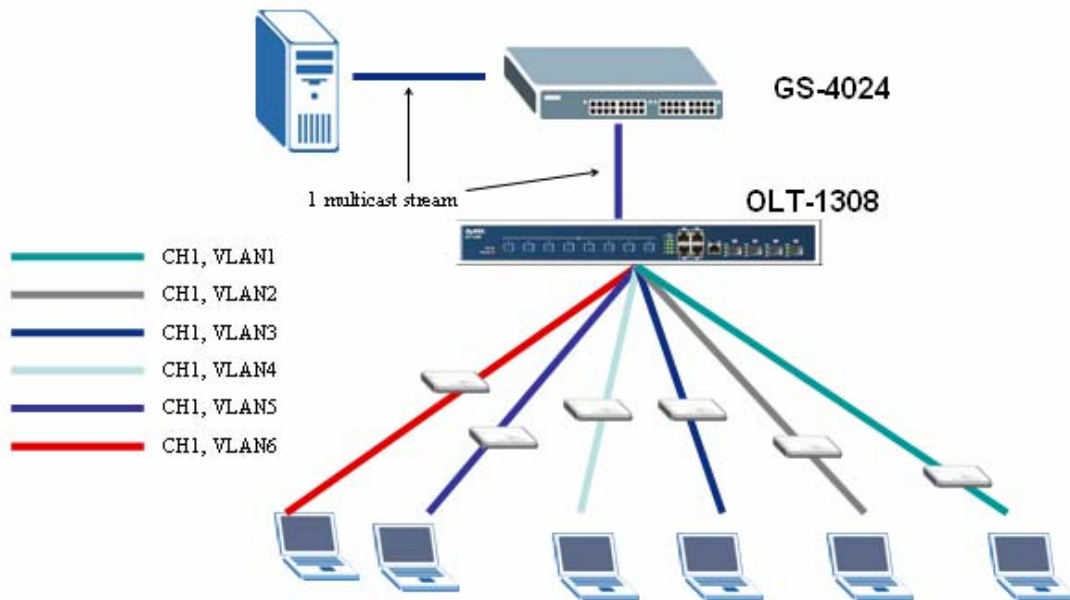


Figure 2



MVR Mode

- **Dynamic Mode**

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source port. Multicast router knows which multicast groups exist on which interface dynamically.

- **Compatible mode**

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router. Multicast router must be statically configured.

Operation Mode

- **Join Operation**

A subscriber sends an IGMP report message to the switch to join the appropriate multicast. It tests whether the IGMP report matches the switch configured multicast MAC address. If matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the MVLAN

- **Leave Operation**

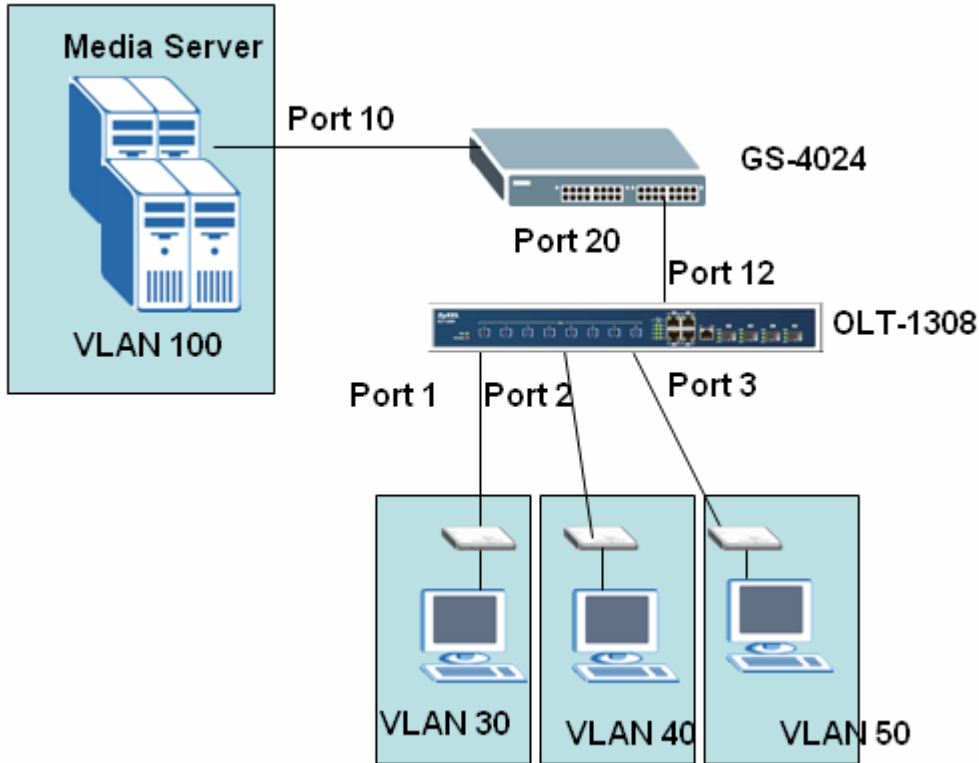
Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch eliminates this receiver port.

- **Immediate Leave Operation**

Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait for the switch CPU to send an IGMP group-specific query through the receiver port VLAN. The switch will immediately eliminate this receiver port.

Scenario of MVR

In the following section, we will provide an example to illustrate how to configure MVR. In this scenario, the main job of media server is to transmit the media stream via port 10 to GS-4024. The multicast traffic flowing into the GS-4024 will be tagged with PVID=100. In the OLT-1308, we enable the MVR function to allocate the multicast traffic from GS-4024 to separate VLAN hosts.



Configuration via Web

1. We need to create a VLAN for multicast traffic in GS-4024. In **GS-4024**, click the **Advanced Application** and then select the **VLAN**. In the VLAN Configuration, create a new VLAN 100.

Figure 4 VLAN Configuration

VLAN Status		VLAN Port Setting														Static VLAN	
The Number Of VLAN = 2																	
Index	VID	Port Number														Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24	26	S2		
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:00:52	Static
2	100	-	-	-	-	U	-	-	-	-	T	-	-	-	-	0:00:51	Static

2. In the **GS-4024**, click the **Advanced Application** and then select the **VLAN**. In the **VLAN port Setting**, set the PVID of the port 10 to 100 as the multicast traffic that flows from media server to port 10 must be tagged with PVID=100 to communicate with the port in MVR VLAN 100 in OLT-1308.

VLAN Port Setting
VLAN Status

GVRP

Port isolation

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	100	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

3. We need to create separate VLANs for different clients. In OLT-1308, in the **Advanced Application > Multicast > Multicast setting** configure the MVR VLAN=100. Define port 1, port 2 and port 3 as the receiver ports for forwarding the multicast stream to the clients in different VLANs; set port 17 as a source port to receive traffic from the media server. Also, select mode as *dynamic* mode. The switch sends IGMP report message to multicast router through its source port.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management
- Switch Advance
- EPON Advance
- VLAN
- Static MAC Forwarding
- Filtering
- Spanning Tree Protocol
- Bandwidth Control
- Broadcast Storm Control
- Mirroring
- Link Aggregation
- Port Security
- Queuing Method
- Classifier
- Policy Rule
- Multicast
- DHCP Relay

Multicast VLAN ID:

Mode: Dynamic Compatible

Port	Source Port	Receiver Port	None	Tagging
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
9	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
10	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
11	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
12	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

4. In **OLT-1308**, after the MVR configuration, click the **Advanced Application, VLAN Status** and check whether there is the new VLAN 100 added in the VLAN list. We also create three separate VLANs, 30, 40, 50 and assign their PVID as 30, 40 and 50 respectively.

Index	VID	Port Number						Elapsed Time	Status
		2	4	6	8	10	12		
		1	3	5	7	9	11		
1	1	U	U	U	U	U	U	0:00:03	Static
		U	U	U	U	U	U		
2	30	-	-	-	-	-	T	0:00:03	Static
		U	-	-	-	-	-		
3	40	U	-	-	-	-	T	0:00:03	Static
		-	-	-	-	-	-		
4	50	-	-	-	-	-	T	0:00:03	Static
		-	U	-	-	-	-		
5	100	U	-	-	-	-	T	0:00:03	Other
		U	U	-	-	-	-		

Open Advanced Application > VLAN > Static VLAN to add a new VLAN. Tick the Active box, type VLAN Name “30” and VLAN ID “30” in the columns. Change Port 1 and Port 17 to fixed and keep port 17 tx tagging.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol Management
- VLAN
 - Static MAC Forwarding
 - Filtering
 - Spanning Tree Protocol
 - Bandwidth Control
 - Broadcast Storm Control
 - Mirroring
 - Link Aggregation
 - Port Authentication
 - Port Security
 - Queuing Method
 - Classifier
 - Policy Rule
 - VLAN Stacking
 - Multicast
 - DiffServ

ACTIVE

Name: 30

VLAN Group ID: 30

Port	Control	Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
12	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
13	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
14	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
15	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
16	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
17	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

Open Advanced Application > VLAN > Static VLAN to add a new VLAN. Tick the Active box, type VLAN Name “40” and VLAN ID “40” in the columns. Change Port 2 and Port 17 to fixed and keep port 17 tx tagging.

Port	Control	Tagging
1	Normal	Tx Tagging
2	Normal	Fixed
3	Normal	Forbidden
4	Normal	Tx Tagging
5	Normal	Fixed
6	Normal	Forbidden
7	Normal	Tx Tagging
8	Normal	Fixed
9	Normal	Forbidden
10	Normal	Tx Tagging
11	Normal	Fixed
12	Normal	Forbidden
13	Normal	Tx Tagging
14	Normal	Fixed
15	Normal	Forbidden
16	Normal	Tx Tagging
17	Normal	Fixed

Open **Advanced Application > VLAN > Static VLAN** to add a new VLAN. Tick the Active box, type VLAN Name “50” and VLAN ID “50” in the columns. Change Port 3 and Port 17 to fixed and keep port 17 tx tagging.

Port	Control	Tagging
1	Normal	Tx Tagging
2	Normal	Fixed
3	Normal	Fixed
4	Normal	Forbidden
5	Normal	Tx Tagging
6	Normal	Fixed
7	Normal	Forbidden
8	Normal	Tx Tagging
9	Normal	Fixed
10	Normal	Forbidden
11	Normal	Tx Tagging
12	Normal	Fixed
13	Normal	Forbidden
14	Normal	Tx Tagging
15	Normal	Fixed
16	Normal	Forbidden
17	Normal	Fixed

Open **Advanced Application > VLAN > VLAN Port Setting** to change PVID for

the ports 1, 2 and 3.

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1	<input type="checkbox"/>	30	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	40	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	50	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
15	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

5. Before we start to use the MVR, it is fundamental to enable the IGMP Snooping first. In the OLT-1308 **Menu**, click the **Multicast**, go to the **Multicast Setting**, and activate the **IGMP Snooping**.

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode
1	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
2	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
3	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
4	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
5	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
6	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
7	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
8	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
9	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
10	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
11	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
12	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto

7. In the **OLT-1308**, go to **Advanced Application> Multicast**, and then to the **Multicast setting**. Choose **MVR** and click the **Group configuration**. Set 233.1.1.1~ 233.1.1.100 as the range of multicast address so that only the clients belonging to that range of multicast group will receive the multicast traffic.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management

Switch Advance

- EPON Advance
- VLAN
- Static MAC Forwarding
- Filtering
- Spanning Tree Protocol
- Bandwidth Control
- Broadcast Storm Control
- Mirroring
- Link Aggregation
- Port Security
- Queuing Method
- Classifier
- Policy Rule
- Multicast
- DHCP Relay

Group Configuration MVR

Multicast VLAN ID: 100

Name	Start Address	End Address
<input type="text"/>	0.0.0.0	0.0.0.0

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
100	test	233.1.1.1	233.1.1.100	<input type="checkbox"/>	<input type="checkbox"/>

Configuration via CLI

1. On the OLT-1308, in the configure mode, create VLAN 100

```

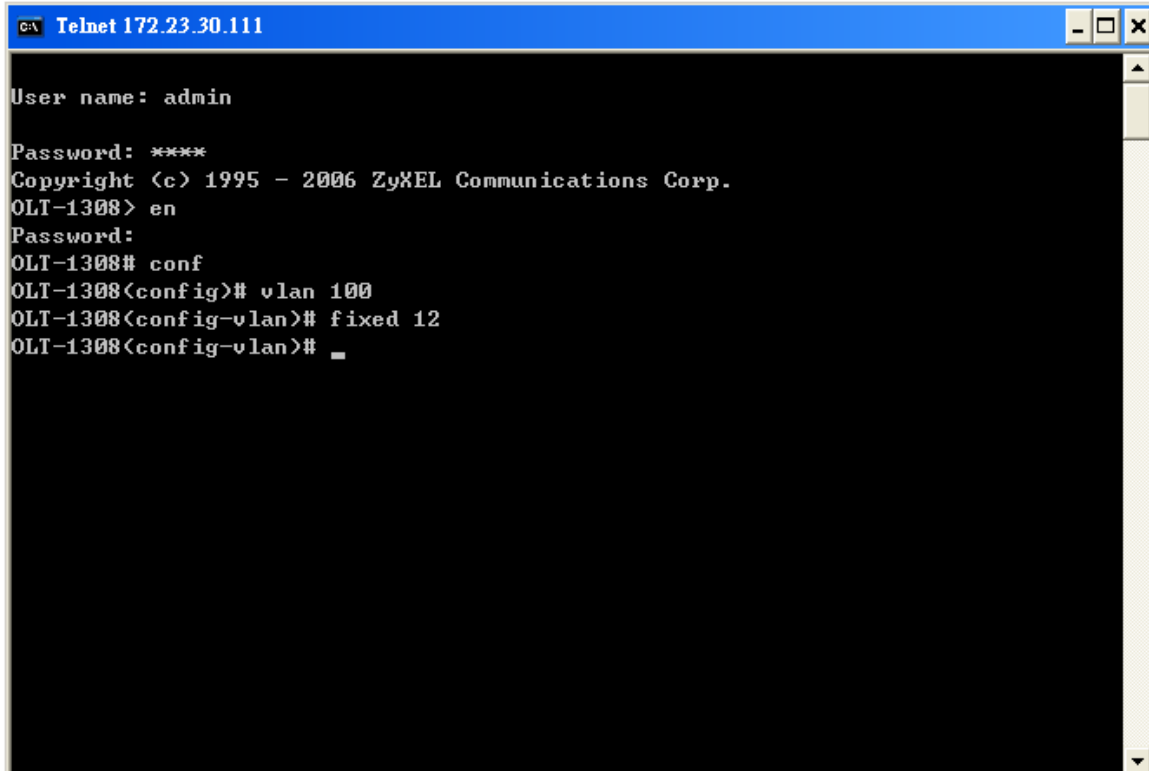
c:\ Telnet 172.23.30.111

User name: admin

Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)#

```

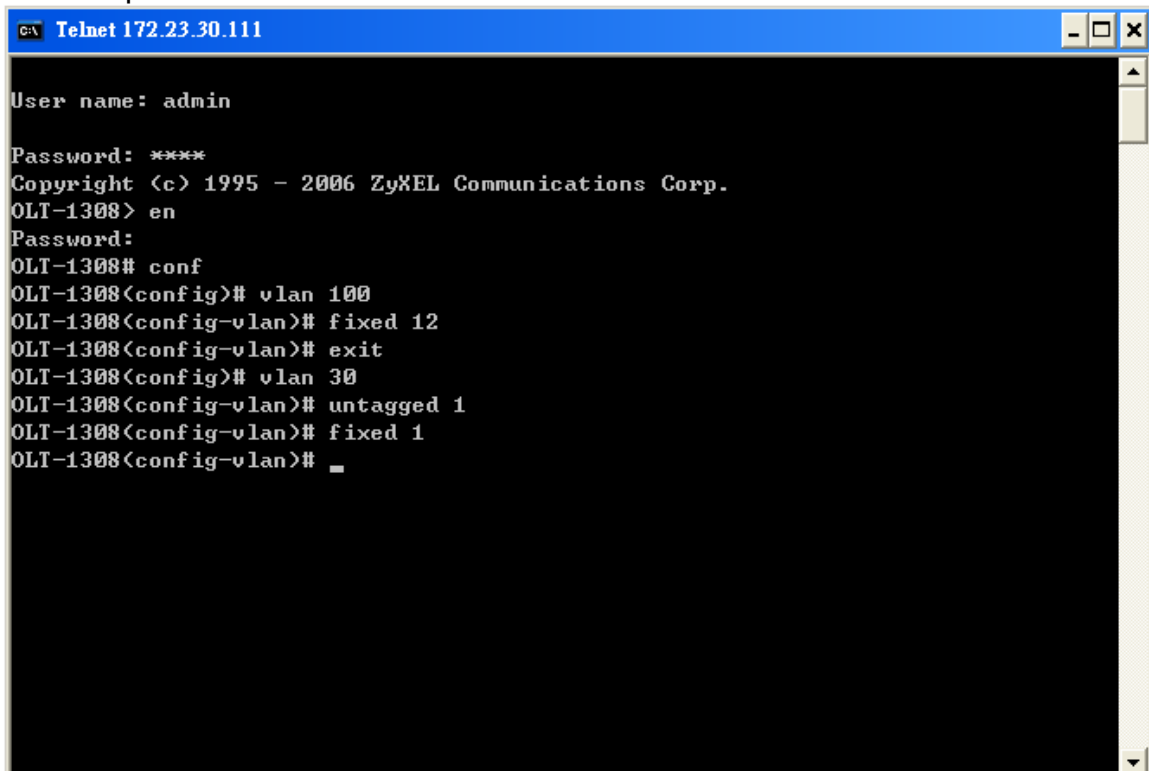
2. In the VLAN 100, set the port 12 to be fixed port.



```
c:\ Telnet 172.23.30.111

User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# _
```

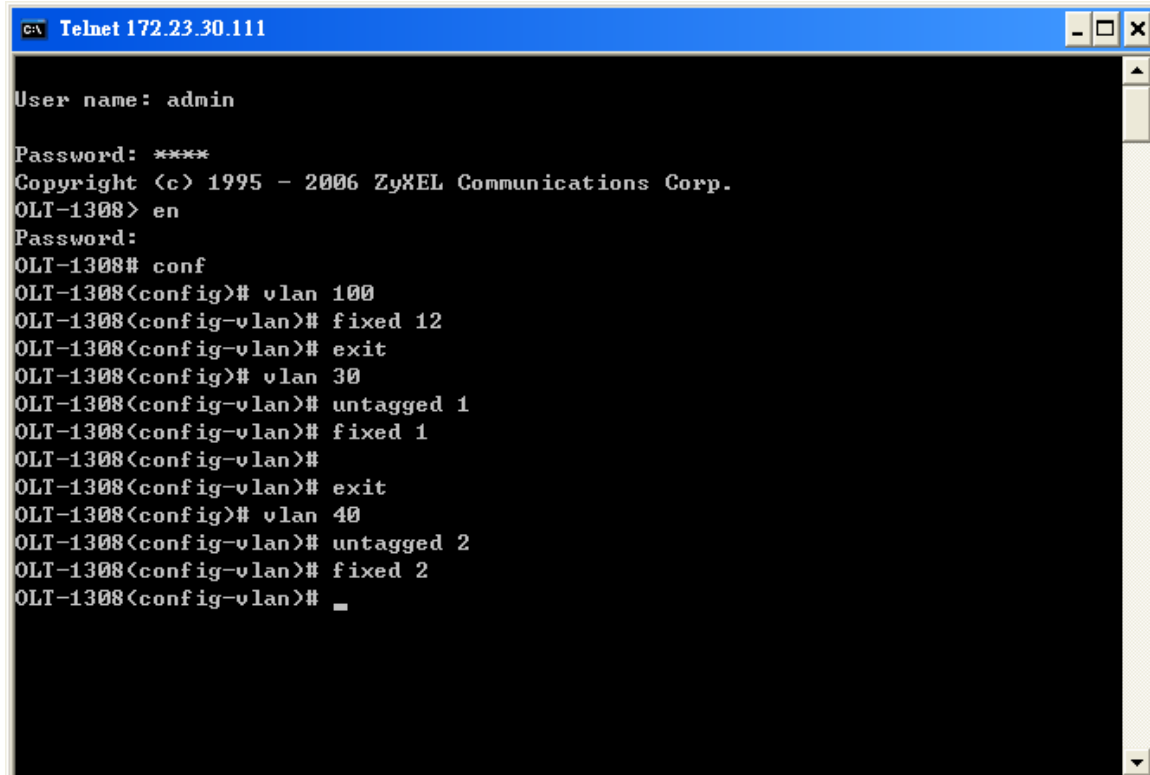
3. On the OLT-1308, in the configure mode, create VLAN 30, and set the port 1 to be fixed port.



```
c:\ Telnet 172.23.30.111

User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 30
OLT-1308(config-vlan)# untagged 1
OLT-1308(config-vlan)# fixed 1
OLT-1308(config-vlan)# _
```

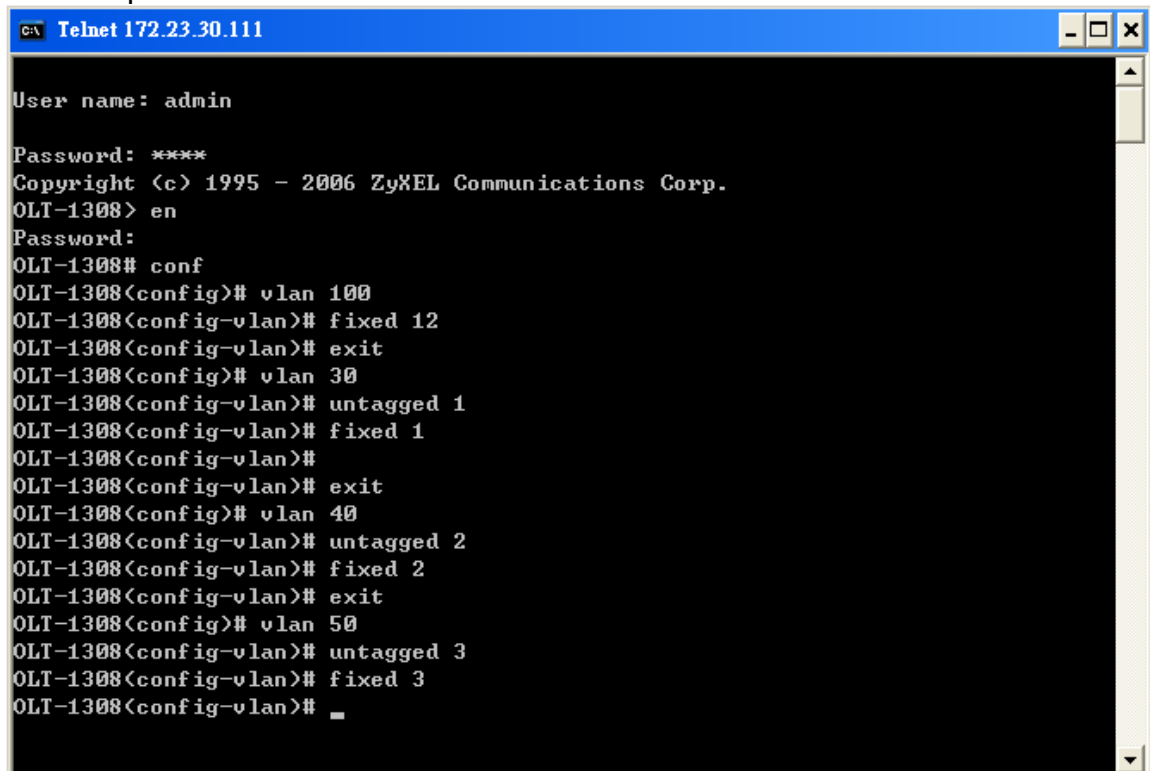
4. On the OLT-1308, in the configure mode, create VLAN 40, and set the port 2 to be fixed port.



```
c:\ Telnet 172.23.30.111

User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 30
OLT-1308(config-vlan)# untagged 1
OLT-1308(config-vlan)# fixed 1
OLT-1308(config-vlan)#
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 40
OLT-1308(config-vlan)# untagged 2
OLT-1308(config-vlan)# fixed 2
OLT-1308(config-vlan)#
```

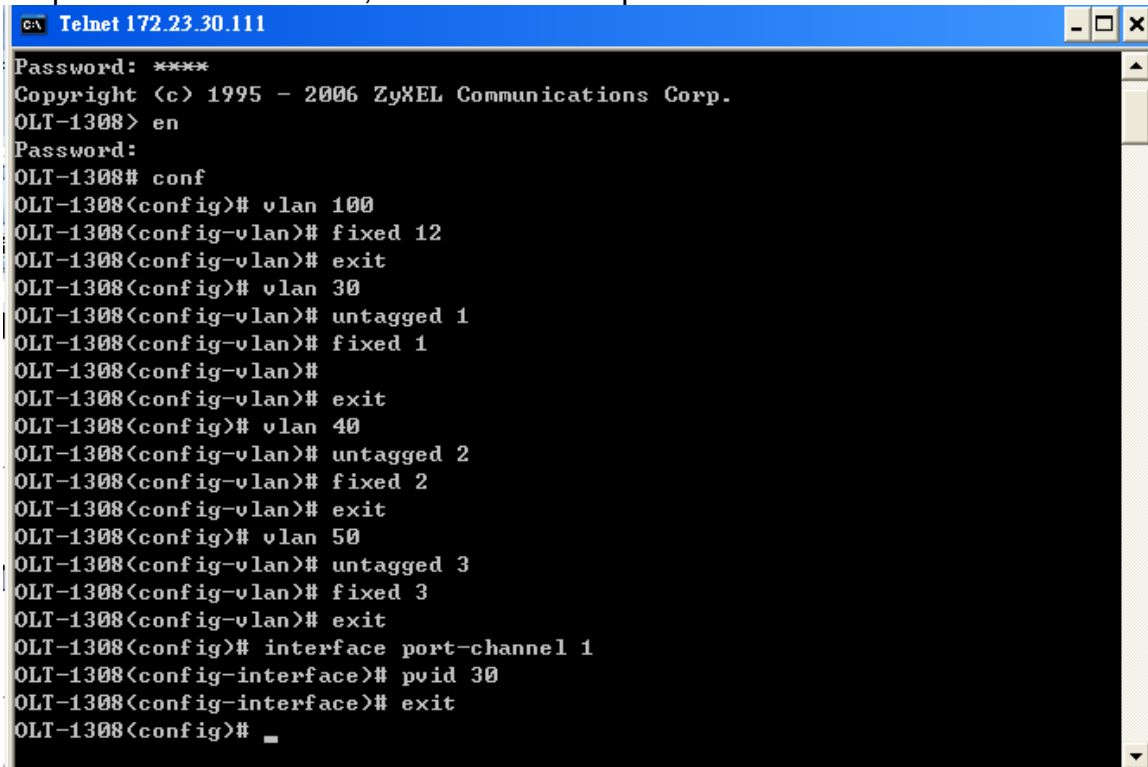
5. On the OLT-1308, in the configure mode, create VLAN 50, and set the port 3 to be fixed port.



```
c:\ Telnet 172.23.30.111

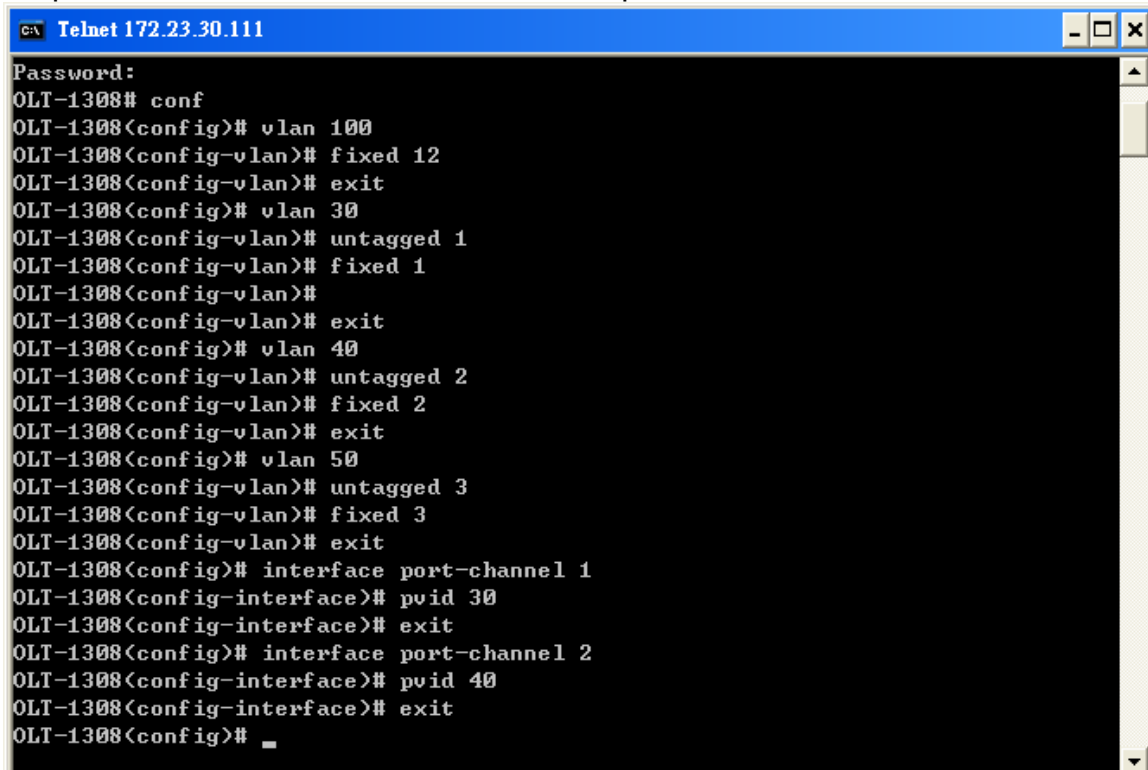
User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 30
OLT-1308(config-vlan)# untagged 1
OLT-1308(config-vlan)# fixed 1
OLT-1308(config-vlan)#
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 40
OLT-1308(config-vlan)# untagged 2
OLT-1308(config-vlan)# fixed 2
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 50
OLT-1308(config-vlan)# untagged 3
OLT-1308(config-vlan)# fixed 3
OLT-1308(config-vlan)#
```

Step 6: On the OLT-1308, set the PVID of specific VLAN 30



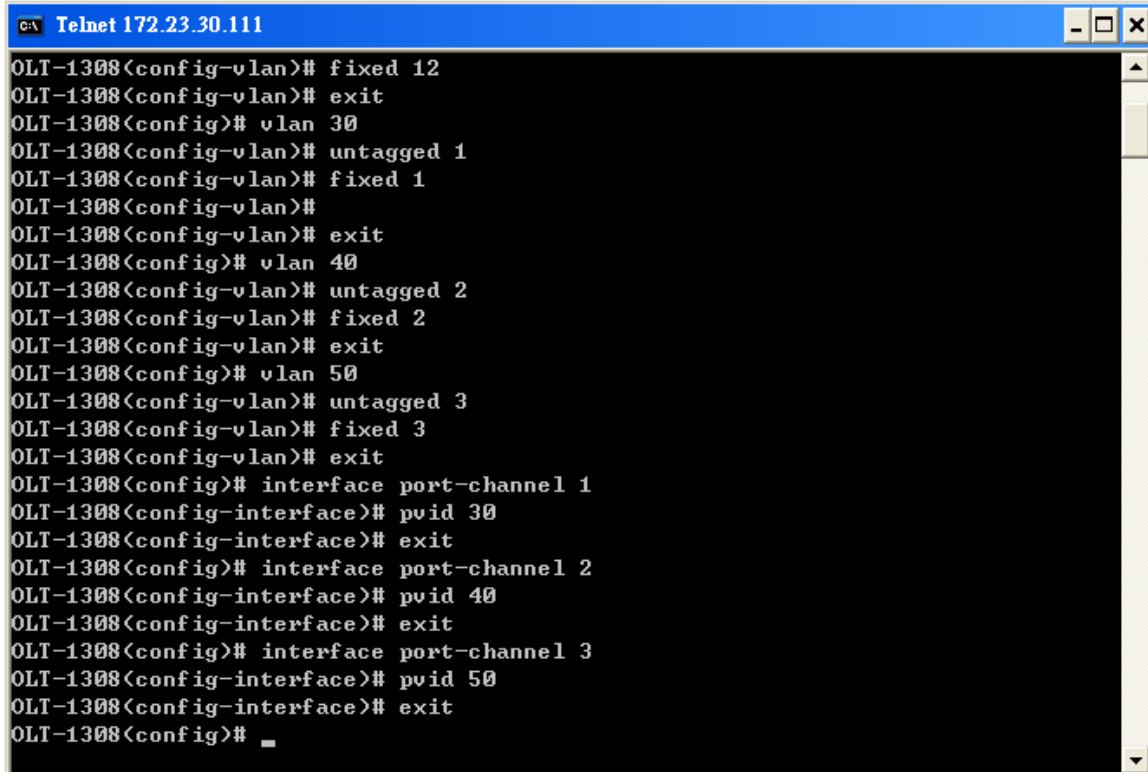
```
c:\ Telnet 172.23.30.111
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 30
OLT-1308(config-vlan)# untagged 1
OLT-1308(config-vlan)# fixed 1
OLT-1308(config-vlan)#
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 40
OLT-1308(config-vlan)# untagged 2
OLT-1308(config-vlan)# fixed 2
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 50
OLT-1308(config-vlan)# untagged 3
OLT-1308(config-vlan)# fixed 3
OLT-1308(config-vlan)# exit
OLT-1308(config)# interface port-channel 1
OLT-1308(config-interface)# pvid 30
OLT-1308(config-interface)# exit
OLT-1308(config)#
```

Step 7: On the OLT-1308, set the PVID of specific VLAN 40



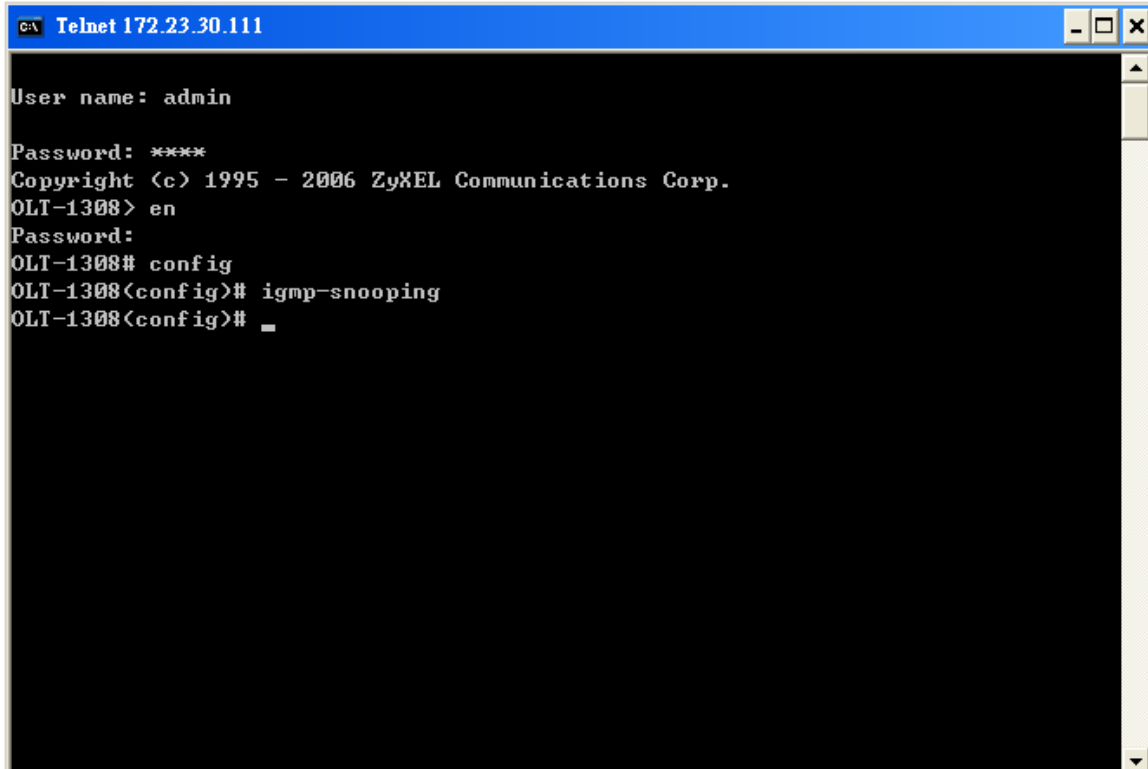
```
c:\ Telnet 172.23.30.111
Password:
OLT-1308# conf
OLT-1308(config)# vlan 100
OLT-1308(config-vlan)# fixed 12
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 30
OLT-1308(config-vlan)# untagged 1
OLT-1308(config-vlan)# fixed 1
OLT-1308(config-vlan)#
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 40
OLT-1308(config-vlan)# untagged 2
OLT-1308(config-vlan)# fixed 2
OLT-1308(config-vlan)# exit
OLT-1308(config)# vlan 50
OLT-1308(config-vlan)# untagged 3
OLT-1308(config-vlan)# fixed 3
OLT-1308(config-vlan)# exit
OLT-1308(config)# interface port-channel 1
OLT-1308(config-interface)# pvid 30
OLT-1308(config-interface)# exit
OLT-1308(config)# interface port-channel 2
OLT-1308(config-interface)# pvid 40
OLT-1308(config-interface)# exit
OLT-1308(config)#
```

8. On the OLT-1308, set the PVID of specific VLAN 50



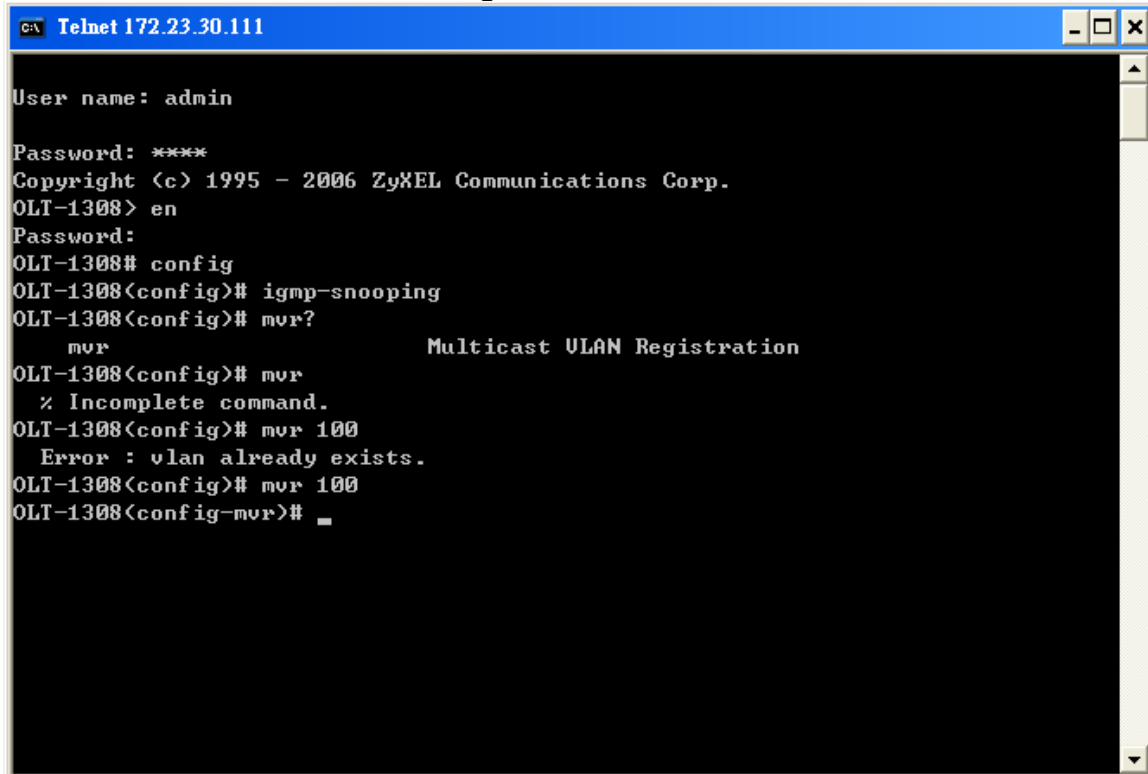
```
OLT-1308<config-vlan># fixed 12
OLT-1308<config-vlan># exit
OLT-1308<config># vlan 30
OLT-1308<config-vlan># untagged 1
OLT-1308<config-vlan># fixed 1
OLT-1308<config-vlan>#
OLT-1308<config-vlan># exit
OLT-1308<config># vlan 40
OLT-1308<config-vlan># untagged 2
OLT-1308<config-vlan># fixed 2
OLT-1308<config-vlan># exit
OLT-1308<config># vlan 50
OLT-1308<config-vlan># untagged 3
OLT-1308<config-vlan># fixed 3
OLT-1308<config-vlan># exit
OLT-1308<config># interface port-channel 1
OLT-1308<config-interface># pvid 30
OLT-1308<config-interface># exit
OLT-1308<config># interface port-channel 2
OLT-1308<config-interface># pvid 40
OLT-1308<config-interface># exit
OLT-1308<config># interface port-channel 3
OLT-1308<config-interface># pvid 50
OLT-1308<config-interface># exit
OLT-1308<config>#
```

Step 9: On the OLT-1308, in the configure mode, enable IGMP snooping



```
User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# config
OLT-1308<config># igmp-snooping
OLT-1308<config>#
```

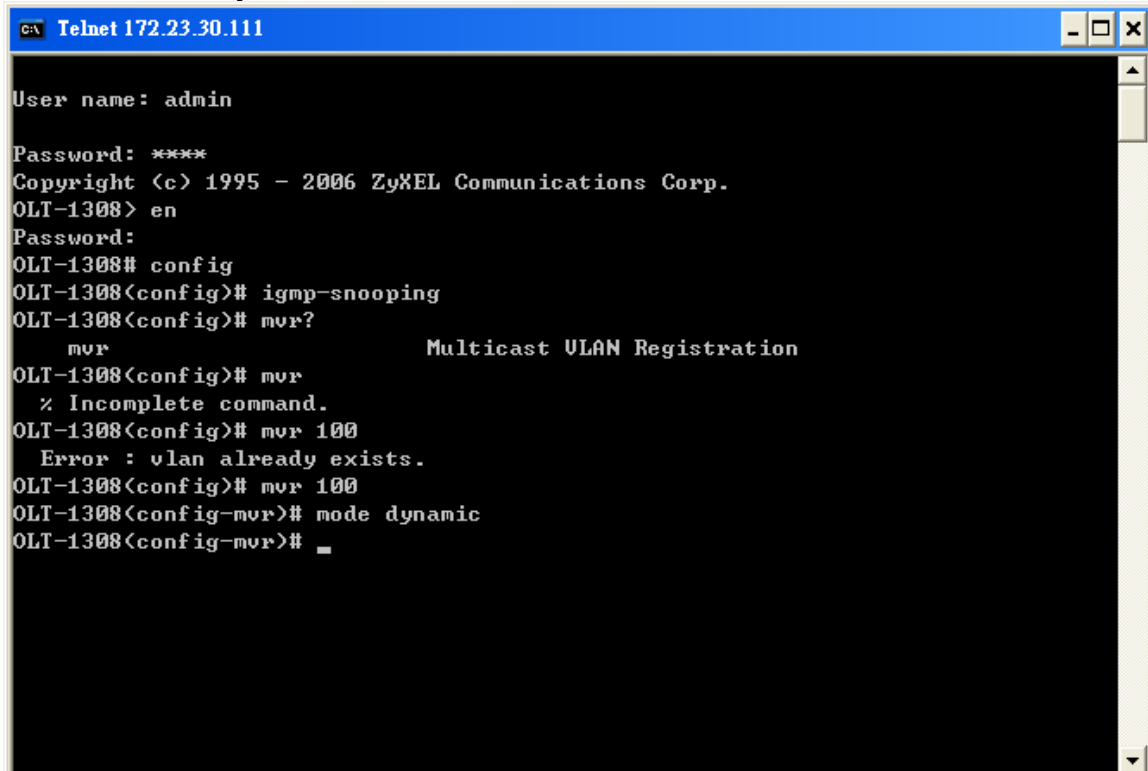
10. On the OLT-1308, in the configure mode, create MVR



```
C:\ Telnet 172.23.30.111

User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# config
OLT-1308(config)# igmp-snooping
OLT-1308(config)# mvr?
      mvr                               Multicast VLAN Registration
OLT-1308(config)# mvr
      % Incomplete command.
OLT-1308(config)# mvr 100
      Error : vlan already exists.
OLT-1308(config)# mvr 100
OLT-1308(config-mvr)#
```

11. Define the Dynamic mode



```
C:\ Telnet 172.23.30.111

User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# config
OLT-1308(config)# igmp-snooping
OLT-1308(config)# mvr?
      mvr                               Multicast VLAN Registration
OLT-1308(config)# mvr
      % Incomplete command.
OLT-1308(config)# mvr 100
      Error : vlan already exists.
OLT-1308(config)# mvr 100
OLT-1308(config-mvr)# mode dynamic
OLT-1308(config-mvr)#
```

12. on the OLT-1308, in the MVR 100, set up the multicast group address.

```

c:\ Telnet 172.23.30.111
User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# config
OLT-1308(config)# igmp-snooping
OLT-1308(config)# mvr?
      mvr                               Multicast VLAN Registration
OLT-1308(config)# mvr
      % Incomplete command.
OLT-1308(config)# mvr 100
      Error : vlan already exists.
OLT-1308(config)# mvr 100
OLT-1308(config-mvr)# mode dynamic
OLT-1308(config-mvr)# group test start-address 233.1.1.1 end-address 233.1.1.100
OLT-1308(config-mvr)# _

```

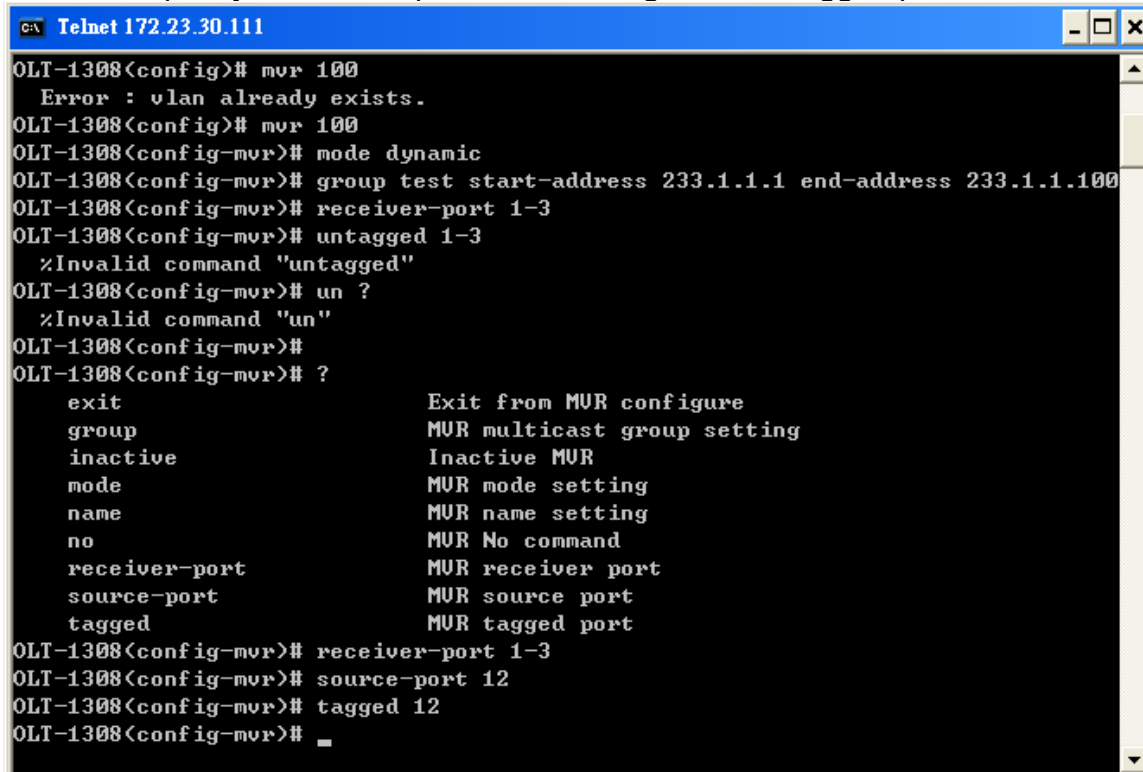
13. In the MVR 100, specify receiver ports on port 1~3.

```

c:\ Telnet 172.23.30.111
OLT-1308(config)# mvr
      % Incomplete command.
OLT-1308(config)# mvr 100
      Error : vlan already exists.
OLT-1308(config)# mvr 100
OLT-1308(config-mvr)# mode dynamic
OLT-1308(config-mvr)# group test start-address 233.1.1.1 end-address 233.1.1.100
OLT-1308(config-mvr)# receiver-port 1-3
OLT-1308(config-mvr)# untagged 1-3
      %Invalid command "untagged"
OLT-1308(config-mvr)# un ?
      %Invalid command "un"
OLT-1308(config-mvr)#
OLT-1308(config-mvr)# ?
      exit                               Exit from MVR configure
      group                               MVR multicast group setting
      inactive                            Inactive MVR
      mode                                MVR mode setting
      name                                MVR name setting
      no                                  MVR No command
      receiver-port                       MVR receiver port
      source-port                         MVR source port
      tagged                               MVR tagged port
OLT-1308(config-mvr)# receiver-port 1-3
OLT-1308(config-mvr)# _

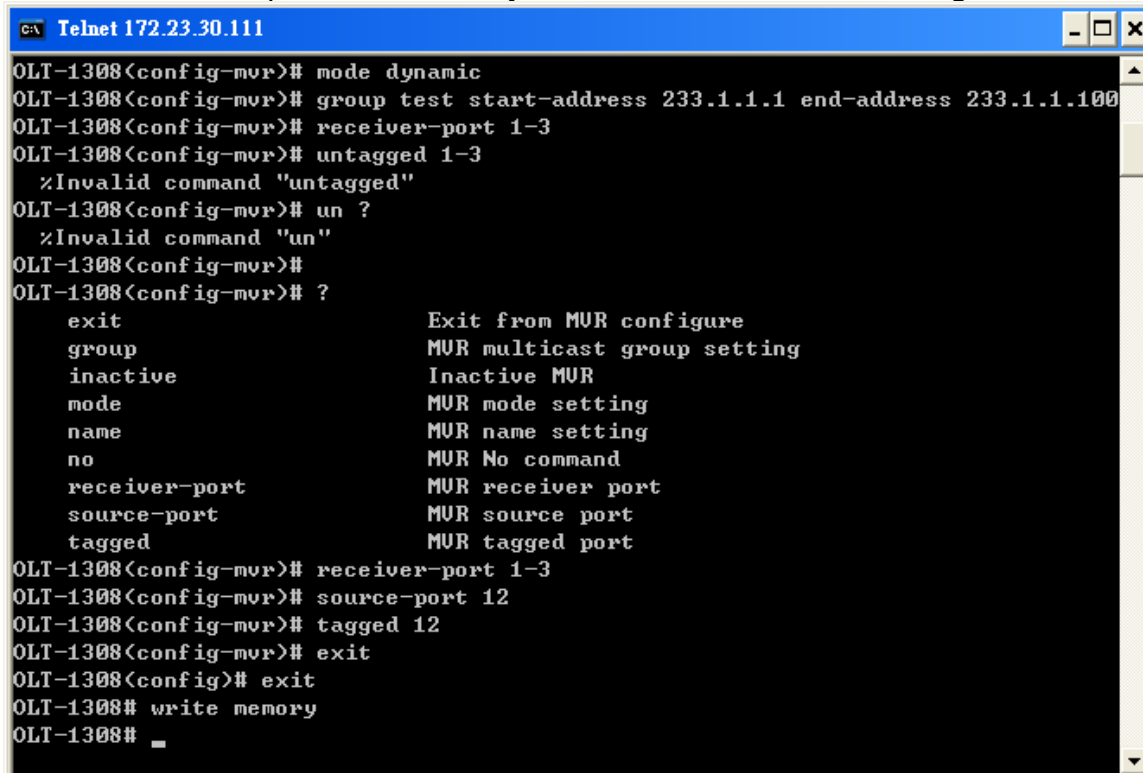
```


14. Then, specify the source port 12 and assign it to be tagged ports.



```
OLT-1308<config># mvr 100
  Error : vlan already exists.
OLT-1308<config># mvr 100
OLT-1308<config-mvr># mode dynamic
OLT-1308<config-mvr># group test start-address 233.1.1.1 end-address 233.1.1.100
OLT-1308<config-mvr># receiver-port 1-3
OLT-1308<config-mvr># untagged 1-3
  %Invalid command "untagged"
OLT-1308<config-mvr># un ?
  %Invalid command "un"
OLT-1308<config-mvr>#
OLT-1308<config-mvr># ?
  exit                Exit from MUR configure
  group               MUR multicast group setting
  inactive            Inactive MUR
  mode                MUR mode setting
  name                MUR name setting
  no                  MUR No command
  receiver-port       MUR receiver port
  source-port         MUR source port
  tagged              MUR tagged port
OLT-1308<config-mvr># receiver-port 1-3
OLT-1308<config-mvr># source-port 12
OLT-1308<config-mvr># tagged 12
OLT-1308<config-mvr>#
```

15. In exec mode, put "write memory" to save all of the above changes.



```
OLT-1308<config-mvr># mode dynamic
OLT-1308<config-mvr># group test start-address 233.1.1.1 end-address 233.1.1.100
OLT-1308<config-mvr># receiver-port 1-3
OLT-1308<config-mvr># untagged 1-3
  %Invalid command "untagged"
OLT-1308<config-mvr># un ?
  %Invalid command "un"
OLT-1308<config-mvr>#
OLT-1308<config-mvr># ?
  exit                Exit from MUR configure
  group               MUR multicast group setting
  inactive            Inactive MUR
  mode                MUR mode setting
  name                MUR name setting
  no                  MUR No command
  receiver-port       MUR receiver port
  source-port         MUR source port
  tagged              MUR tagged port
OLT-1308<config-mvr># receiver-port 1-3
OLT-1308<config-mvr># source-port 12
OLT-1308<config-mvr># tagged 12
OLT-1308<config-mvr># exit
OLT-1308<config># exit
OLT-1308# write memory
OLT-1308#
```

Ringring a network by building redundant

links and connections between Switch

What is Spanning Tree Protocol?

Spanning Tree Overview

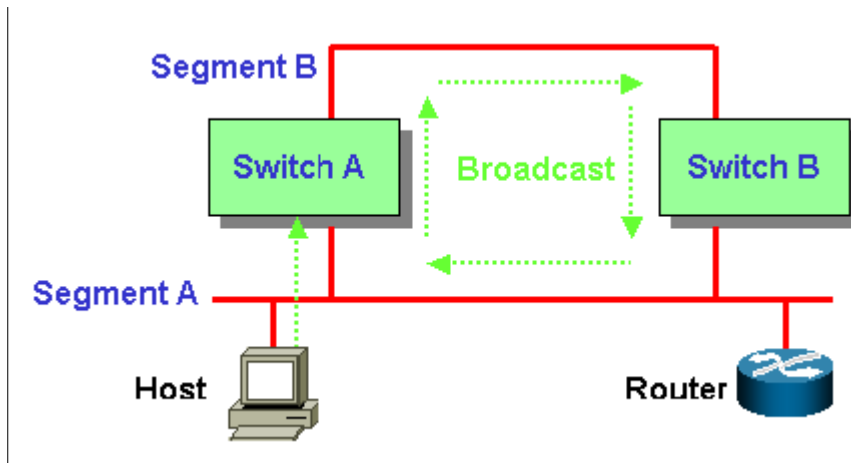
Spanning-Tree Protocol (STP) is a Layer 2 protocol designed to run on the bridges and the switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops and provides backup links between switches or bridges. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.

The redundant topology without STP will cause the following problem:

1. Broadcast storm:

Without Spanning Tree loop avoidance mechanism, each switch will endlessly flood broadcast packets to all ports. This situation is called broadcast storm.

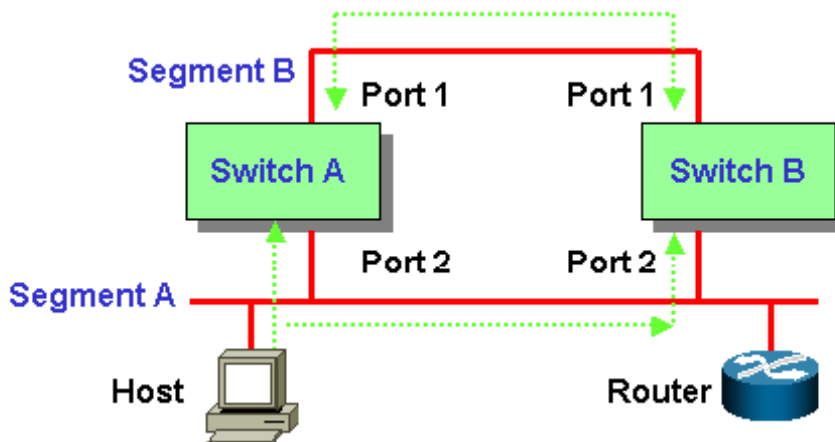
- When Host sends a broadcast frame, like an ARP request to Router, the frame will be received by Switch A.
- Switch A identifies the destination MAC address field (broadcast FF:FF:FF:FF:FF:FF) in the frame and determine to flood it onto Segment B.
- When the broadcast frame arrives at Switch B, the switch will repeat above process, flood it to Segment A.
- The broadcast frame will endlessly travel around the loop network even id the router has already received this frame.



2. Filtering Database Instability:

When multiple copies of a frame arrive at different ports of a switch, the MAC entry instability in Filtering Database will occur.

- Host sends a unicast frame to a router (source MAC address is host's MAC, destination MAC address is Router's MAC). Both Switch A and Switch B will receive this frame and learn the MAC address of the host on Port 2.
- Switch A has not yet learned the MAC address of Router. So Switch A will flood a copy of the received frame to Segment B.
- When the copy of the frame from Switch A arrives at Switch B, Switch B will remove the first entry (Host MAC address on Port 2) in Filtering Database and add a new mapping of Host MAC address on Port 1. Switch B incorrectly learn Host MAC address on Port 1.
- Switch B can't forward the frames properly because the instability of mapping MAC address to Port.



How STP Works

Spanning Tree provides a loop-free network. When a switch supporting STP

recognizes a loop in the network topology, it blocks one or more redundant ports. Spanning Tree Protocol continually explores the network, so when the network topology changes, STP automatically reconfigures the switch ports in order to avoid the failure by blocking certain port.

Spanning tree algorithm aware switches (bridges) exchange configuration messages periodically. The configuration message is a multicast frame called BPDU (Bridge Protocol Data Unit) or Hello message. According to BPDU, these STP aware switches (bridges) will construct a loop free network with a "tree" architecture.

STP operation is described below:

1. Select a root bridge

Only one switch/ bridge can be selected as the root bridge in a given network. All other decisions in the network, such as which port is blocked and which port is put in forwarding mode, are made regarding this root bridge. The root bridge is the "root" of the constructed "tree".

- One of the important fields included in the BPDU is the bridge ID. Each bridge has unique bridge ID. The root bridge is the bridge with the lowest bridge ID in the spanning tree network.
- The bridge ID includes two parts, bridge priority (2 bytes) and bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768. E.g. for a switch with default priority 32768 (8000 hex), MAC address is 00:A0:C5:12:34:56, its bridge ID is 8000:00A0:C512:3456.
- On the root bridge, all its ports are **designated ports**. **Designated ports are always in the forwarding state**. While in forwarding state, port can receive and send traffic.

2. Select a root port for the non-root bridge

For the non-root switch/bridge, there will be one root port. The root port is the port through which this non-root switch / bridge communicates with the root bridge (the "leaf" side of the "tree").

- The root port is the port on the non-root bridge with the lowest path cost to the root bridge. **The root port is normally in forwarding state**.
- Path cost is the total cost of transmitting a frame on to a LAN through that port to bridge root. It is assigned according to the bandwidth of the link. The slower the media, the higher the cost. Some of the path costs specified in the IEEE 802.1d specification are listed below.

Link Speed	Recommended Cost	Recommended Cost Range
4Mbps	250	100 to 1000
10Mbps	100	50 to 600
16Mbps	62	40 to 400
100Mbps	19	10 to 60
1Gbps	4	3 to 10
10Gbps	2	1 to 5

- 3. When multiple ports have the same path cost to root bridge, **the port with lowest port priority is selected as root port.**

3. Select a designated port on each segment

For each LAN segment (collision domain), there is a designated port. The designated port has the lowest cost to the root bridge. Designated ports are normally in the forwarding state to forward and receive traffic to the segment. If more than one port in the segment have the same path cost, the port on which bridge has the lowest bridge ID is selected as a designated port.

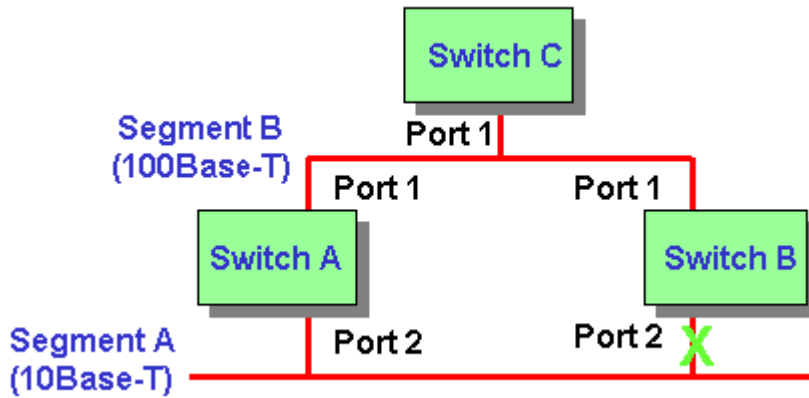
How STP works

After STP determines the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP-aware devices exchange Bridge Protocol Data Units (BPDUs) periodically. Whenever the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

For example:

Switch A: MAC = 00A0C5111111, Priority = 32768		Switch B: MAC = 00A0C5222222, Priority = 32768		Switch C: MAC = 00A0C5333333 Priority = 1	
	Port 1	Port 2		Port 1	Port 2
Cost	19	100	Cost	19	100
Priority	128	128	Priority	128	128



1. Switch A bridge ID = 8000:00A0:C511:1111, Switch B bridge ID = 8000:00A0:C522:2222, Switch C bridge ID = 0001:00A0:C533:3333. Switch C has the lowest bridge ID, so Switch C is the root bridge. All ports of the root bridge are designated ports, so Port 1 is designated port.
2. For non-root bridge Switch A, Port 1 path cost to root bridge is 19, Port 2 path cost is 119, 100 (Switch A Port 2) + 19 (Switch B Port 1). For Switch B, Port 1 path cost is 19, Port 2 path cost is 119. Root port = Port 1 of Switch A and Switch B because it has the lowest path cost to the root bridge Switch C.
3. On Segment A, both Port 2 of Switch A and Switch B have the same path cost to root bridge. Since Switch A has lower bridge ID than Switch B, the designated port is selected on Switch A. So Port 2 of Switch A is designated port. Blocking = Port 2 of Switch B, the non designated port on the segment. Forwarding = All designated ports and root ports.

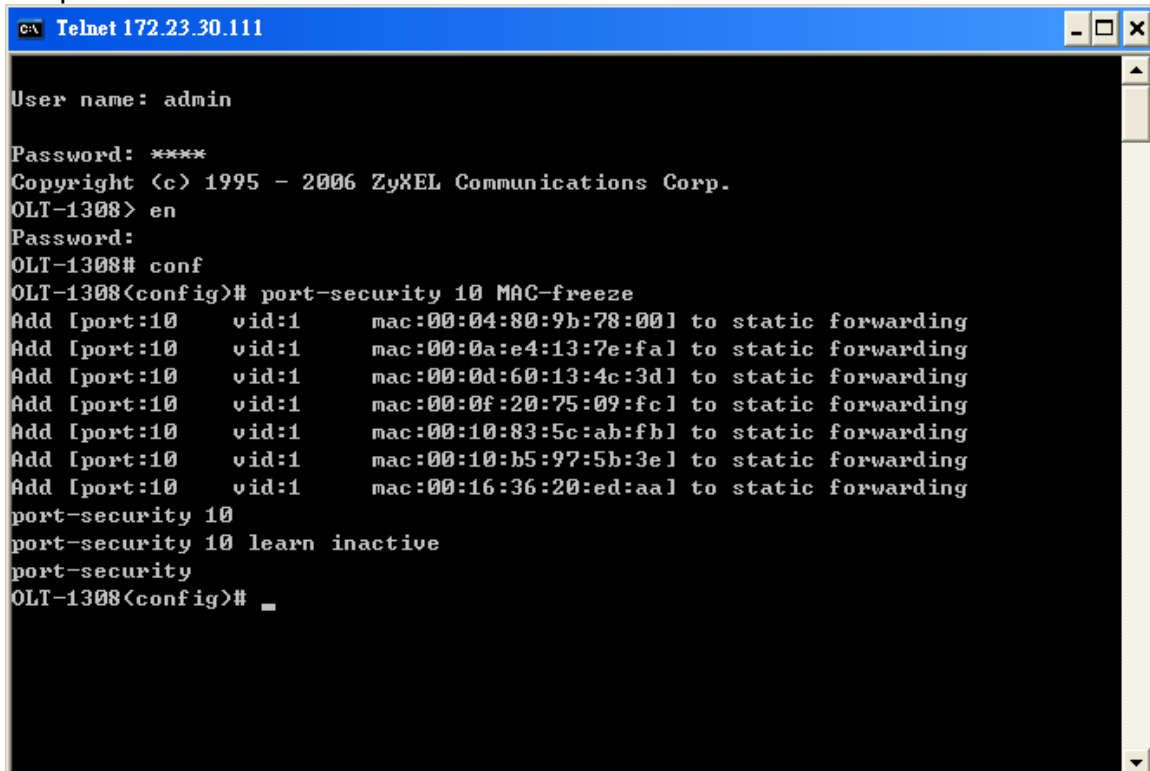
Switching security

MAC freeze

As an added protection against network intrusion attacks, ZyXEL has implemented the MAC Freeze feature on OLT-1308. Security has been the main focus of our Ethernet switch design. With the MAC freeze feature enabled, dynamic MAC addresses on specified ports are stored in the static MAC address table. At the same time, MAC address learning is disabled on these ports thus denying network access for computers within unknown MAC addresses. Without the MAC freeze function, any computer can access the network through a switch port. The port automatically learns the computer's MAC address and stores it to the MAC address table.

Activate the MAC freeze function on a port by entering the `port-security [port number] MAC-freeze` command in the CLI.

The following figure shows an example where the MAC freeze feature is enabled on port 6. The switch automatically copies all dynamically learnt MAC address on the port 6 to the static MAC address.

A screenshot of a Telnet session window titled "Telnet 172.23.30.111". The session shows a user logging in as 'admin' and entering the configuration mode. The user enters the command 'port-security 10 MAC-freeze', which results in seven MAC addresses being added to the static forwarding table for port 10. The user then enters 'port-security 10 learn inactive' and 'port-security' before returning to the configuration prompt.

```

Telnet 172.23.30.111
User name: admin
Password: ****
Copyright (c) 1995 - 2006 ZyXEL Communications Corp.
OLT-1308> en
Password:
OLT-1308# conf
OLT-1308(config)# port-security 10 MAC-freeze
Add [port:10 vid:1 mac:00:04:80:9b:78:00] to static forwarding
Add [port:10 vid:1 mac:00:0a:e4:13:7e:fa] to static forwarding
Add [port:10 vid:1 mac:00:0d:60:13:4c:3d] to static forwarding
Add [port:10 vid:1 mac:00:0f:20:75:09:fc] to static forwarding
Add [port:10 vid:1 mac:00:10:83:5c:ab:fb] to static forwarding
Add [port:10 vid:1 mac:00:10:b5:97:5b:3e] to static forwarding
Add [port:10 vid:1 mac:00:16:36:20:ed:aal] to static forwarding
port-security 10
port-security 10 learn inactive
port-security
OLT-1308(config)#
```

You can display the **Static MAC Address** screen in the web configurator to view the copied MAC addresses.

Figure 2: Displaying MAC Addresses from MAC Freeze

The screenshot shows the 'MAC Table' configuration page. On the left is a navigation menu with categories: MENU, Basic Setting, Advanced Application, Routing Protocol, Management, Maintenance, Access Control, Diagnostic, Syslog, Cluster Management, MAC Table, ARP Table, and IGMP Table. The main content area has a title 'MAC Table' and controls for 'Sort by' (set to 'MAC'), 'Port Select' (set to 'Switch'), and buttons for 'Get' and 'Clear'. Below these is a table with the following data:

Index	MAC Address	VID	Port	Type
1	00:04:80:9b:78:00	1	CPU	static
2	00:0a:e4:13:7e:fa	1	CPU	static
3	00:0d:60:13:4c:3d	1	CPU	static
4	00:0f:20:75:09:fc	1	CPU	static
5	00:10:83:5c:ab:fb	1	CPU	static
6	00:10:b5:97:5b:3e	1	CPU	static
7	00:16:36:20:ed:aa	1	CPU	static

After you enabled MAC freeze on the port 6 using the CLI command, the switch automatically disables MAC address learning on that port. Display the **Port Security** screen to verify this.

Figure 3: Disabled Automatic MAC Address Learning After MAC Freeze

The screenshot shows the 'Port Security' configuration page. On the left is a navigation menu with categories: MENU, Basic Setting, Advanced Application, Routing Protocol, Management, Switch Advance, EPON Advance, VLAN, Static MAC Forwarding, Filtering, Spanning Tree Protocol, Bandwidth Control, Broadcast Storm Control, Mirroring, Link Aggregation, Port Security, Queuing Method, Classifier, Policy Rule, Multicast, and DHCP Relay. The main content area has a title 'Port Security' and a toggle for 'Active' which is checked. Below is a table with the following data:

Port	Active	Address Learning	Limited Number of Learned MAC Address
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
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 checked="" type="checkbox"/>	<input type="checkbox"/>	10
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

At the bottom of the page are 'Apply' and 'Cancel' buttons.

Setting up 802.1x Radius Authentication.

Port Authentication: RADIUS Setup

Click **Advanced Application > EPON Advance > Port Authentication** in the navigation panel to display the configuration screen as shown. Set the RADIUS server **IP address**, **UDP port** and **shared Secret**. Make sure the information you have entered is the same as the RADIUS server. Then click **Apply** to make the settings take effect.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol Management
- Switch Advance
- EPON Advance**
- Classifier Filter Profile
- VLAN Profile
- Priority Profile
- Static MAC Forwarding
- Destination Filter Status
- Port Authentication

RADIUS Authentication Server Port Authentication

IP Address	192.168.1.3
UDP Port	1812
Shared Secret	12345678

Click the **802.1x** link to display the **802.1x** configuration screen. Select the **Active** check box to enable and then select the **Active** for a port to enable 802.1x authentication on that port. You can leave the other settings to the default values. Click **Apply** to save your changes.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol Management
- Switch Advance
- EPON Advance**
- Classifier Filter Profile
- VLAN Profile
- Priority Profile
- Static MAC Forwarding
- Destination Filter Status
- Port Authentication

802.1x Port Authentication

Active

Port	Active	Quiet period	Transmission period	Supplicant timeout	Server timeout	Max Reauth No.	Max Request No.
1	<input checked="" type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
2	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
3	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
4	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
5	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
6	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
7	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times
8	<input type="checkbox"/>	60 seconds	30 seconds	30 seconds	30 seconds	2 times	2 times

RADIUS Server Setup

Click **RADIUS > RADIUS SERVER** in the navigation panel to display the configuration screen as shown. You can use the default values or change the settings in the **Authentication port** and **Shared Secret** fields. Make sure you configure the same settings on the client.

ZyXEL

ADVANCED

RADIUS
 ROOT CA
 SERVER CERTIFICATE
 RADIUS SERVER
 USER ACCOUNT

MAINTENANCE

MANAGEMENT

LOGOUT

RADIUS SERVER

Server Port

Authentication Port : 1812 (1~65535)
 Accounting Port : 1813 (1~65535)

Allowed Access Type

Allow Any IP Address
 Shared Secret 12345678 (max. 20 characters)
 Allowed Specified IP Address / Network Address

Apply

Allowed IP Address (max. 20)

Add

No.	IP Address	Shared Secret	Description	Action	Delete
					Delete

Create User Account

Click **RADIUS > USER ACCOUNT** in the navigation panel to display the configuration screen as shown. You can use the existing user accounts or create a new one by clicking the **Add New User** button. Note that the client site **MUST** use the account in the RADIUS server.

ZyXEL

ADVANCED

RADIUS
 ROOT CA
 SERVER CERTIFICATE
 RADIUS SERVER
 USER ACCOUNT

MAINTENANCE

MANAGEMENT

LOGOUT

USER ACCOUNT

User Account List (max. 200 Accounts)

Add New User Select All

No.	User Name	Action	Delete
1	abyss	Change Password	<input type="checkbox"/>
2	zyxel	Change Password	<input type="checkbox"/>

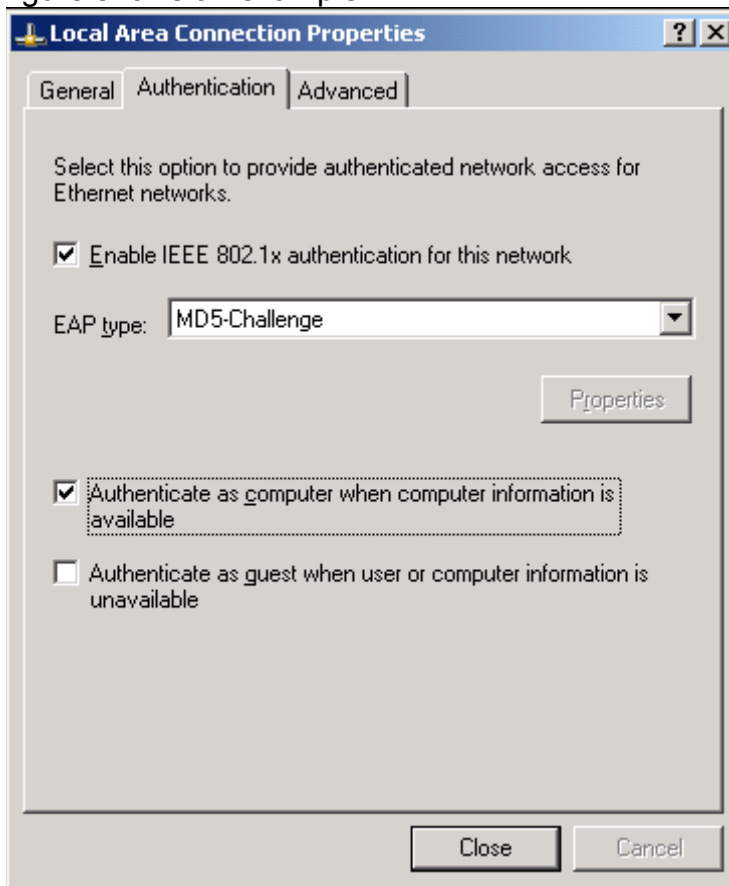
Delete

Supplicant Setup (Windows XP)

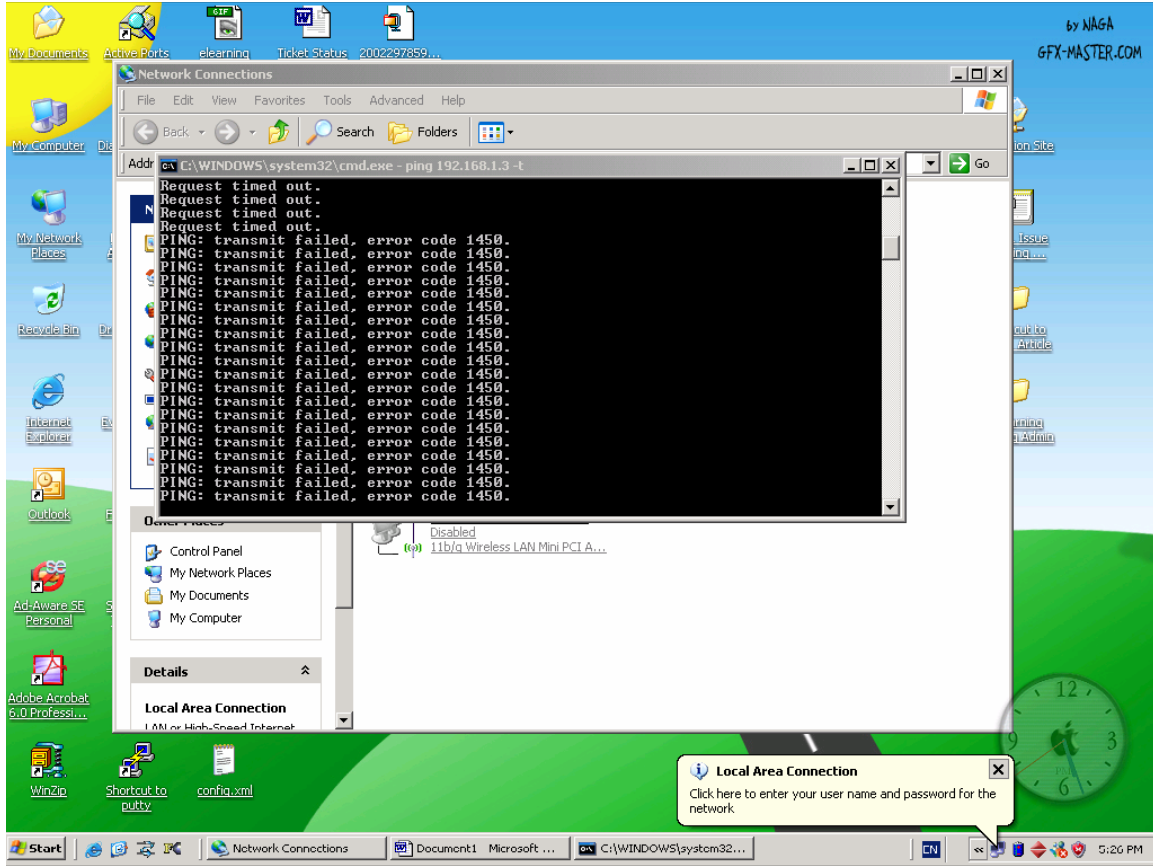
You can use any supplicant software (such as MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client). For this example, we will show you how to configure the Microsoft 802.1x client.

802.1x/MD5-challenge setup

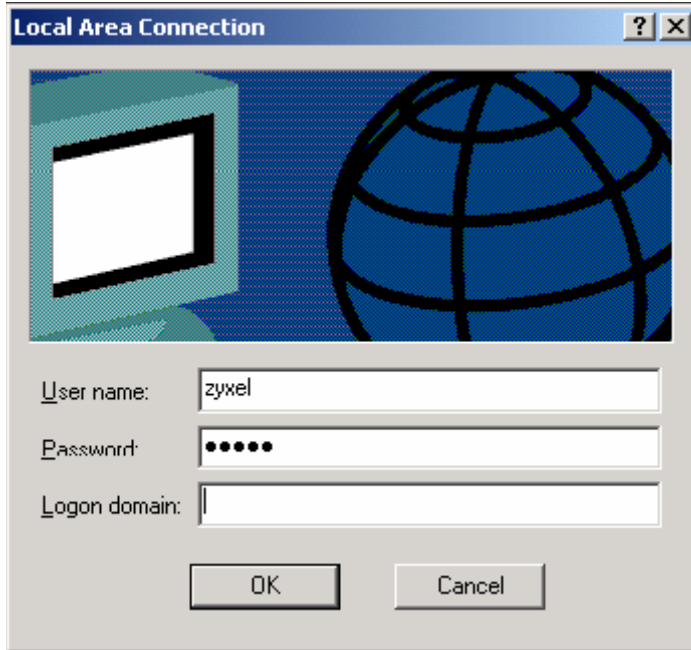
Open the **Local Area Connection Properties** screen and click the **Authentication** tab. Select the **Enable IEEE 802.1x authentication for this network** option and select **MD5-challenge** in the **EAP type** field. The following figure shows an example.



When 802.1x authentication process starts, you are prompted to enter the user name and password. The following figure shows the prompt.



Click on the message window and a login screen displays as shown. Enter your account user name and password in the fields provided. After you click **OK** and the authentication server has verified your account, you can log into the system successfully. This indicates that you have configured the client for 802.1x authentication correctly.



After the configuration, the port is authenticated and the computer connected to this port is allowed to access the network. Otherwise, the computer cannot access the network.

Classifier & Policy rule setup on your Switch

This section shows you how to allow traffic from certain IP addresses and deny others. This can be done easily using classifier and policy rules.

First, you need to create a classifier rule to group traffic into data flows based on information such as the source address, destination address, port number and packet format. In this example, we group traffic based on the packet format and set the OLT-1308 to apply its policy rules. The following lists the three classifier rules that we will define in this example:

1. Packet with a source IP address of 192.168.1.20
2. Packets on port 2
3. ARP traffic for testing

Once packet classification settings are done, we create policy rules to specify the actions on the matched packets so they get the deserved treatment in the network. Here, we also define three policy rules.

1. Forward traffic from 192.168.1.20 only (on the first classifier)
2. Discard all the traffic from port 2 (on the second classifier)
3. Forward ARP packets (on the third classifier)

The following figures show the screen settings for each classifier rule.

Classifier Configuration

Classifier 1

<ul style="list-style-type: none"> Basic Setting Advanced Application Routing Protocol Management Switch Advance EPON Advance VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Security Queuing Method Classifier Policy Rule Multicast DHCP Relay 	Packet Format	All	
	Layer 2	VLAN	<input checked="" type="radio"/> Any <input type="radio"/> []
		Priority	<input checked="" type="radio"/> Any <input type="radio"/> 0
		Ethernet Type	<input checked="" type="radio"/> IP <input type="radio"/> Others [] (Hex)
		Source	MAC Address
	Port		Port 2
	Destination	MAC Address	<input checked="" type="radio"/> Any <input type="radio"/> MAC [] : [] : [] : [] : [] : []
		DSCP	<input checked="" type="radio"/> Any <input type="radio"/> []
	Layer 3	IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
		Source	IP Address / Prefix
Socket			<input checked="" type="radio"/> Any

Classifier 2

<ul style="list-style-type: none"> Basic Setting Advanced Application Routing Protocol Management Switch Advance EPON Advance VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Security Queuing Method Classifier Policy Rule Multicast DHCP Relay 	Classifier		
	Active	<input checked="" type="checkbox"/>	
	Name	2	
	Packet Format	All	
	Layer 2	VLAN	<input checked="" type="radio"/> Any <input type="radio"/> []
		Priority	<input checked="" type="radio"/> Any <input type="radio"/> 0
		Ethernet Type	<input checked="" type="radio"/> IP <input type="radio"/> Others [] (Hex)
		Source	MAC Address
	Port		Port 2
	Destination	MAC Address	<input checked="" type="radio"/> Any <input type="radio"/> MAC [] : [] : [] : [] : [] : []
DSCP		<input checked="" type="radio"/> Any <input type="radio"/> []	

Classifier 3

Basic Setting	Classifier
Advanced Application	Active <input checked="" type="checkbox"/>
Routing Protocol	Name 3
Management	Packet Format All
Switch Advance	Layer 2
EPON Advance	VLAN <input checked="" type="radio"/> Any
VLAN	<input type="radio"/> []
Static MAC Forwarding	Priority <input checked="" type="radio"/> Any
Filtering	<input type="radio"/> 0
Spanning Tree Protocol	Ethernet Type <input checked="" type="radio"/> ARP
Bandwidth Control	<input type="radio"/> Others [] (Hex)
Broadcast Storm Control	Source Address <input checked="" type="radio"/> Any
Mirroring	<input type="radio"/> MAC [: [] : [] : [] : [] : []
Link Aggregation	Port Port 2
Port Security	Destination Address <input checked="" type="radio"/> Any
Queuing Method	<input type="radio"/> MAC [: [] : [] : [] : [] : []
Classifier	

Policy Rule Configuration

The following figures show the screen settings for each policy rule.

1. Policy rule on Classifier 1

MENU	Policy
Basic Setting	Active <input checked="" type="checkbox"/>
Advanced Application	Name 1
Routing Protocol	Classifier(s) 1
Management	
Switch Advance	Parameters
EPON Advance	VLAN ID 1
VLAN	EgressPort Port 12
Static MAC Forwarding	Outgoing packet format for Egress port <input checked="" type="radio"/> Tag <input type="radio"/> Untag
Filtering	Priority 0
Spanning Tree Protocol	DSCP []
Bandwidth Control	TOS 0
Broadcast Storm Control	Forwarding
Mirroring	<input type="radio"/> No change
Link Aggregation	<input type="radio"/> Discard the packet
Port Security	<input checked="" type="radio"/> Do not drop the matching frame previously marked for dropping
Queuing Method	Priority
Classifier	
Policy Rule	
Multicast	
DHCP Relay	

2. Policy rule on classifier 2

MENU		Policy	
Basic Setting	Active	<input checked="" type="checkbox"/>	
Advanced Application	Name	2	
Routing Protocol	Classifier(s)	<div style="border: 1px solid black; padding: 2px;"> 2 3 1 </div>	
Management	Parameters	VLAN ID	General: 1
Switch Advance		EgressPort	Port 12
EPON Advance		Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag
VLAN		Priority	0
Static MAC Forwarding		DSCP	
Filtering		TOS	0
Spanning Tree Protocol		Forwarding	<input type="radio"/> No change <input checked="" type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping
Bandwidth Control		Metering	Bandwidth: 9 Kbps Out-of-Profile DSCP: 3

3. Policy rule on classifier 3

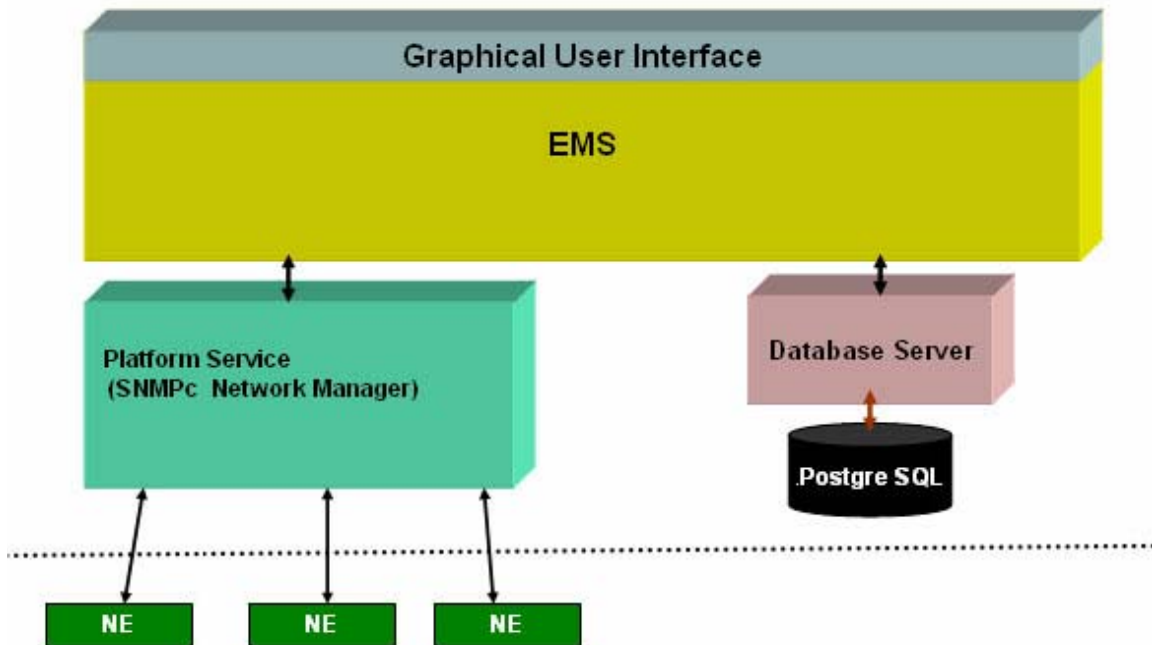
MENU		Policy	
Basic Setting	Active	<input checked="" type="checkbox"/>	
Advanced Application	Name	3	
Routing Protocol	Classifier(s)	<div style="border: 1px solid black; padding: 2px;"> 2 3 1 </div>	
Management	Parameters	VLAN ID	General: 1
Switch Advance		EgressPort	Port 12
EPON Advance		Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag
VLAN		Priority	0
Static MAC Forwarding		DSCP	
Filtering		TOS	0
Spanning Tree Protocol		Forwarding	<input type="radio"/> No change <input type="radio"/> Discard the packet <input checked="" type="radio"/> Do not drop the matching frame previously marked for dropping
Bandwidth Control		Metering	Bandwidth: 9 Kbps Out-of-Profile DSCP: 3

Centralized Management

Introduction to SNMPc and NetAtlas

With the number of network device increasing, the demand to detect and respond to network failures or events in a short time post a great challenge to network administrators. How to easily manage and monitor network devices across networks has become more and more important in network management. Figure 1 presents the main elements of the system architecture. As an Element Management System (EMS), NetAtlas provides a centralized remote management platform and acts as an SNMPc manager to perform network configuration, system management, event/alarm management, performance management and security for all ZyXEL's Ethernet switches. SNMPc is a network management software produced by Castle Rock that constantly probes the network element (NE) and collects information from these NE for the EMS. Running in the background to provide queries for the EMS is PostgreSQL, an enterprise relational database system

Figure 1 System Architecture

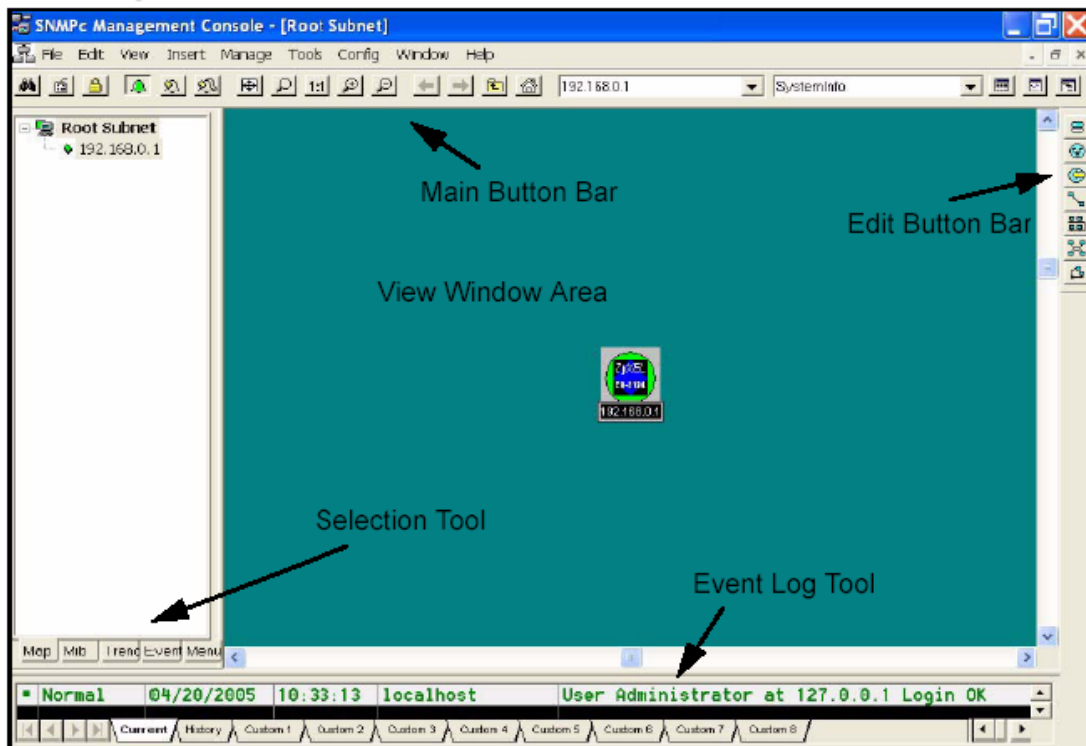


SNMPc Overview

The following figure shows the main screen elements of SNMPc.

- **Main Button Bar:** Button and controls to execute commands quickly
- **Edit Button Bar:** Button to quickly insert map element
- **Event Log Tool:** Button display filtered event log entries
- **View Window Area:** Map View, Mib Tables and Mib Graph windows are displayed here.
- **View Window Area:** Map View, Mib Tables and Mib Graph windows.

Figure 2 Main elements of SNMPc

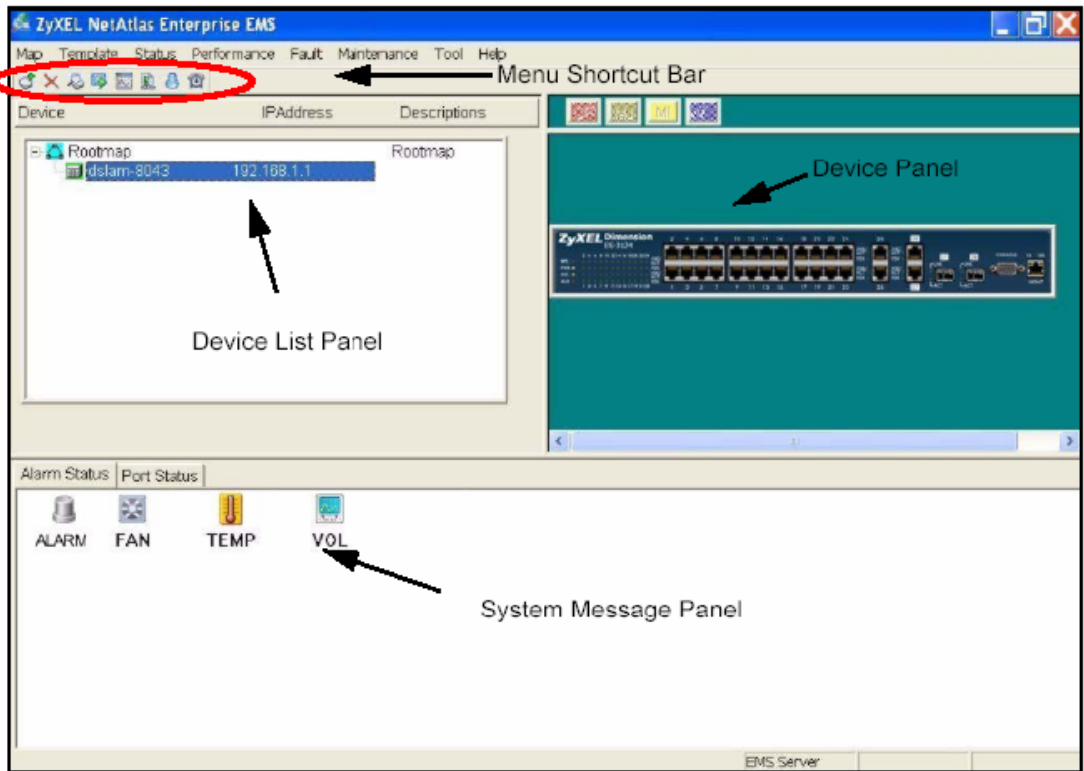


EMS Overview

The following figure illustrates the main elements in the EMS.

- **Menu Shortcut Bar:** The buttons execute common commands
- **Device Panel:** This is a graphical device display.
- **Device List Panel:** View devices in a tree structure. The colors of the device indicate the status of the devices. Green means the device is working properly and Red indicates no response from the device.
- **System message Panel:** View the alarm and port status of the selected switch.

Figure 3 EMS Overview



Adding a new device in SNMPc

This section shows you how to add a new device in SNMPc and access the EMS screen.

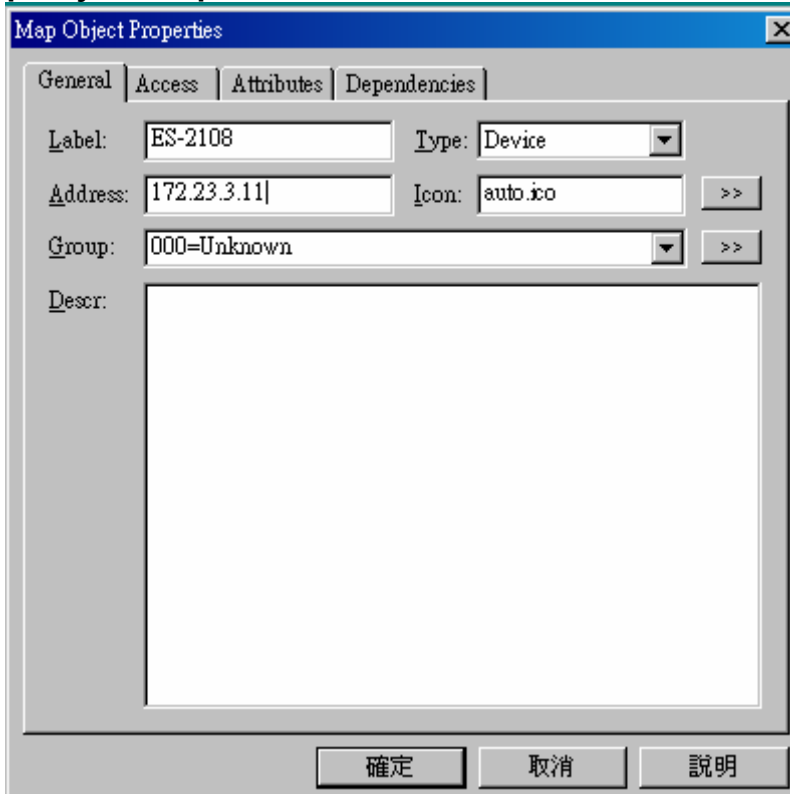
1. In the edit button bar shown in Figure 4, click the **Insert Device** icon to create a new device node.

Figure 4 Adding a new Device



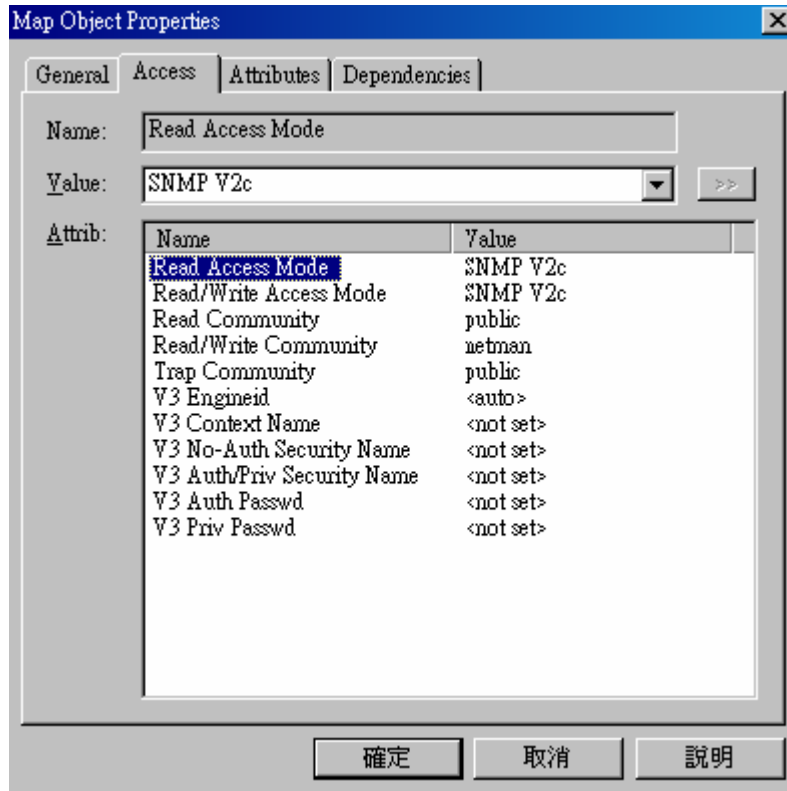
2. A **Map Object Properties** screen displays. Enter a descriptive name in the **Label** field. Then enter the IP address of the device in the **Address** field. For this example, we enter “192.168.0.1” as the IP address of the switch.

Figure 5 Map Object Properties



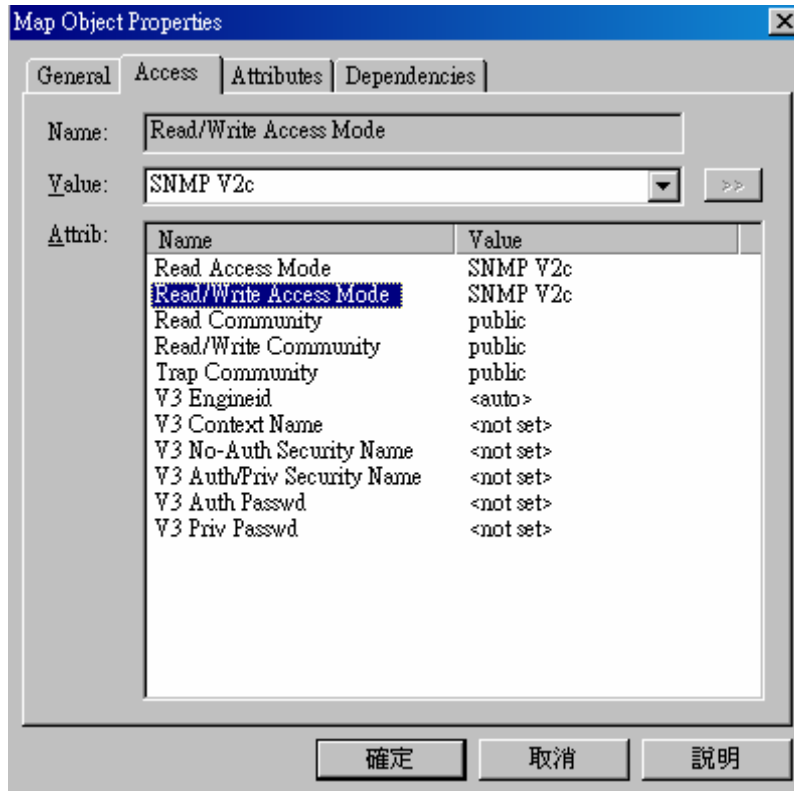
3. Click the **Access** tab to configure SNMP settings. Change the value for **Read Access Mode** to **SNMP V2c**.

Figure 6 Read Access mode



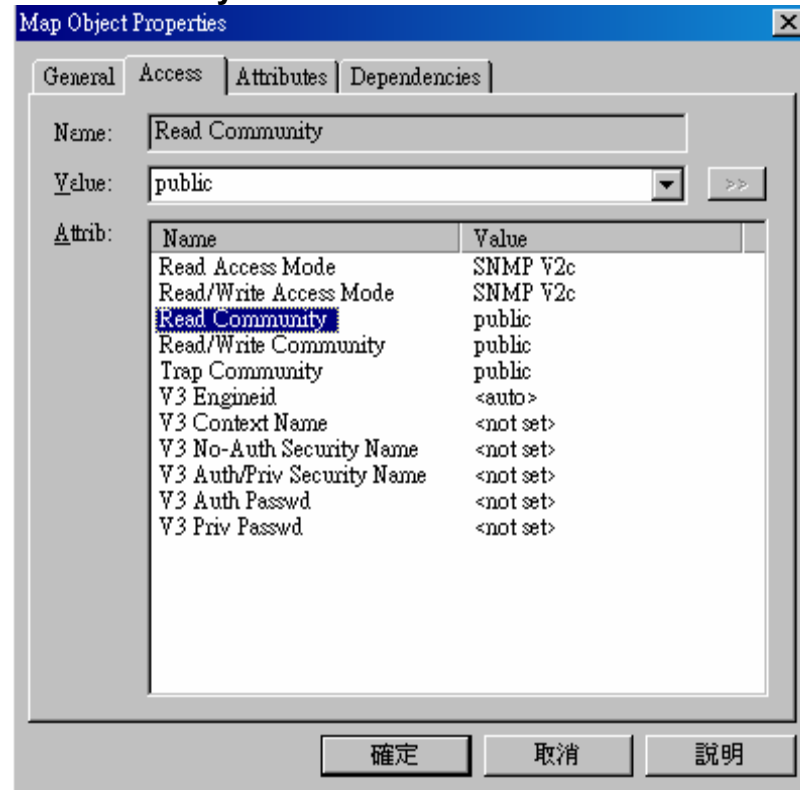
4. Change the value for **Read/Write Access Mode** to **SNMP V2c**. Screen settings should be similar to the one shown.

Figure 7 Read/Write Access Mode



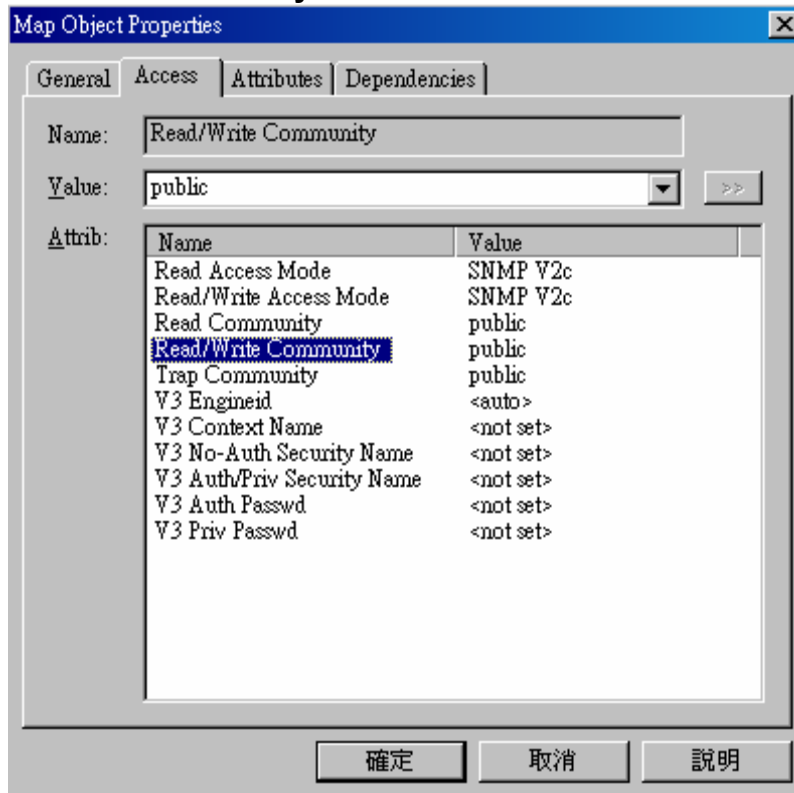
5. Change the value for **Read Community** to **public**.

Figure 8 Read Community



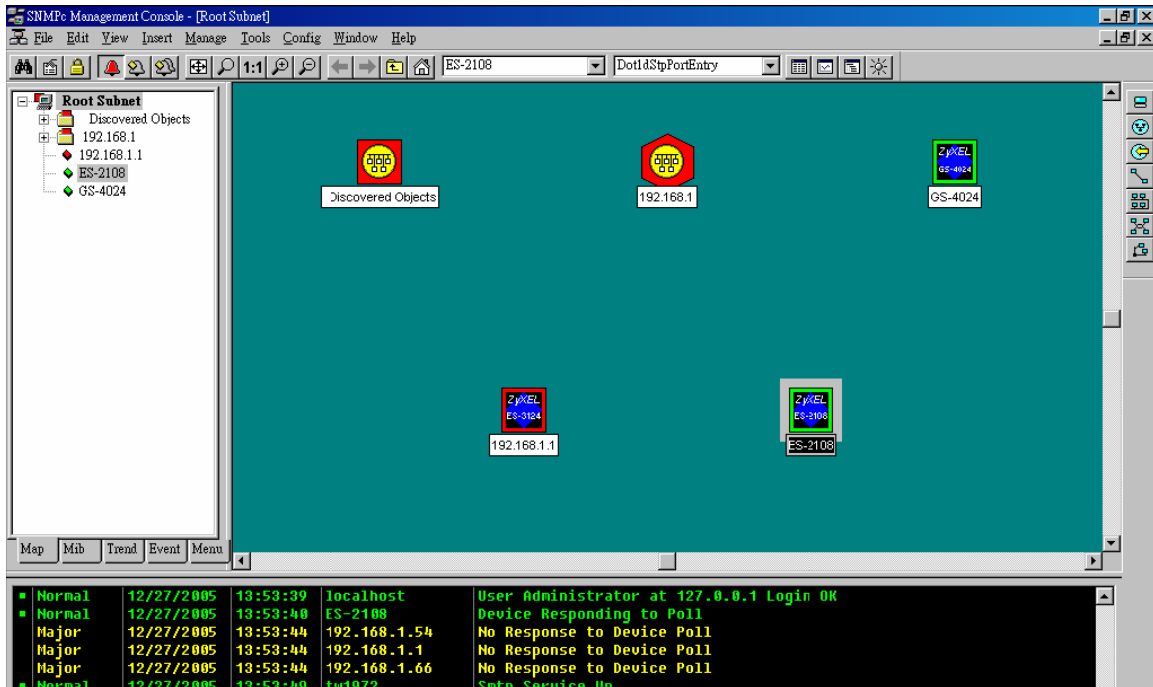
6. Change the value for **Read/Write Community** to **public**. Click **OK** to save the settings and close this screen.

Figure 9 Read/write Community



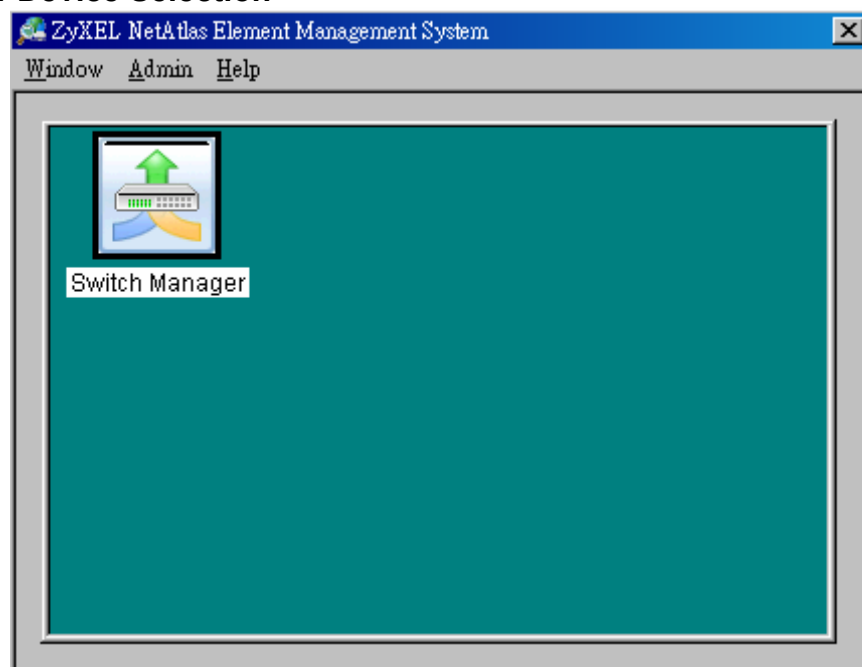
7. In the Selection tool menu, click the name of the switch you have just created to manage the device.

Figure 10 Device Selection

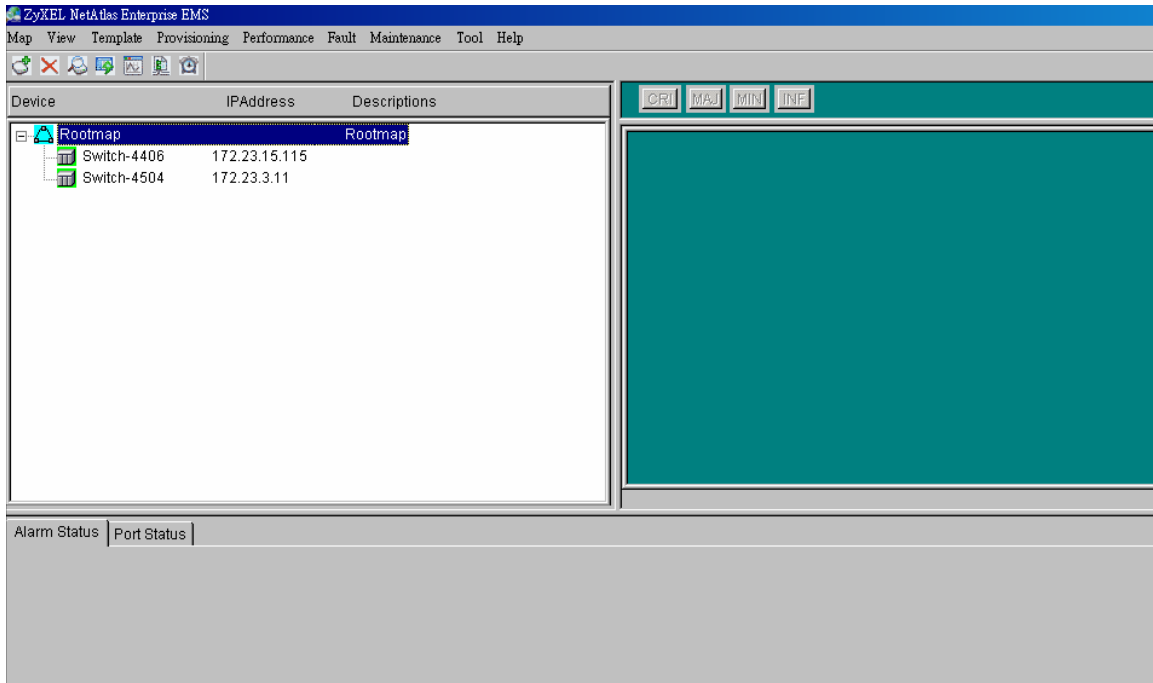


8. A screen displays as shown. Click **Switch Manager** to display the main EMS screen as shown in Figure 11

Figure 11 Device Selection

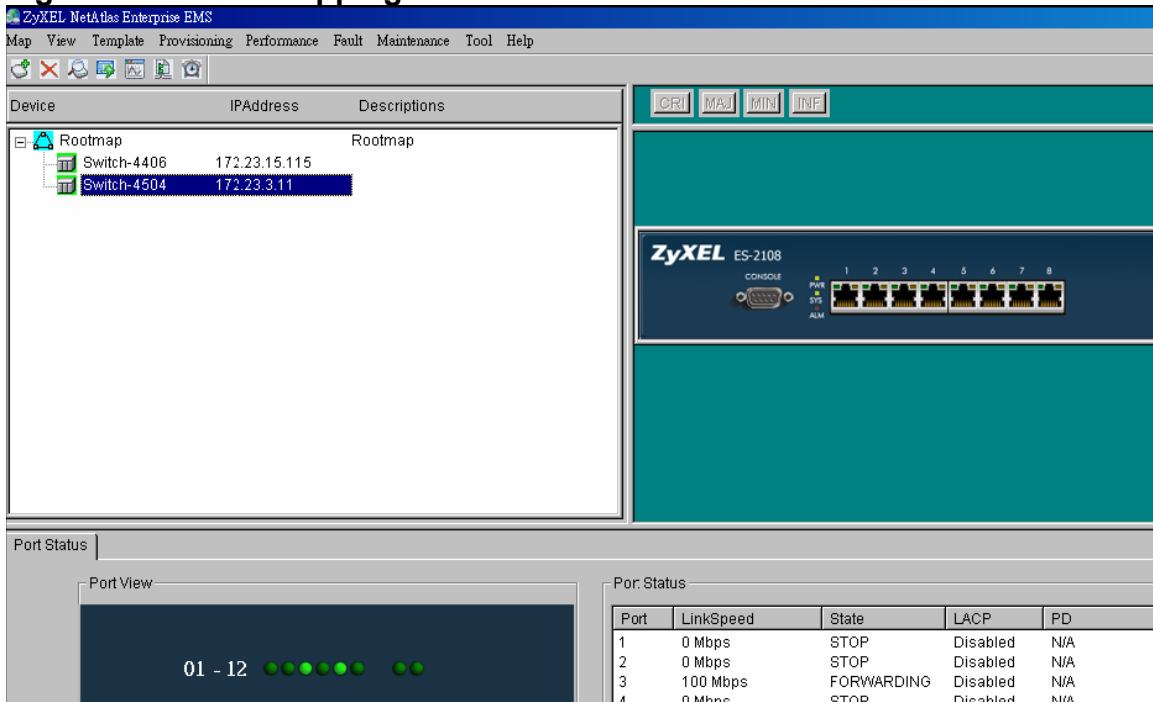


9. The device list panel on the left displays a logical hierarchy of the devices. You can also see the devices added under the Rootmap in this list. Figure 12 shows an example.



10. Click on a switch icon to display the device panel and status screen as shown in Figure 13.

Figure 13 Device mapping

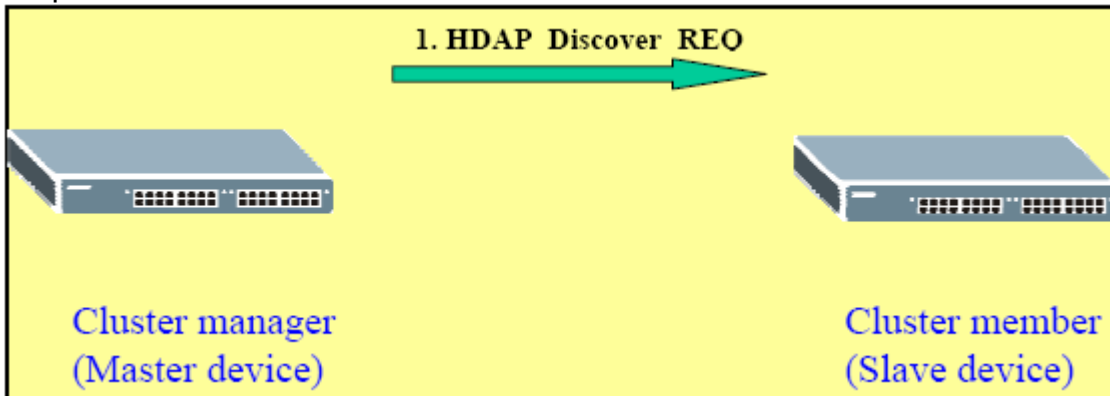


Cluster Management Overview

Cluster Management (also known as “istacking”) allows you to manage up to 8 switches through a single IP. This allows you to manage up to 8 switches simultaneously in the same broadcast domain and using the same VLAN group ID. The cluster manager which can manage other switches is called the master device.

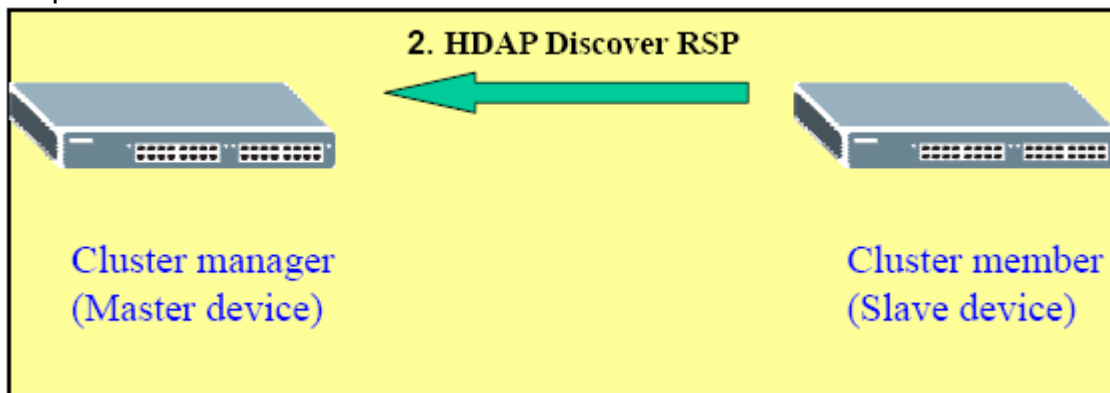
How Cluster Management works

Step 1:



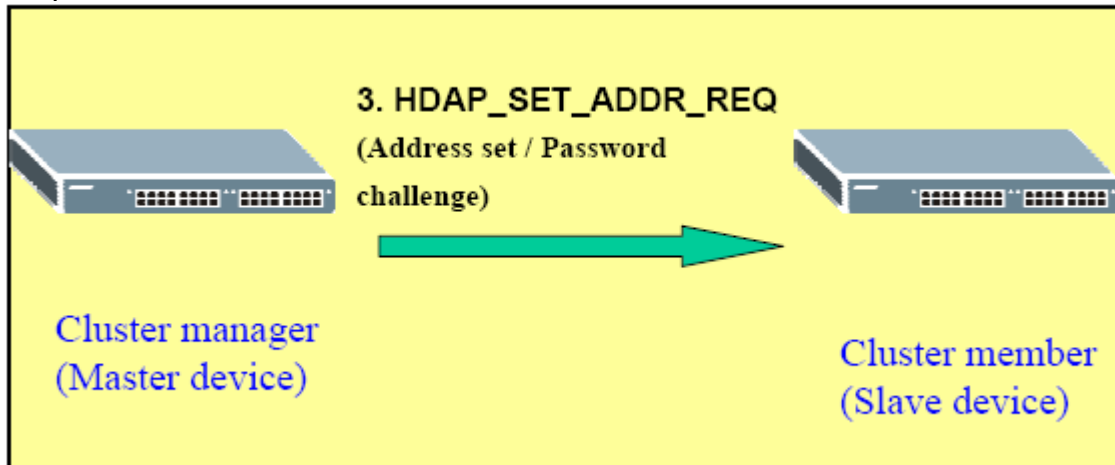
To discover the cluster members, the cluster manager broadcasts an HDAP (Host Discovery and Address assignment Protocol) Discover request.

Step 2:



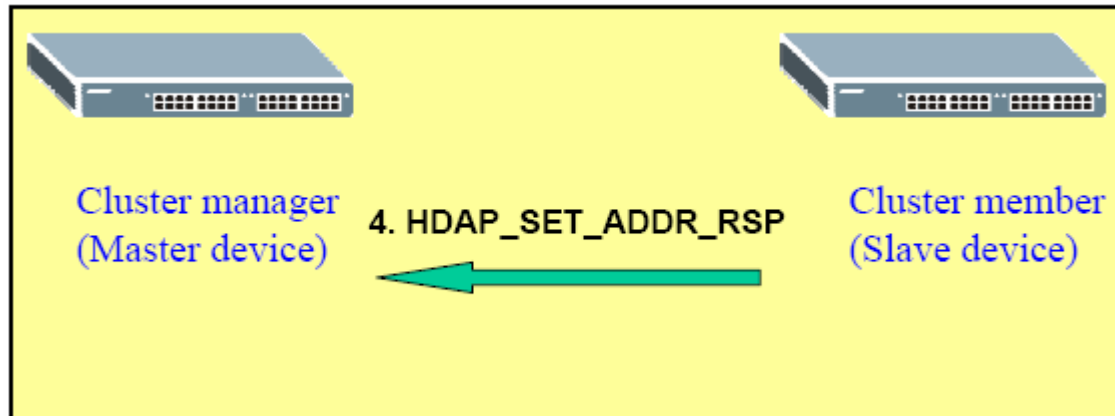
A cluster member listens on UDP port 263. When a cluster member receives a request with the matching signature, it answers with an HDAP Discover Response. In response, the cluster member returns with its identity information.

Step 3:



HDAP_SET_ADDR_REQ (Master device) packet request is used for a cluster manager to assign an IP address and subnet mask to a cluster member.

Step 4:



A cluster member uses an HDPA_SET_ADDR_RSP (Slave device) packet to acknowledge a "Set Address" request. The hardware address uniquely identifies the sender of this response.

After the process is done, the cluster master will be able to manage the slave switch.

Configuring Cluster Management

For this example, an OLT-1308 and OLT-1308 series switch are used to show you how to configure cluster management in the switch.

Step 1:

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management
- Maintenance
- Access Control
- Diagnostic
- Syslog
- Cluster Management
- MAC Table
- ARP Table
- IGMP Table

Clustering Management Configuration [Status](#)

Clustering Manager:

Active	<input type="checkbox"/>
Name	<input type="text"/>
VID	<input type="text" value="1"/>

Clustering Candidate:

List	<input type="text"/>
Password	<input type="text"/>

Access the web configurator on the switch and click **Management > Cluster Management > Clustering Management Configuration** in the navigation panel. In the **Clustering Management Configuration** screen, select the **Active** check box to enable this feature.

In the **Clustering Member List**, select a switch to add that switch as a cluster member.

Step 2:

You must then enter the administrator login account password for the selected switch. Click **Add**.

Step 3:

Index	MacAddr	Name	Model	Status
1	00:13:49:df:59:71	VES-1616F-35	VES-1616F-35	Online

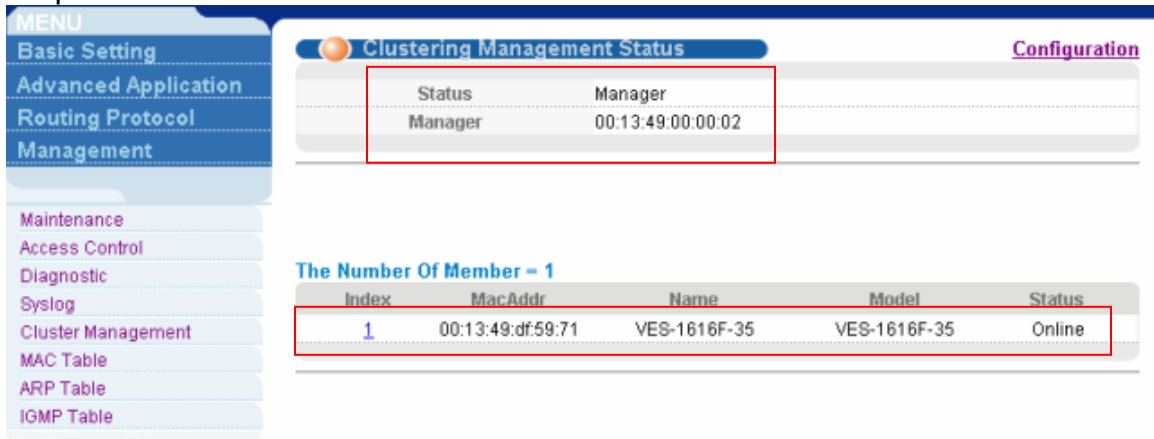
In the **Clustering Management Status** screen, click the index number for a cluster member to access the configuration screen for that device.

Step 4:



In **Member Menu** screen, you can click to change the settings of the cluster member, except **Cluster Management, Firmware Upgrade and Restore Configuration**.

Step 5:



To check the status of each cluster member, click **Management - Cluster Management - Clustering Management Status**.

FAQ

What are the default IP parameter settings?

IP address: 192.168.1.1
Subnet: 255.255.255.0

What is the default login Name and Password to log into the Web

Configurator?

ID: admin
Password: 1234

How to access my SWITCH through the console port?

Connect the male 9-pin end of the console cable to the console port of the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer. Launch a terminal emulation software configured to the follow settings:
Terminal emulation: VT100
Baud rate: 115200 bps
Data bits: 8
Parity: none
Stop bit: 1
Flow control: none

What is default login password for console, telnet, and FTP login?

Password: 1234

How to change the password?

You can only change the administrator login password in the web configurator.. After you log in for the first time, it is recommended you change the default administrator password.

In the Web Configurator: Click **Management > Access Control > Logins** to

display the configuration screen as shown. Then change the password by settings the password fields.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management
- Maintenance
- Access Control
- Diagnostic
- Syslog
- Cluster Management
- MAC Table
- ARP Table
- IGMP Table

Logins Access Control

Administrator

Old Password	<input type="text"/>
New Password	<input type="text"/>
Retype to confirm	<input type="text"/>

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

How to access the Command Line Interface (CLI)?

There are two ways to access the Command Line Interface: through the console port or Telnet.

If you want to access through the console port, Refer to the “How to access the Switch through the console port?” section for more information.

If I have forgotten the password, how to reset the password to the default setting?

If you have changed and forgotten the password, you will need to reload the factory default configuration. Note that all your previous configuration will be lost.

1. Connect the console cable to your computer and launch a terminal emulation software.
2. Restart the switch, and press any key to enter the debug mode at the “Press any key to enter Debug Mode within 3 seconds” prompt.
3. Enter “atlc”.
4. When the “starting XMODEM upload” message displays, start XMODEM upload of the default configuration (rom) file to the switch.

5. After the file upload process is complete, enter “atgo” to exit from the debug mode.
6. The system will automatically restart. Wait until the system has restarted before you log in again. The default IP address is 192.168.1.1 and the default password is 1234.

How to configure the IP address?

Using the Web Configurator

Click **Basic Setting > IP Setup** in the navigation panel to display the configuration screen.

MENU

- Basic Setting
- Advanced Application
- Routing Protocol
- Management

System Info

General Setup

Switch Setup

IP Setup

Port Setup

EPON Setup

IP Setup

Domain Name Server: 0.0.0.0

Default Management: In-band Out-of-band

In-band Management IP Address

DHCP Client

Static IP Address

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

VID: 1

Out-of-band Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

Is Online Help available on the Web Configurator?

Yes. You can click on the Help link in any web configurator screen to display the help content for that screen.

How to restart device from the Web Configurator?

1. Click **Management > Maintenance** in the navigation panel to display the screen as shown.

The screenshot shows the web interface of a ZyXEL OLT-1308/OLT-1308H switch. On the left is a 'MENU' sidebar with options: Basic Setting, Advanced Application, Routing Protocol, Management, Maintenance (highlighted), Access Control, Diagnostic, Syslog, Cluster Management, MAC Table, ARP Table, and IGMP Table. The main content area is titled 'Maintenance' and contains two sections of options:

Option	Action
Remote Firmware Upgrade	Click here
OLT Chip Reset	Click here
ONU Device Reset	Click here
Firmware Upgrade	Click here
Restore Configuration	Click here
Backup Configuration	Click here
Load Factory Default	<input type="button" value="Click here"/>
Reboot System	<input type="button" value="Click here"/>

The 'Reboot System' option and its 'Click here' button are highlighted with a red rectangular box.

2. Click **Click Here** button next to **Reboot System** will restart the switch.

How to check the current running firmware version?

Access the console and enter the “show system-information” command. This will display the firmware version the switch is currently using.

Is the mini GBIC transceiver hot-swappable?

Yes, it is hot-swappable. You can change transceivers while the switch is operating.

What is "Dual-Personality interface" on a VDSL Switch?

Dual-Personality GbE interface means that one 1000Base-T Copper port and one SFP port shares the same physical interface. Only one of them can be used at a time. Dual-Personality interface is also known as a "Combo Port".

Can I enable IGMP snooping on the Switch which is acting as an IGMP

Router?

No. You do not need to enable IGMP Snooping on an IGMP Router. IGMP Snooping should be enabled on the access layer device, which is normally a L2 switch.

Can I enable MVR and IGMP snooping at the same time?

Yes.