# ZyXEL ES-4024A Series

(ES-4024A)

**Ethernet Switch**

# Support Notes

Version 3.60

March 2006

ZyXEL Unleash Networking Power

## INDEX

**What is the default login Name and Password of the Web Configuration?**
**How to access the Switch through the console port?**
**What is default login password of the console, telnet, and FTP?**
**How to change the password?**
**How to access the Command Line Interface?**
**If I forgot the Switch password, how can I reset the password to default?**
**How do I configure an IP address?**
**Is Online Help available on the Web GUI?**
**How to restart device from Web?**
**How to check the current running firmware version?**
**Is the mini GBIC transceiver hot-swappable?**
**What is so called "Dual-Personality interface" in Ethernet Switching?**

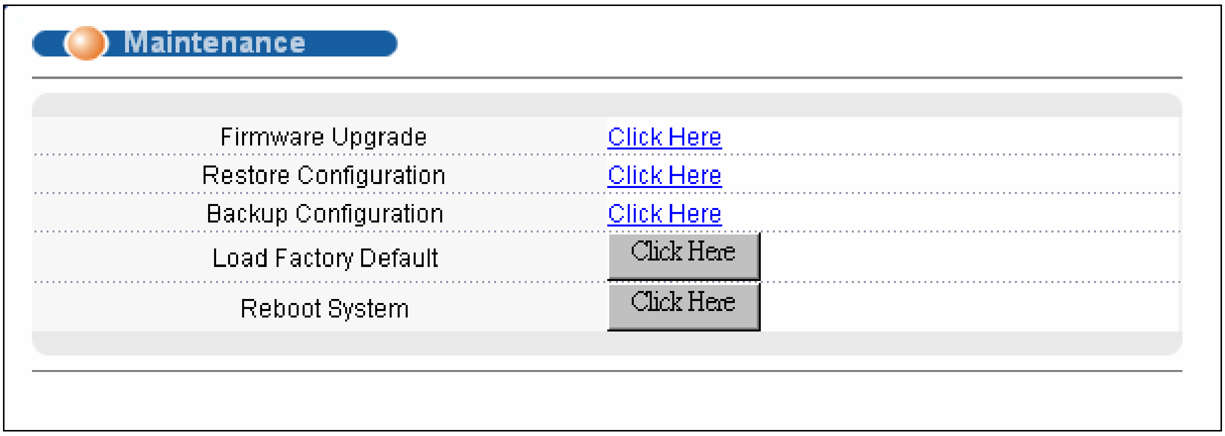
*Remaining:*
*Some demonstration in this support note may not use the exact model that you are using. However, their functions and settings work the same way.*

# How to manage & maintain your Switch?

## Firmware Upgrade

**From Web GUI:**

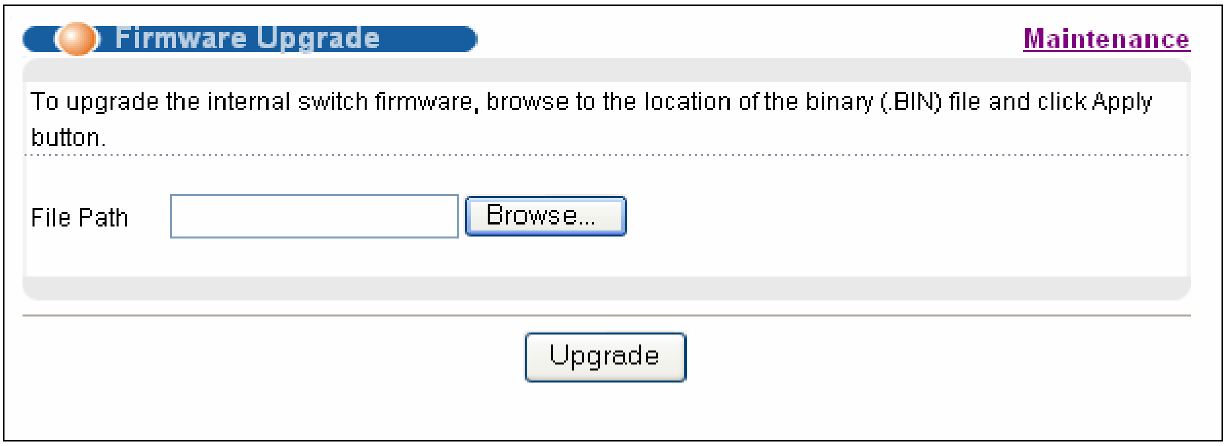
1. Download (and unzipped) the correct model firmware to your computer.
2. Click Management and then Maintenance in the navigator panel to bring up the following screen.



Maintenance

| | |
|---|---|
| Firmware Upgrade | Click Here |
| Restore Configuration | Click Here |
| Backup Configuration | Click Here |
| Load Factory Default | Click Here |
| Reboot System | Click Here |

3. Click on the "Click Here" link of the Firmware Upgrade to bring up the following screen.



Firmware Upgrade

To upgrade the internal switch firmware, browse to the location of the binary (.BIN) file and click Apply button.

File Path

4. Browse the firmware located or type in the path into the "File Path" field.
5. Click on the Upgrade button.

**From Console Port:**

1. Download (and unzipped) the correct model firmware to your computer.
2. Connect to the console port and open the Terminal Emulation Software.
3. Restarting the switch to enter the debug mode via the terminal.
4. Enter “ATUR”.
5. Use X-modem protocol to transfer (Send File) the firmware.
6. Enter “ATGO” to restart the switch after done uploading the firmware.

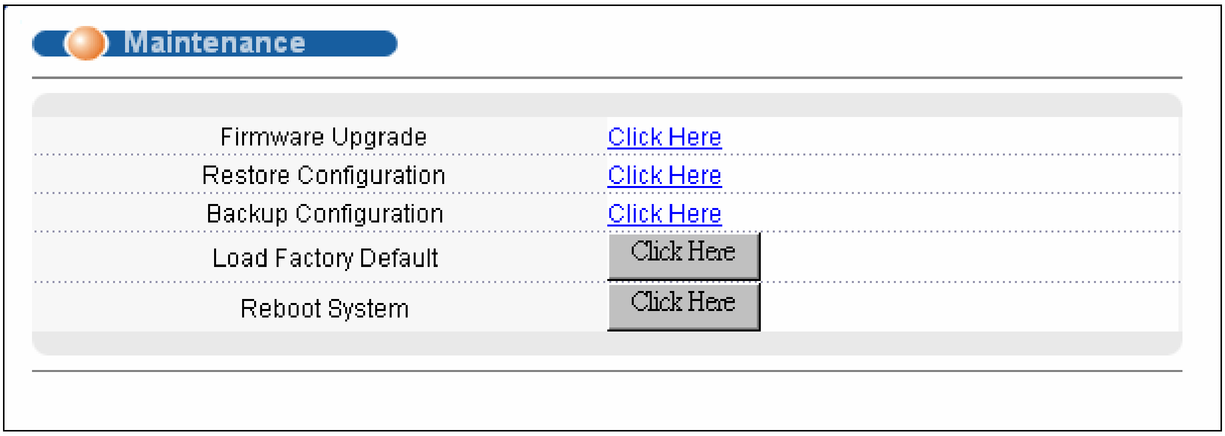
**From Command Line FTP:**

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your PC to login to Switch. (From the command prompt, type “ftp <Switch IP>”
3. Press “Enter” for the User name
4. Enter password to get the ftp prompt.
5. Enter “bin” to set 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 “ras”.
7. Enter “quit” to exit the ftp prompt.

## Restore a Configuration File

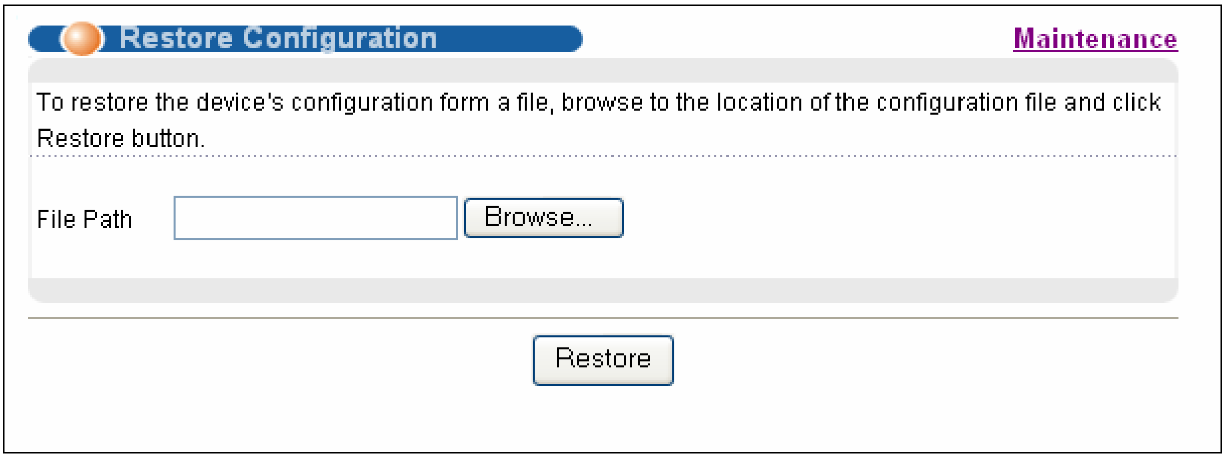
**From Web GUI:**

1. Click Management and then Maintenance in the navigator panel to bring up the following screen.



| | |
|---|---|
| Firmware Upgrade | Click Here |
| Restore Configuration | Click Here |
| Backup Configuration | Click Here |
| Load Factory Default | Click Here |
| Reboot System | Click Here |

2. Click on the “Click Here” link of the Restore Configuration to bring up the following screen.



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

File Path

3. Browse to locate the file with the file name or type in the path and the file name into the “File Path” field.
4. Click on the Restore button.

**From Console Port:**

1. Connect to the console port and open the Terminal Emulation Software.

2. Restarting the Switch to enter the debug mode via the terminal.
3. Enter “ATLC”
4. Use X-modem protocol to transfer (Send File) the firmware.
5. Enter “ATGO” to restart the Switch after done uploading the configuration file.

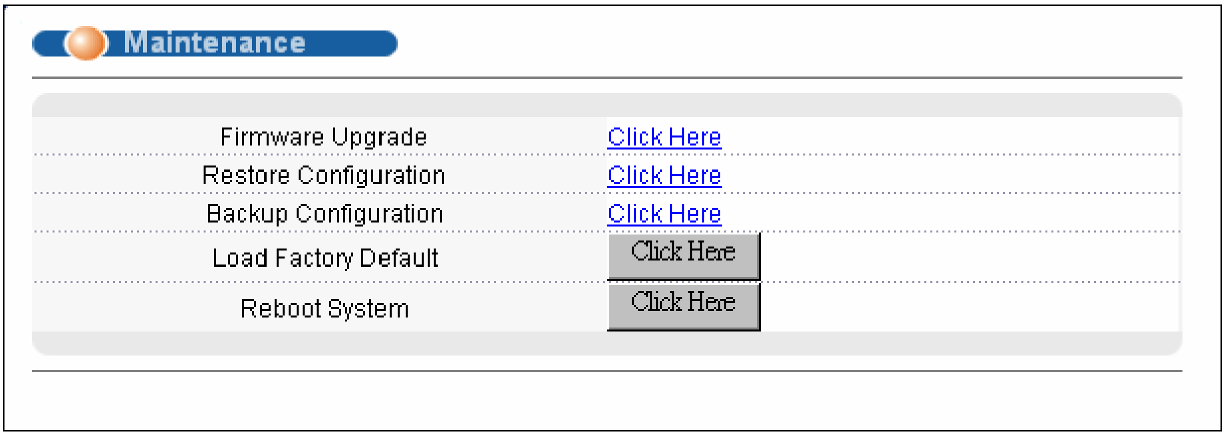
**From Command Line FTP:**

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your PC to login to Switch. (From the command prompt, type “ftp <Switch IP>”.
3. Press “Enter” for the User name
4. Enter password to get the ftp prompt.
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer the the configuration file from the computer to the switch, for example: “put comfig.rom rom-0” transfers the firmware on your computer (config.rom) to the switch and renames it “rom-0”.
7. Enter “quit” to exit the ftp prompt.

# Backing Up a Configuration File

**From Web GUI:**

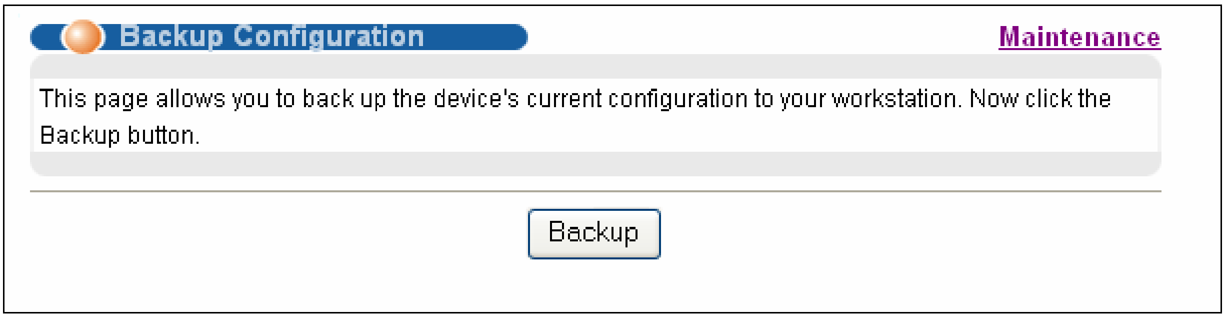
1. Click Management and then Maintenance in the navigator panel to bring up the following screen.



Maintenance

| | |
|---|---|
| Firmware Upgrade | Click Here |
| Restore Configuration | Click Here |
| Backup Configuration | Click Here |
| Load Factory Default | Click Here |
| Reboot System | Click Here |

2. Click on the "Click Here" link of the Backup Configuration to bring up the following screen.



Backup Configuration

Maintenance

This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.

Backup

3. Click on the "Backup" button to bring up the File Download dialog. Then, clicking on the Save button to backup the configuration rom file to a proper location.

**From Console Port:**

1. Connect to the console port and open the Terminal Emulation Software.
2. Restarting the Switch to enter the debug mode via the terminal.
3. Enter "ATTD"

4. Use X-modem protocol to transfer (Receive File) the firmware.
5. Enter “ATGO” to restart the Switch after done uploading the configuration file.

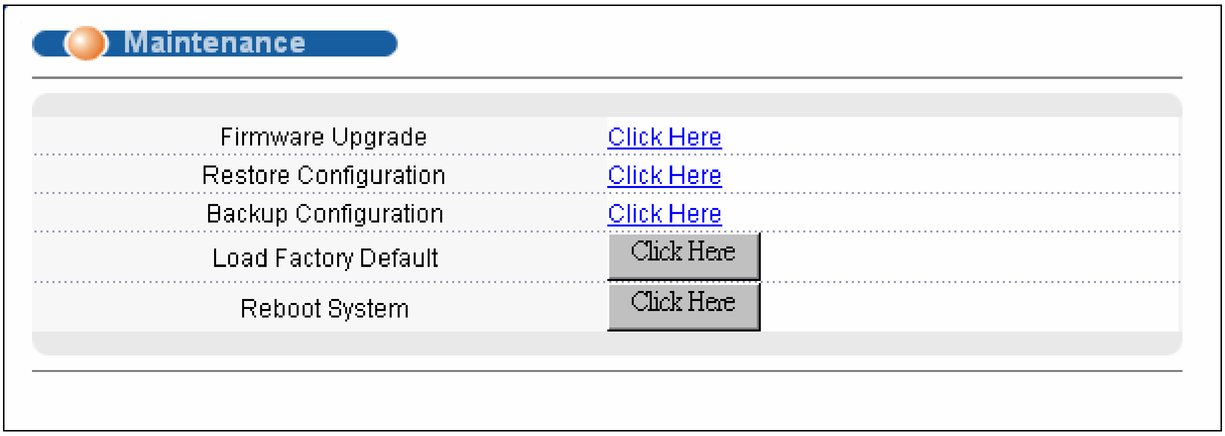
**From Command Line FTP:**

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your PC to login Switch. (From the command prompt, type “ftp <Switch IP>”
3. Press “Enter” for the User name
4. Enter password to get the ftp prompt.
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer the firmware from the computer to the switch, for example: “get rom-0 config.rom” transfers the firmware on your computer (config.rom) to the switch and renames it “config.rom”.
7. Enter “quit” to exit the ftp prompt.

# Load Factory Defaults

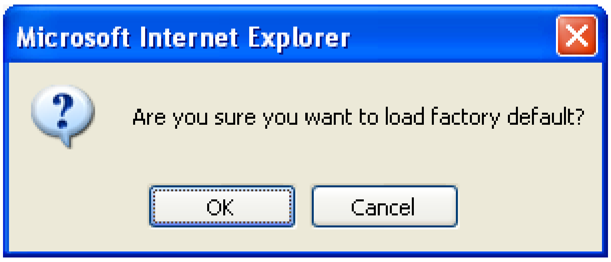
**From Web GUI:**

1. Click Management and then Maintenance in the navigator panel to bring up the following screen.



| Maintenance | |
|---|---|
| Firmware Upgrade | Click Here |
| Restore Configuration | Click Here |
| Backup Configuration | Click Here |
| Load Factory Default | Click Here |
| Reboot System | Click Here |

2. Click on the “Click Here” button of the Load Factory Defaults to bring up the following screen.
3. A dialog pops up with the message “Are you sure you want to load factory defaults?”.



Microsoft Internet Explorer

Are you sure you want to load factory default?

4. Click OK to go to the following dialog.
5. Click on the OK button. Now, all switch configurations has been reset to the factory defaults and the system will be restarted.
6. Please note that the switch IP address is now 192.168.1.1.

**From Console Port:**

1. Connect to the console port and open the Terminal Emulation Software.
2. Type in the correct password to bring up the prompt.

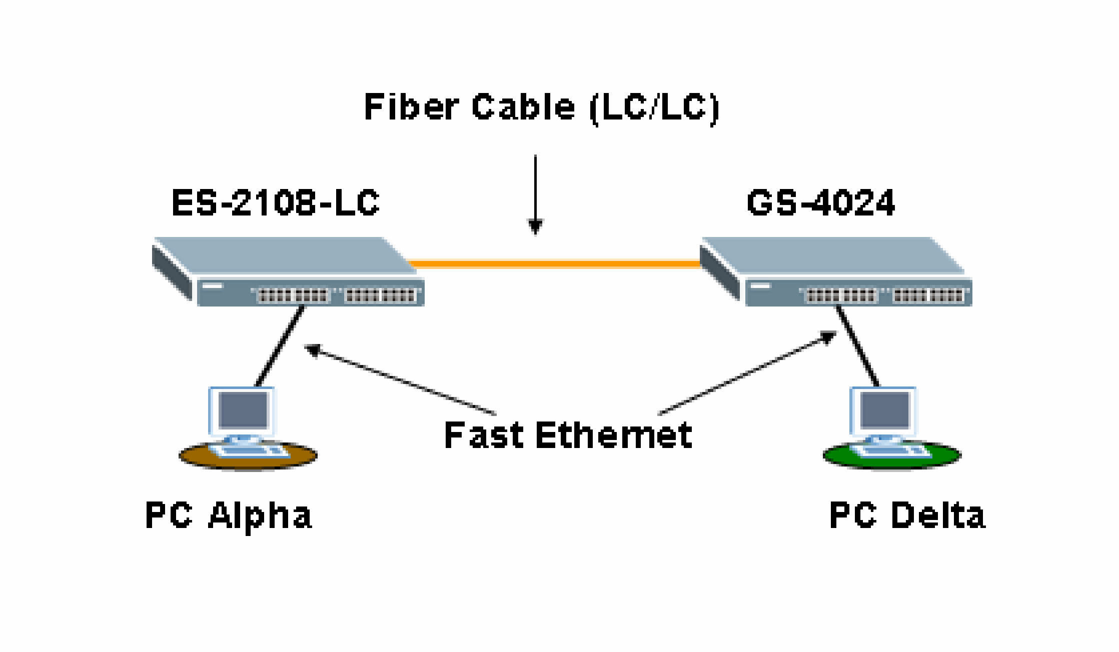
   Type “erase run” to load the factory default configurations.

# Physical Switch connection

## How to connect two switches via Fiber Channel

Your Switch may come with one or many mini-GB ports. ZyXEL offers Small Form-factor Pluggable (SFP) transceivers for Gigabit Ethernet and Fiber Channel applications. These small, modular optical interface transceivers offer a convenient and cost effective solution for the adoption of Gigabit Ethernet and Fiber Channel in data center, campus, metropolitan area access, ring networks, and storage area networks. It supports full duplex Gigabit speeds and hot-pluggable feature.

## Scenario

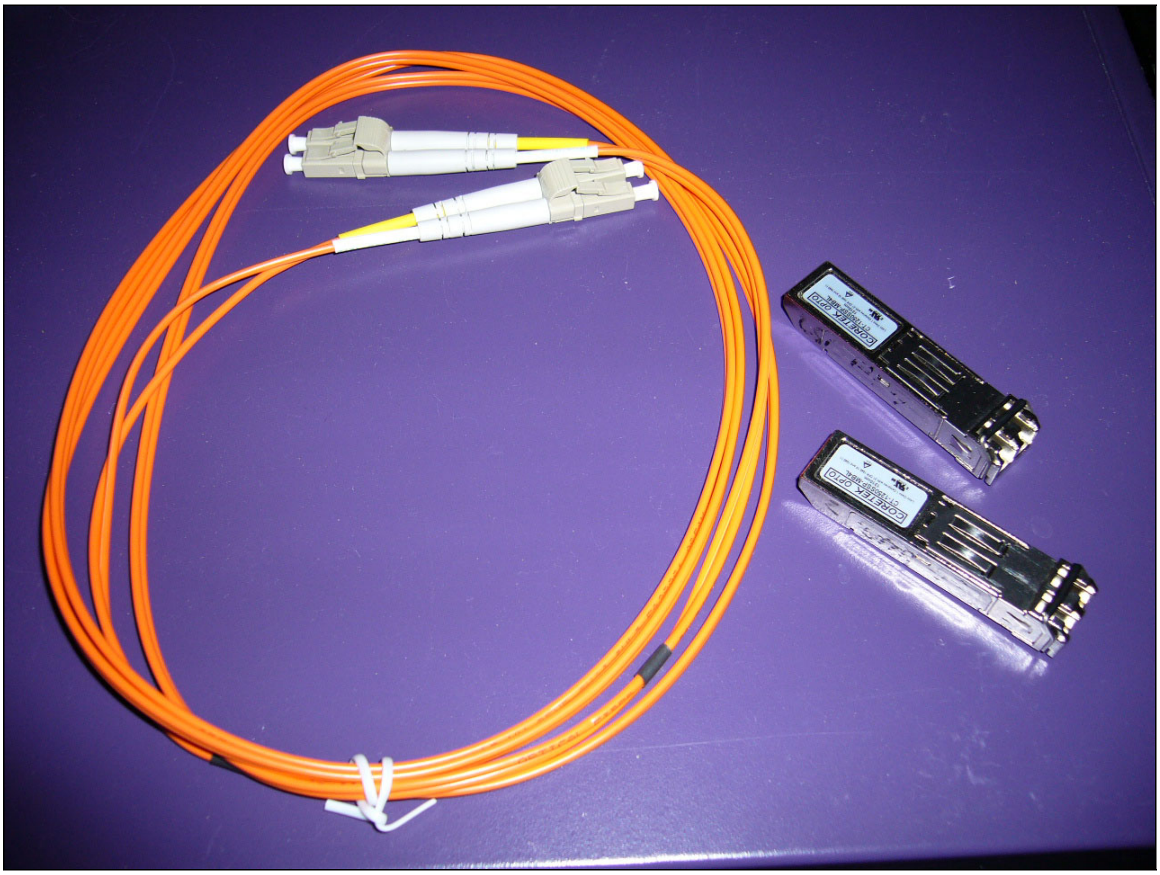


In this scenario, ES-2108-LC is connected to GS-4024 via the mini-GB Port with a LC/LC Fiber cable (62.5/125MM). PC “Alpha” is connected to ES-2108-LC and another PC “Delta” is connected to the GS-4024 Switch via the RJ45 Port.

What you need here to complete this scenario:

- **ZyXEL Switch with Mini-GB port x2**
  **(note: Each ES-4024A Series Switch comes with 2 Mini-GB Port)**
- **SFP-SX Transceiver x2**
- **LC/LC Fiber Cable (62.5/125MM) x1**

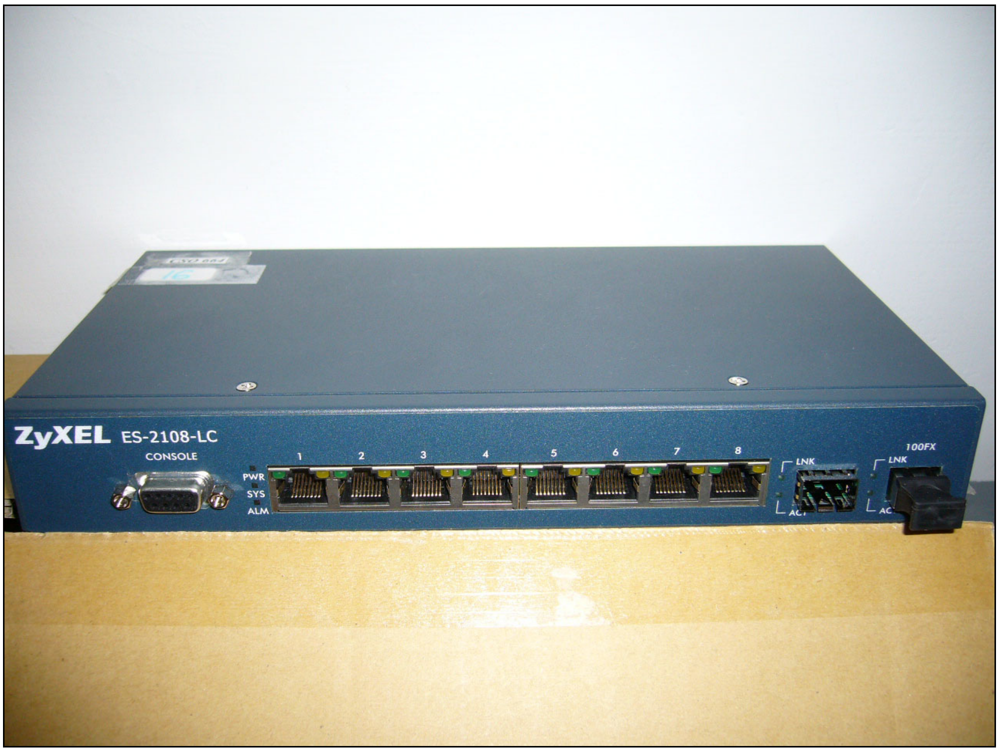
Here is the photo of the SFP-SX Transceiver & the LC/LC Fiber Cable.



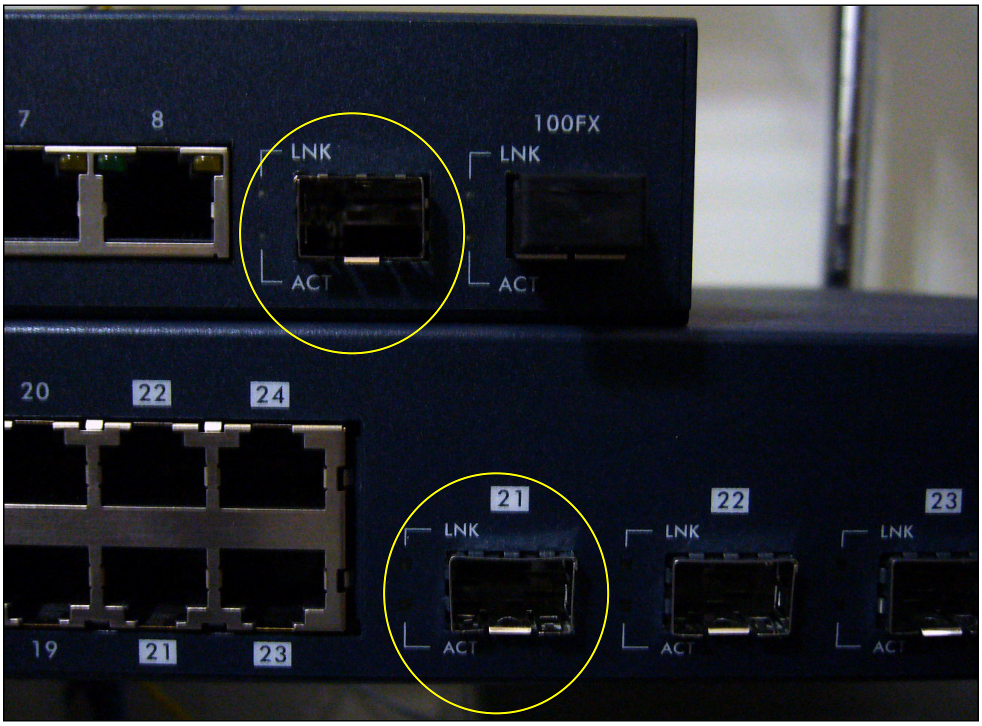
## Steps to complete this scenario

1. First, pick up your ES-2108-LC and GS-4024Switch and power them up.

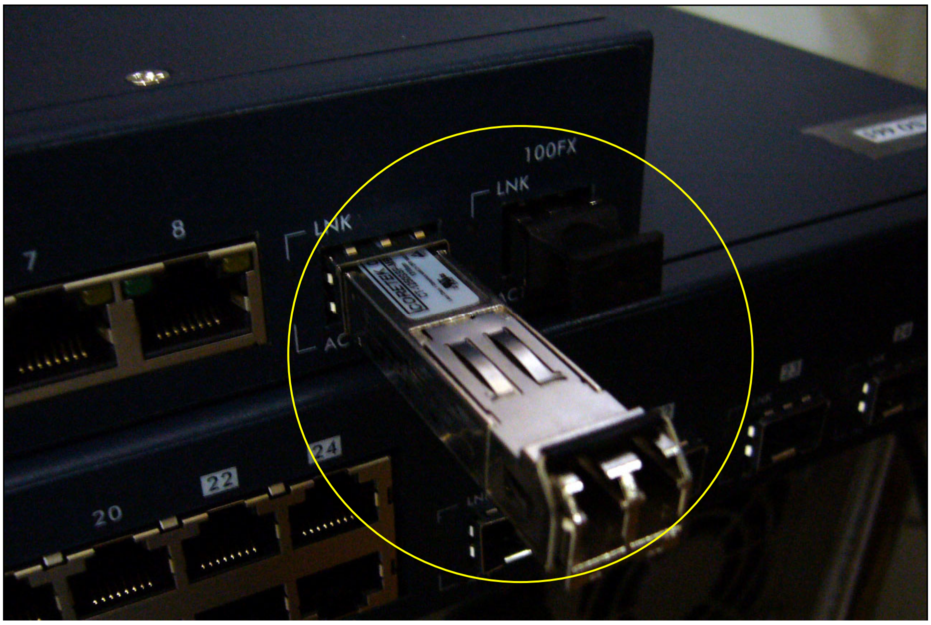
Photo of the ES-2108-LC Switch



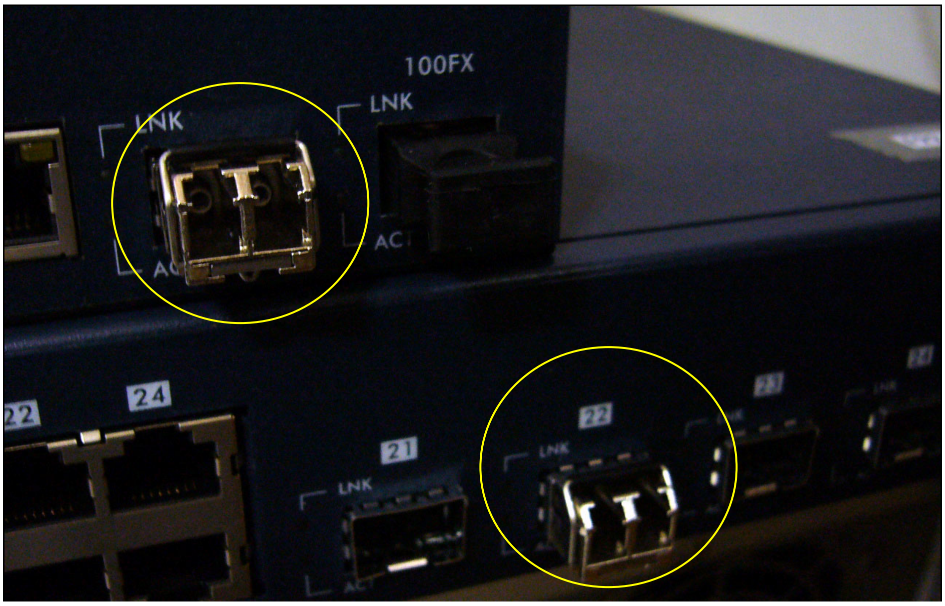
2. Find both Mini-GB Port on ES-2108-LC and GS-4024.



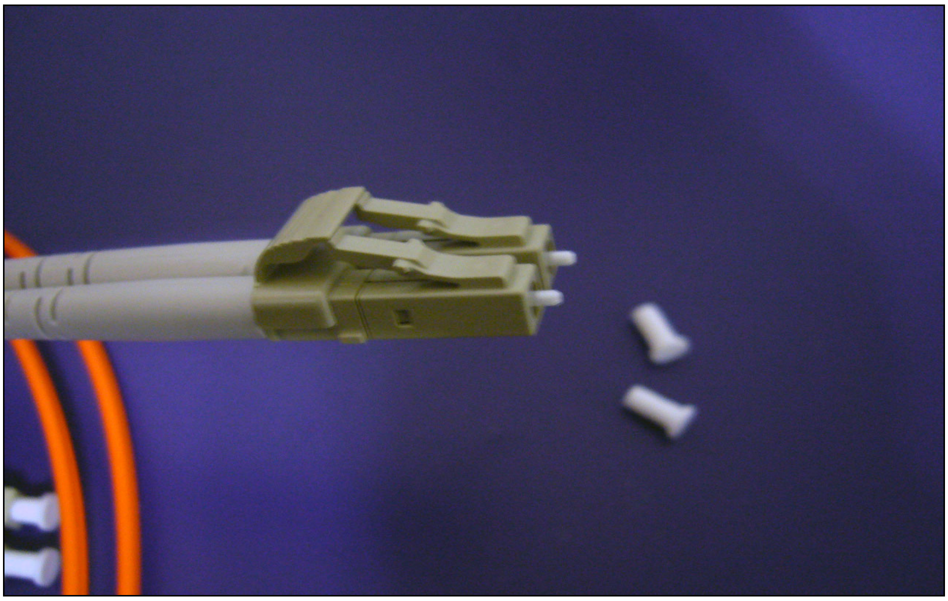
3. Get one transceiver and plug it into the Mini-GB Port of ES-2108-LC



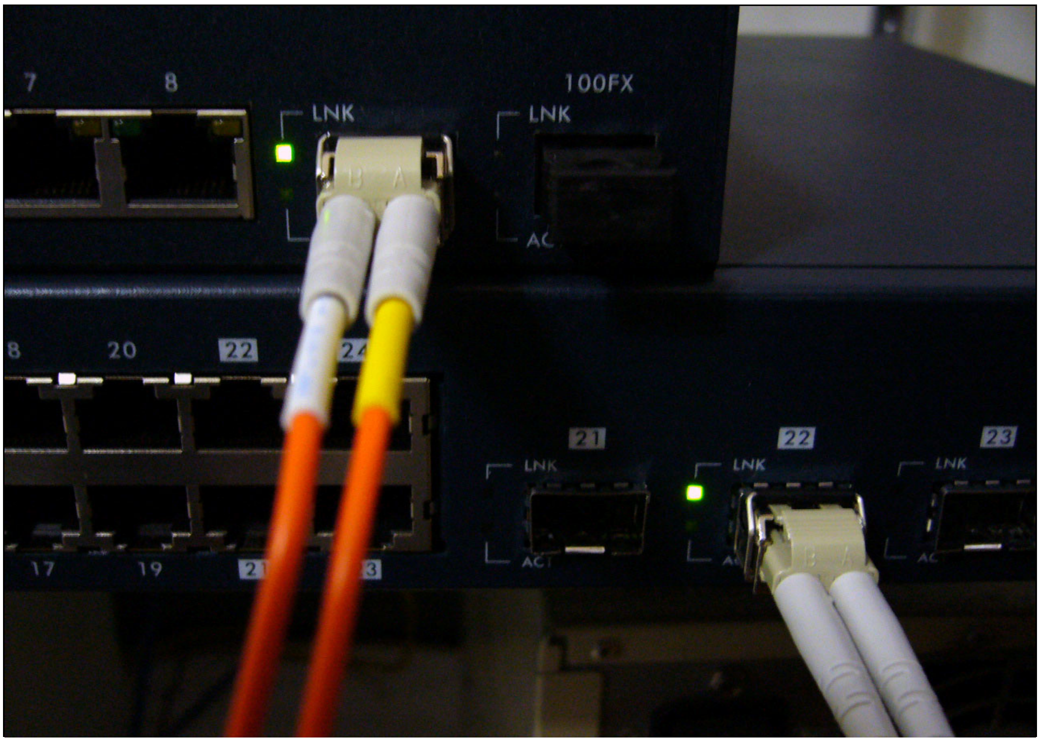
4. Plug another transceiver into the Mini-GB Port of GS-4024 Switch



5. Remove both side of the protection cap from the LC/LC Fiber Cable.

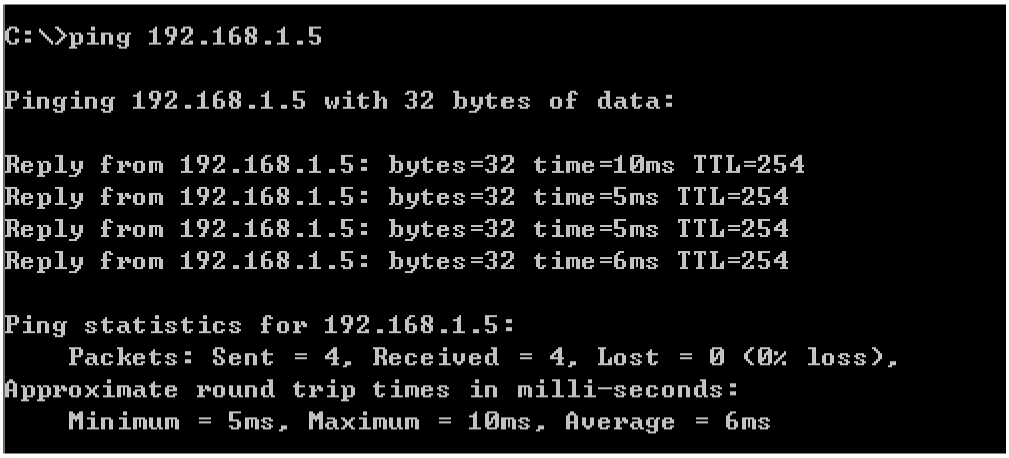


6. Plug the LC/LC Fiber Cable into the transceivers on both ES-2108-LC and GS-4024 Switch.



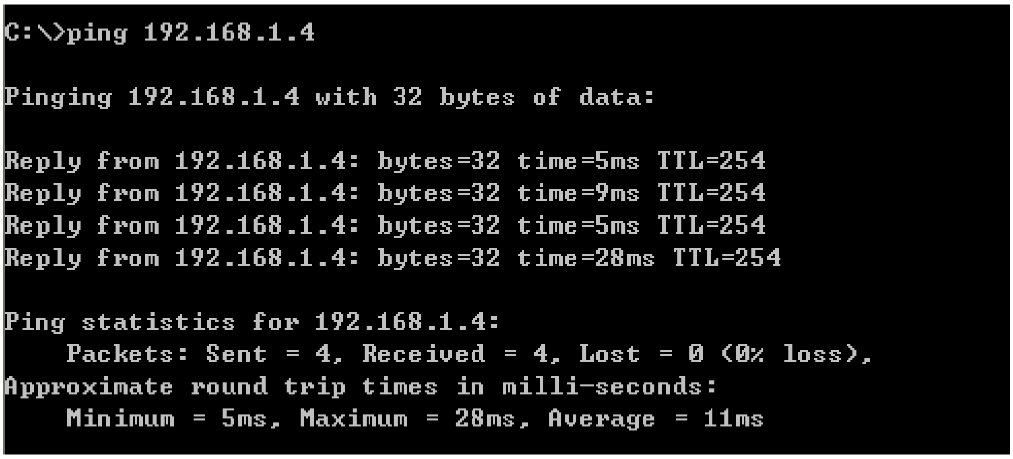
If you connected the cable correctly, the LED of the "LINK" will light up.

7. Now, connect the first PC “Alpha” to ES-2108-LC and the second PC “Delta” to the GS-4024 via the regular Ethernet cable.
8. Set the NICs in both computers to the same IP Domain.
   (ex, PC “Alpha” :192.168.1.4/24;      PC “Delta” : 192.168.1.5/24)
9. From PC “Alpha”, PING PC “Delta” at 192.168.1.5



```
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=10ms TTL=254
Reply from 192.168.1.5: bytes=32 time=5ms TTL=254
Reply from 192.168.1.5: bytes=32 time=5ms 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 = 5ms, Maximum = 10ms, Average = 6ms
```

10. From PC “Delta”, PING PC” Alpha” at 192.168.1.4



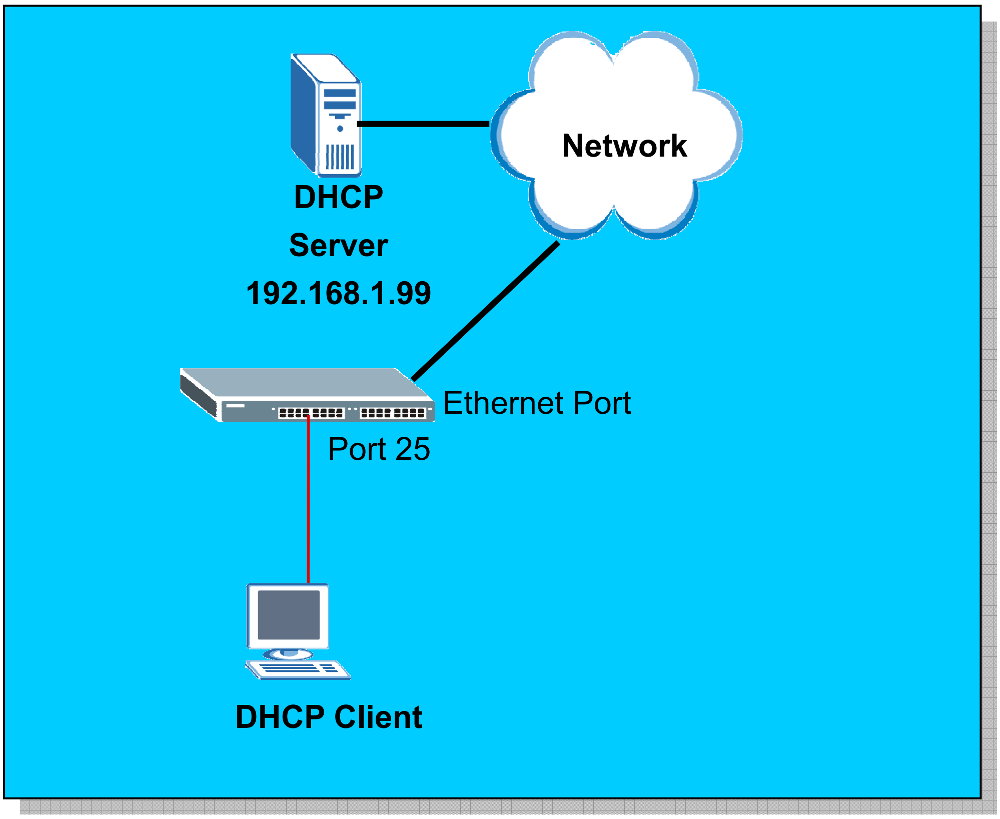
```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=5ms TTL=254
Reply from 192.168.1.4: bytes=32 time=9ms TTL=254
Reply from 192.168.1.4: bytes=32 time=5ms TTL=254
Reply from 192.168.1.4: bytes=32 time=28ms TTL=254

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 28ms, Average = 11ms
```

11. Now you can confirm that the network connection between ES-2108-LC and GS-4024 is up and running.

# General Networking

## DHCP Relay Option 82 Application

ISP may want to limit the number of IP address or deliver some specific IP addresses according to certain Switch port, VLAN ID and option 82 string. They can easily to achieve this with DHCP Relay Option 82 feature and a DHCP server supporting Option 82 function.

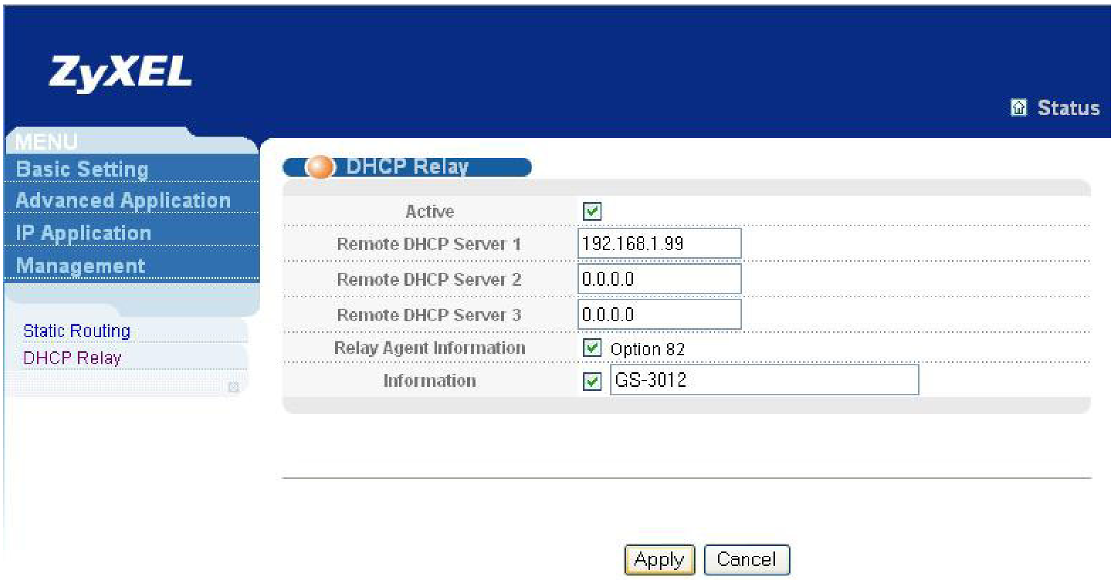


# How to set up DHCP Relay Option 82 Environment

Here, we will set up an environment to allow a PC to get DHCP IP address in specific IP pool according to its Switch port, VLAN ID and the option 82 string. In this case, we are using GS-3012 for the demonstration. PC is behind 25th Switch port and the option 82 string is a string “GS-3012”. We use the IP Commander as DHCP server. Its IP is 192.168.1.99 and the IP pool is between 192.168.1.201 and 192.168.1.203 for VID=1, Switch port=25 and the option 82 string is “GS-3012”.

## 1. Switch (GS-3012) settings

Click **IP Application**, **DHCP Relay** in the navigation panel to display configuration screen as shown. You will see the **DHCP Relay** setup page. Active the DHCP relay and Option 82 function. Also, click **Information** to make “GS-3012” as the Option 82 string. **Information** is READ ONLY here and it is the same as the host name of the Switch.

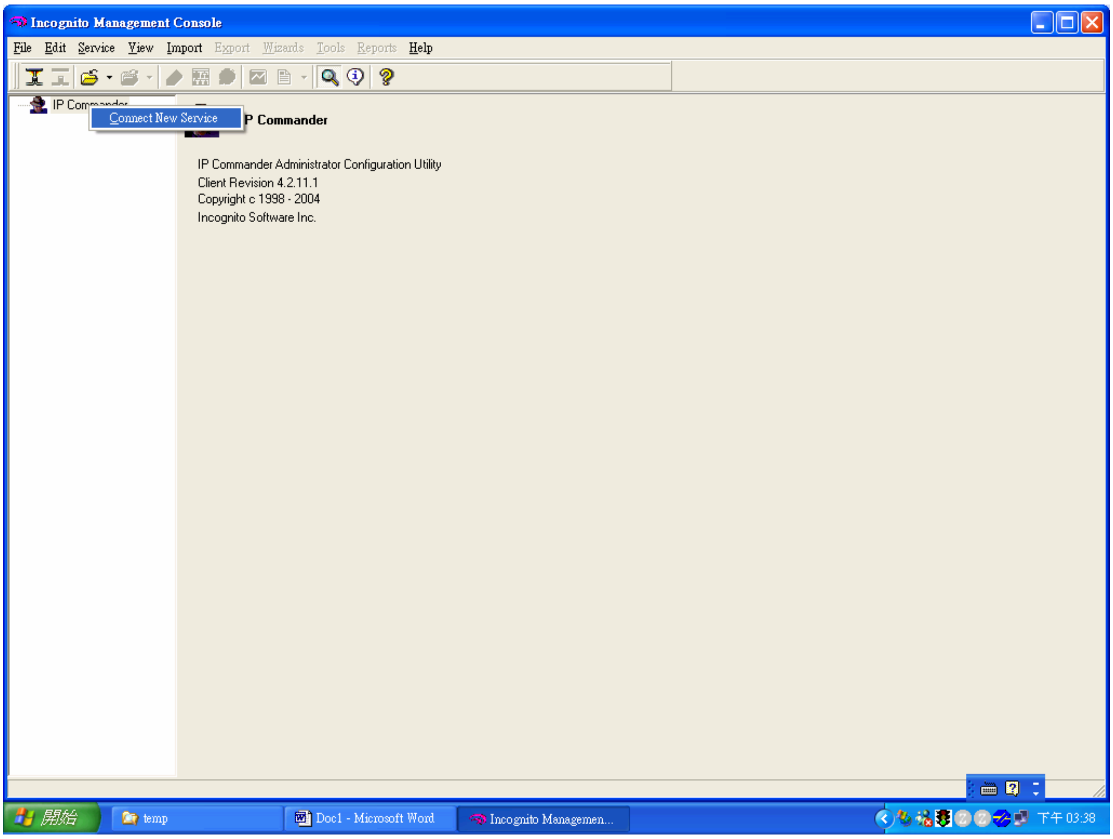


| | |
|---|---|
| Active | ☑ |
| Remote DHCP Server 1 | 192.168.1.99 |
| Remote DHCP Server 2 | 0.0.0.0 |
| Remote DHCP Server 3 | 0.0.0.0 |
| Relay Agent Information | ☑ Option 82 |
| Information | ☑ GS-3012 |

Now we can connect PC to the 25th SWITCH port. Please see former applications for detailed settings.

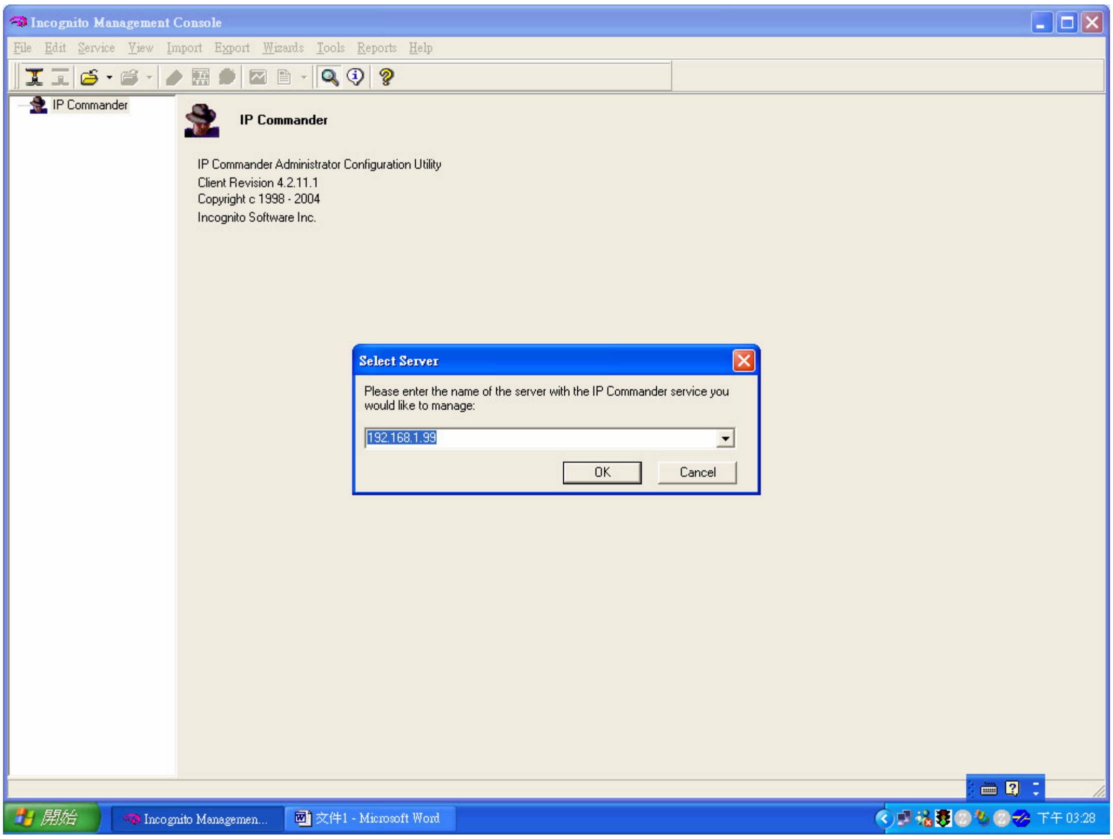
## 3. IP Commander settings

Open IP Commander. Right click “IP commander and then click “**connect new server**”.



IP Commander Administrator Configuration Utility
Client Revision 4.2.11.1
Copyright c 1998 - 2004
Incognito Software Inc.

Input the DHCP IP address or domain name and click “ok”. Our IP is 192.168.1.99.



Incognito Management Console
File Edit Service View Import Export Wizards Tools Reports Help
IP Commander
開始
Incognito Managemen...
文件1 - Microsoft Word
下午 03:28

IP Commander

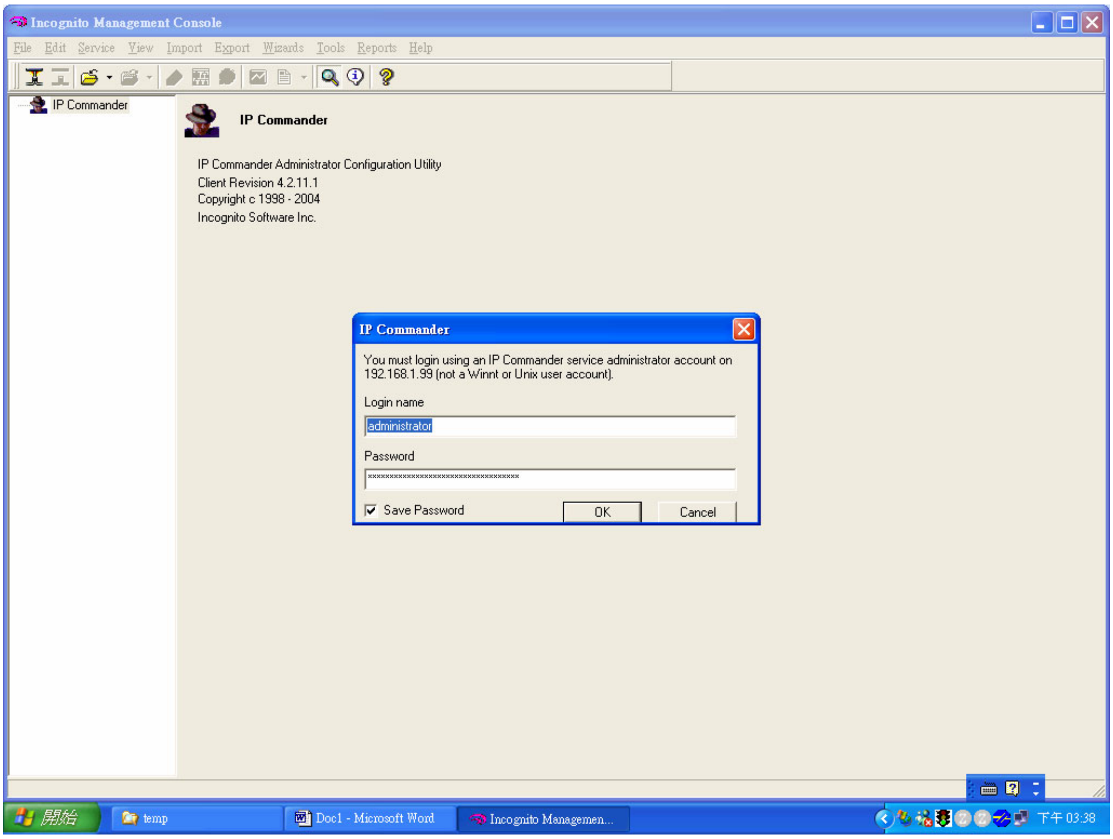
IP Commander Administrator Configuration Utility
Client Revision 4.2.11.1
Copyright c 1998 - 2004
Incognito Software Inc.

Select Server

Please enter the name of the server with the IP Commander service you would like to manage:

192.168.1.99

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


Incognito Management Console
File Edit Service View Import Export Wizards Tools Reports Help
IP Commander
IP Commander
開始
temp
Doc1 - Microsoft Word
Incognito Managemen...
下午 03:38

IP Commander Administrator Configuration Utility
Client Revision 4.2.11.1
Copyright c 1998 - 2004
Incognito Software Inc.

IP Commander

You must login using an IP Commander service administrator account on 192.168.1.99 (not a Winnt or Unix user account).

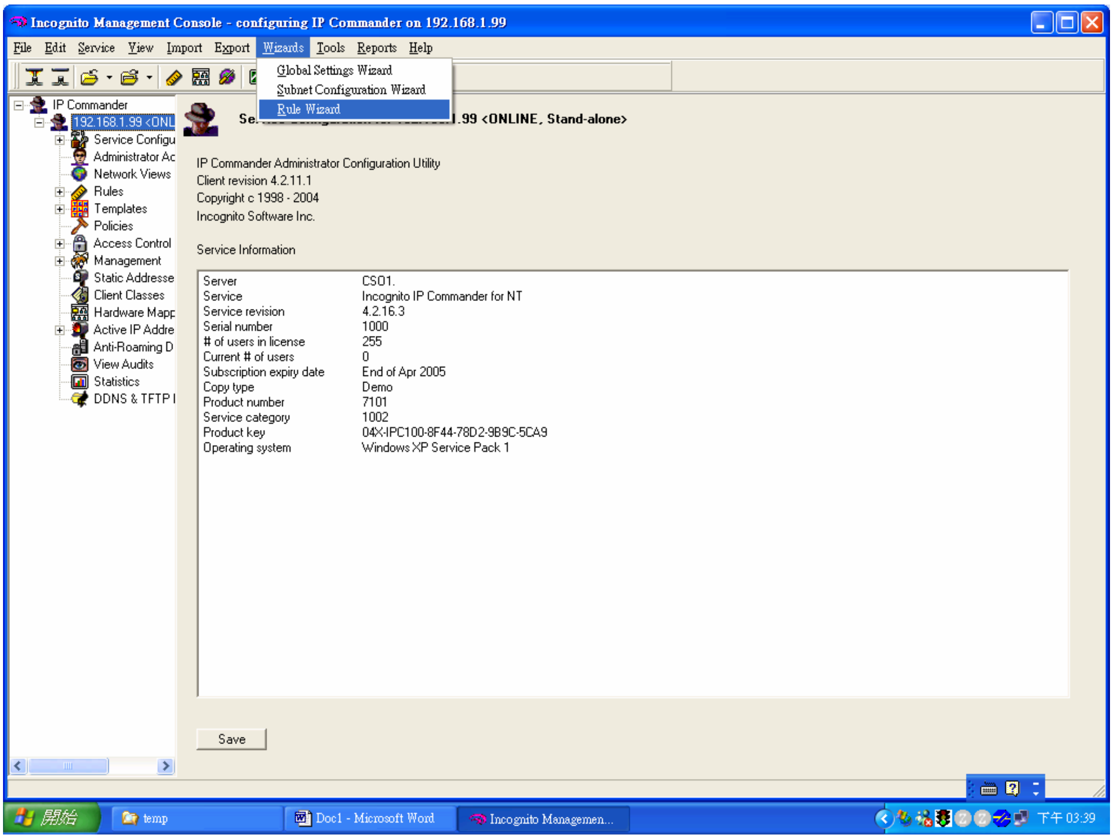
Login name: administrator

Password: ********************************

☑ Save Password

OK Cancel

It will bring up the following screen, please make sure that your DHCP is in "**online**" status. Then click "**wizard**" in the top tool bars and select "**rule wizard**".

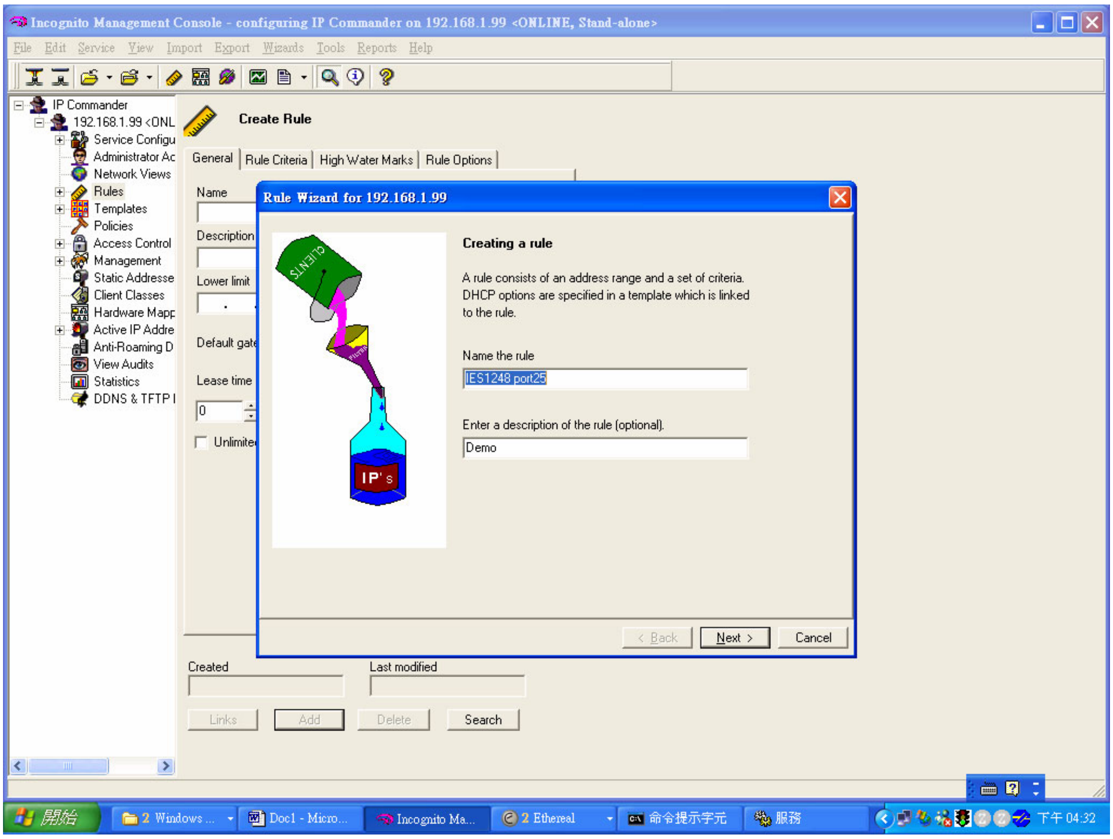


IP Commander Administrator Configuration Utility
Client revision 4.2.11.1
Copyright c 1998 - 2004
Incognito Software Inc.

Service Information

| | |
|---|---|
| Server | CS01. |
| Service | Incognito IP Commander for NT |
| Service revision | 4.2.16.3 |
| Serial number | 1000 |
| # of users in license | 255 |
| Current # of users | 0 |
| Subscription expiry date | End of Apr 2005 |
| Copy type | Demo |
| Product number | 7101 |
| Service category | 1002 |
| Product key | 04X-IPC100-8F44-78D2-9B9C-5CA9 |
| Operating system | Windows XP Service Pack 1 |

Give a name and description to the new rule.



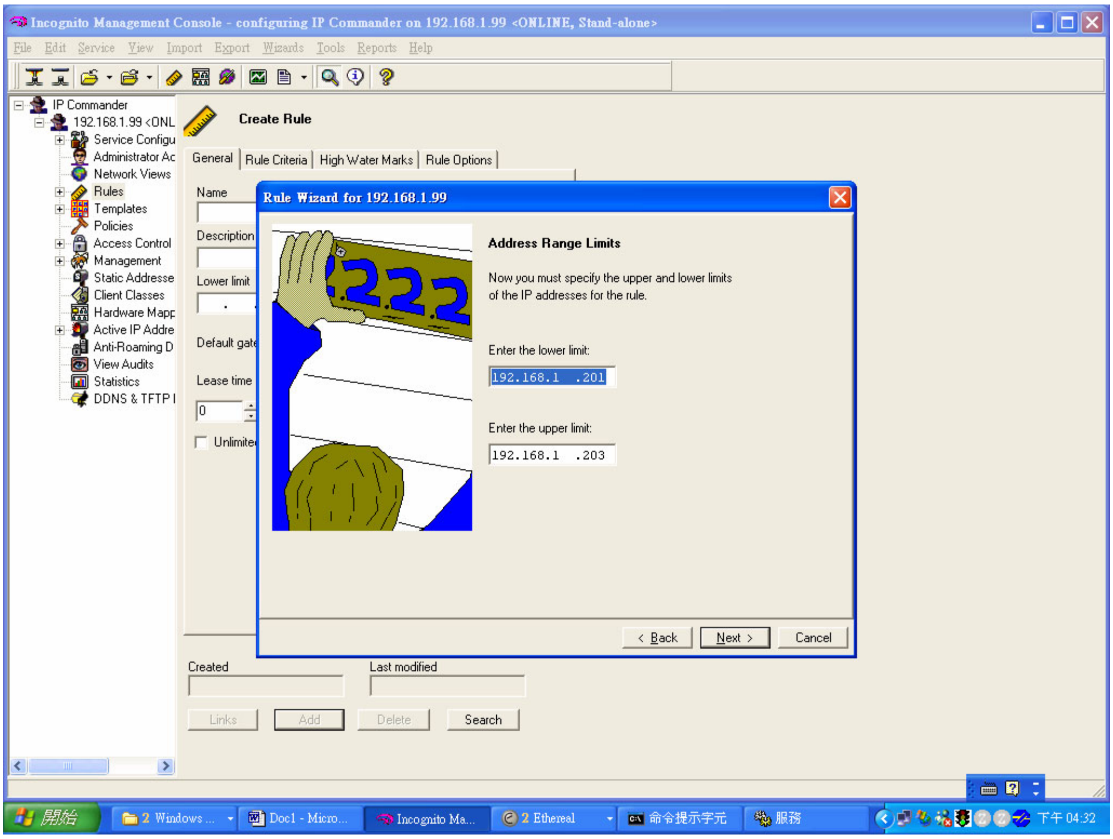
Creating a rule

A rule consists of an address range and a set of criteria. DHCP options are specified in a template which is linked to the rule.

Name the rule
ES1248 port25

Enter a description of the rule (optional).
Demo

Assign a range of IP addresses or just one IP address to this rule. In our case, we set the IP pool from 192.168.1.201 to 192.168.1.203.



Incognito Management Console - configuring IP Commander on 192.168.1.99 <ONLINE, Stand-alone>

Rule Wizard for 192.168.1.99

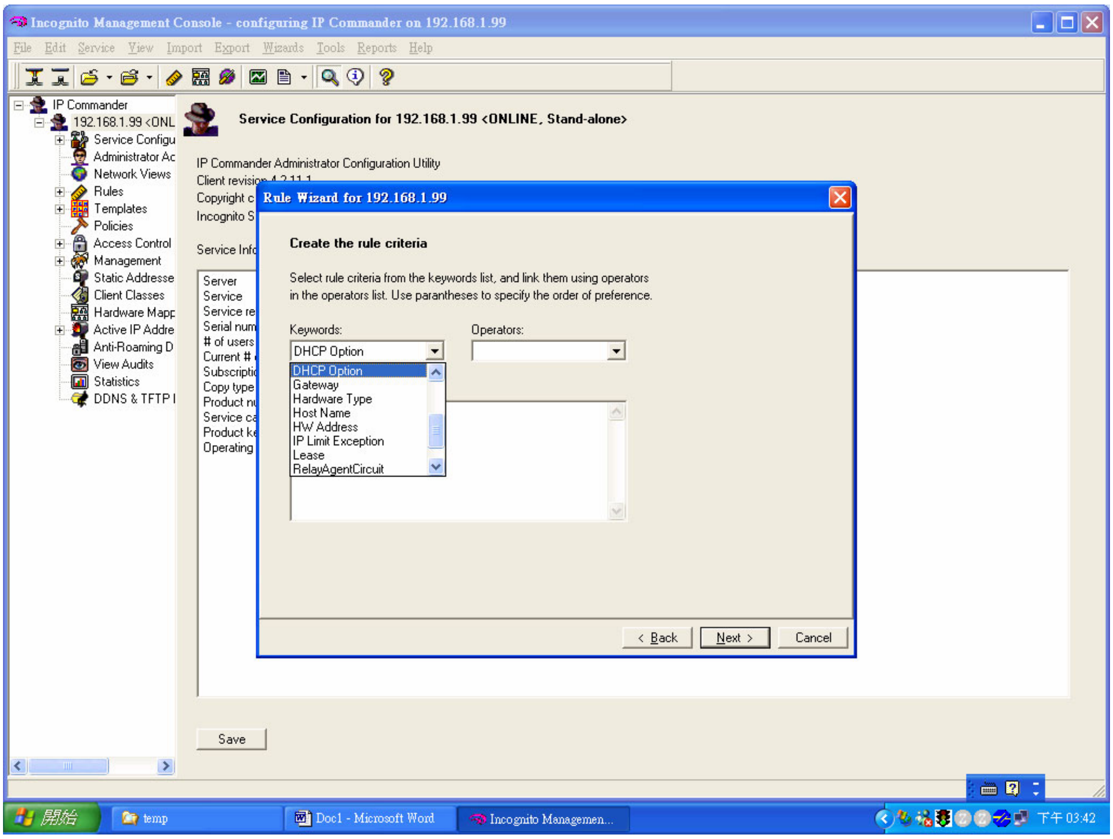
**Address Range Limits**

Now you must specify the upper and lower limits of the IP addresses for the rule.

Enter the lower limit: 192.168.1 .201

Enter the upper limit: 192.168.1 .203

After input IP pool, we select “DHCP Option” in Keywords combobox.

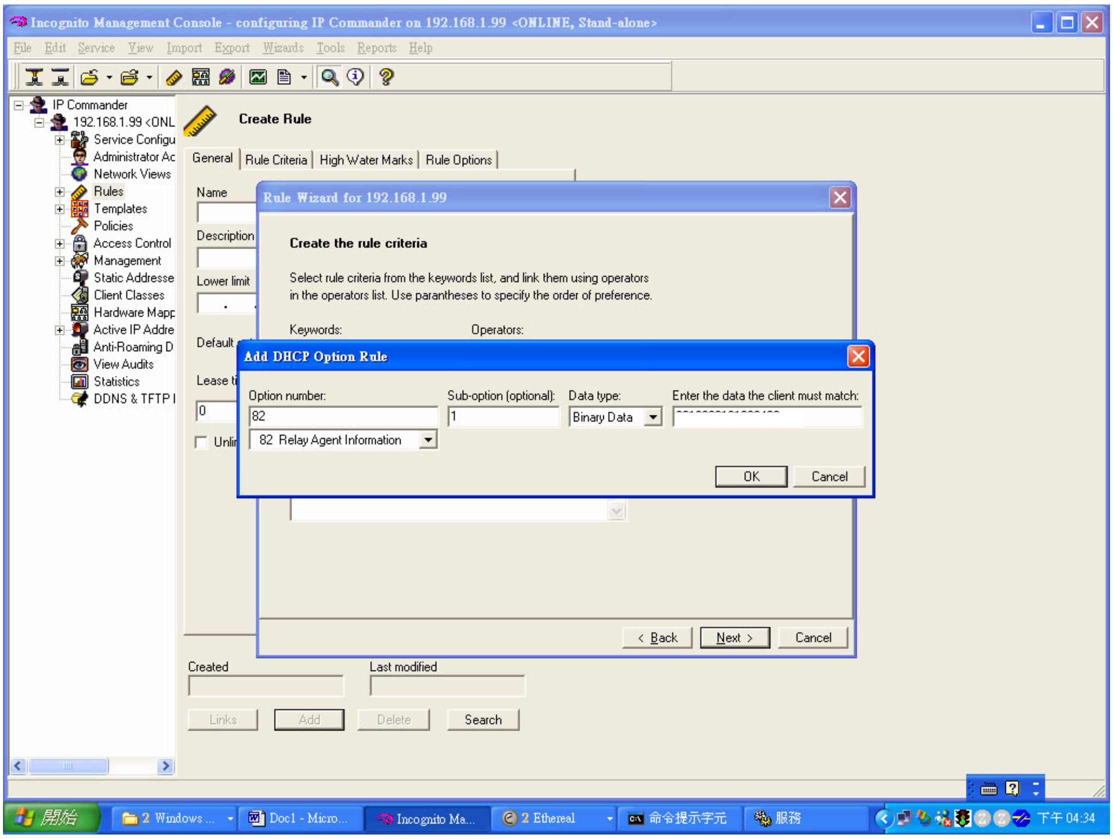


Create the rule criteria

Select rule criteria from the keywords list, and link them using operators in the operators list. Use parantheses to specify the order of preference.

Keywords: DHCP Option

After select the “DHCP Option”, it will pop up “Add DHCP Option Rule” dialog. Select “option 82 Relay Agent Information”, sub-option 1, binary data. For port 25, VLAN 1, “GS-3012”, please key in “0019000147532d33303132” as the key value and click OK. Please note that the first 2 bytes define port number, the second 2 bytes is VLAN ID and the other bytes are the Option 82 string.



**Create the rule criteria**

Select rule criteria from the keywords list, and link them using operators in the operators list. Use parantheses to specify the order of preference.

Keywords:

Operators:

**Add DHCP Option Rule**

Option number: 82

82 Relay Agent Information

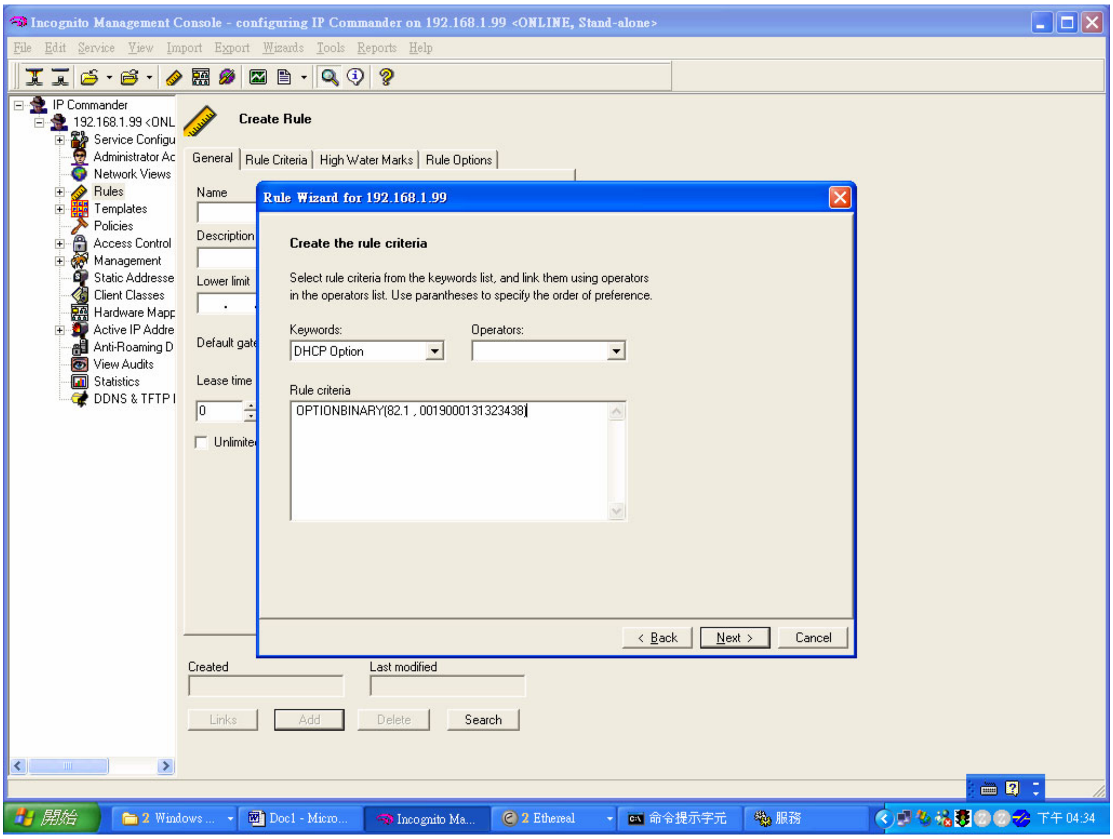
Sub-option (optional): 1

Data type: Binary Data

Enter the data the client must match:

OK Cancel

After you finish above step, you will see the following figure.



**Rule Wizard for 192.168.1.99**

**Create the rule criteria**

Select rule criteria from the keywords list, and link them using operators in the operators list. Use parantheses to specify the order of preference.

Keywords: DHCP Option

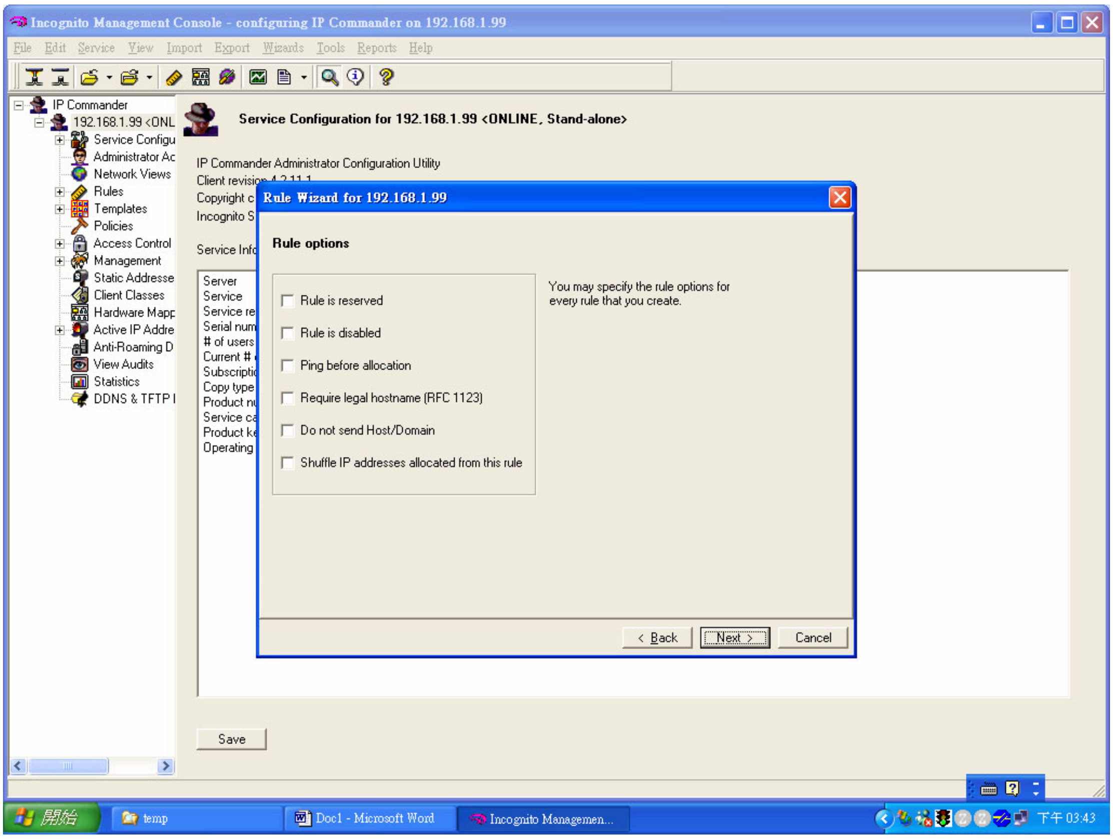
Operators:

Rule criteria

```
OPTIONBINARY(82.1 , 0019000131323438)
```

Lease time: 0

Then pop up the following screen and you can just press **Next** button.



Service Configuration for 192.168.1.99 <ONLINE, Stand-alone>

Rule Wizard for 192.168.1.99

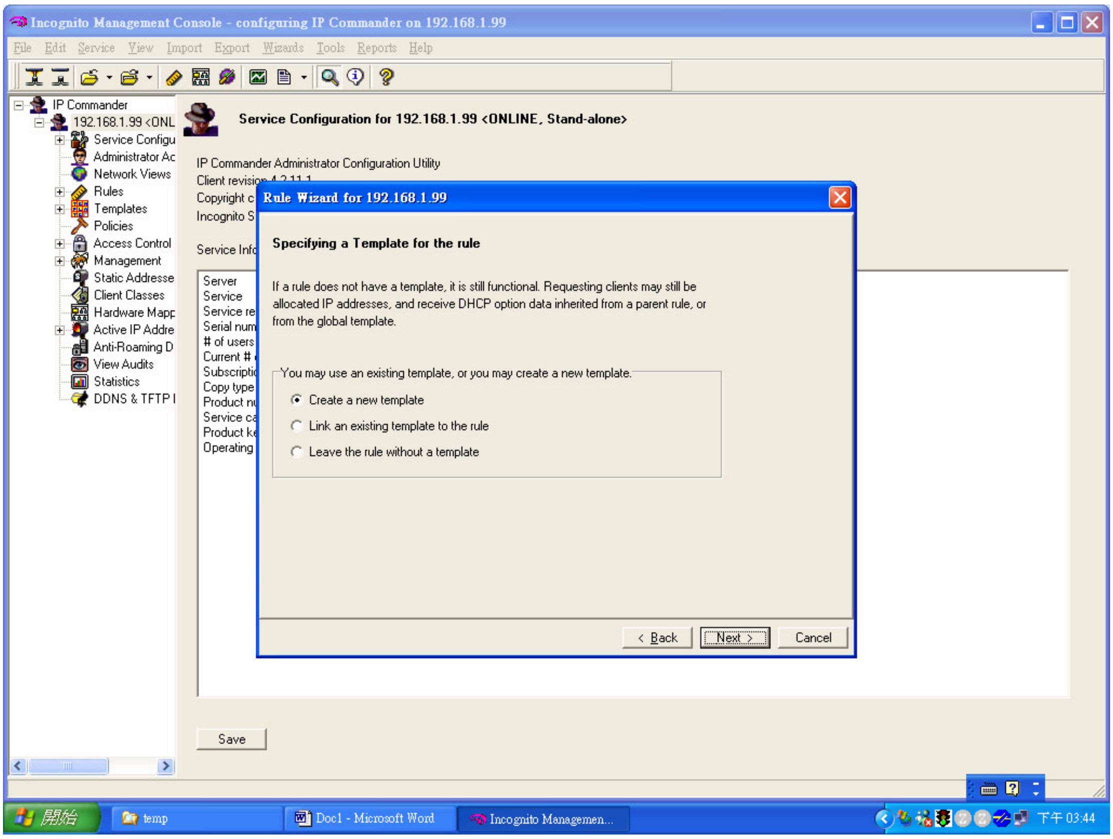
Rule options

- □ Rule is reserved
- □ Rule is disabled
- □ Ping before allocation
- □ Require legal hostname (RFC 1123)
- □ Do not send Host/Domain
- □ Shuffle IP addresses allocated from this rule

You may specify the rule options for every rule that you create.

< Back | Next > | Cancel

Then you can add DHCP template (option) such as gateway, DNS server and so on.



Service Configuration for 192.168.1.99 <ONLINE, Stand-alone>

IP Commander Administrator Configuration Utility

**Rule Wizard for 192.168.1.99**

**Specifying a Template for the rule**

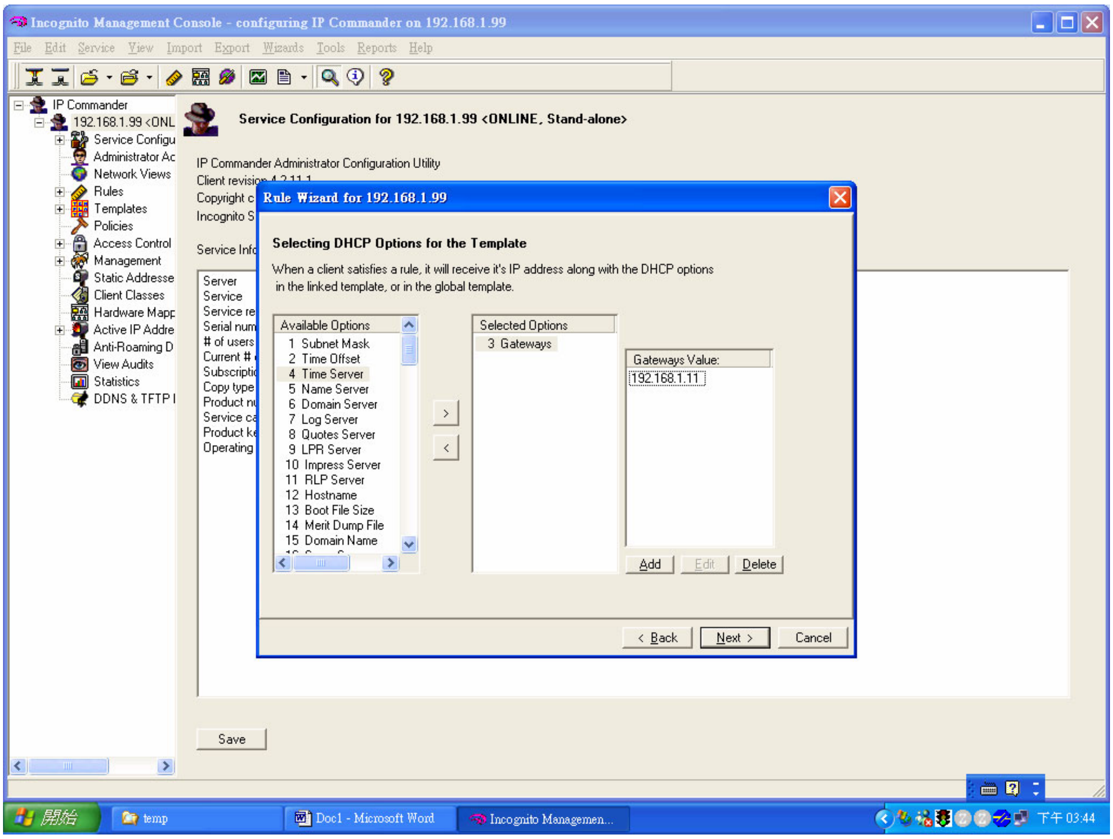
If a rule does not have a template, it is still functional. Requesting clients may still be allocated IP addresses, and receive DHCP option data inherited from a parent rule, or from the global template.

You may use an existing template, or you may create a new template.

- ● Create a new template
- ○ Link an existing template to the rule
- ○ Leave the rule without a template

< Back | Next > | Cancel

Here we use “192.168.1.1” as gateway IP address of DHCP client PC.



Service Configuration for 192.168.1.99 <ONLINE, Stand-alone>

IP Commander Administrator Configuration Utility

**Rule Wizard for 192.168.1.99**

**Selecting DHCP Options for the Template**

When a client satisfies a rule, it will receive it's IP address along with the DHCP options in the linked template, or in the global template.

Available Options:
1 Subnet Mask
2 Time Offset
4 Time Server
5 Name Server
6 Domain Server
7 Log Server
8 Quotes Server
9 LPR Server
10 Impress Server
11 RLP Server
12 Hostname
13 Boot File Size
14 Merit Dump File
15 Domain Name

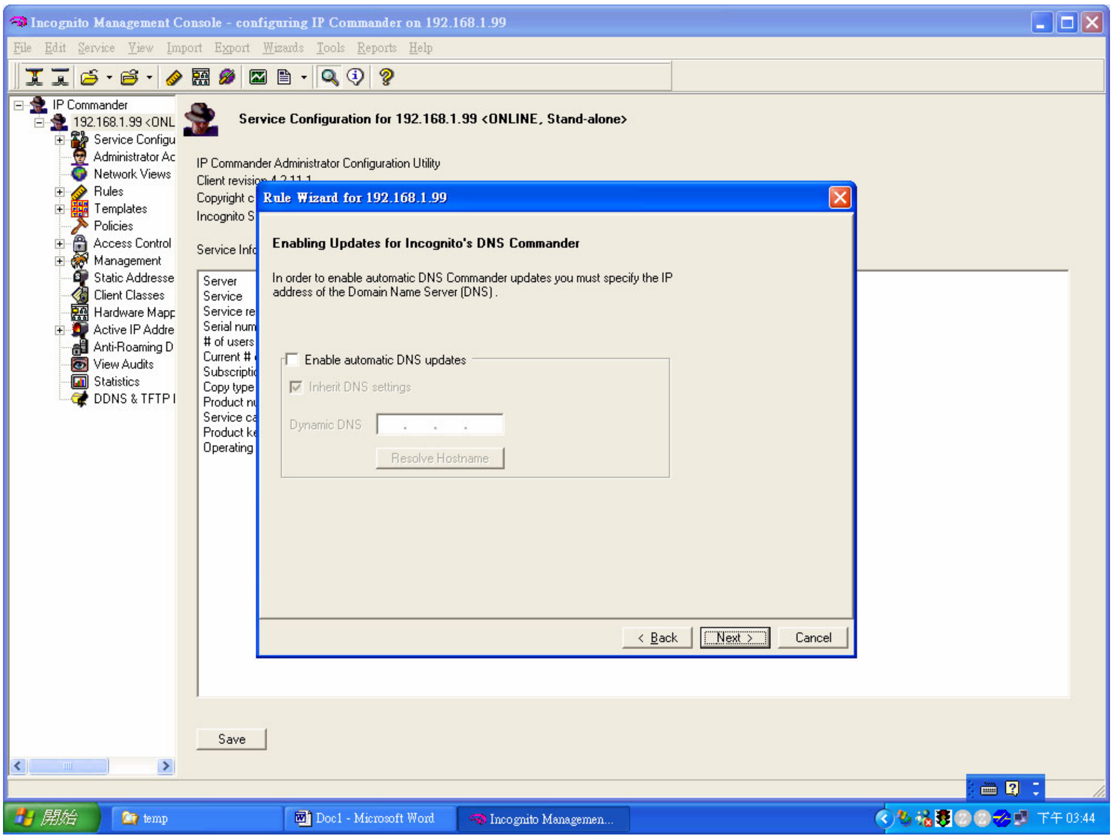
Selected Options:
3 Gateways

Gateways Value:
192.168.1.11

Add | Edit | Delete

< Back | Next > | Cancel

You can apply DDNS service to DHCP server or not.



Service Configuration for 192.168.1.99 <ONLINE, Stand-alone>

IP Commander Administrator Configuration Utility

Rule Wizard for 192.168.1.99

Enabling Updates for Incognito's DNS Commander

In order to enable automatic DNS Commander updates you must specify the IP address of the Domain Name Server (DNS).

□ Enable automatic DNS updates

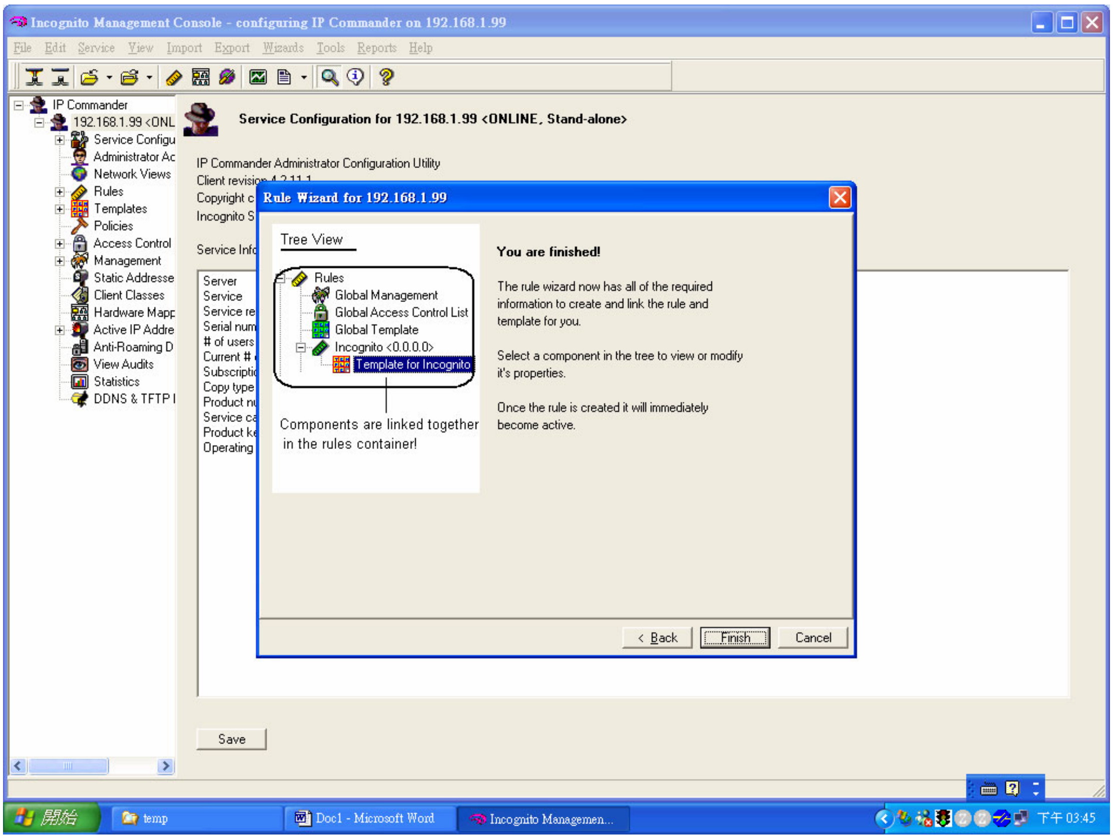
☑ Inherit DNS settings

Dynamic DNS . . .

Resolve Hostname

< Back | Next > | Cancel

The rule creation has been finished.



Incognito Management Console - configuring IP Commander on 192.168.1.99

Service Configuration for 192.168.1.99 <ONLINE, Stand-alone>

IP Commander Administrator Configuration Utility

Rule Wizard for 192.168.1.99

Tree View

Components are linked together in the rules container!

You are finished!

The rule wizard now has all of the required information to create and link the rule and template for you.

Select a component in the tree to view or modify it's properties.

Once the rule is created it will immediately become active.

After finishing all above procedures, your PC will get the IP address 192.168.1.201 when you send a DHCP request.

# Separating a physical network into many 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 one group called VLAN Group. A station can belong to more than one group. The stations on the same VLAN group can communicate with each other. With VLAN, a station cannot directly talk to or hear from stations that are not in the same VLAN group(s); the traffic must first go through a router.

In MTU or IP-DSLAM applications, VLAN is vital in providing isolation and security among the 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.

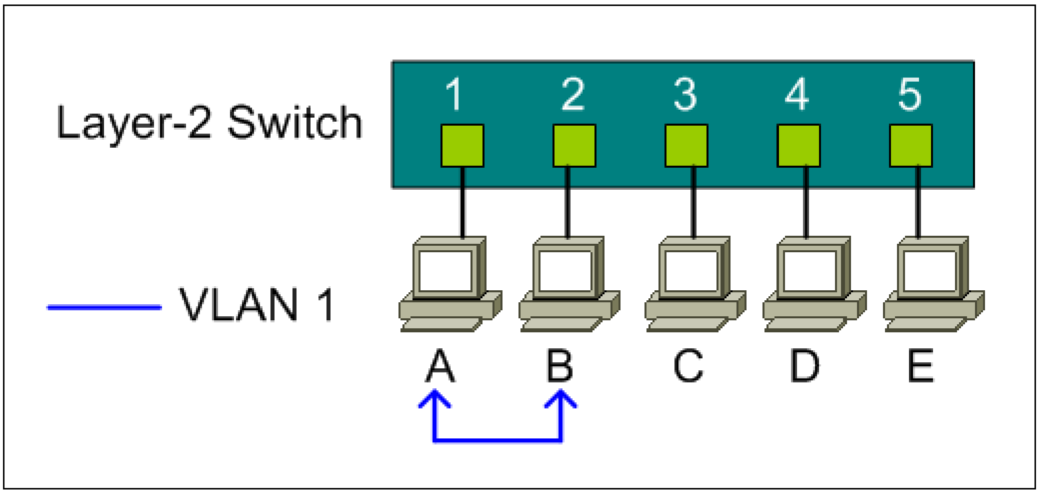
There are two most popular VLAN implementations, Port-based VLAN and IEEE 802.1q Tagged VLAN. ES-4024A series supports both VLAN implementations. The most difference between both VLAN implementations is Tagged VLAN can across Layer-2 switch but Port-based VLAN cannot.

- **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.

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

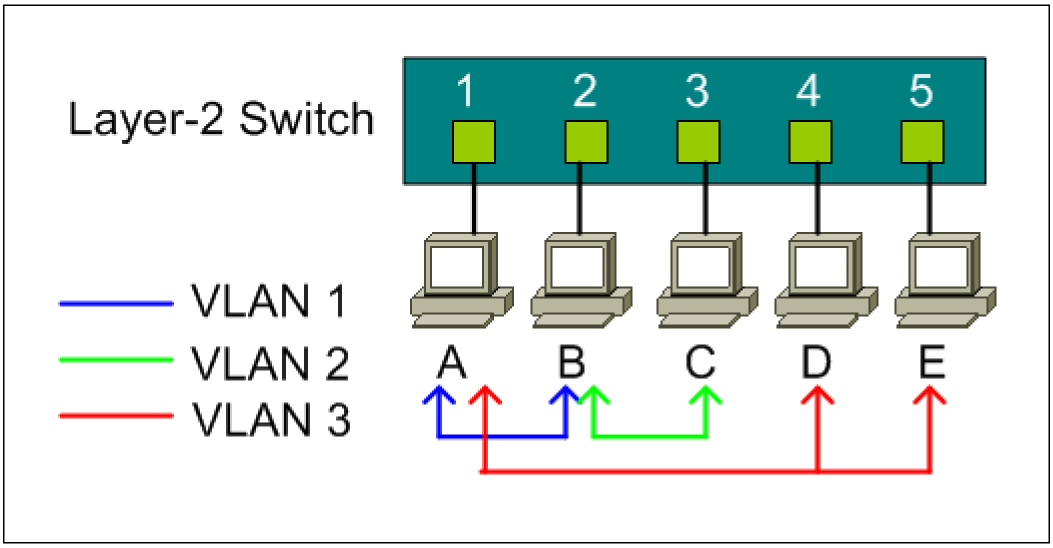
**Case 1:** Host A and Host B can talk to each other, because they are in the same VLAN group. But Host A and Host B can't talk to Host C, D, and E.



**Port-based VLAN definition**:

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

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

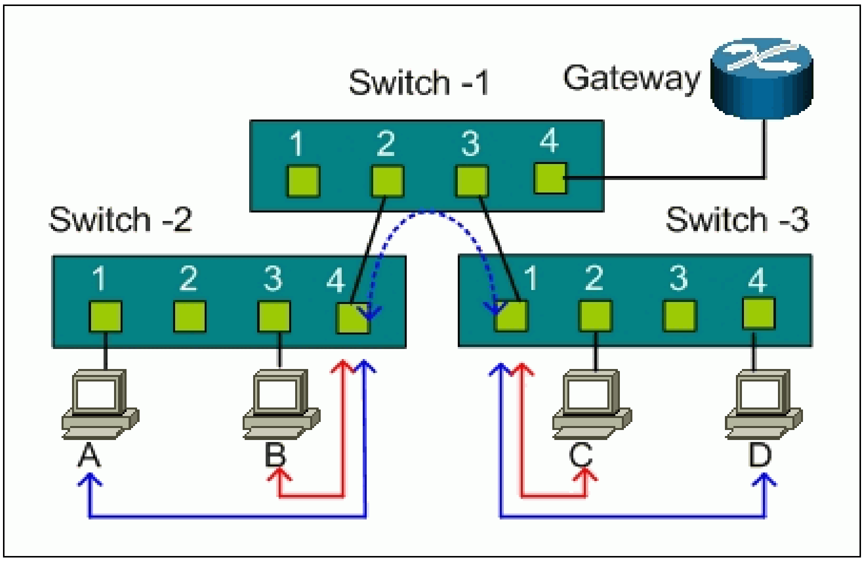


**Port-based VLAN definition**:

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

## Port-based VLAN across different switch

Port-based VLAN is specific only to the switch on which it was created. Definitely, Port-based VLAN can't across different switches. As the following network diagram shown in most MTU case, for the sake of security, subscribers are isolated with each other except for the gateway. There are two switches, Switch-2 and Switch-3, supported port-based VLAN and uplink to a none-port-based VLAN switch, Switch-1.



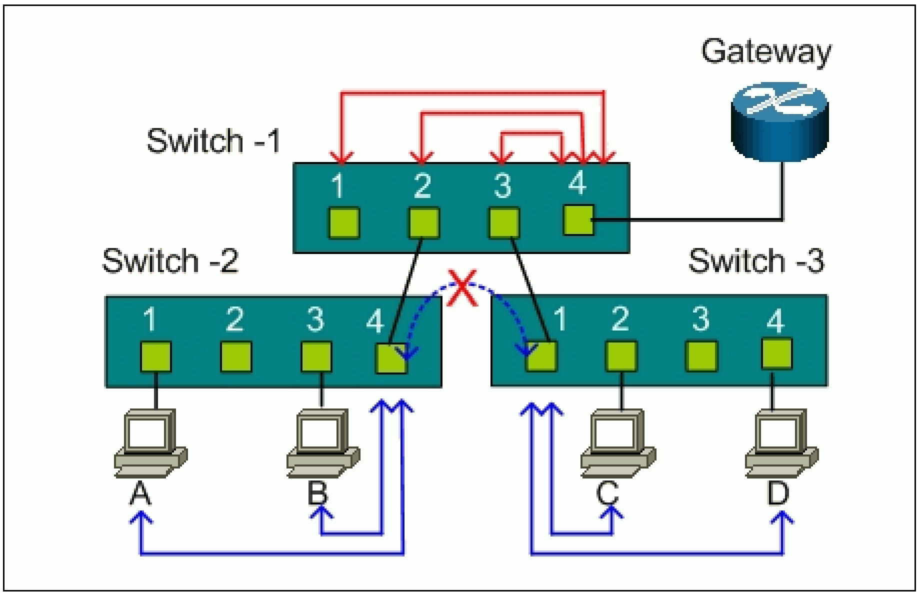
For Switch-2, port 1, port 2, and port 3 are allowed to communicate back and forth with uplink port 4, but not with other ports.

- 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, port 2, port 3, and port 4 are allowed to communicate back and forth 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 can't talk to Host B due to the port-based VLAN in Switch-2, and Host C can't talk to Host D due to the port-based VLAN in Switch-3. But both Switch-2 and Switch-3 uplink to the none VLAN Switch-1. Host A and Host B will talk to Host C and Host D via the none VLAN switch because port-based VLAN can't across different switches.
To achieve the security between different switches, you must put another port-based VLAN switch for the uplink. Each port on the uplink switch also should be separated into different VLAN, except for the port to the gateway. So subscribers only can talk to the gateway for Internet access but not communicate with each other.



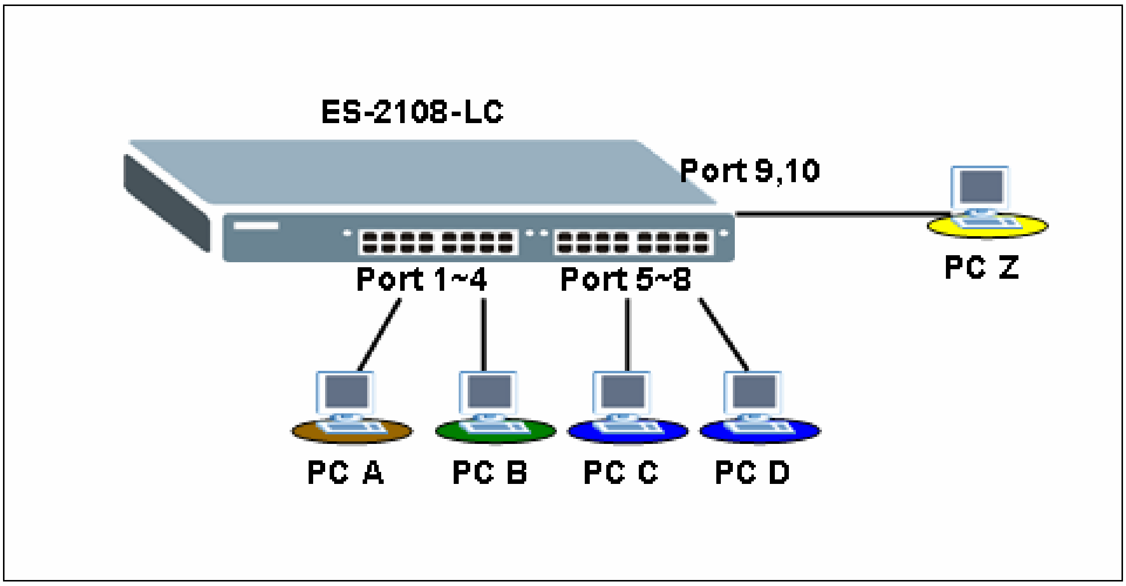
For Switch-1, port 1, port2, and port 3 are allowed to communicate back and forth with uplink port 4, but not with other ports.

- 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.

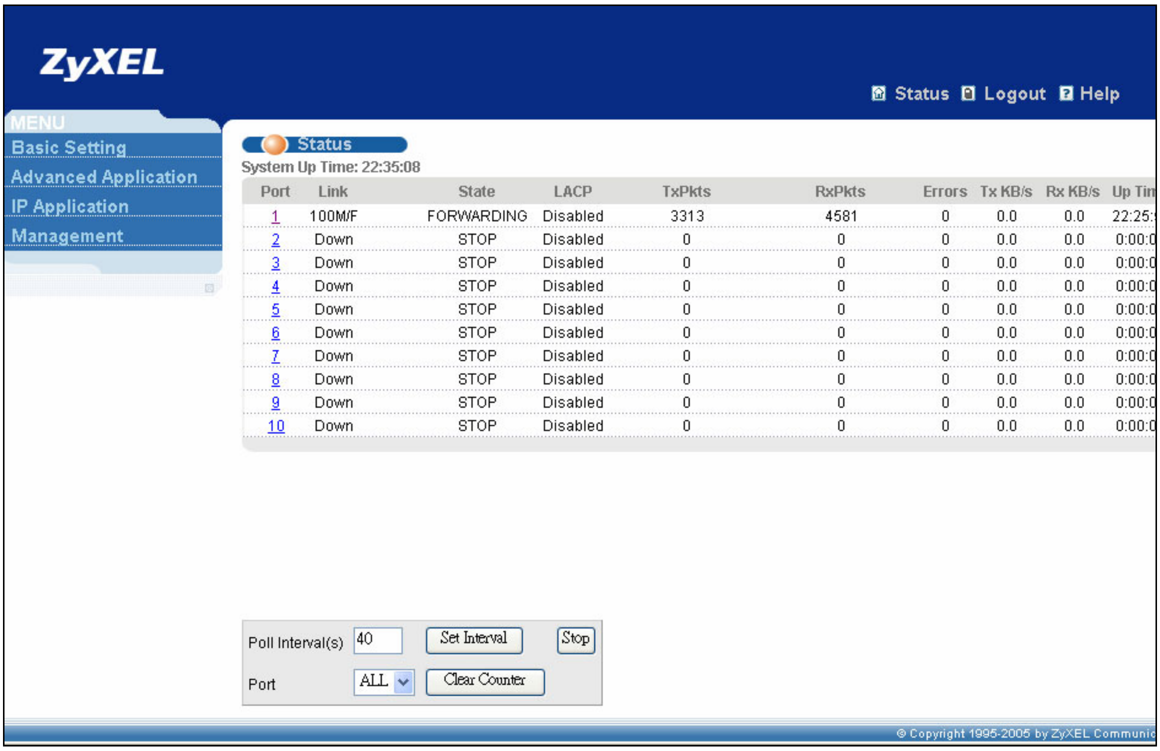
## Scenario



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

## Configuring your Switch to fulfill this scenario (GUI)

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



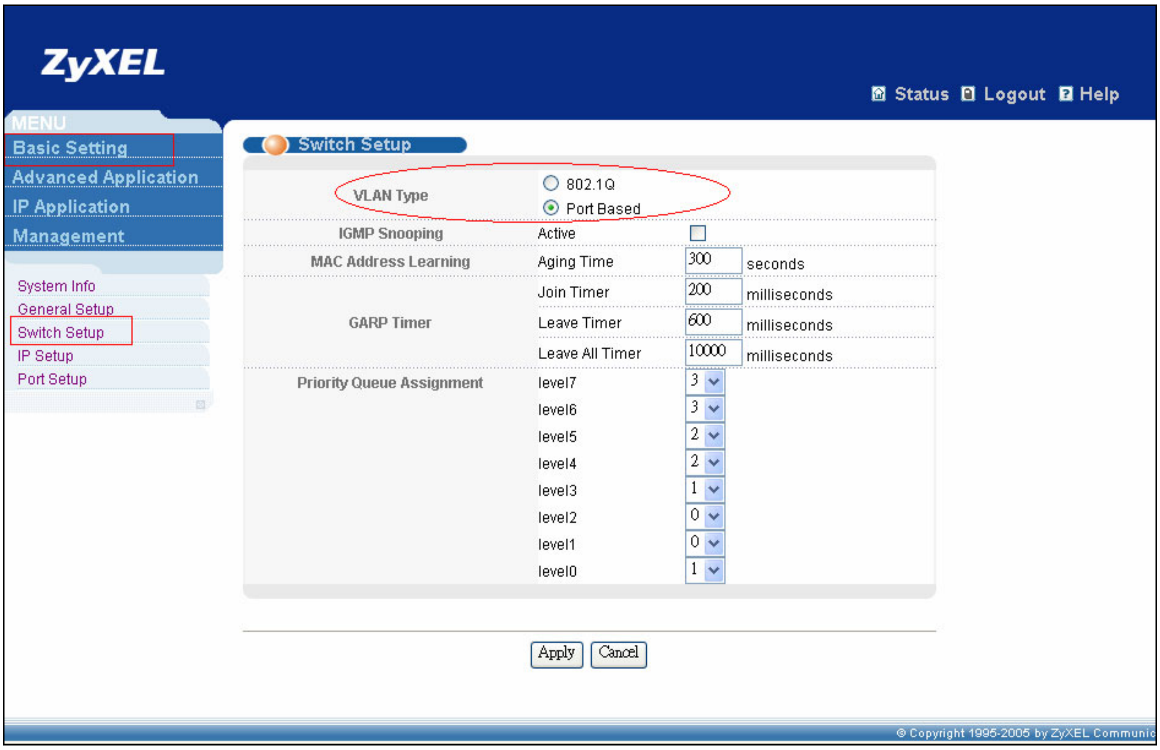
System Up Time: 22:35:08

| Port | Link | State | LACP | TxPkts | RxPkts | Errors | Tx KB/s | Rx KB/s | Up Tim |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 100M/F | FORWARDING | Disabled | 3313 | 4581 | 0 | 0.0 | 0.0 | 22:25: |
| 2 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 3 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 4 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 5 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 6 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 7 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 8 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 9 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |
| 10 | Down | STOP | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:0 |

Poll Interval(s) 40

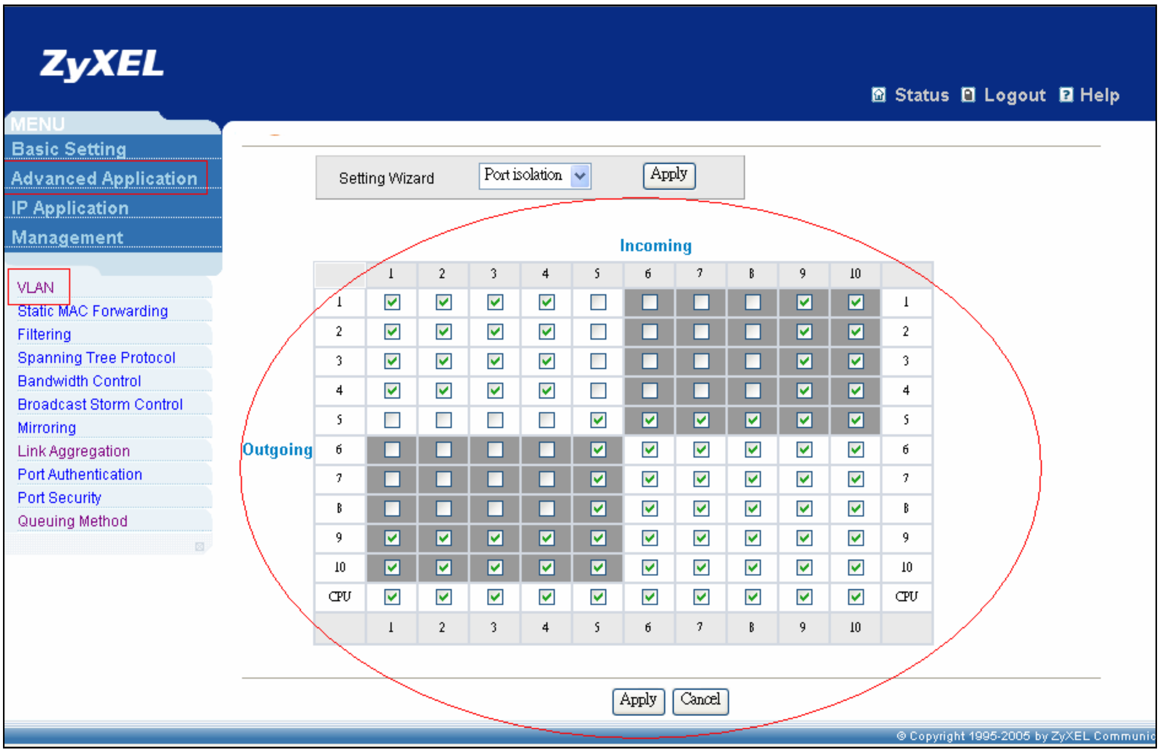
Port ALL

7. First, we need to tell the Switch to run VLAN as port based instead of 802.1q based. In order to do so, we first click on the “Basic Setting”, then “Switch Setup”; on your right screen the VLAN Type, choose “Port Based” instead of “802.1Q”, and click “Apply” to save your changes.



| | | | |
|---|---|---|---|
| VLAN Type | ○ 802.1Q<br>● Port Based | | |
| IGMP Snooping | Active | □ | |
| MAC Address Learning | Aging Time | 300 | seconds |
| GARP Timer | Join Timer | 200 | milliseconds |
| | Leave Timer | 600 | milliseconds |
| | Leave All Timer | 10000 | milliseconds |
| Priority Queue Assignment | level7 | 3 | |
| | level6 | 3 | |
| | level5 | 2 | |
| | level4 | 2 | |
| | level3 | 1 | |
| | level2 | 0 | |
| | level1 | 0 | |
| | level0 | 1 | |

8. Now, you need to tell the Switch how you are going to separate the physical Switch into some logical small Switches. Thus, we click “Advanced Application” then “VLAN”. On the right screen, check the boxes to suit your need. In this case, we need to make port 1~4 and port 9, 10 in a group in order for them to communicate in both ways. And port 5~10 in another group but these two groups cannot talk with each others. Here we also logically defined Port 9 and Port 10 as the uplink ports. Therefore, both groups can pass data to Port 9 and Port 10. In another word, these two ports belong to both of the groups on the same time. Please confirm if your setting looks similar to below.



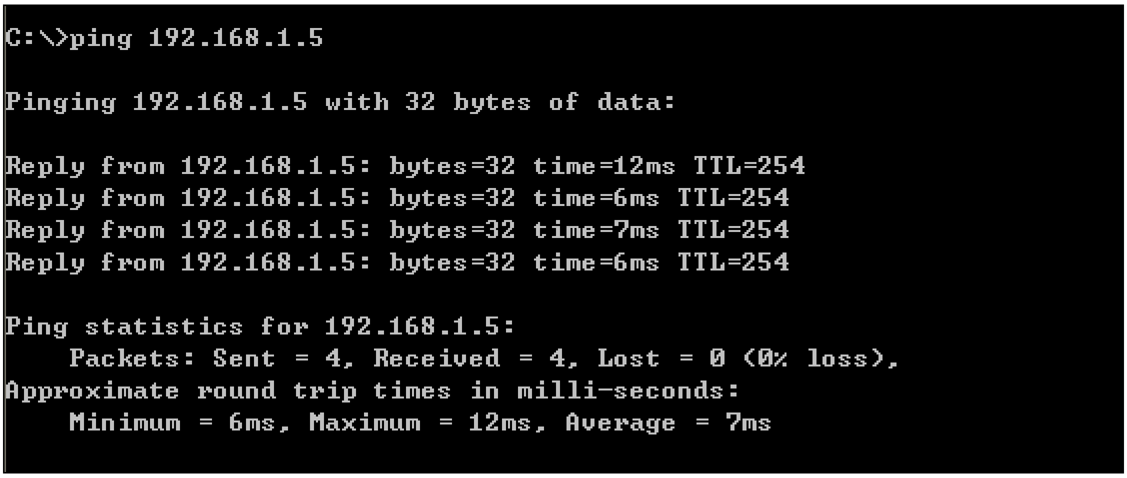
Setting Wizard: Port isolation [Apply]

Incoming

Outgoing

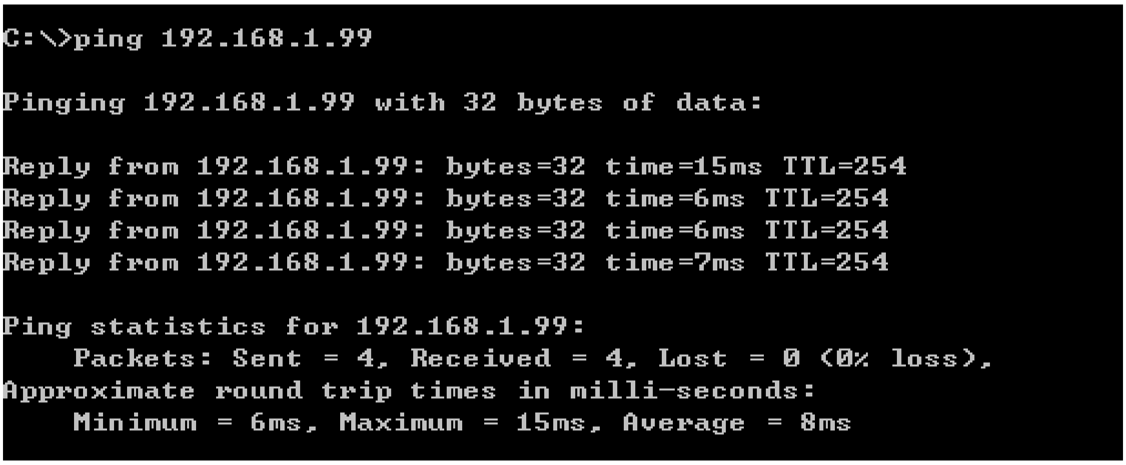
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | ☑ | ☑ | ☑ | □ | □ | □ | □ | ☑ | ☑ | 1 |
| 2 | ☑ | ☑ | ☑ | ☑ | □ | □ | □ | □ | ☑ | ☑ | 2 |
| 3 | ☑ | ☑ | ☑ | ☑ | □ | □ | □ | □ | ☑ | ☑ | 3 |
| 4 | ☑ | ☑ | ☑ | ☑ | □ | □ | □ | □ | ☑ | ☑ | 4 |
| 5 | □ | □ | □ | □ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 5 |
| 6 | □ | □ | □ | □ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 6 |
| 7 | □ | □ | □ | □ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 7 |
| 8 | □ | □ | □ | □ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 8 |
| 9 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 9 |
| 10 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | 10 |
| CPU | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | CPU |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |

9. Finally, you can now verify your result. If everything works fine, PC A can ping PC B and PC Z. But it cannot ping PC C or PC D. On the same time, this should work 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 (Should work)



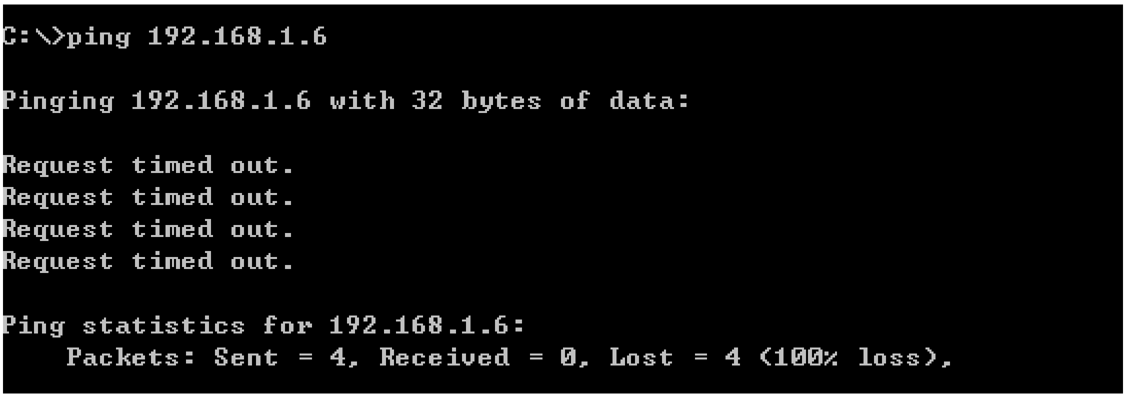
```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

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

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

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



```
C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

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

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

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

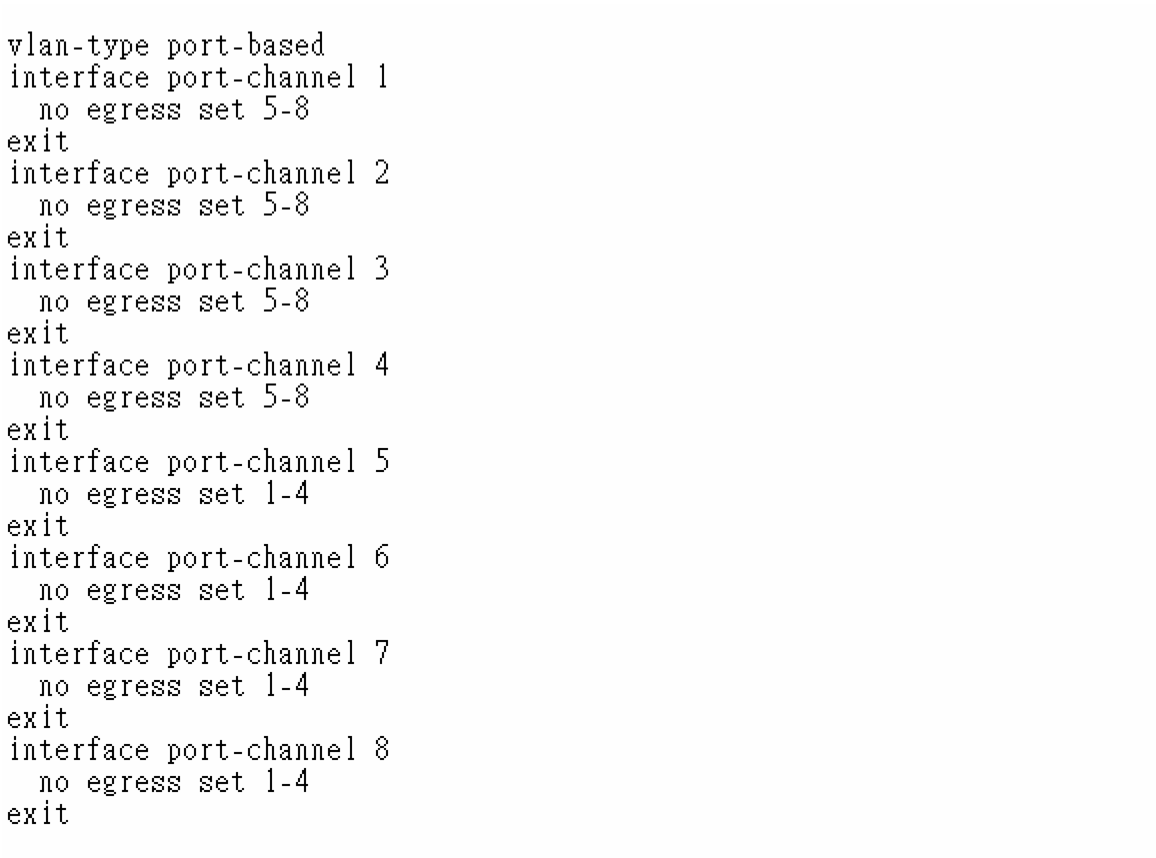


```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

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

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

## Configuring your Switch to fulfill this scenario (CLI)

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

scenario.



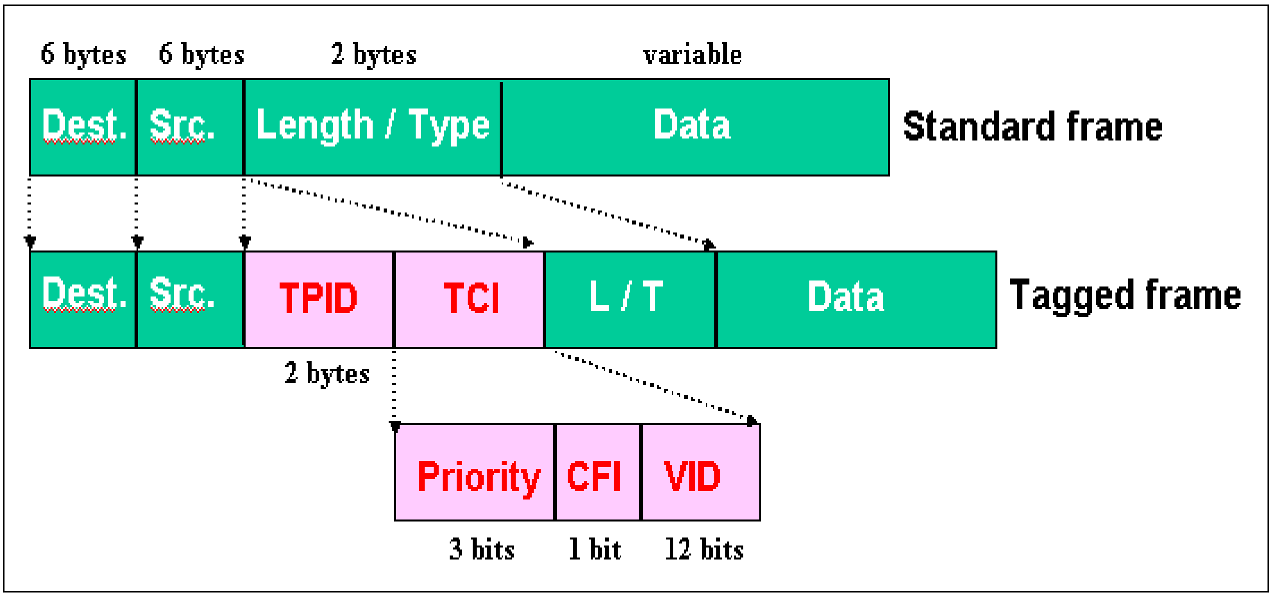
```
vlan-type port-based
interface port-channel 1
  no egress set 5-8
exit
interface port-channel 2
  no egress set 5-8
exit
interface port-channel 3
  no egress set 5-8
exit
interface port-channel 4
  no egress set 5-8
exit
interface port-channel 5
  no egress set 1-4
exit
interface port-channel 6
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

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

# What is IEEE 802.1Q Tag-based VLAN?

- ## Tag-based VLAN Overview

Regarding 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 hand 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).

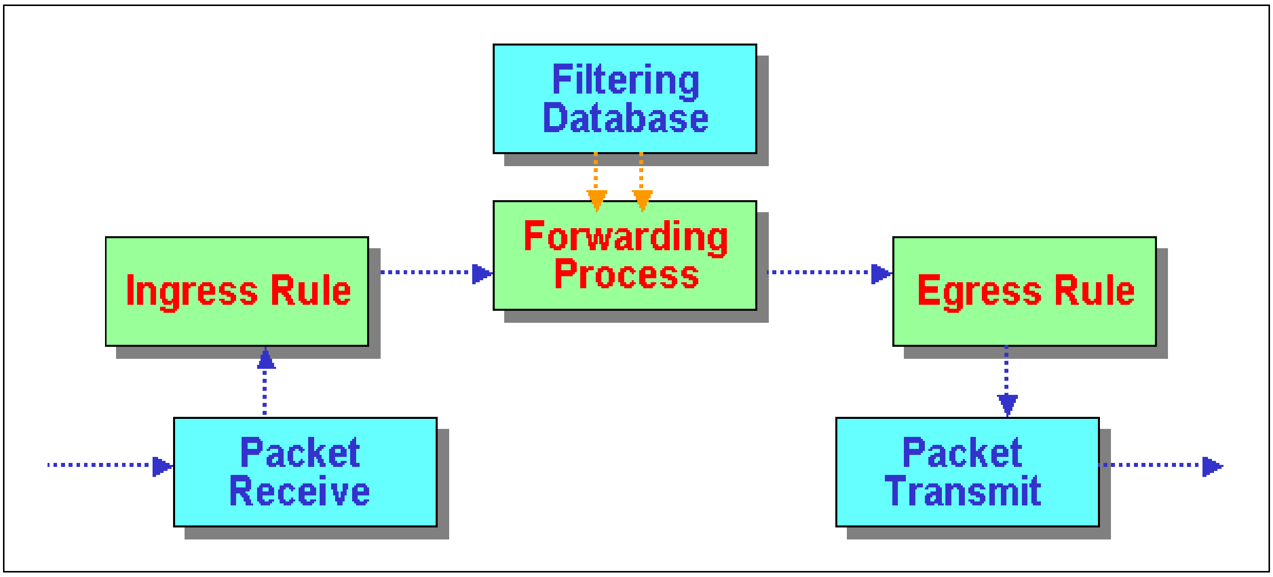


- **TPID:** TPID has a defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the tag IEEE 802.1Q / 802.1P.
- **Priority:** The first three bits of the TCI define user priority, giving eight (2^3) priority levels. IEEE 802.1P defines the operation for these 3 user 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 basically used by the standard 802.1Q. It has 12 bits 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**

According to the VID information in the tag, the switch forward and filter the frames among ports. These ports with same VID can communicate with each other. IEEE 802.1Q VLAN function contains the following three tasks, Ingress Process, Forwarding Process and Egress Process.

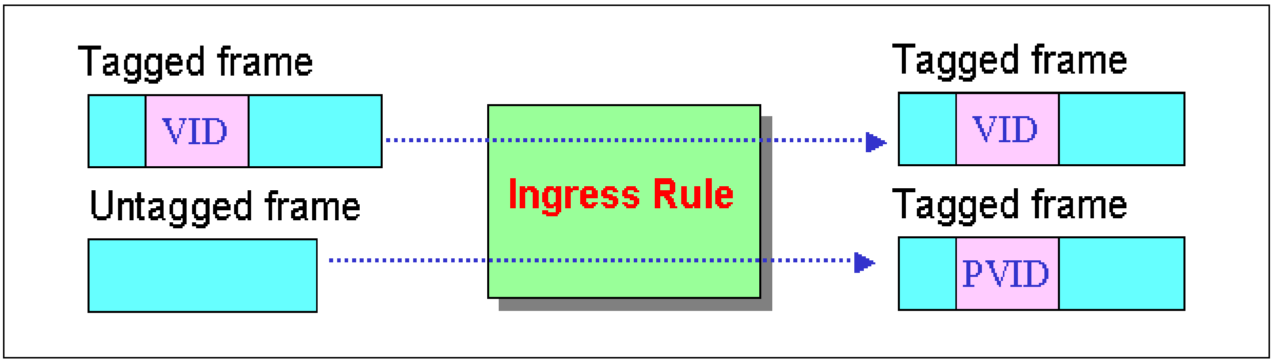


**1. Ingress Process:**

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

- When a tagged frame is received on a port, it carries a tag header that has a explicit VID. Ingress Process directly pass the tagged frame to Forwarding Process.
- An untagged frame doesn't carry any VID to which it belongs. When a

untagged frame is received, Ingress Process insert 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 4-bytes tag and VID information, and then go to Forwarding Process.

**2. Forwarding Process:**

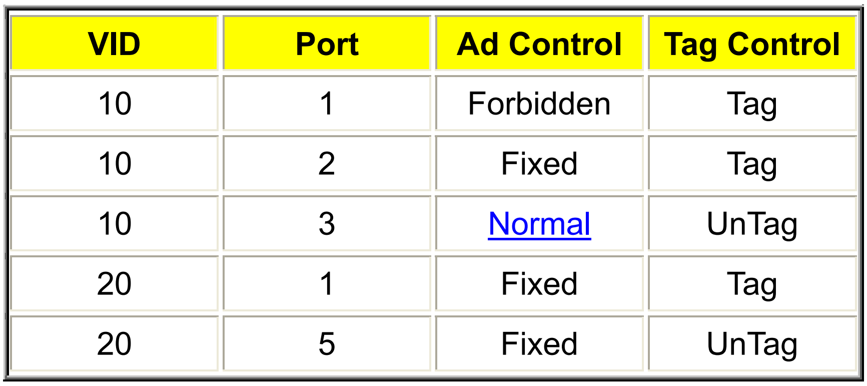
The Forwarding Process decides to forward the received frames according to the Filtering Database. If you want to allow the tagged frames can be forwarded to certain port, this port must be the egress port of this VID. The egress port is an outgoing port for the specified VLAN, that is, frames with specified VID tag can go through this port. The 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 and upgraded by the administrator.

The 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 type of ad control, including **forbidden** registration, **fixed** registration and **normal** registration.

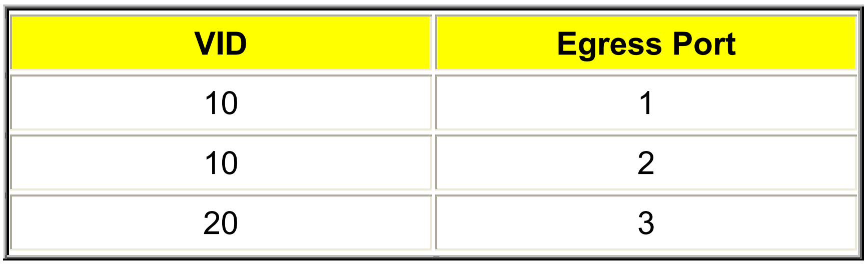
- **Forbidden** registration: This port is forbidden to be the egress port of specified VID..
- **Fixed** registration: While ad control is fixed registration, it means this is a static registration entry. This port is the egress port of the specified VID (a member port of the specified VLAN). The frames with 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 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, the outgoing frame on the egress port is tagged. If the value is untagged, the tag will be removed before 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

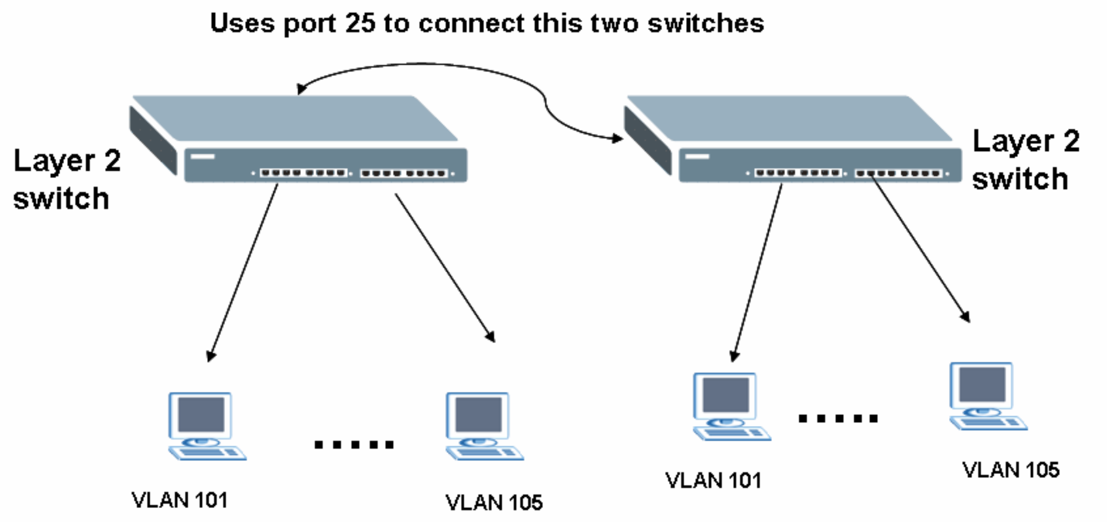
**3. Egress Process:**

The Egress Process decides if the outgoing frames but be sent tagged or untagged. The Egress Process refers to the egress tag control information in

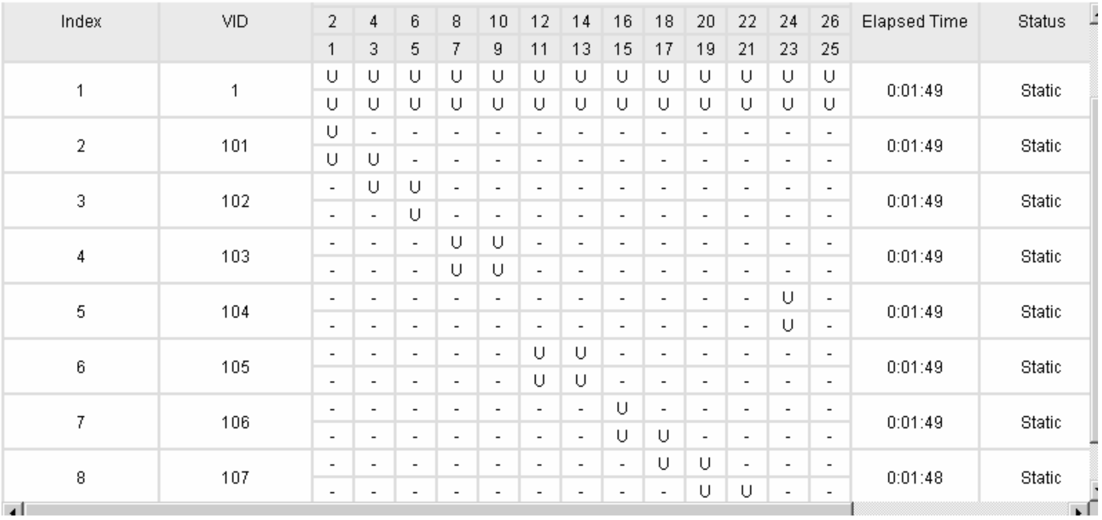
Filtering Database. If the value is tagged, the outgoing frame on the egress port is tagged. If the value is untagged, the tag will be removed before frame leaves the egress port.

## How to connect two switches using VLAN?

I want to make VLAN on two layer 2 switches, and I want to connect first switch to second switch with trunk port. There will be 5 VLAN on first Switch and there will be 7 VLAN on second switch. Trunk port will be port 25 on both switches as well. I made VLAN s on both switch, but I did not find trunk options on both switches. How can I use Port 25 as trunk port?
The scenario is described as below:



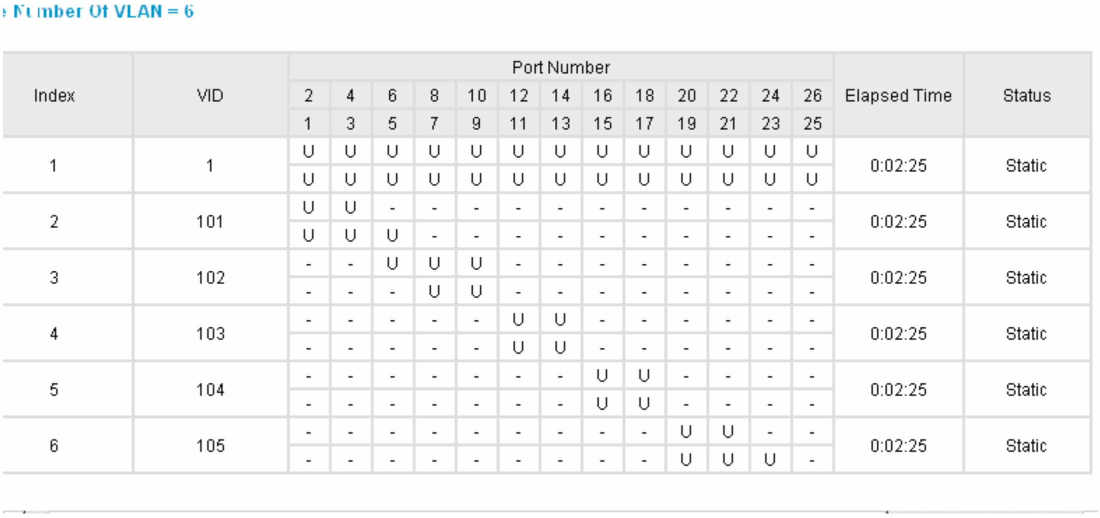
Where the configurations of VLAN in this two switches are:
VLAN 2, 3, 4, 5, 6, 7, 8 on switch A
VLAN 2, 3, 4, 5, 6 on switch B
Configuration of VLAN on switch A



| Index | VID | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | Elapsed Time | 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. Configuration of VLAN 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 | 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 | 0:02:25 | 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 same VLAN on both switches can communicate each other.

PVID:

- Set PVID on switch 1

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 2:

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

Port 6, 7, 8, 9, 10, : **102**

Port 11, 12, 13, 14, : **103**

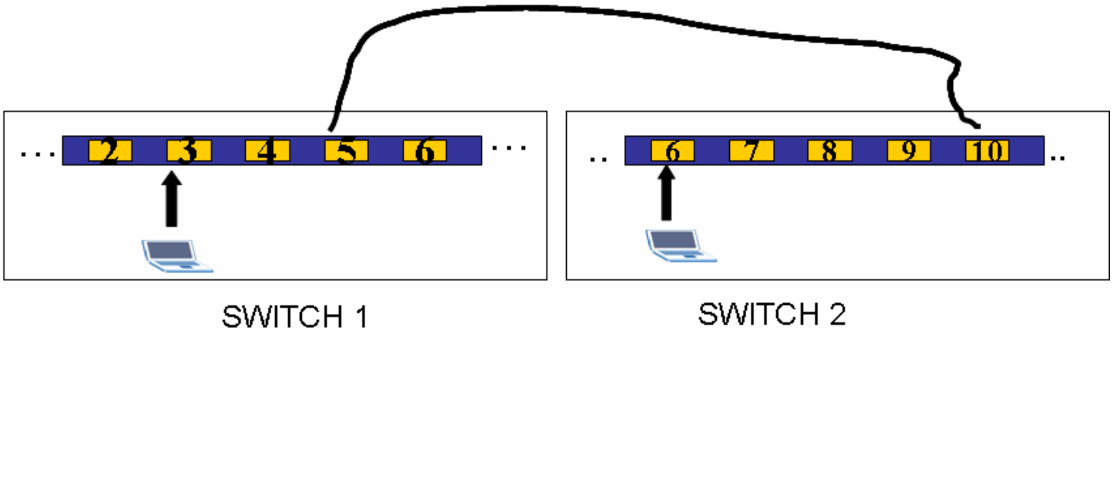
Port 15, 16, 17, 18: **104**

Port 19, 20, 21, 22, 23: **105**

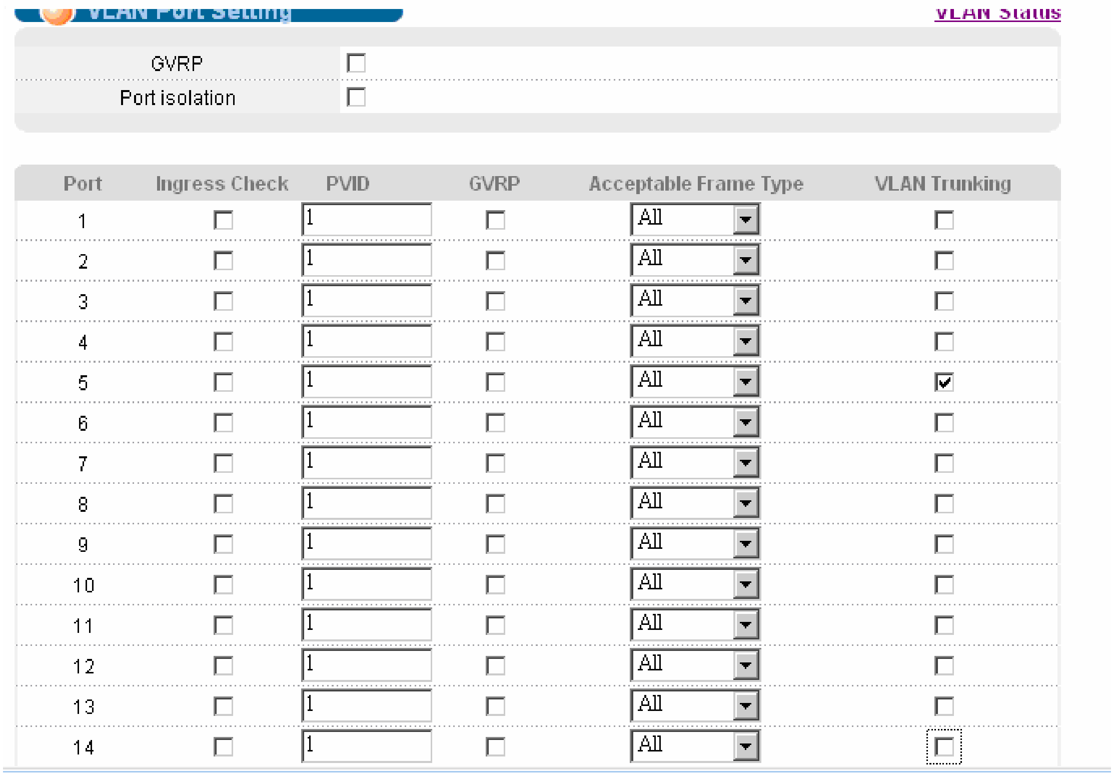
Port 25:PVID=any

## Setting up VLAN Trunking

With the benefit of deploying VLAN trunking, we can connect two switches by a port that is configured as VLAN trunking port. PC1 with each VLAN tag frames from switch 1 can communicate with PC2 with another VLAN tag frames in switch 2 via VLAN trunking port. In our example, we set up port 5 in switch 1 as the VLAN Trunking port while in switch 2, we set up port 10 as the VLAN Trunking port.



In the switch 1, the configuration is:

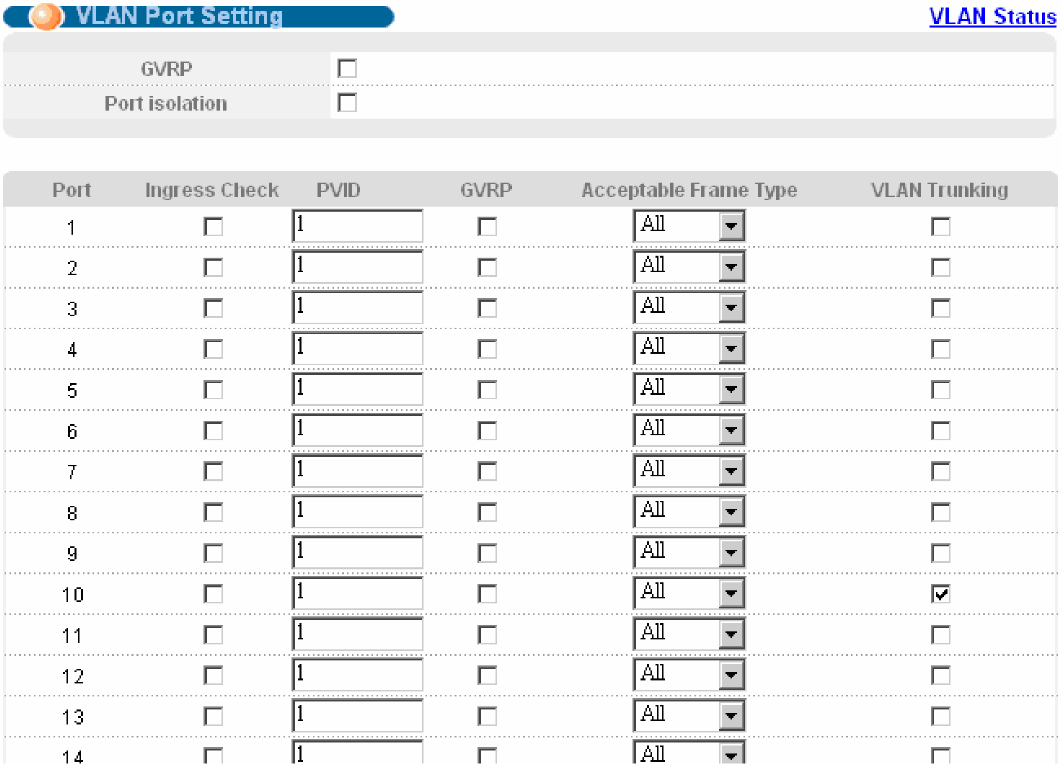


VLAN Port Setting VLAN Status

| | |
|---|---|
| GVRP | ☐ |
| Port isolation | ☐ |

| Port | Ingress Check | PVID | GVRP | Acceptable Frame Type | VLAN Trunking |
|---|---|---|---|---|---|
| 1 | ☐ | 1 | ☐ | All | ☐ |
| 2 | ☐ | 1 | ☐ | All | ☐ |
| 3 | ☐ | 1 | ☐ | All | ☐ |
| 4 | ☐ | 1 | ☐ | All | ☐ |
| 5 | ☐ | 1 | ☐ | All | ☑ |
| 6 | ☐ | 1 | ☐ | All | ☐ |
| 7 | ☐ | 1 | ☐ | All | ☐ |
| 8 | ☐ | 1 | ☐ | All | ☐ |
| 9 | ☐ | 1 | ☐ | All | ☐ |
| 10 | ☐ | 1 | ☐ | All | ☐ |
| 11 | ☐ | 1 | ☐ | All | ☐ |
| 12 | ☐ | 1 | ☐ | All | ☐ |
| 13 | ☐ | 1 | ☐ | All | ☐ |
| 14 | ☐ | 1 | ☐ | All | ☐ |

In the switch 2, the configuration is



VLAN Port Setting VLAN Status

| | |
|---|---|
| GVRP | ☐ |
| Port isolation | ☐ |

| Port | Ingress Check | PVID | GVRP | Acceptable Frame Type | VLAN Trunking |
|---|---|---|---|---|---|
| 1 | ☐ | 1 | ☐ | All | ☐ |
| 2 | ☐ | 1 | ☐ | All | ☐ |
| 3 | ☐ | 1 | ☐ | All | ☐ |
| 4 | ☐ | 1 | ☐ | All | ☐ |
| 5 | ☐ | 1 | ☐ | All | ☐ |
| 6 | ☐ | 1 | ☐ | All | ☐ |
| 7 | ☐ | 1 | ☐ | All | ☐ |
| 8 | ☐ | 1 | ☐ | All | ☐ |
| 9 | ☐ | 1 | ☐ | All | ☐ |
| 10 | ☐ | 1 | ☐ | All | ☑ |
| 11 | ☐ | 1 | ☐ | All | ☐ |
| 12 | ☐ | 1 | ☐ | All | ☐ |
| 13 | ☐ | 1 | ☐ | All | ☐ |
| 14 | ☐ | 1 | ☐ | All | ☐ |

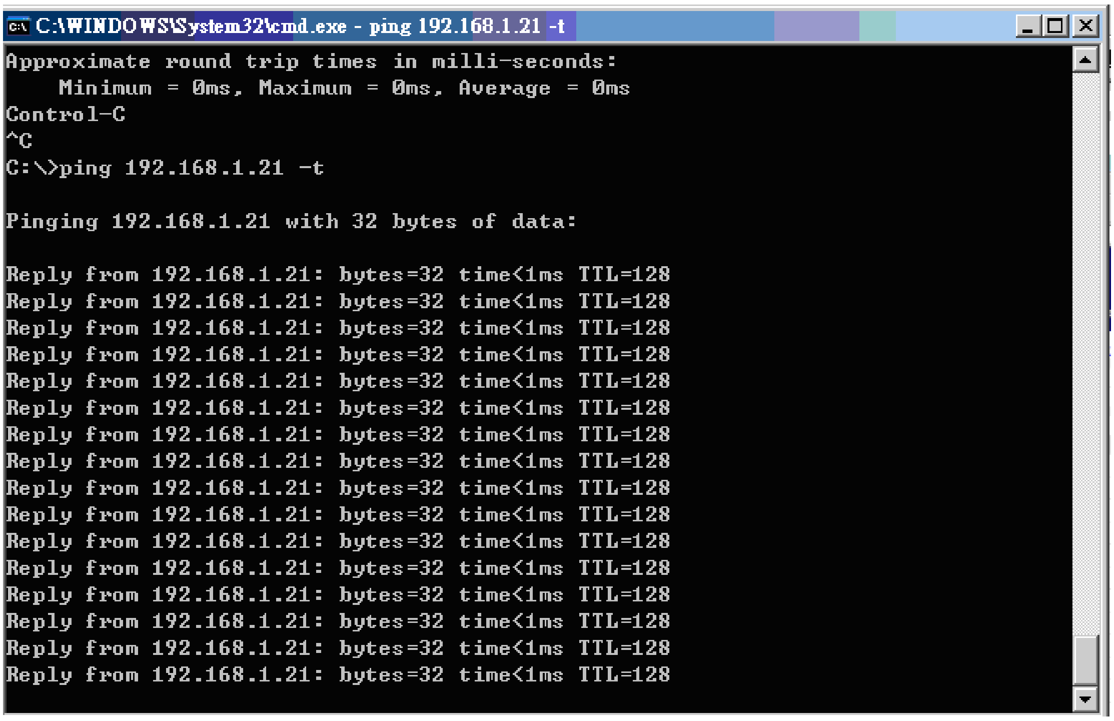
In the switch 1, we set port 2 as VLAN 2 untag

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, we can observe that in the switch 1, the $PC_1$ running on port 2 can find the $PC_2$ running on port 6 in the switch 2.

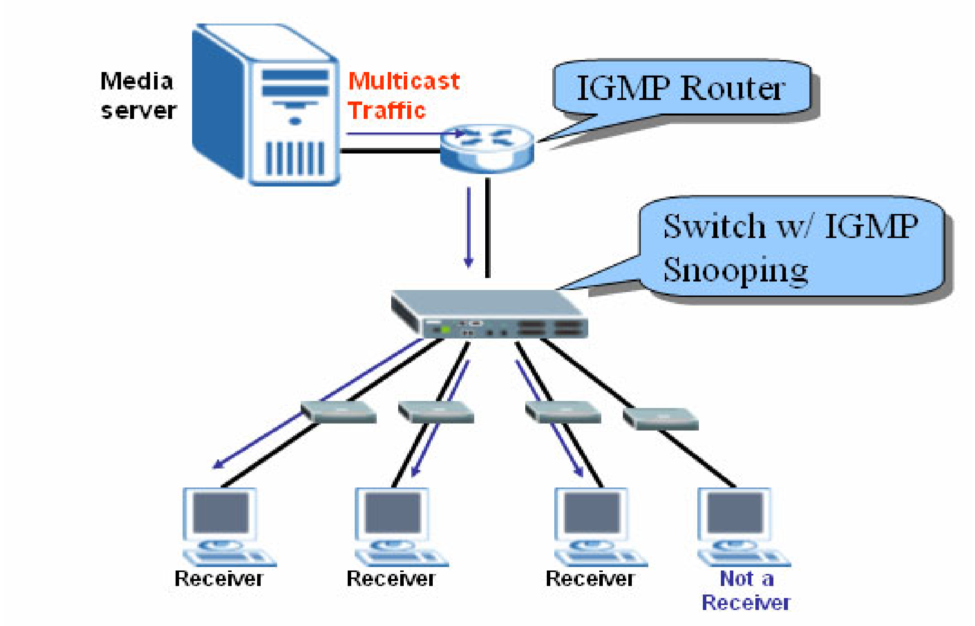


```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>ping 192.168.1.21 -t

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

# IP Multicasting

## How to setup IGMP snooping in your switch?

**Figure 1: IGMP and IGMP snooping**

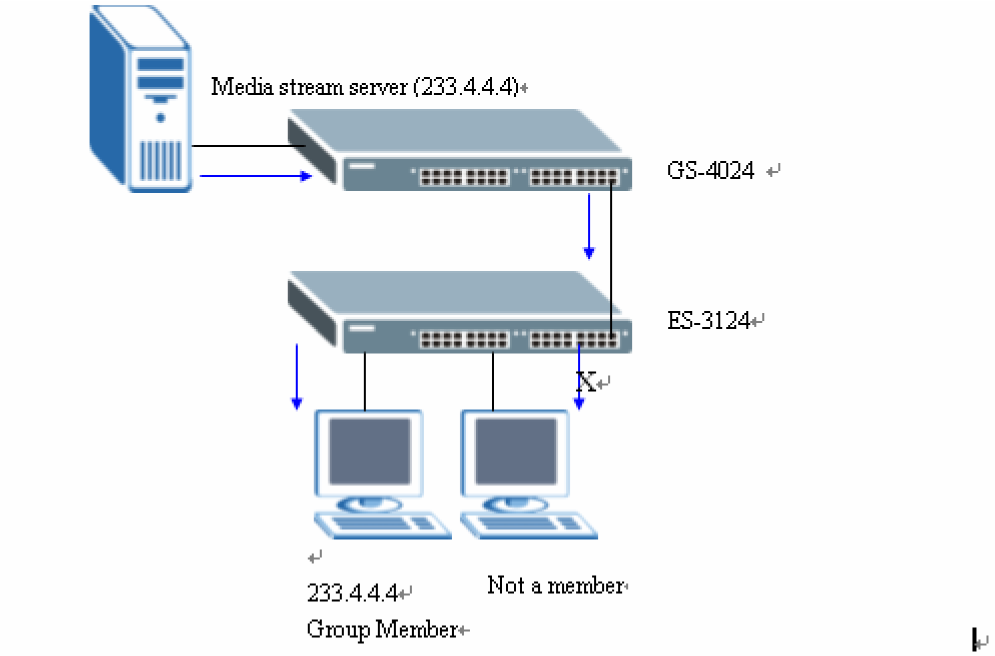


IGMP snooping is designed for application with deployment of multicast traffic. It operates on the underlying IGMP mechanism where a layer two switch passively listens to the IGMP Query, Report and Leave (IGMP version 2) packets transmitted between the IGMP router and clients and collects passing IGMP messages. After that, the switch records the message's group registration information, and configures 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

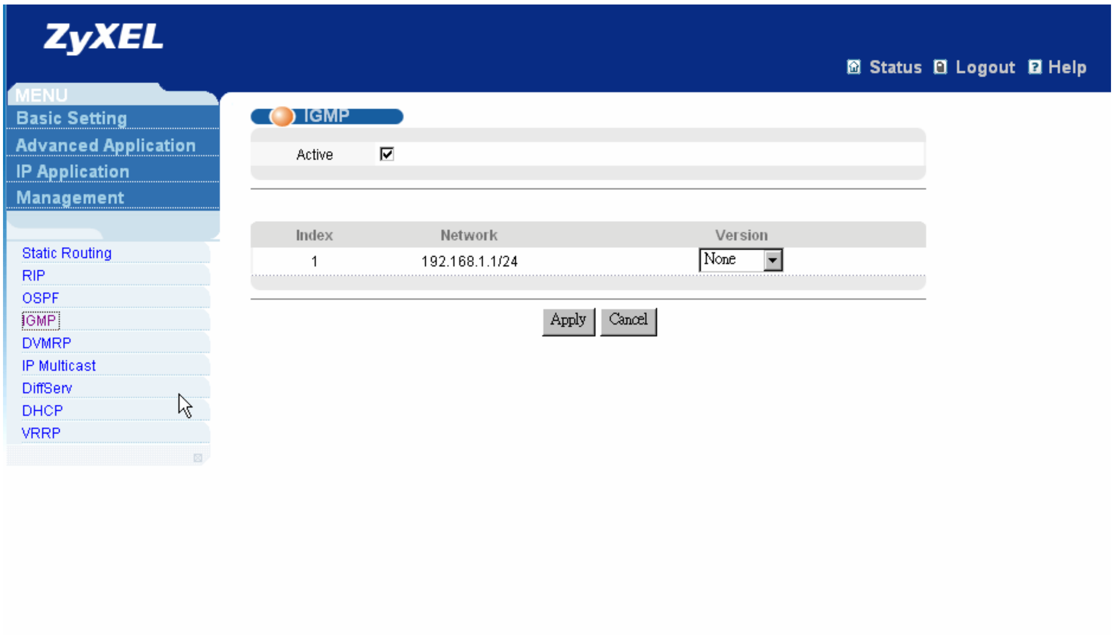
In this example, we enable the IGMP function on the GS-4024 (an IGMP router) to connect to a multimedia server. Also, we enable IGMP snooping function on the ES-3124 or other ZyXEL L2 Switch to connect to the multimedia clients.

**Figure 2: IGMP snooping Example**



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

**Figure 3: IGMP Setup**

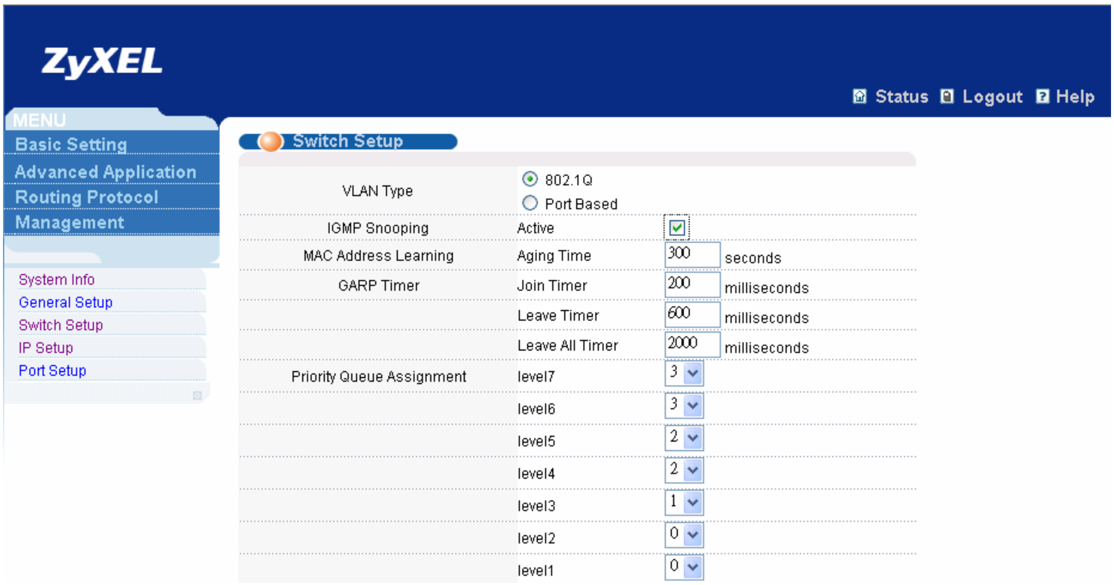


Active ☑

| Index | Network | Version |
|---|---|---|
| 1 | 192.168.1.1/24 | None |

**Step two:** In the L2 Switch, click **Basic Setting** and then **Switch Setup** where we can enable IGMP snooping function with WEB-GUI.

**Figure 4: IGMP Snooping Setup**



| | | | |
|---|---|---|---|
| VLAN Type | ● 802.1Q<br>○ Port Based | | |
| IGMP Snooping | Active | ☑ | |
| MAC Address Learning | Aging Time | 300 | seconds |
| GARP Timer | Join Timer | 200 | milliseconds |
| | Leave Timer | 600 | milliseconds |
| | Leave All Timer | 2000 | milliseconds |
| Priority Queue Assignment | level7 | 3 | |
| | level6 | 3 | |
| | level5 | 2 | |
| | level4 | 2 | |
| | level3 | 1 | |
| | level2 | 0 | |
| | level1 | 0 | |

## Configuration of IGMP and IGMP snooping by CLI

Step one: Enable IGMP function

In the configure mode

GS-4024(config)# **router igmp**

Step two: Enable IGMP snooping

In the configure mode of CLI,

L2Switch(config)# **igmp-snooping**

Step three: Display the IGMP Status

In the exec mode of CLI

GS-4024# **show router igmp**

Step Four: Display the IGMP snooping Status

In the exec mode of CLI

L2Switch# **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 intend to join or leave the multicast group simply by sending the IGMP Join/leave message to a receiver port. The receiver port belongs to one of the multicast group can receive multicast stream from media server. In the Figure 1, without support of MVR, the Multicast stream from media server and 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 once to clients in different VLANs.

**Figure 1**

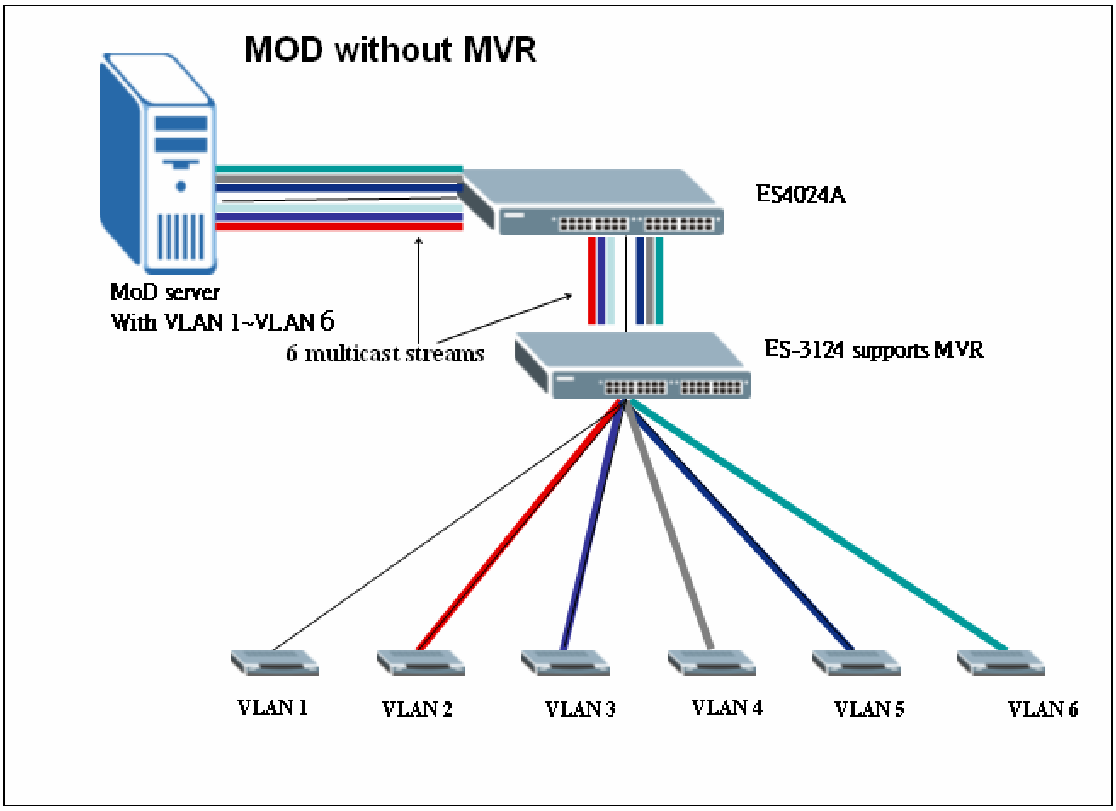
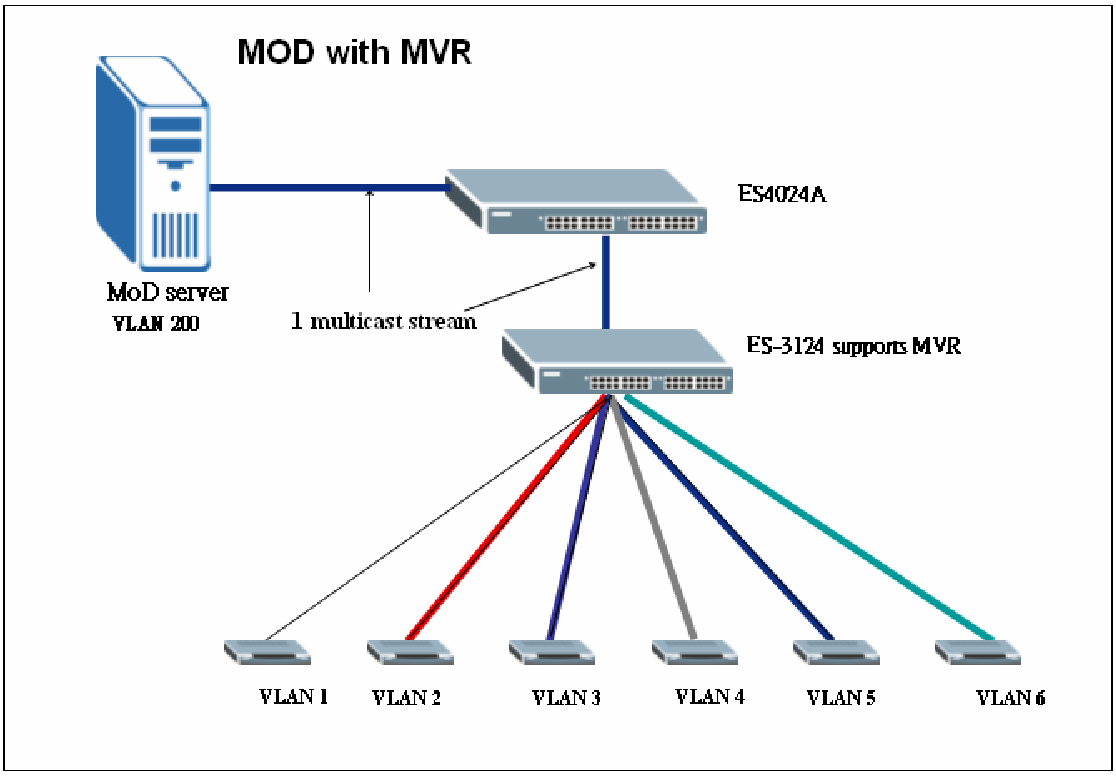


Figure 2



## 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. Whether 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.

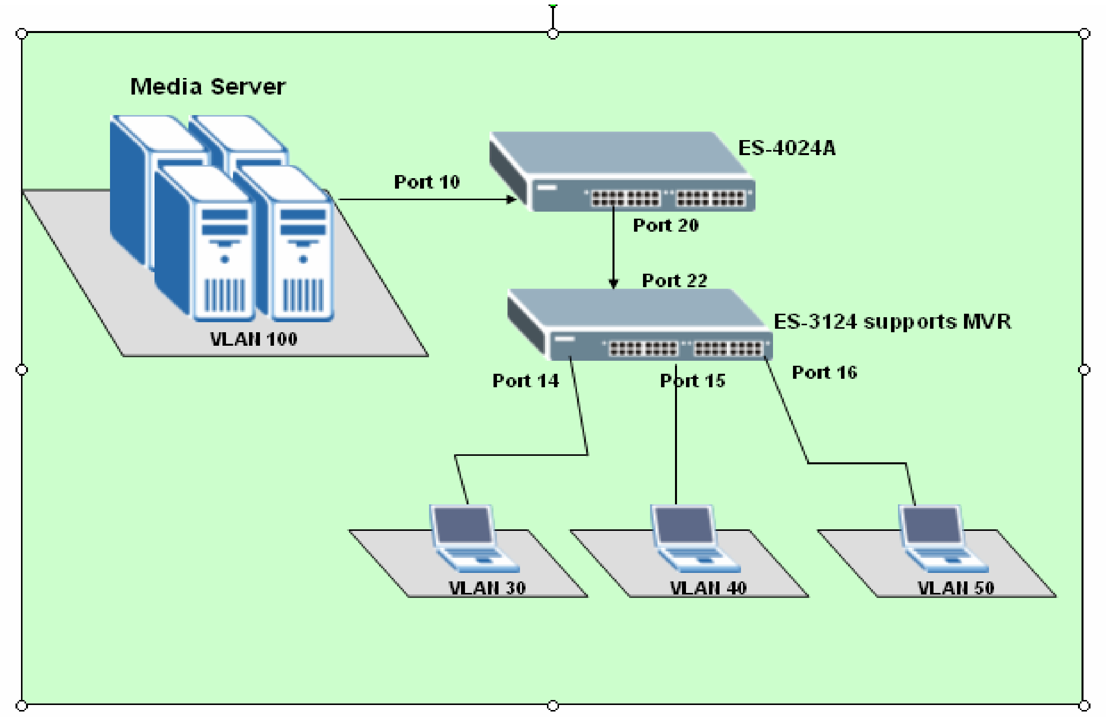
- **Immediate Leave Operation**

  Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait 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 ES-4024A and the multicast traffic flowing into the ES-4024A will be tagged with PVID=100. In the ES-3124, we enable the MVR function to allocate the multicast traffic from ES-4024A to separate VLAN hosts.

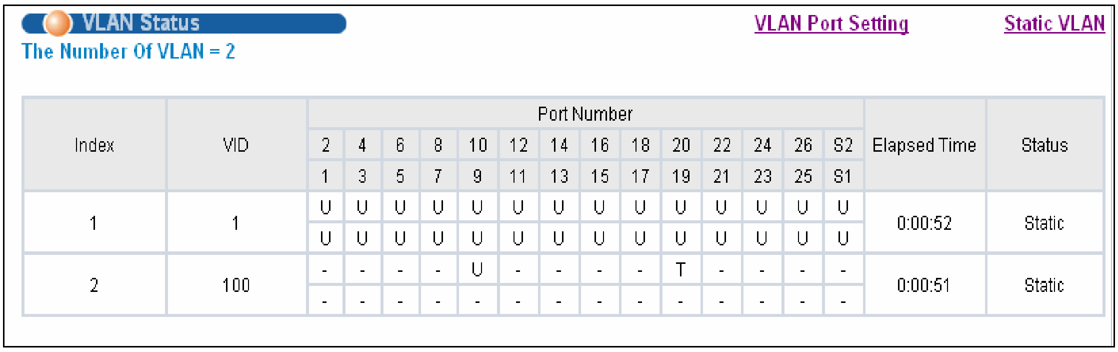
**Figure 3 illustration of MVR**



## Configuration via Web

**Step 1**: We need to create a VLAN for multicast traffic in ES-4024A. In the **ES-4024A**, Click the **Advanced Application** and then select the **VLAN** and in the VLAN Configuration, create a new VLAN 100.

**Figure 4 VLAN Configuration**

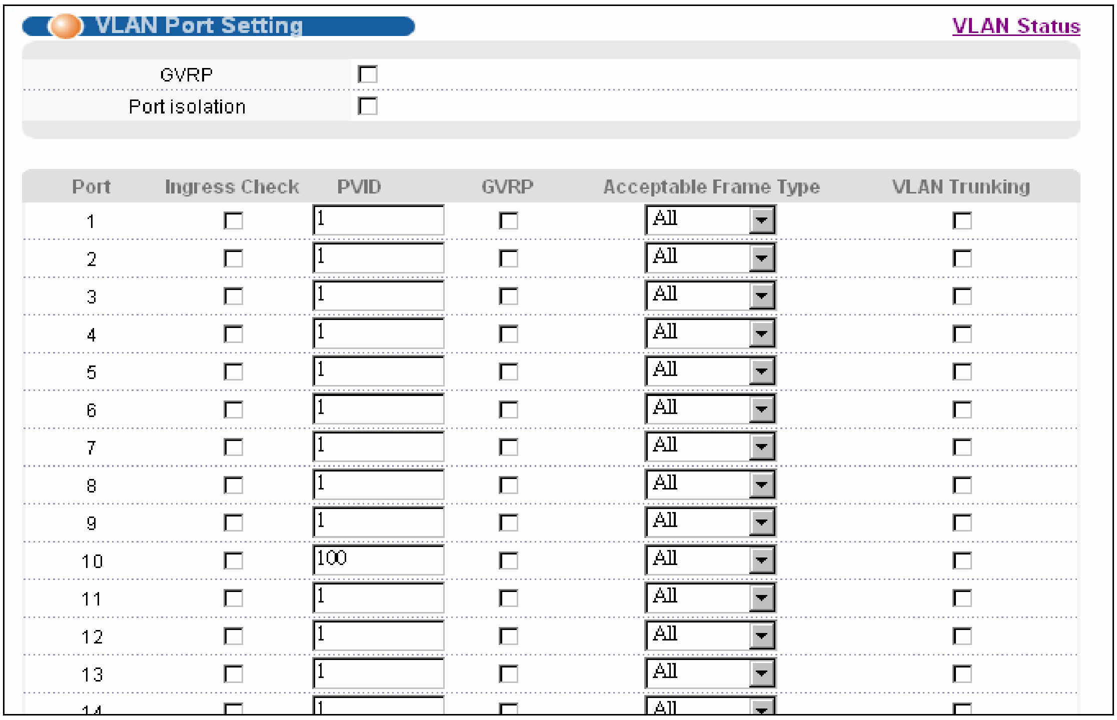


The Number Of VLAN = 2

| Index | VID | Port Number | | | | | | | | | | | | | | Elapsed Time | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | S2 | | |
| | | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | S1 | | |
| 1 | 1 | U | U | U | U | U | U | U | U | U | U | U | U | U | U | 0:00:52 | Static |
| | | U | U | U | U | U | U | U | U | U | U | U | U | U | U | | |
| 2 | 100 | - | - | - | - | U | - | - | - | - | T | - | - | - | - | 0:00:51 | Static |
| | | - | - | - | - | - | - | - | - | - | - | - | - | - | - | | |

**Step 2**, In the **ES-4024A**, click the **Advanced Application** and then select the **VLAN.** In the **VLAN port Setting**, please be noted to set the PVID of the port 10 to 100 as the multicast traffic that flowing from media server in port 10 must be tagged with PVID=100 to communicate with the port in MVR VLAN 100 in ES-3124.

### Figure 5 VLAN Port Setting



VLAN Port Setting

VLAN Status

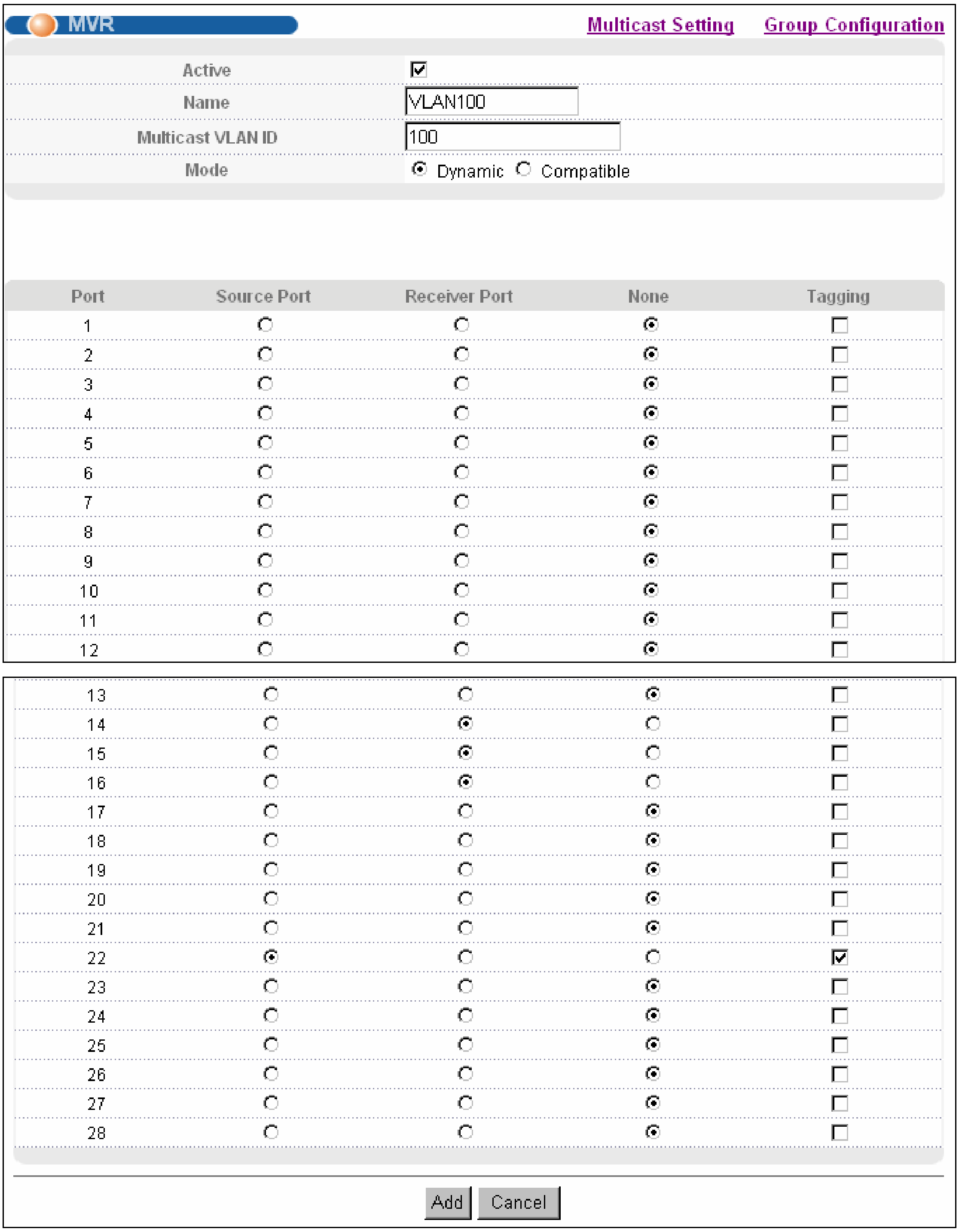
GVRP □

Port isolation □

| Port | Ingress Check | PVID | GVRP | Acceptable Frame Type | VLAN Trunking |
|---|---|---|---|---|---|
| 1 | □ | 1 | □ | All | □ |
| 2 | □ | 1 | □ | All | □ |
| 3 | □ | 1 | □ | All | □ |
| 4 | □ | 1 | □ | All | □ |
| 5 | □ | 1 | □ | All | □ |
| 6 | □ | 1 | □ | All | □ |
| 7 | □ | 1 | □ | All | □ |
| 8 | □ | 1 | □ | All | □ |
| 9 | □ | 1 | □ | All | □ |
| 10 | □ | 100 | □ | All | □ |
| 11 | □ | 1 | □ | All | □ |
| 12 | □ | 1 | □ | All | □ |
| 13 | □ | 1 | □ | All | □ |
| 14 | □ | 1 | □ | All | □ |

**Step 3**, we need to create separate VLANs for different Clients. In the **ES-3124**, in the **Advanced Application**, click **Multicast** to enter the **Multicast Setting** and configure the MVR VLAN=100. Define port 14, port 15 and port 16 as the receiver ports to forward multicast stream to clients in different VLANs; set port 22 as a source port to receive traffic from the media server. Also, we select mode as *dynamic* mode. The switch sends IGMP report message to multicast router through its source port.

### Figure 6 MVR Configuration

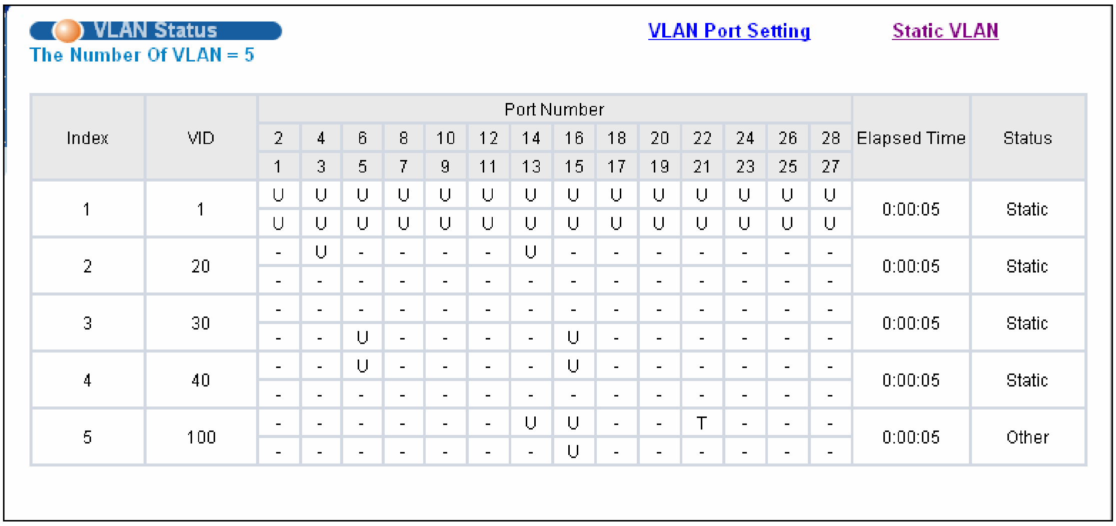


| | |
|---|---|
| Active | ☑ |
| Name | VLAN100 |
| Multicast VLAN ID | 100 |
| Mode | ● Dynamic ○ Compatible |

| Port | Source Port | Receiver Port | None | Tagging |
|---|---|---|---|---|
| 1 | ○ | ○ | ● | □ |
| 2 | ○ | ○ | ● | □ |
| 3 | ○ | ○ | ● | □ |
| 4 | ○ | ○ | ● | □ |
| 5 | ○ | ○ | ● | □ |
| 6 | ○ | ○ | ● | □ |
| 7 | ○ | ○ | ● | □ |
| 8 | ○ | ○ | ● | □ |
| 9 | ○ | ○ | ● | □ |
| 10 | ○ | ○ | ● | □ |
| 11 | ○ | ○ | ● | □ |
| 12 | ○ | ○ | ● | □ |
| 13 | ○ | ○ | ● | □ |
| 14 | ○ | ● | ○ | □ |
| 15 | ○ | ● | ○ | □ |
| 16 | ○ | ● | ○ | □ |
| 17 | ○ | ○ | ● | □ |
| 18 | ○ | ○ | ● | □ |
| 19 | ○ | ○ | ● | □ |
| 20 | ○ | ○ | ● | □ |
| 21 | ○ | ○ | ● | □ |
| 22 | ● | ○ | ○ | ☑ |
| 23 | ○ | ○ | ● | □ |
| 24 | ○ | ○ | ● | □ |
| 25 | ○ | ○ | ● | □ |
| 26 | ○ | ○ | ● | □ |
| 27 | ○ | ○ | ● | □ |
| 28 | ○ | ○ | ● | □ |

**Step 4**: In the **ES-3124,** after the MVR configuration, click the **Advanced Application** to browse the **VLAN Status** and see we have add a new VLAN 100 in the VLAN list. We also create three separate VLANs, 20, 30, 40 and assign their PVID as 20, 30 and 40 respectively.

**Figure 7 VLAN Status**



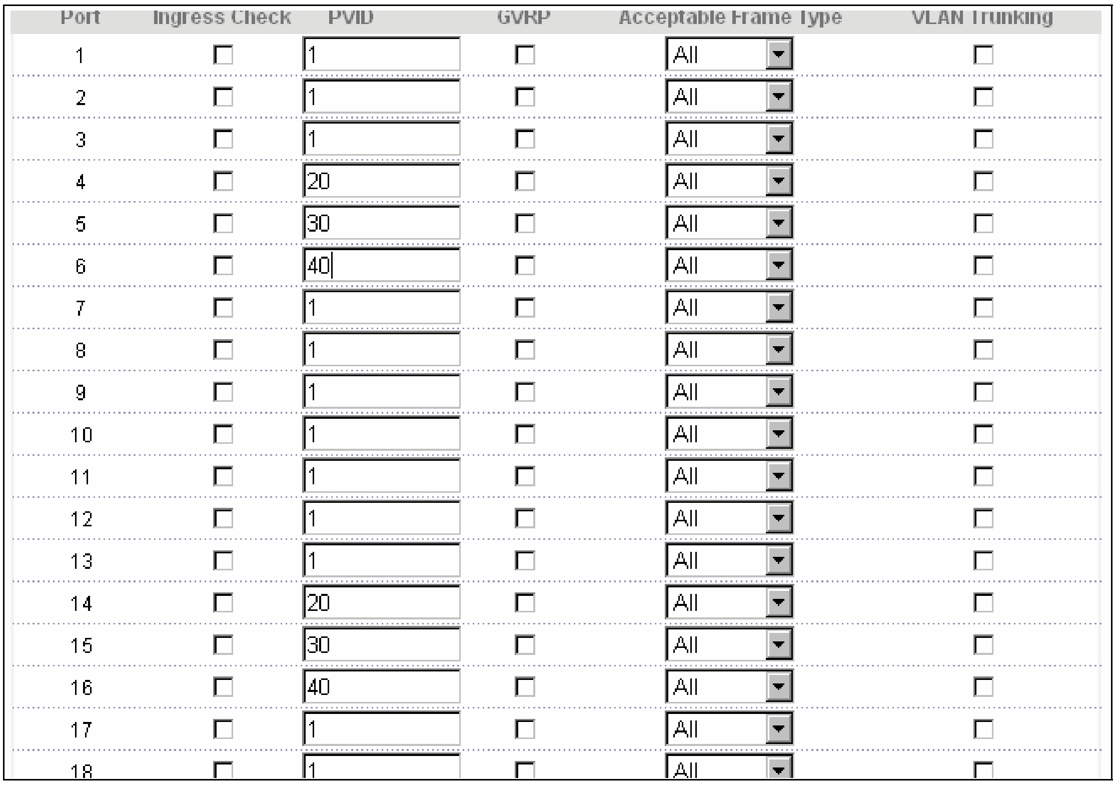
VLAN Status

The Number Of VLAN = 5

VLAN Port Setting    Static VLAN

| Index | VID | Port Number | | | | | | | | | | | | | | Elapsed Time | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 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 | U | U | U | U | U | U | 0:00:05 | Static |
| | | U | U | U | U | U | U | U | U | U | U | U | U | U | U | | |
| 2 | 20 | - | U | - | - | - | - | U | - | - | - | - | - | - | - | 0:00:05 | Static |
| | | - | - | - | - | - | - | - | - | - | - | - | - | - | - | | |
| 3 | 30 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 0:00:05 | Static |
| | | - | - | U | - | - | - | - | U | - | - | - | - | - | - | | |
| 4 | 40 | - | - | U | - | - | - | - | U | - | - | - | - | - | - | 0:00:05 | Static |
| | | - | - | - | - | - | - | - | - | - | - | - | - | - | - | | |
| 5 | 100 | - | - | - | - | - | - | U | U | - | - | T | - | - | - | 0:00:05 | Other |
| | | - | - | - | - | - | - | - | U | - | - | - | - | - | - | | |

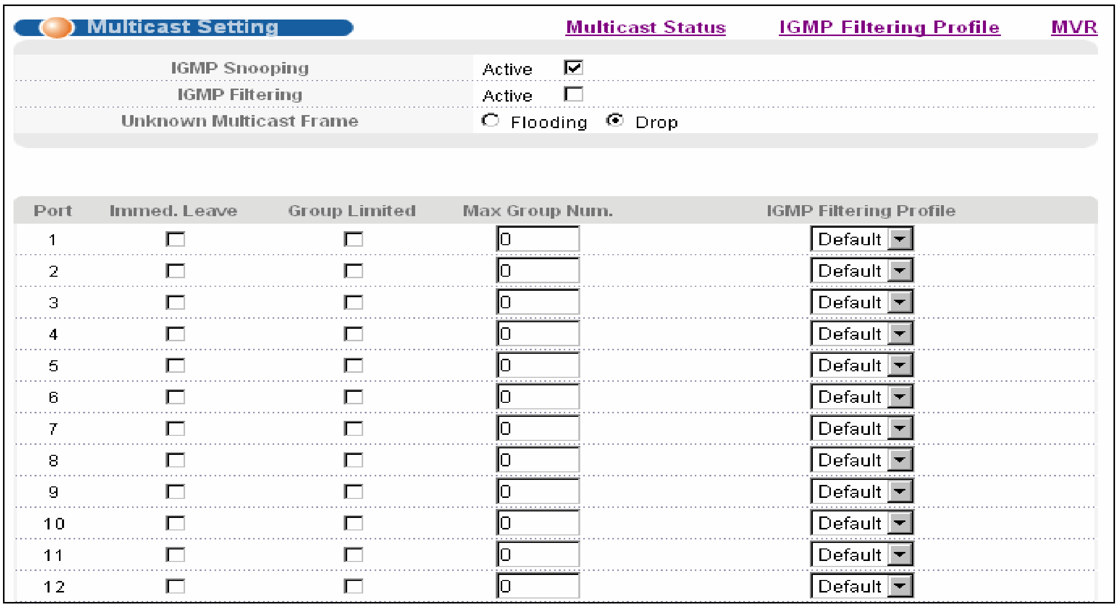
## Figure 8 VLAN Port Setting



| Port | Ingress Check | PVID | GVRP | Acceptable Frame Type | VLAN Trunking |
|---|---|---|---|---|---|
| 1 | □ | 1 | □ | All | □ |
| 2 | □ | 1 | □ | All | □ |
| 3 | □ | 1 | □ | All | □ |
| 4 | □ | 20 | □ | All | □ |
| 5 | □ | 30 | □ | All | □ |
| 6 | □ | 40 | □ | All | □ |
| 7 | □ | 1 | □ | All | □ |
| 8 | □ | 1 | □ | All | □ |
| 9 | □ | 1 | □ | All | □ |
| 10 | □ | 1 | □ | All | □ |
| 11 | □ | 1 | □ | All | □ |
| 12 | □ | 1 | □ | All | □ |
| 13 | □ | 1 | □ | All | □ |
| 14 | □ | 20 | □ | All | □ |
| 15 | □ | 30 | □ | All | □ |
| 16 | □ | 40 | □ | All | □ |
| 17 | □ | 1 | □ | All | □ |
| 18 | □ | 1 | □ | All | □ |

**Step 5**: Before we start to use the MVR, it is quite fundamental to enable the IGMP Snooping first. In the **ES-3124 Menu**, click the **Multicast** and go toe the **Multicast Setting**, activate the **IGMP Snooping.**

## Figure 10 Multicast Setting



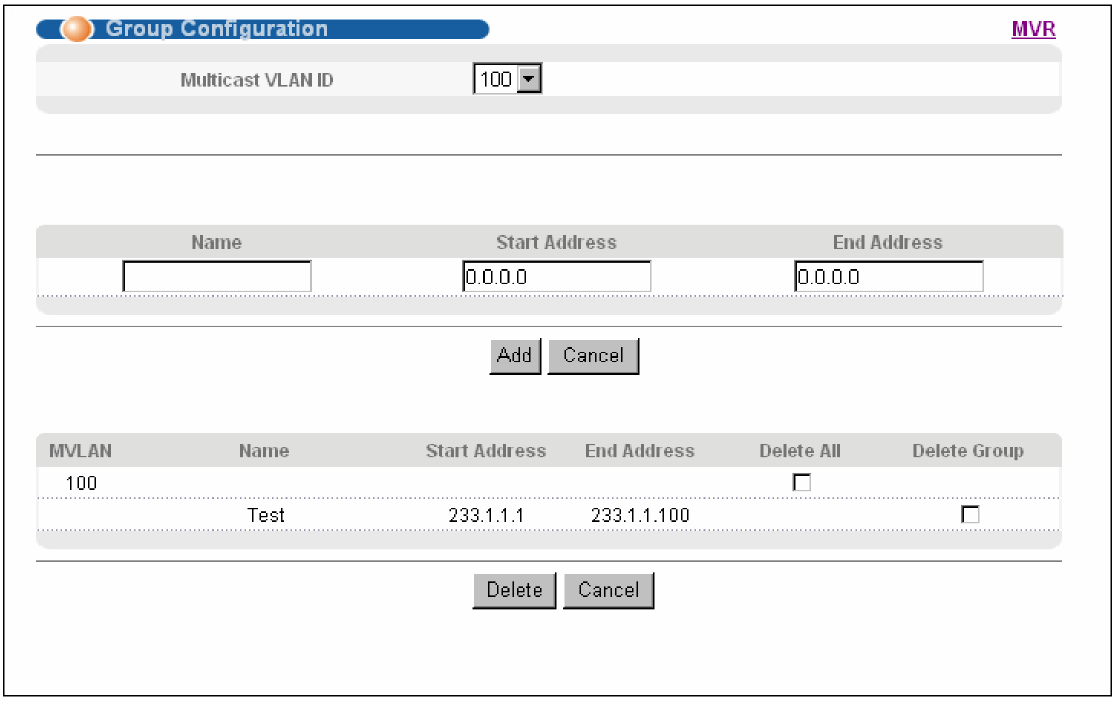
Multicast Setting | Multicast Status | IGMP Filtering Profile | MVR

| | |
|---|---|
| IGMP Snooping | Active ☑ |
| IGMP Filtering | Active □ |
| Unknown Multicast Frame | ○ Flooding ● Drop |

| Port | Immed. Leave | Group Limited | Max Group Num. | IGMP Filtering Profile |
|---|---|---|---|---|
| 1 | □ | □ | 0 | Default |
| 2 | □ | □ | 0 | Default |
| 3 | □ | □ | 0 | Default |
| 4 | □ | □ | 0 | Default |
| 5 | □ | □ | 0 | Default |
| 6 | □ | □ | 0 | Default |
| 7 | □ | □ | 0 | Default |
| 8 | □ | □ | 0 | Default |
| 9 | □ | □ | 0 | Default |
| 10 | □ | □ | 0 | Default |
| 11 | □ | □ | 0 | Default |
| 12 | □ | □ | 0 | Default |

**Step 6**: In the **ES-3124,** in the **advanced application**, select **Multicast**, and then in the **Multicast setting**, and choose **MVR** and click the **Group configuration**. Here, we configure 233.1.1.1~ 233.1.1.100 as the range of multicast address and only the clients belong to that range of multicast group will receive the multicast traffic.

**Figure 11 Group Configuration**



Group Configuration | MVR

Multicast VLAN ID: 100

| Name | Start Address | End Address |
|---|---|---|
| | 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 | | □ |

## Configuration via CLI

**Step 1: On the ES-3124, in the configure mode, create VLAN 100**

```
ES-3124# config
ES-3124(config)# vlan 100
```

**Step 2: In the VLAN 100, set the port 22 to be fixed port.**

```
ES-3124(config-vlan)# fixed 22
```

**Step 3: On the ES-3124, in the configure mode, create VLAN 20, and set the port 4 and port 14 to be fixed port.**

```
ES-3124(config)# vlan 20
ES-3124(config-vlan)# untagged 4
ES-3124(config-vlan)# fixed 4
ES-3124(config-vlan)# untagged 14
ES-3124(config-vlan)# fixed 14
```

**Step 4: On the ES-3124, in the configure mode, create VLAN 30, and set the port 5 and port 15 to be fixed port.**

```
ES-3124(config)# vlan 30
ES-3124(config-vlan)# untagged 5
ES-3124(config-vlan)# fixed 5
ES-3124(config-vlan)# untagged 15
ES-3124(config-vlan)# fixed 15
```

**Step 5: On the ES-3124, in the configure mode, create VLAN 40, and set the port 6 and port 16 to be fixed port.**

```
ES-3124(config)# vlan 40
ES-3124(config-vlan)# untagged 6
ES-3124(config-vlan)# fixed 6
ES-3124(config-vlan)# untagged 16
ES-3124(config-vlan)# fixed 16
```

**Step 6: On the ES-3124, set the PVID of specific VLAN 20**

```
ES-3124(config)# interface port-channel 4
```

```
ES-3124(config-interface)# pvid 20
ES-3124(config-interface)# exit
ES-3124(config)# interface port-channel 14
ES-3124(config-interface)# pvid 20
```

**Step 7: On the ES-3124, set the PVID of specific VLAN 30**

```
ES-3124(config)# interface port-channel 5
ES-3124(config-interface)# pvid 30
ES-3124(config-interface)# exit
ES-3124(config)# interface port-channel 15
ES-3124(config-interface)# pvid 30
```

**Step 8: On the ES-3124, set the PVID of specific VLAN 40**

```
ES-3124(config)# interface port-channel 6
ES-3124(config-interface)# pvid 40
ES-3124(config-interface)# exit
ES-3124(config)# interface port-channel 16
ES-3124(config-interface)# pvid 40
```

**Step 9: On the ES-3124, in the configure mode, enable IGMP snooping**

```
ES-3124(config)#igmpsnooping
```

**Step 10: On the ES-3124, in the configure mode, create MVR**

```
ES-3124(config)# mvr 100
```

**Step 11: Define the Dynamic mode**

```
ES-3124(config-mvr)# mode dynamic
```

**Step 12: on the ES-3124, in the MVR 100, set up the multicast group address.**

```
ES-3124(config-mvr)# group test start-address 233.1.1.1 end-address 233.1.1.100
```

**Step 13: In the MVR 100, specify receiver ports on port 14~16 as tagged ports**

```
ES-3124(config-mvr)# receiver-port 14-16
ES-3124(config-mvr)# untagged 14-16
```

**Step 14: Then, specify the source port 22 and assign it to be tagged ports**

```
ES-3124(config-mvr)# source-port 22
ES-3124(config-mvr)# tagged 22
```

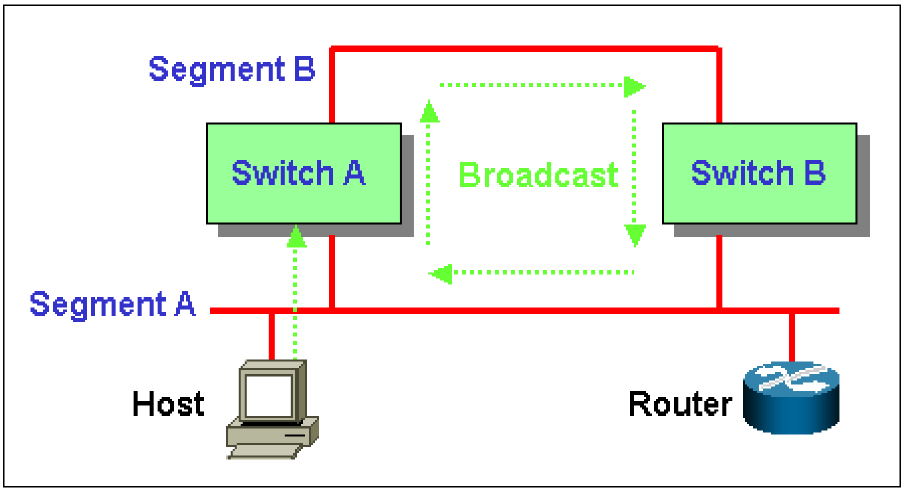
# To ring a network by building reducdent links and connections between Switch

## What is Spanning Tree Protocol

- ### Spanning Tree Overview

Spanning-Tree Protocol (STP) is a Layer 2 protocol designed to run on bridges and 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.

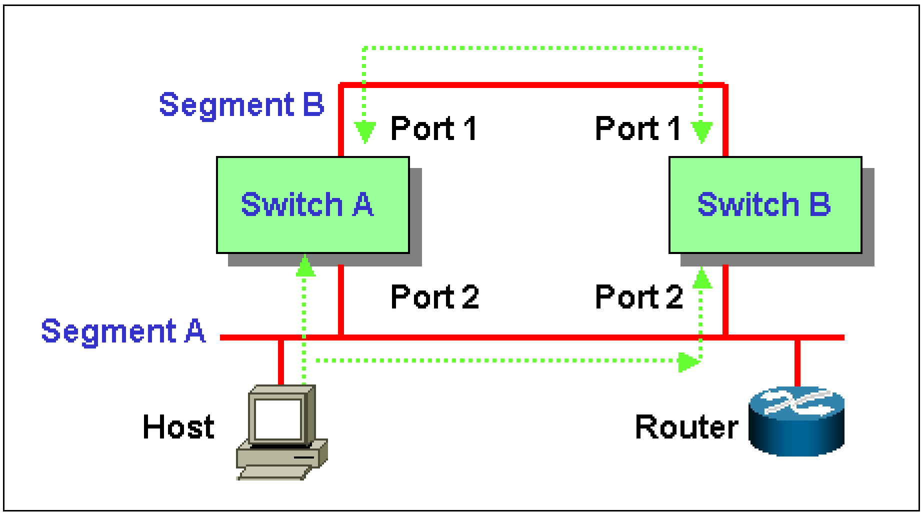
1. When Host sends a broadcast frame, like an ARP request to Router, the frame will be received by Switch A.
2. Switch A identify the destination MAC address field (broadcast FF:FF:FF:FF:FF:FF) in the frame and determine to flood it onto Segment B.
3. When the broadcast frame arrives at Switch B, Switch will repeat above process, flood it to Segment A.
4. The broadcast frame will endlessly travel around the loop network even 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.

1. Host sends an unicast frame to 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 MAC address of Host on Port 2.
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.
3. 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 frames properly because the instability of mapping MAC address to Port.



## How STP Works

Spanning Tree provide a loop-free network. When a switch supported STP recognize a loop in the network topology, it blocks one or more redundant ports. Spanning Tree Protocol continually explore the network, so when the network topology changes, STP automatically reconfigure switch ports 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 will construct a loop free network with "tree" architecture.

STP operation is listed as the following:

***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".

1. One of the important field 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.

2. The bridge ID includes two parts, bridge priority (2 bytes) and bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768. For example, 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.
3. On the root bridge, all its ports are **designated ports**. **Designated ports are always in the forwarding state**. While in forwarding state, a 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").

1. 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**.
2. 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 lowest bridge ID is selected as a designated port.

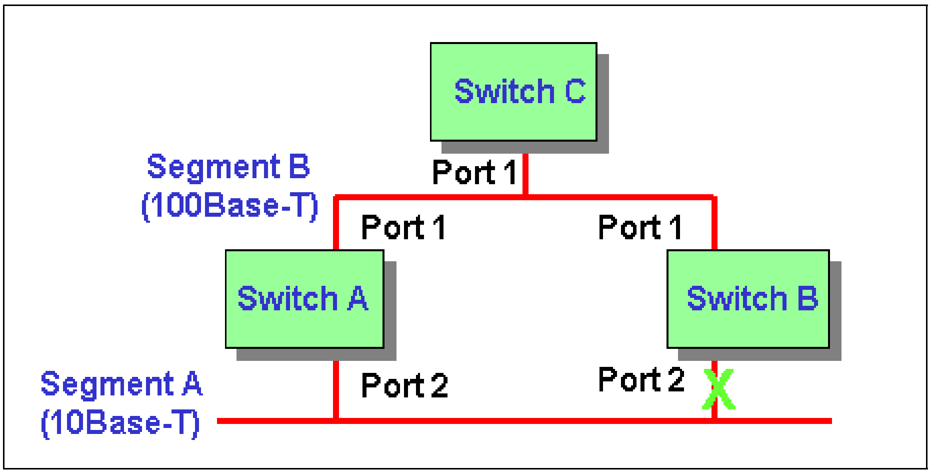
### 1. *How STP works*

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. When 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:

<table>
<tr><td colspan="3"><b>Switch A:</b><br>MAC = 00A0C5111111,<br>Priority = 32768</td><td colspan="3"><b>Switch B:</b><br>MAC = 00A0C5222222,<br>Priority = 32768</td><td colspan="2"><b>Switch C:</b> MAC =<br>00A0C5333333<br>Priority = 1</td></tr>
<tr><td></td><td>Port 1</td><td>Port 2</td><td></td><td>Port 1</td><td>Port 2</td><td></td><td>Port 1</td></tr>
<tr><td>Cost</td><td>19</td><td>100</td><td>Cost</td><td>19</td><td>100</td><td>Cost</td><td>19</td></tr>
<tr><td>Priority</td><td>128</td><td>128</td><td>Priority</td><td>128</td><td>128</td><td>Priority</td><td>128</td></tr>
</table>



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

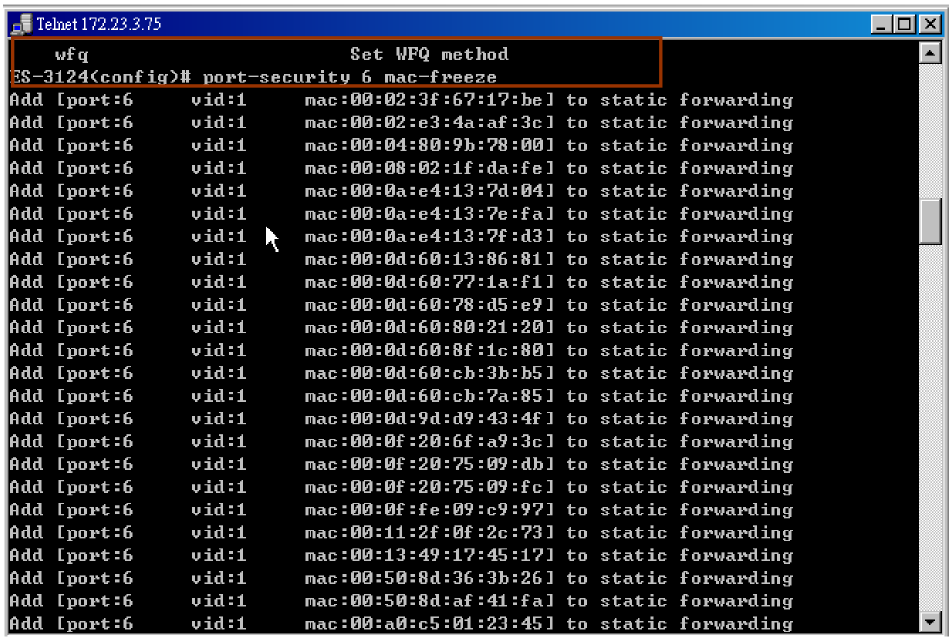
As an added protection against network intrusion attacks, ZyXEL has implemented the MAC Freeze feature on ES-2108 Series, ES-3124, ES-2024, ES-3100 Series and ES-4024A. Security has been the focus of our Ethernet switch design. This feature will also be available for GS-4024, GS-4012F, GS-3012 Series, GS-2024 and new switch models in future firmware releases.

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 that 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 port 6 to the static MAC address.

Figure 1: Enable MAC Freeze Example

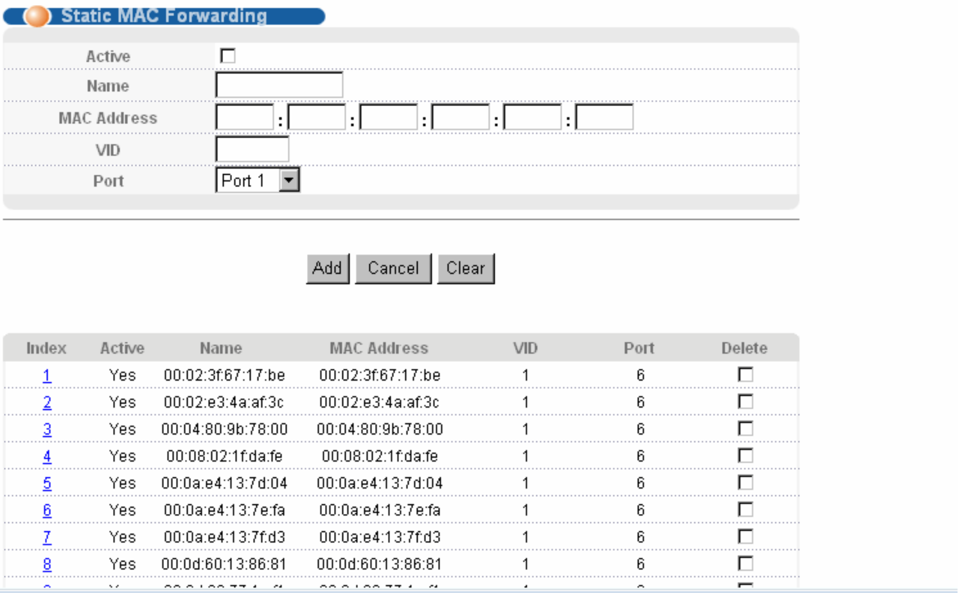


Telnet 172.23.3.75

```
    wfq                                  Set WFQ method
ES-3124(config)# port-security 6 mac-freeze
Add [port:6      vid:1      mac:00:02:3f:67:17:be] to static forwarding
Add [port:6      vid:1      mac:00:02:e3:4a:af:3c] to static forwarding
Add [port:6      vid:1      mac:00:04:80:9b:78:00] to static forwarding
Add [port:6      vid:1      mac:00:08:02:1f:da:fe] to static forwarding
Add [port:6      vid:1      mac:00:0a:e4:13:7d:04] to static forwarding
Add [port:6      vid:1      mac:00:0a:e4:13:7e:fa] to static forwarding
Add [port:6      vid:1      mac:00:0a:e4:13:7f:d3] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:13:86:81] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:77:1a:f1] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:78:d5:e9] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:80:21:20] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:8f:1c:80] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:cb:3b:b5] to static forwarding
Add [port:6      vid:1      mac:00:0d:60:cb:7a:85] to static forwarding
Add [port:6      vid:1      mac:00:0d:9d:d9:43:4f] to static forwarding
Add [port:6      vid:1      mac:00:0f:20:6f:a9:3c] to static forwarding
Add [port:6      vid:1      mac:00:0f:20:75:09:db] to static forwarding
Add [port:6      vid:1      mac:00:0f:20:75:09:fc] to static forwarding
Add [port:6      vid:1      mac:00:0f:fe:09:c9:97] to static forwarding
Add [port:6      vid:1      mac:00:11:2f:0f:2c:73] to static forwarding
Add [port:6      vid:1      mac:00:13:49:17:45:17] to static forwarding
Add [port:6      vid:1      mac:00:50:8d:36:3b:26] to static forwarding
Add [port:6      vid:1      mac:00:50:8d:af:41:fa] to static forwarding
Add [port:6      vid:1      mac:00:a0:c5:01:23:45] to static forwarding
```

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



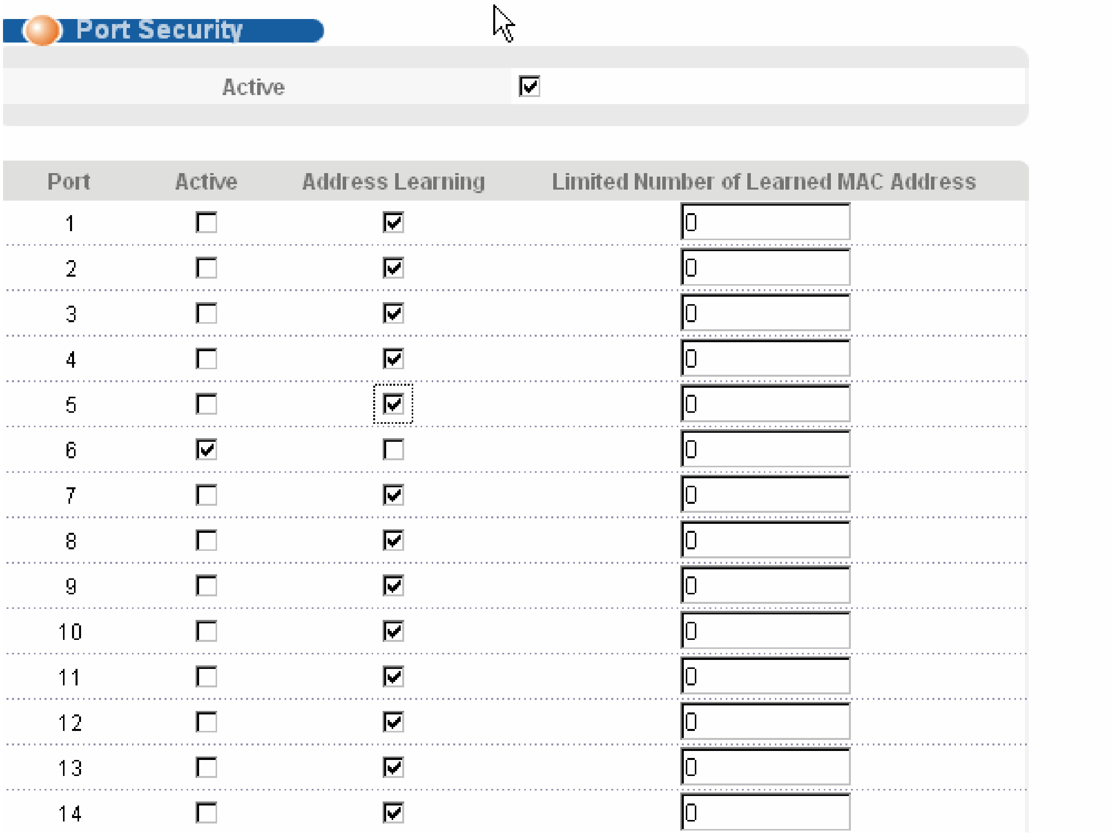
Static MAC Forwarding

| | |
|---|---|
| Active | □ |
| Name | |
| MAC Address | : : : : : |
| VID | |
| Port | Port 1 |

| Index | Active | Name | MAC Address | VID | Port | Delete |
|---|---|---|---|---|---|---|
| 1 | Yes | 00:02:3f:67:17:be | 00:02:3f:67:17:be | 1 | 6 | □ |
| 2 | Yes | 00:02:e3:4a:af:3c | 00:02:e3:4a:af:3c | 1 | 6 | □ |
| 3 | Yes | 00:04:80:9b:78:00 | 00:04:80:9b:78:00 | 1 | 6 | □ |
| 4 | Yes | 00:08:02:1f:da:fe | 00:08:02:1f:da:fe | 1 | 6 | □ |
| 5 | Yes | 00:0a:e4:13:7d:04 | 00:0a:e4:13:7d:04 | 1 | 6 | □ |
| 6 | Yes | 00:0a:e4:13:7e:fa | 00:0a:e4:13:7e:fa | 1 | 6 | □ |
| 7 | Yes | 00:0a:e4:13:7f:d3 | 00:0a:e4:13:7f:d3 | 1 | 6 | □ |
| 8 | Yes | 00:0d:60:13:86:81 | 00:0d:60:13:86:81 | 1 | 6 | □ |

After you enabled MAC freeze on 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



Port Security

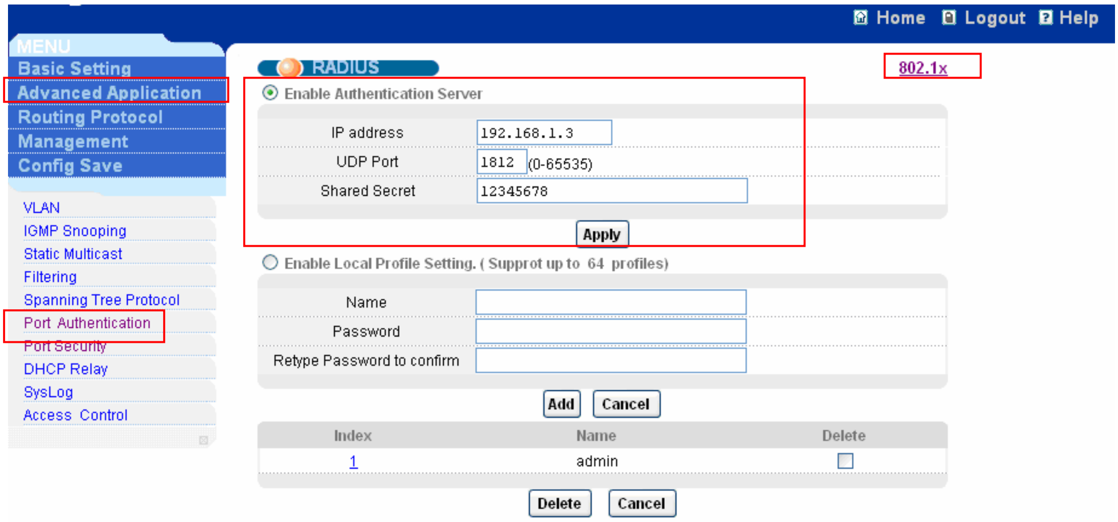
Active ☑

| Port | Active | Address Learning | Limited Number of Learned MAC Address |
|---|---|---|---|
| 1 | □ | ☑ | 0 |
| 2 | □ | ☑ | 0 |
| 3 | □ | ☑ | 0 |
| 4 | □ | ☑ | 0 |
| 5 | □ | ☑ | 0 |
| 6 | ☑ | □ | 0 |
| 7 | □ | ☑ | 0 |
| 8 | □ | ☑ | 0 |
| 9 | □ | ☑ | 0 |
| 10 | □ | ☑ | 0 |
| 11 | □ | ☑ | 0 |
| 12 | □ | ☑ | 0 |
| 13 | □ | ☑ | 0 |
| 14 | □ | ☑ | 0 |

# Setting up 802.1x Radius Authentication.

Port-Authentication -- RADIUS settings:

Click **Advanced Application**, **Port Authentication** in the navigation panel to display configuration screen as shown. Click **Enable Authentication Server** and set the RADIUS server **IP address**, **UDP port** and **shared Secret,** which is the same as Radius server. Then click **Apply** to make the settings take effect.



● Enable Authentication Server

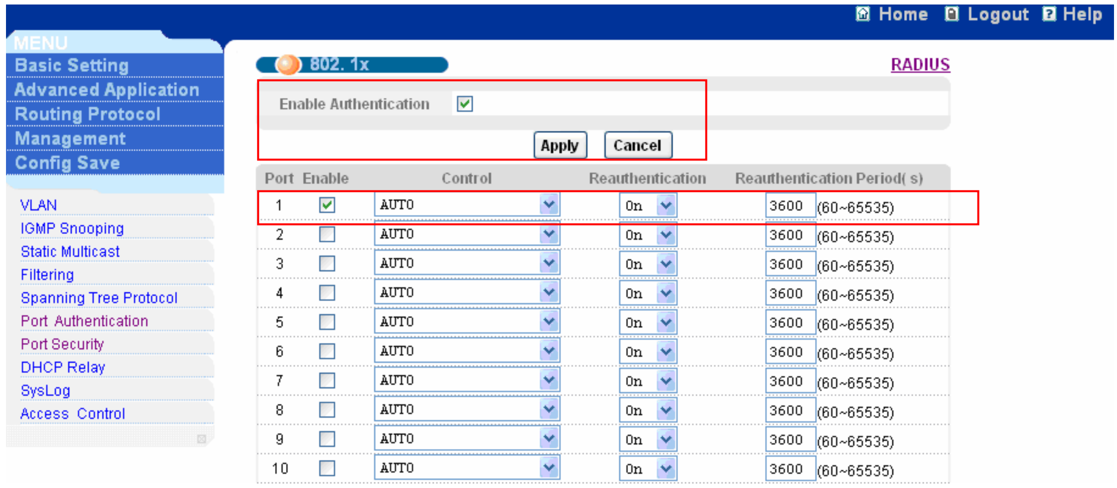
| | |
|---|---|
| IP address | 192.168.1.3 |
| UDP Port | 1812 (0-65535) |
| Shared Secret | 12345678 |

○ Enable Local Profile Setting. ( Supprot up to 64 profiles)

| | |
|---|---|
| Name | |
| Password | |
| Retype Password to confirm | |

| Index | Name | Delete |
|---|---|---|
| 1 | admin | □ |

Click the **802.1x** link to enter the 802.1x settings. Check the **Enable Authentication** and click **Apply** button to enable 802.1x authentication. Check **Enable** to turn on 802.1x authentication on that port. You can leave other settings as default values. Click **Apply** to save your changes.

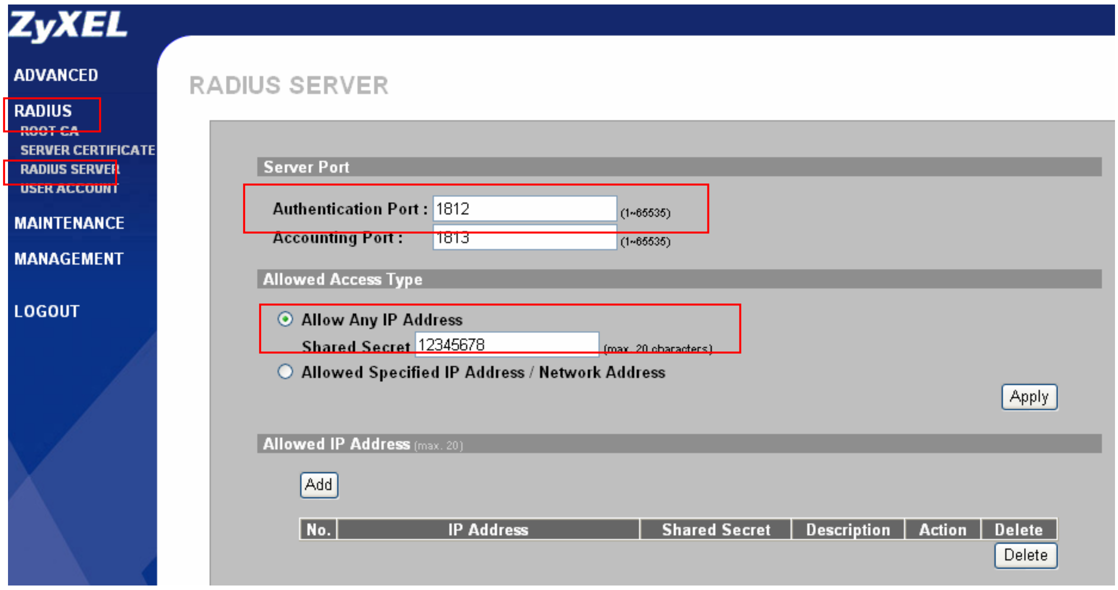


Enable Authentication ☑

| Port | Enable | Control | Reauthentication | Reauthentication Period( s) |
|---|---|---|---|---|
| 1 | ☑ | AUTO | On | 3600 (60~65535) |
| 2 | □ | AUTO | On | 3600 (60~65535) |
| 3 | □ | AUTO | On | 3600 (60~65535) |
| 4 | □ | AUTO | On | 3600 (60~65535) |
| 5 | □ | AUTO | On | 3600 (60~65535) |
| 6 | □ | AUTO | On | 3600 (60~65535) |
| 7 | □ | AUTO | On | 3600 (60~65535) |
| 8 | □ | AUTO | On | 3600 (60~65535) |
| 9 | □ | AUTO | On | 3600 (60~65535) |
| 10 | □ | AUTO | On | 3600 (60~65535) |

RADIUS server setup

Click **RADIUS**, **RADIUS SERVER** in the navigation panel to display configuration screen as shown. You can use the default values or change the **Authentication port**, **Shared Secret**. Remember these values MUST be the as the settings of client.



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)

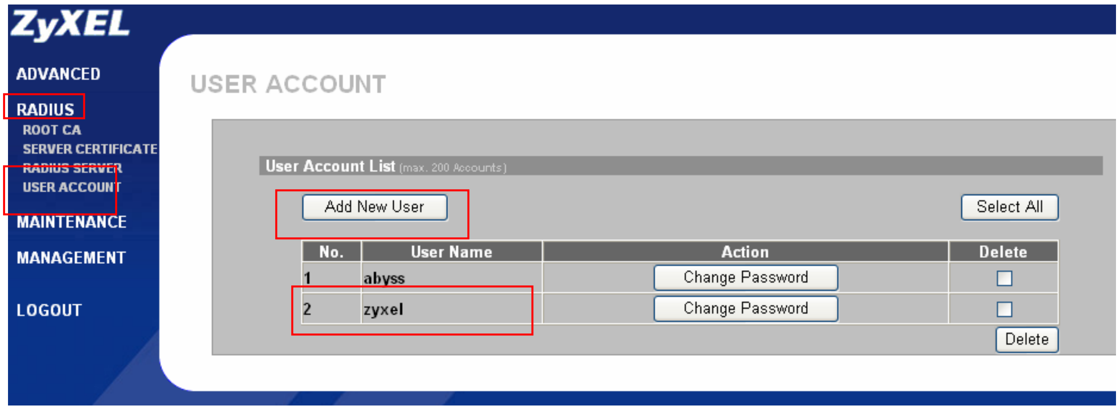
Add

| No. | IP Address | Shared Secret | Description | Action | Delete |
|---|---|---|---|---|---|

Delete

Create User Account

Click **RADIUS**, **USER ACCOUNT** in the navigation panel to display configuration screen as shown. You can use the existed user account or create the new one by clicking **Add New User** button. Remember the client site MUST use the account in RADIUS server.



USER ACCOUNT

User Account List (max. 200 Accounts)

Add New User

Select All

| No. | User Name | Action | Delete |
|---|---|---|---|
| 1 | abyss | Change Password | □ |
| 2 | zyxel | Change Password | □ |

Delete

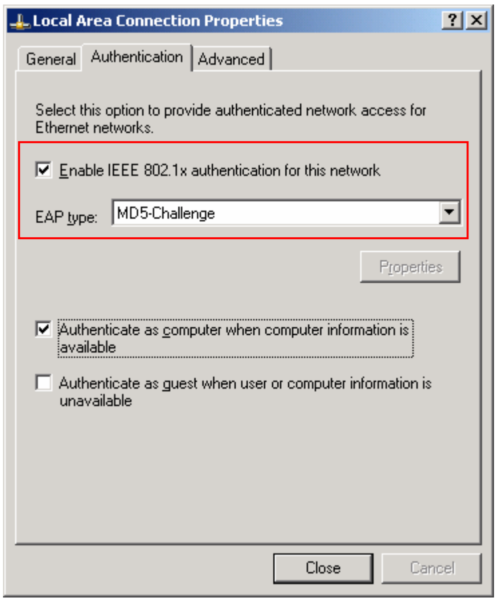
Windows XP(Supplicant) settings:

There are many supplicants we can choose like MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client. We take Microsoft

802.1x client as an example here.

802.1x/MD5-challenge setup

Open the **Local Area connection Properties**, and then click **Authentication** page. Check the **Enable IEEE 802.1x authentication for this network** and select the **MD5-challenge** in EAP type combobox. Please see the following figure.



Local Area Connection Properties

General | Authentication | Advanced

Select this option to provide authenticated network access for Ethernet networks.

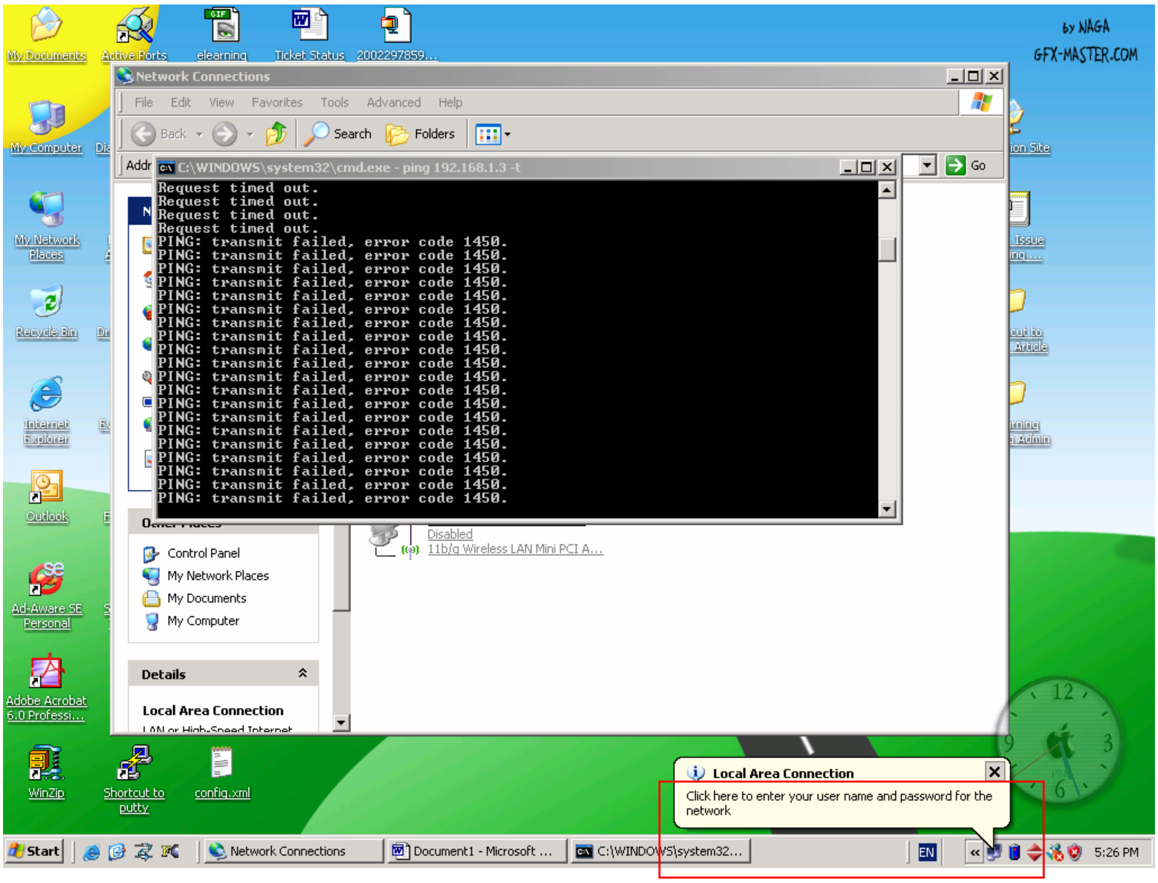
☑ Enable IEEE 802.1x authentication for this network

EAP type: MD5-Challenge

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

When the 802.1x starts, it will prompt you to enter the user name and password. Please see the following figure.



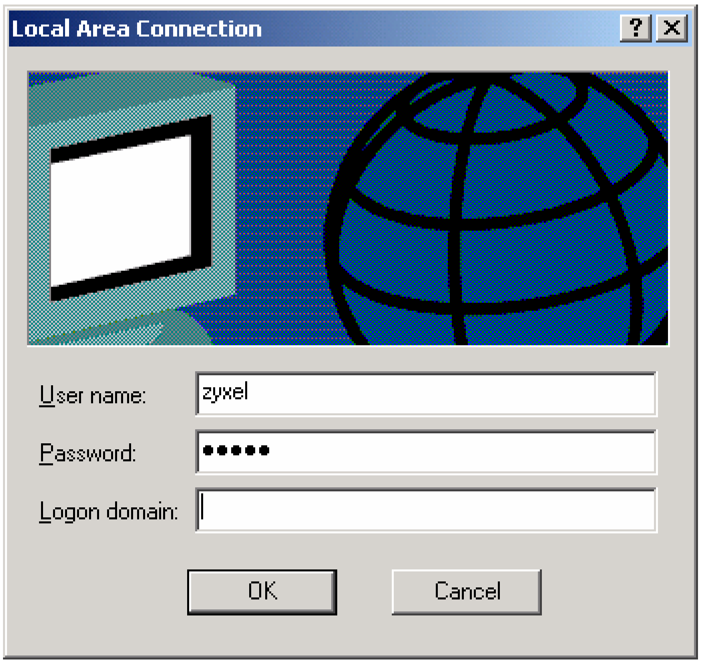
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.3 -t

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
PING: transmit failed, error code 1450.
```

Local Area Connection

Click here to enter your user name and password for the network

After click the icon, there will be a dialog for entering the user name and password. Click ok after input the correct user name and password that are in the database of authentication server. The settings of client site are finished.



User name: zyxel

Password: •••••

Logon domain:

After finishing the above procedures, we can allow the authenticated port the access the server. If the switch port doesn't be authenticated, the PCs behind the port can't access the network.

## Setting up Classifier & Policy rule on your Switch

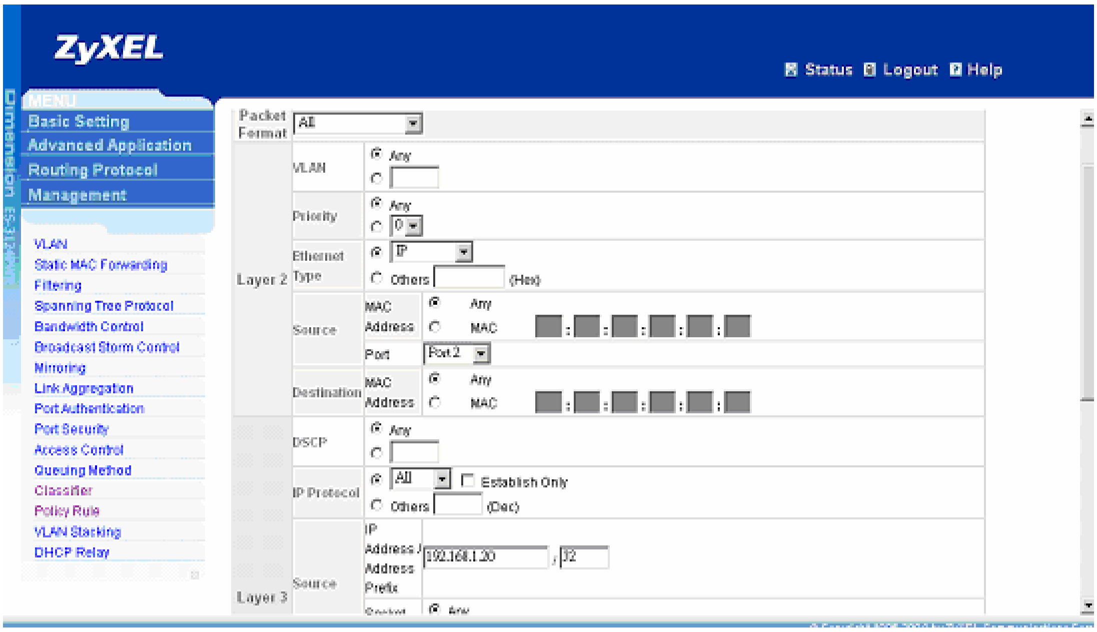
How should I configure if I only allow certain IP address on a certain port to forward its traffic but deny all others?

In the beginning, we need to set up the classifier to group traffic into data flows based on some such as source address, destination address, port number and packet format. In this example, we specify which format of the packet that ES-3124 applies its policy rules. We define three rules. Firstly, we define a classifier that source address is coming from 192.168.1.20; secondly, we specify a classifier that is based on port 2; finally, we define a classifier that is ARP traffic for testing.

After the classification, we need to define the policy rule to ensure that the traffic gets the deserved treatment in the network. Here, we also define three policy rules. The first policy rule is to forward only the traffic from 192.168.1.20. The second policy rule is to discard all the traffic from port 2 on first classifier; and we apply the second policy rule on second classifier. Finally, the last policy rule is set to forward the traffic that is ARP packet format.

Below is the configuration of classifier and policy rule.

Classifier 1

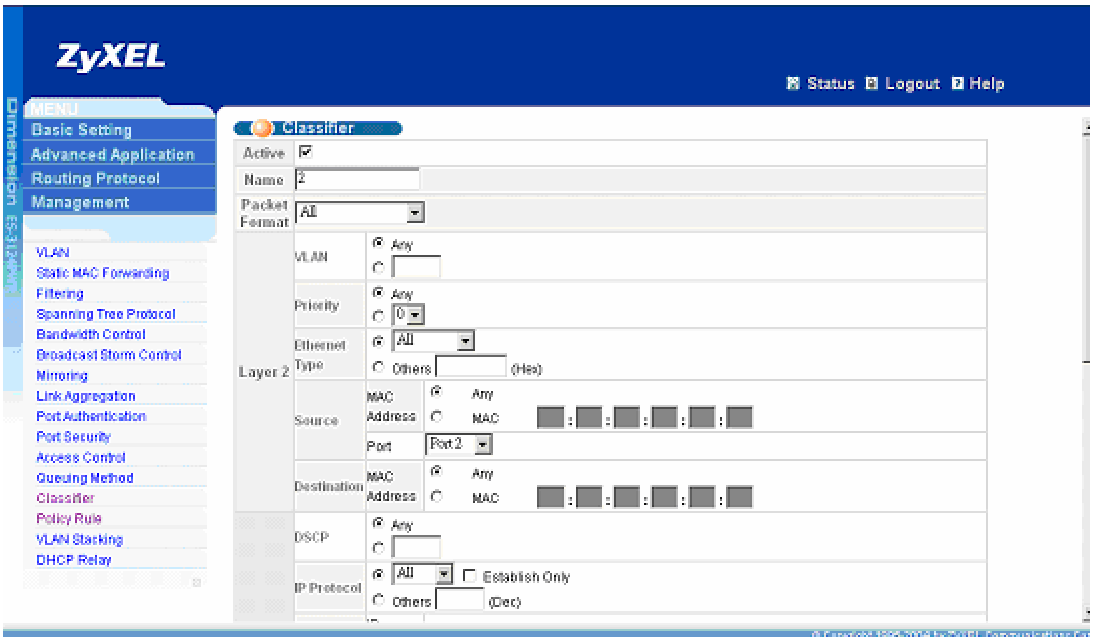


Packet Format: All

Layer 2
- VLAN: ● Any ○
- Priority: ● Any ○ 0
- Ethernet Type: ● IP ○ Others (Hex)
- Source MAC Address: ● Any ○ MAC : : : : :
- Source Port: Port 2
- Destination MAC Address: ● Any ○ MAC : : : : :

Layer 3
- DSCP: ● Any ○
- IP Protocol: ● All □ Establish Only ○ Others (Dec)
- Source IP Address / Address Prefix: 192.168.1.20 / 32
- Socket: ● Any

● Classifier 2



Classifier

Active: ☑

Name: 2

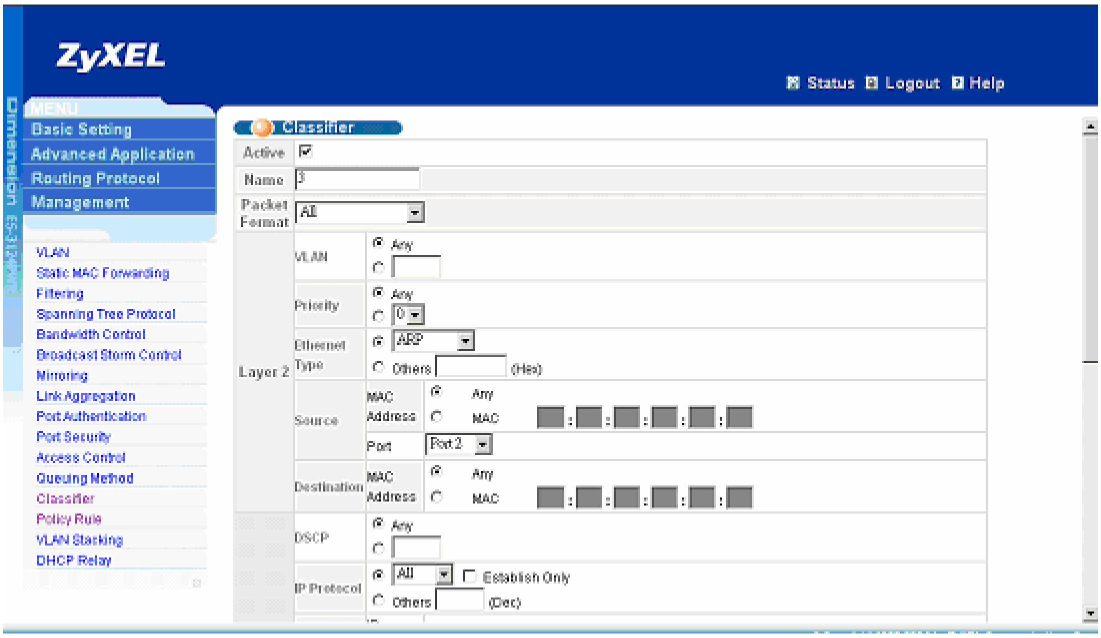
Packet Format: All

Layer 2
- VLAN: ● Any ○
- Priority: ● Any ○ 0
- Ethernet Type: ● All ○ Others (Hex)
- Source MAC Address: ● Any ○ MAC : : : : :
- Source Port: Port 2
- Destination MAC Address: ● Any ○ MAC : : : : :

DSCP: ● Any ○

IP Protocol: ● All □ Establish Only ○ Others (Dec)

3. Classifier 3



Classifier

Active ☑

Name 3

Packet Format All

Layer 2

VLAN ● Any ○

Priority ● Any ○ 0

Ethernet Type ● ARP ○ Others (Hex)

Source MAC Address ● Any ○ MAC : : : : :

Source Port Port 2

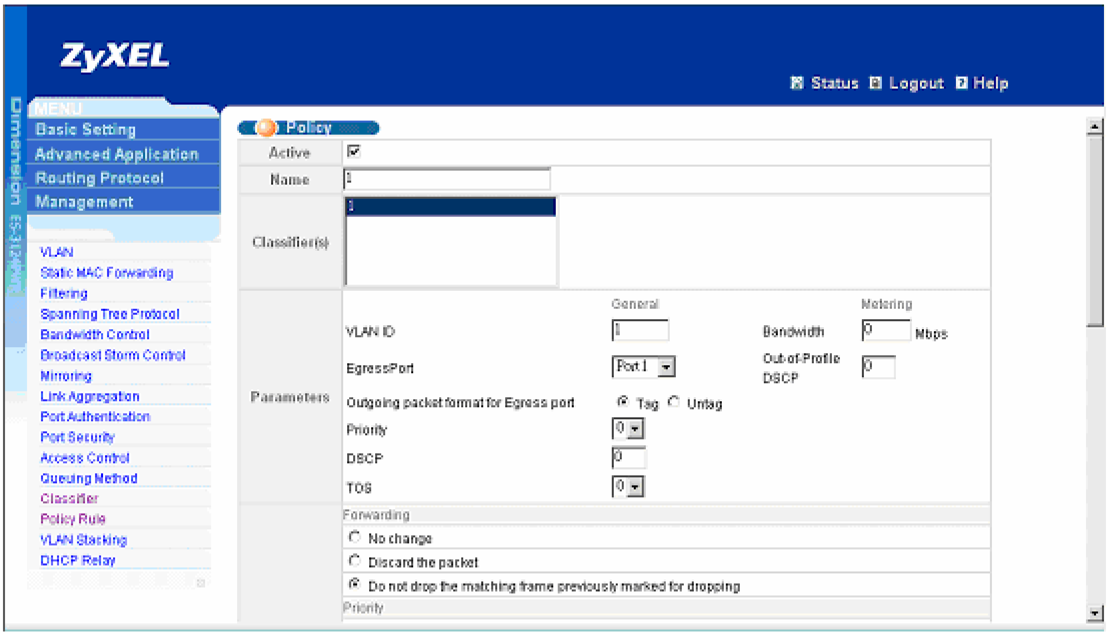
Destination MAC Address ● Any ○ MAC : : : : :

DSCP ● Any ○

IP Protocol ● All □ Establish Only ○ Others (Dec)

## Policy Rule Configuration

1. Policy rule on Classifier 1



Policy

Active ☑

Name 1

Classifier(s) 1

Parameters

General

VLAN ID 1

EgressPort Port 1

Outgoing packet format for Egress port ● Tag ○ Untag

Priority 0

DSCP 0

TOS 0

Metering

Bandwidth 0 Mbps

Out-of-Profile DSCP 0

Forwarding

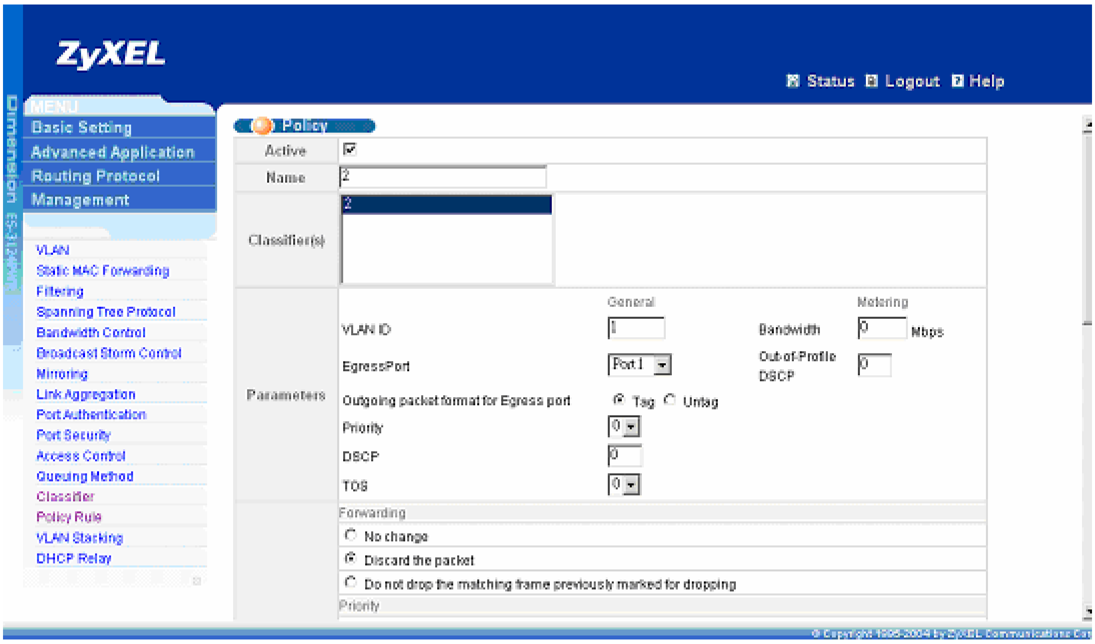
○ No change

○ Discard the packet

● Do not drop the matching frame previously marked for dropping

Priority

2. Policy rule on classifier 2



Policy

| | |
|---|---|
| Active | ☑ |
| Name | 2 |
| Classifier(s) | 2 |

Parameters

| General | | Metering | |
|---|---|---|---|
| VLAN ID | 1 | Bandwidth | 0 Mbps |
| EgressPort | Port 1 | Out-of-Profile DSCP | 0 |
| Outgoing packet format for Egress port | ● Tag ○ Untag | | |
| Priority | 0 | | |
| DSCP | 0 | | |
| TOS | 0 | | |

Forwarding

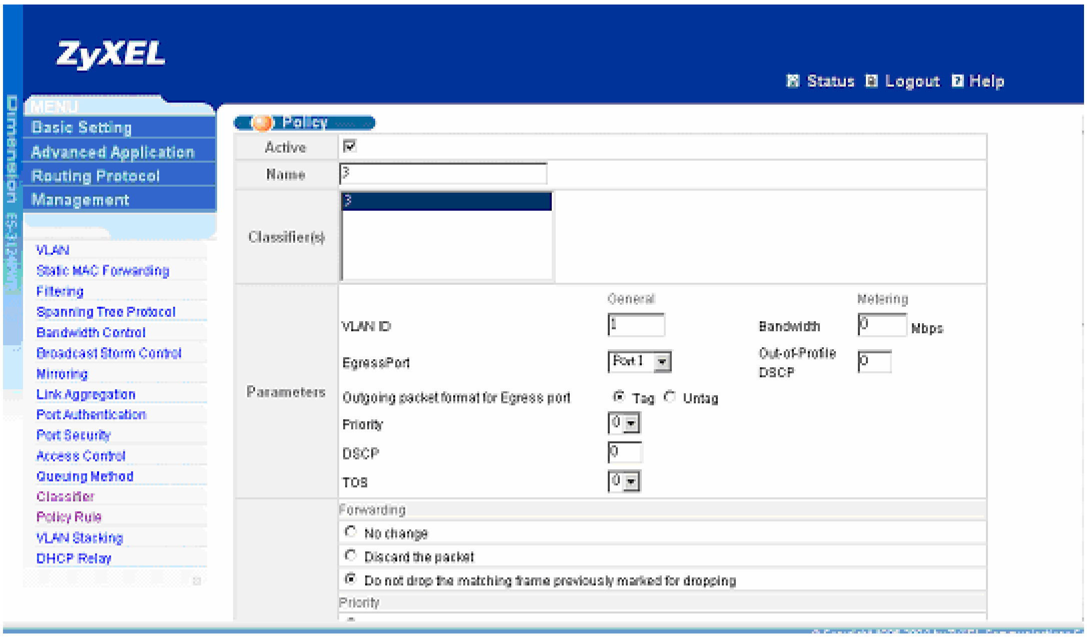
○ No change

● Discard the packet

○ Do not drop the matching frame previously marked for dropping

Priority

3. Policy rule on classifier 3



Policy

| | |
|---|---|
| Active | ☑ |
| Name | 3 |
| Classifier(s) | 3 |

Parameters

| General | | Metering | |
|---|---|---|---|
| VLAN ID | 1 | Bandwidth | 0 Mbps |
| EgressPort | Port 1 | Out-of-Profile DSCP | 0 |
| Outgoing packet format for Egress port | ● Tag ○ Untag | | |
| Priority | 0 | | |
| DSCP | 0 | | |
| TOS | 0 | | |

Forwarding

○ No change

○ Discard the packet

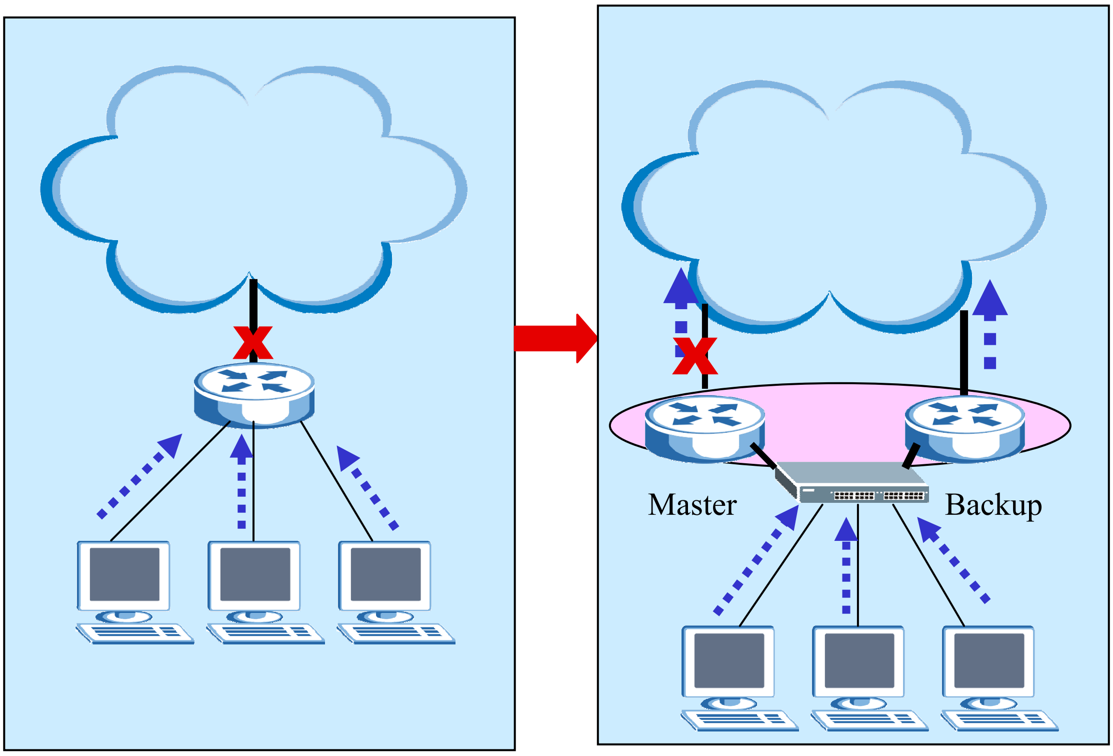
● Do not drop the matching frame previously marked for dropping

Priority

# Fault Free Protection

## Overview of VRRP

Traditional network has one and only one gateway to put between internal network and external network. When the link of router has some trouble, the user can't access to internet anymore. But when we enable VRRP,.if MASTER router fails, and the BACKUP router will take over, and ensure the traffic still go through.



Without VRRP

With VRRP

**VRRP** (**V**irtual **R**edundancy **R**outing **P**rotocol) provides a fail-over solution to increase network high availability and prevent single point of failure. Basically, VRRP utilizes two or more switches to work together. The master switch handles all packets while the others are backup devices. When the master one fails, the backup device with highest priority will take over the packet handling.

## Terminology:

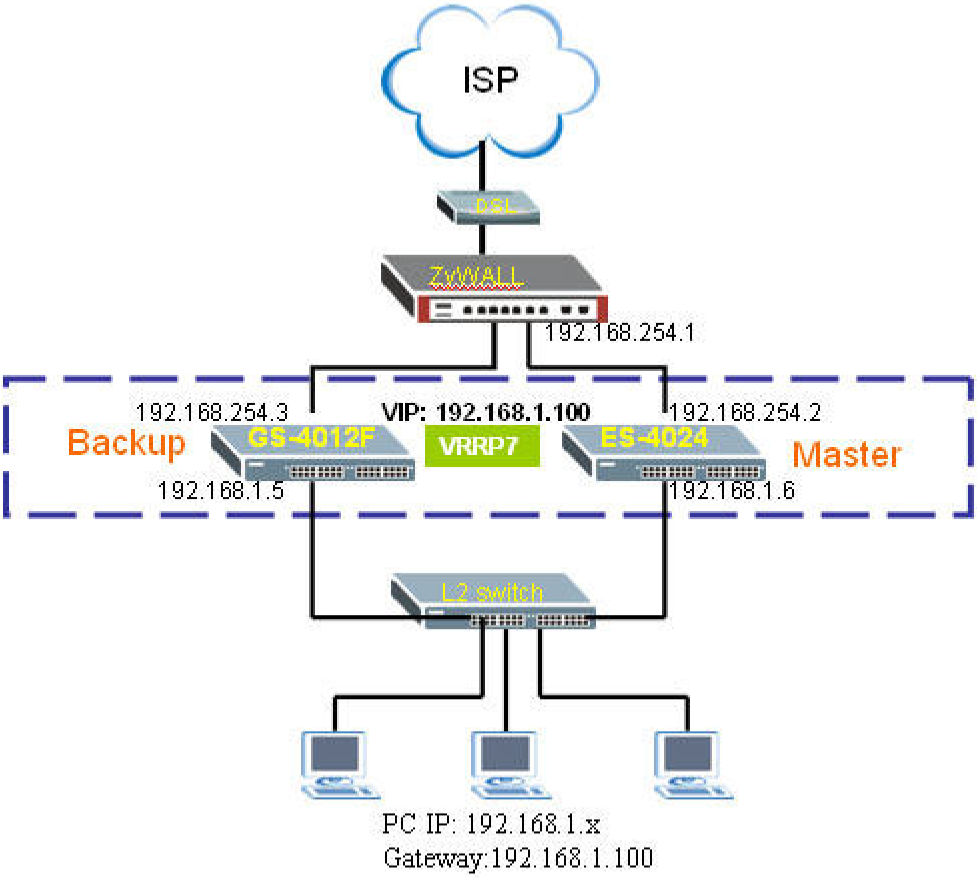
- VRRP Router: A router running the Virtual Router Redundancy Protocol.
- Virtual Router: An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN.
- Virtual Router Master: VRRP Router with forwarding responsibility of a VR.
- Virtual Router Backup: Set of VRRP Routers available to assume forwarding responsibility when VR Master fails.

## When do you need it?

VRRP is a L3 virtual routing protocol. For a network administrator, to ensure serice/network always available without down time at gateway, VRRP can benefit this and further provide load sharing if more than one uplink is applied.

## Scenario 1 -- Redundancy

The network administrator Peter of ZyCompany wants to ensure the high available of their server farm from LAN users. According to vendor's recommendation, they buy two ZyXEL ES-4024 switches and have the configuration step by step as following.



**PC**

IP:192.168.1.x

Gateway:192.168.1.100

**Switch A – ES-4024**

downlink network:192.168.1.6

uplink IP:192.168.254.2

uplink gateway:192.168.254.1

virtual IP:192.168.1.100

**Switch B – GS-4012F**

downlink network:192.168.1.5

uplink IP:192.168.254.3

uplink gateway:192.168.254.1

virtual IP:192.168.1.100

Note1. Please notice that two IPs in switch A and switch B should be in different vlan groups. For example:

Switch A: 192.168.1.6 in vlan 1; 192.168.254.2 in vlan 2
Switch B: 192.168.1.5 in vlan 1; 192.168.254.3 in vlan 2

**Note2.** For VRRP application, you must configure two different VLAN groups for downlink network and uplink network. Otherwise, it's not secure that the authentication will be forwarded under same VLAN group.

**Step 1.** Configure a PC's IP as same subnet of switchA (by default, it's 192.168.1.1). Login switch's GUI by http://switch's_IP. Please refer to quick start quick if you got problem at this step.

**Step 2.** Setup the switch A's VLAN info to apply the environment.

By default, ZyXEL switch has all ports with VLAN=1 setting already. We need to create another VLAN2 for uplink interface. In addition, please notice the "Tx tagging" setting to be unchecked if uplink device might be VLAN-unaware.

In this example, we assume

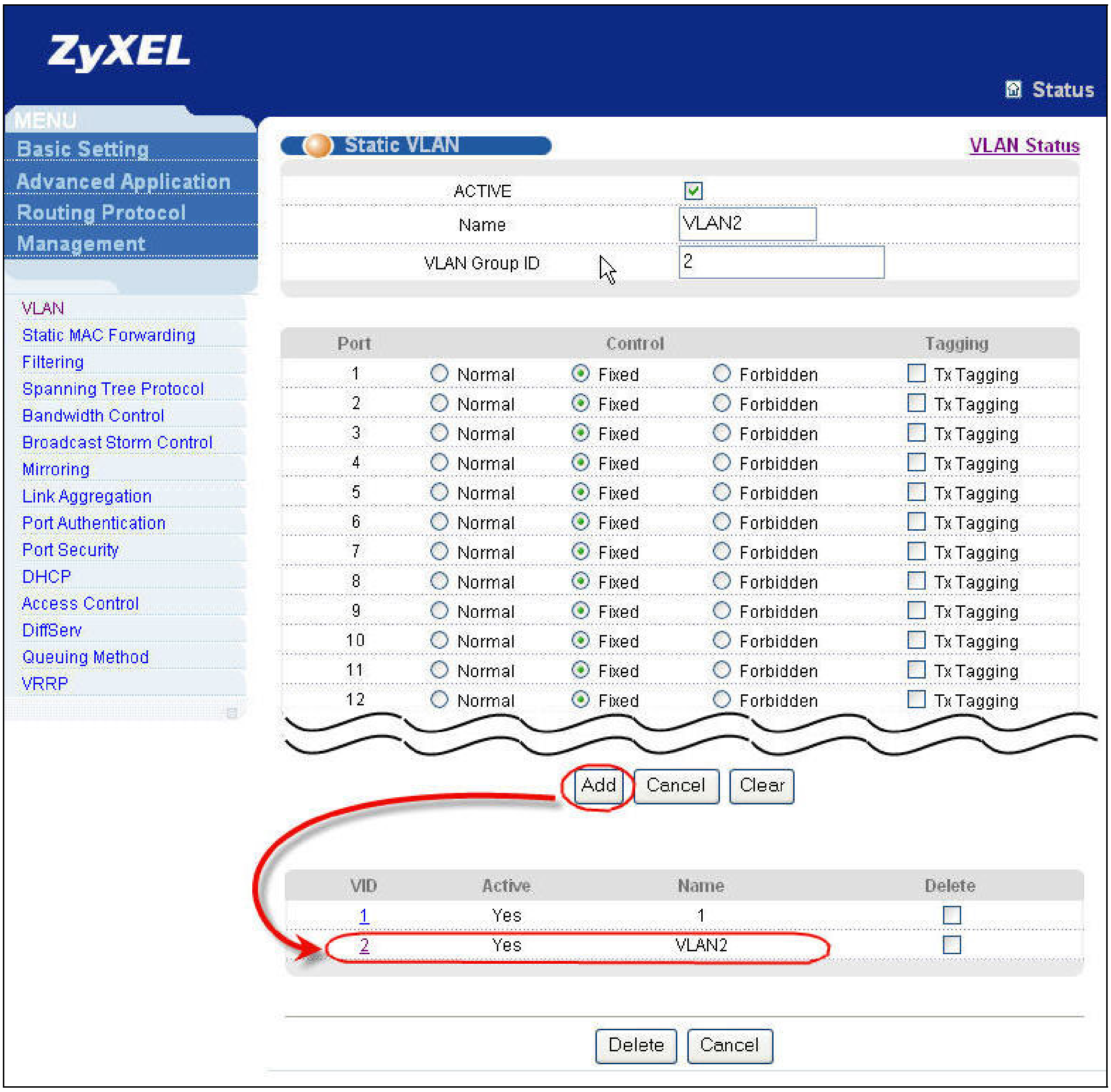
1. the ZyWALL which is VLAN-unaware is the uplink gateway, so here we configure VLAN1 and VLAN2 groups are with Tx tagging "untagged".

2. the network is very simple and we configure all ports are the member of both VLAN1 & VLAN2 groups

a. Go to GUI menu **Advanced Application** >> **VLAN** >> **Static VLAN** >> choose **VLAN1** to show the detail. Modify VLAN1 with all ports with “Fixed” and uncheck “Tx Tagging”. Press **Add** button then.

b. Create the VLAN2 via GUI menu **Advanced Application** >> **VLAN** >> **Static VLAN**, and configure all ports with “Fixed” and uncheck “Tx Tagging”. Press **Add** button then. See the figure below.

c. Configure uplink port in GUI menu. Set the PVID to the same ID with uplink is 20.



| | |
|---|---|
| ACTIVE | ☑ |
| Name | VLAN2 |
| VLAN Group ID | 2 |

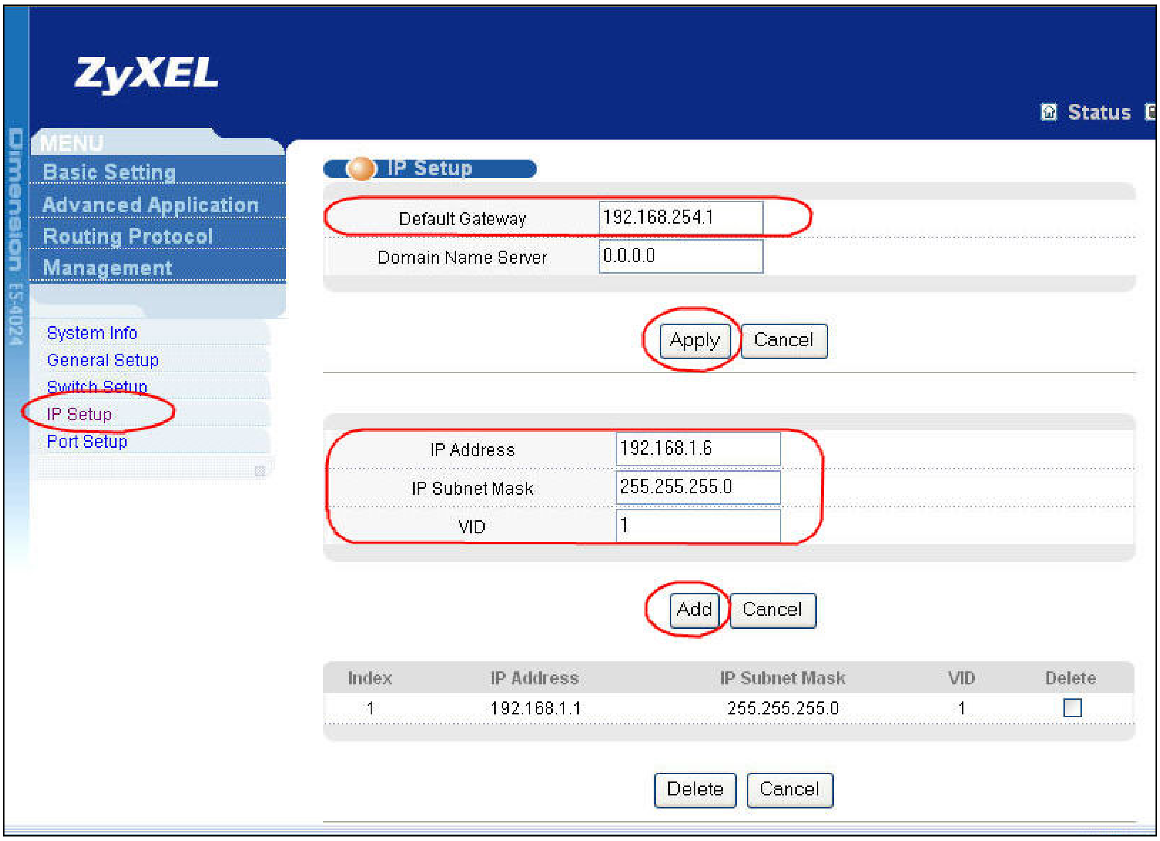
| Port | Control | | | Tagging |
|---|---|---|---|---|
| 1 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 2 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 3 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 4 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 5 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 6 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 7 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 8 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 9 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 10 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 11 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 12 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |

| VID | Active | Name | Delete |
|---|---|---|---|
| 1 | Yes | 1 | □ |
| 2 | Yes | VLAN2 | □ |

**Step 3.** Setup the switch A's IP address of two interfaces for layer 3 routing and its uplink gateway. Take ES-4024 for example.

Configure Switch A's IP setting via GUI menu **Basic Setting** >> **IP Setup**.

- Default Gateway: 192.168.254.1
- 1st IP address: 192.168.1.6/24 with VID=1, see figure example as below.
- 2nd IP address: 192.168.254.2/24 with VID=2

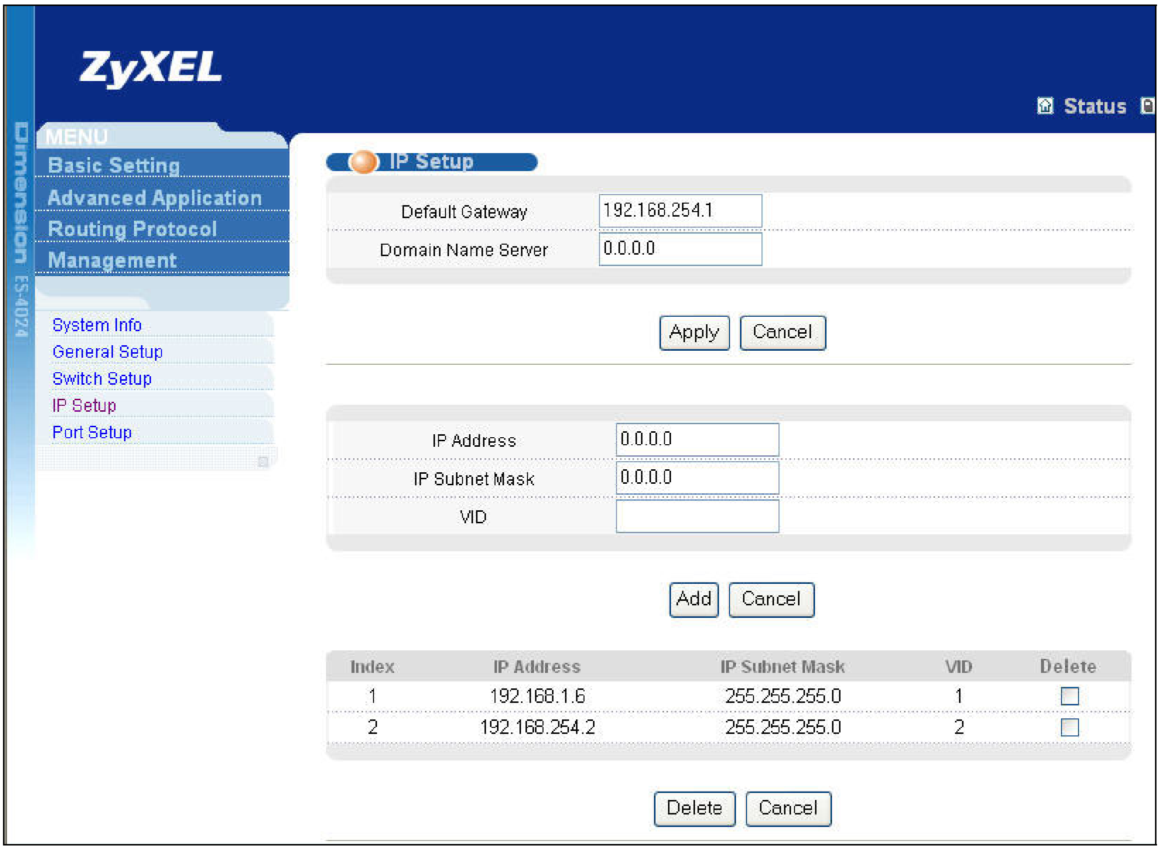


| | |
|---|---|
| Default Gateway | 192.168.254.1 |
| Domain Name Server | 0.0.0.0 |

| | |
|---|---|
| IP Address | 192.168.1.6 |
| IP Subnet Mask | 255.255.255.0 |
| VID | 1 |

| Index | IP Address | IP Subnet Mask | VID | Delete |
|---|---|---|---|---|
| 1 | 192.168.1.1 | 255.255.255.0 | 1 | □ |

After add the change, it will become as following setting.



| | |
|---|---|
| Default Gateway | 192.168.254.1 |
| Domain Name Server | 0.0.0.0 |

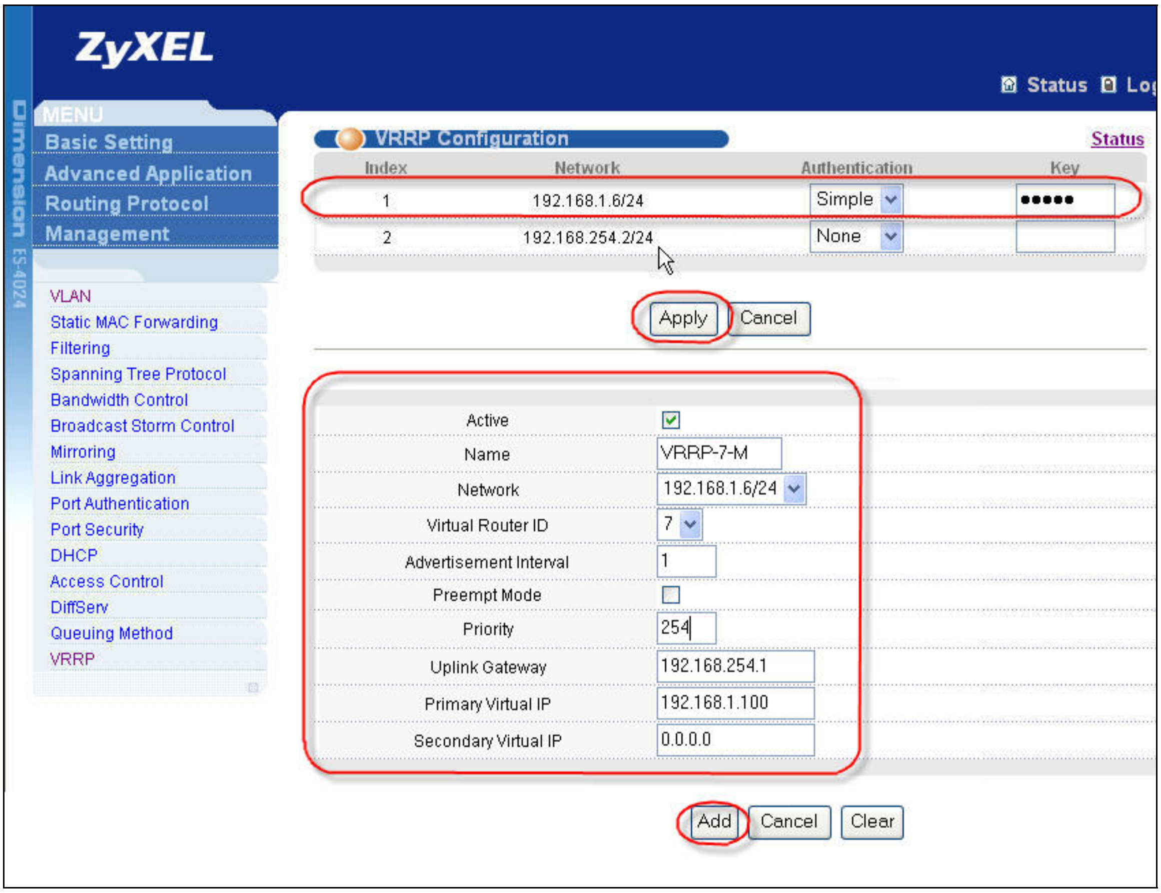
| | |
|---|---|
| IP Address | 0.0.0.0 |
| IP Subnet Mask | 0.0.0.0 |
| VID | |

| Index | IP Address | IP Subnet Mask | VID | Delete |
|---|---|---|---|---|
| 1 | 192.168.1.6 | 255.255.255.0 | 1 | □ |
| 2 | 192.168.254.2 | 255.255.255.0 | 2 | □ |

**Step 4.** Setup the switch A's VRRP as the Master of group 1.

In the GUI menu **Advanced Application** >> **VRRP**, enter the "**Configuration**" link.

1. choose 'Simple' for authentication
2. Enter type '12345' for the key.
3. Press '**add**' button.
4. Then input the VRRP information as following figure. Here we use VRRP=7 and use priority=254 to indicate it is the Master role.



VRRP Configuration    Status

| Index | Network | Authentication | Key |
|---|---|---|---|
| 1 | 192.168.1.6/24 | Simple | ●●●●● |
| 2 | 192.168.254.2/24 | None | |

Apply    Cancel

| | |
|---|---|
| Active | ☑ |
| Name | VRRP-7-M |
| Network | 192.168.1.6/24 |
| Virtual Router ID | 7 |
| Advertisement Interval | 1 |
| Preempt Mode | □ |
| Priority | 254 |
| Uplink Gateway | 192.168.254.1 |
| Primary Virtual IP | 192.168.1.100 |
| Secondary Virtual IP | 0.0.0.0 |

Add    Cancel    Clear

**Step 5.** Setup the switch B's VLAN to apply the environment. Refer to Step2 for the same setting.

**Step 6.** Setup the switch B's IP address of two interfaces and uplink gateway. Similar as switch A's setting at Step3, but different IP address as following.

Configure Switch B's IP setting via GUI menu **Basic Setting** >> **IP Setup**.

- Default Gateway: 192.168.254.1
- 1st IP address for user subnet interface: 192.168.1.5/24 with VID=1, see figure example as below.
- 2nd IP address for uplink interface: 192.168.254.3/24 with VID=2

**Step 7.** Setup the switch B's VRRP as the Backup of group 1. Please refer to Step6. Please note to use

1. choose ‘Simple’ for authentication
2. type ‘12345’ for the key and press ‘Apply’ button
3. same ‘Virtual Router ID” (=7 in this example)
4. lower priority (=100 in this example) to be a backup role
5. same uplink gateway in this scenario example (192.168.254.1)
6. same primary virtual IP (192.168.1.100 in this example)

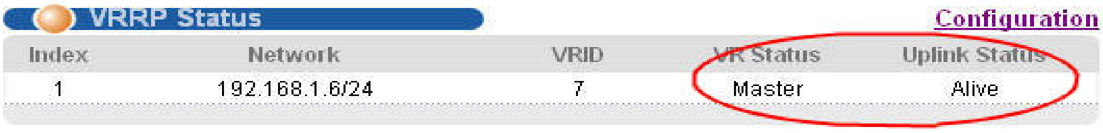
Note: The design of authentication and key is for the authentication between Master and Backup. It only takes effect to configure for downlink network.

**Step 8.** Make sure uplink is ok to be ping. (Otherwise, the uplink status will stay at ‘Init’.

Note: The redundancy works when it detect uplink gateway can be ping and other VRRP group members are not available or the switch is with the highest priority among alive VRRP switches.

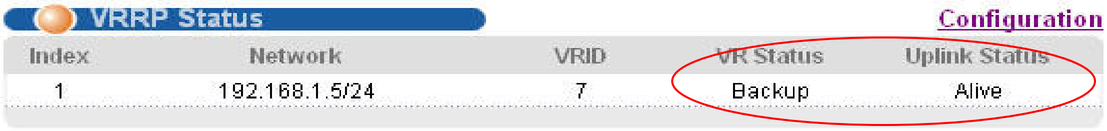
**Step 9.** Check the VRRP status via GUI. Both Master and Backup switches should be alive as following.

For Master,



| Index | Network | VRID | VR Status | Uplink Status |
|---|---|---|---|---|
| 1 | 192.168.1.6/24 | 7 | Master | Alive |

For Backup,

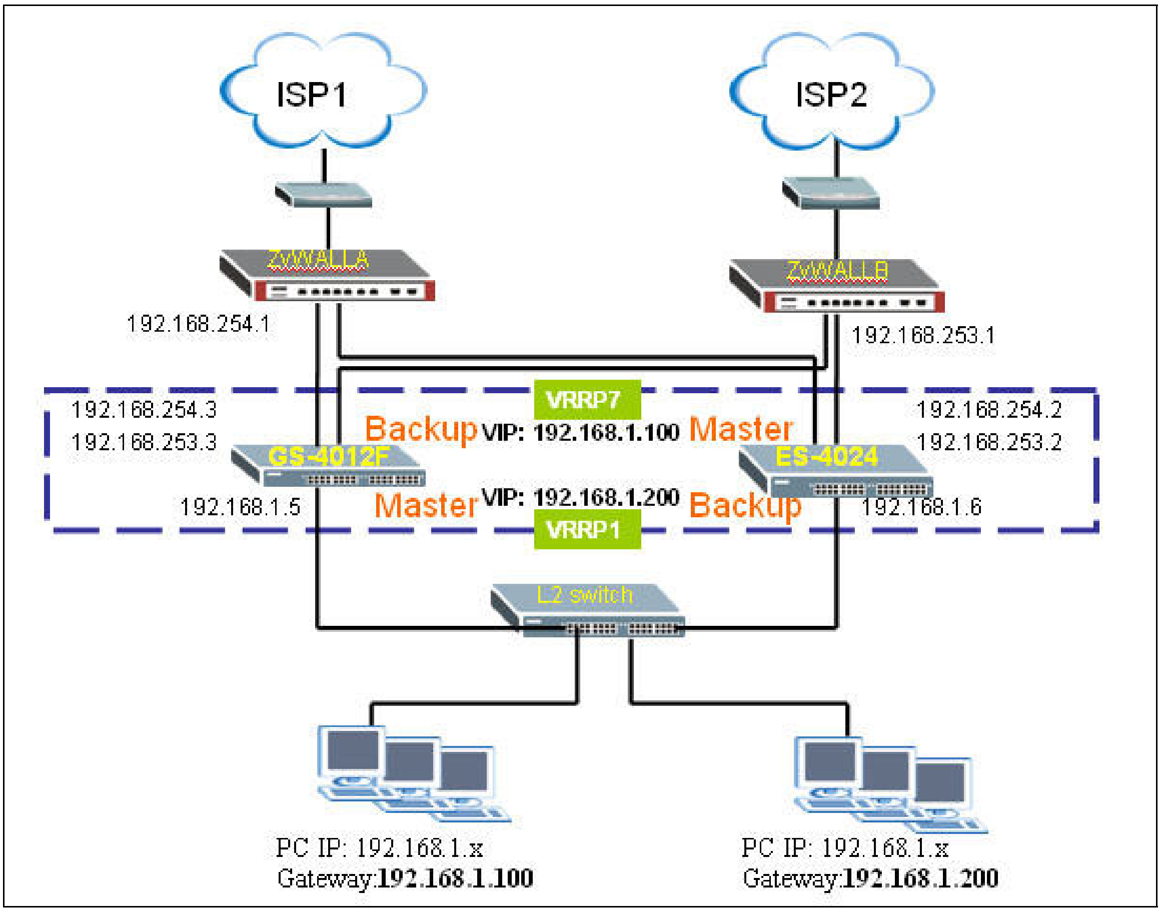


| Index | Network | VRID | VR Status | Uplink Status |
|---|---|---|---|---|
| 1 | 192.168.1.5/24 | 7 | Backup | Alive |

## Scenario 2 – Load Sharing

Furthermore, ZyCompany wants to achieve load sharing based on the high availability application. To reach this target, two VRRP groups would be recommended. Each switch is a Master of one VRRP group and also acts a Backup of another VRRP group.

Network Admin will need to separate LAN users to two groups, each one use one virtual IP to share LAN traffic loading. So if the both Master are alive, PC group1's traffic will mainly go via SwitchA while PC group2's will mainly go via SwitchB. See following topology and configuration step by step.



**PCs in group1**

IP:192.168.1.x

Gateway:192.168.1.100

**PCs in group2**

IP:192.168.1.x

Gateway:192.168.1.200

**Switch A – ES-4024**

downlink network:192.168.1.5

downlink VLAN ID=1

| VLAN ID | Uplink Interface IP | Uplink gateway | Virtual IP | VRRP ID | VRRP Role |
|---|---|---|---|---|---|
| 2 | 192.168.254.2 | 192.168.254.1 | 192.168.1.100 | 7 | Master |
| 3 | 192.168.253.2 | 192.168.253.1 | 192.168.1.200 | 1 | Backup |

**Switch B – GS-4012F**

downlink network:192.168.1.6

downlink VLAN ID=1

| VLAN ID | Uplink Interface IP | Uplink gateway | Virtual IP | VRRP ID | VRRP Role |
|---|---|---|---|---|---|
| 2 | 192.168.254.3 | 192.168.254.1 | 192.168.1.100 | 7 | Backup |
| 3 | 192.168.253.3 | 192.168.253.1 | 192.168.1.200 | 1 | Master |

**Note1.** Two IPs in switch A and switch B should be in different vlan groups. For example:

Switch A: 192.168.1.6 in vlan 1; 192.168.253.2 in vlan 2
Switch B: 192.168.1.5 in vlan 1; 192.168.254.3 in vlan 2

**Note2.** In this example, we connect to two ISPs to simulate the real world. It's in order to prevent the single point of failure additionally.

**Step 1.** Here we assume that all setting are based on Scenario1's configuration. Therefore, we will skip the basic setting in this Scenario.

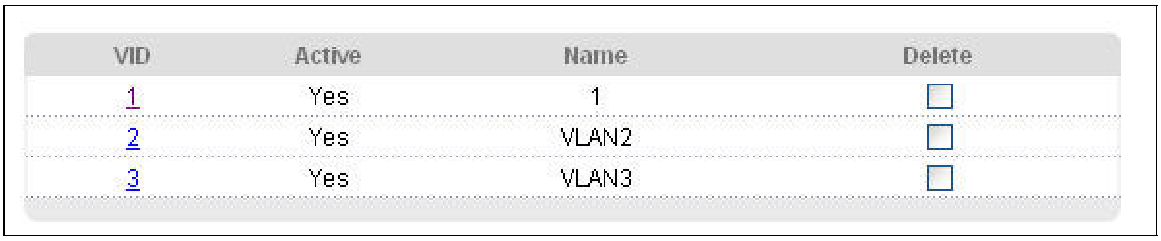
**Step 2.** Add one more VLAN ID on SwitchA for another subnet connecting to ISP2.

Same as Scenario1, in this example, we assume

1. The uplink gateway, ZyWALL, which is VLAN-unaware

2. The network is very simple and we configure all ports are the member of both VLAN1, VLAN2, and VLAN3 groups

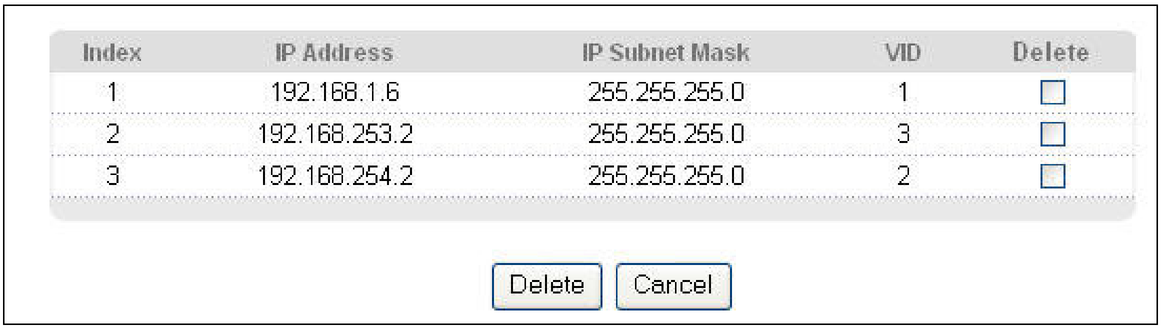
a. Create the VLAN3 via GUI menu **Advanced Application** >> **VLAN** >> **Static VLAN**, and configure all ports with "Fixed" and uncheck "Tx Tagging". Press **Add** button then. See the figure below.



| VID | Active | Name | Delete |
|---|---|---|---|
| 1 | Yes | 1 | □ |
| 2 | Yes | VLAN2 | □ |
| 3 | Yes | VLAN3 | □ |

**Step 3.** Add one more Switch A's IP setting via GUI menu **Basic Setting** >> **IP Setup**.

- Default Gateway: no change
- Add 3rd IP address: 192.168.253.2/24 with VID=3, see following figure after the change.

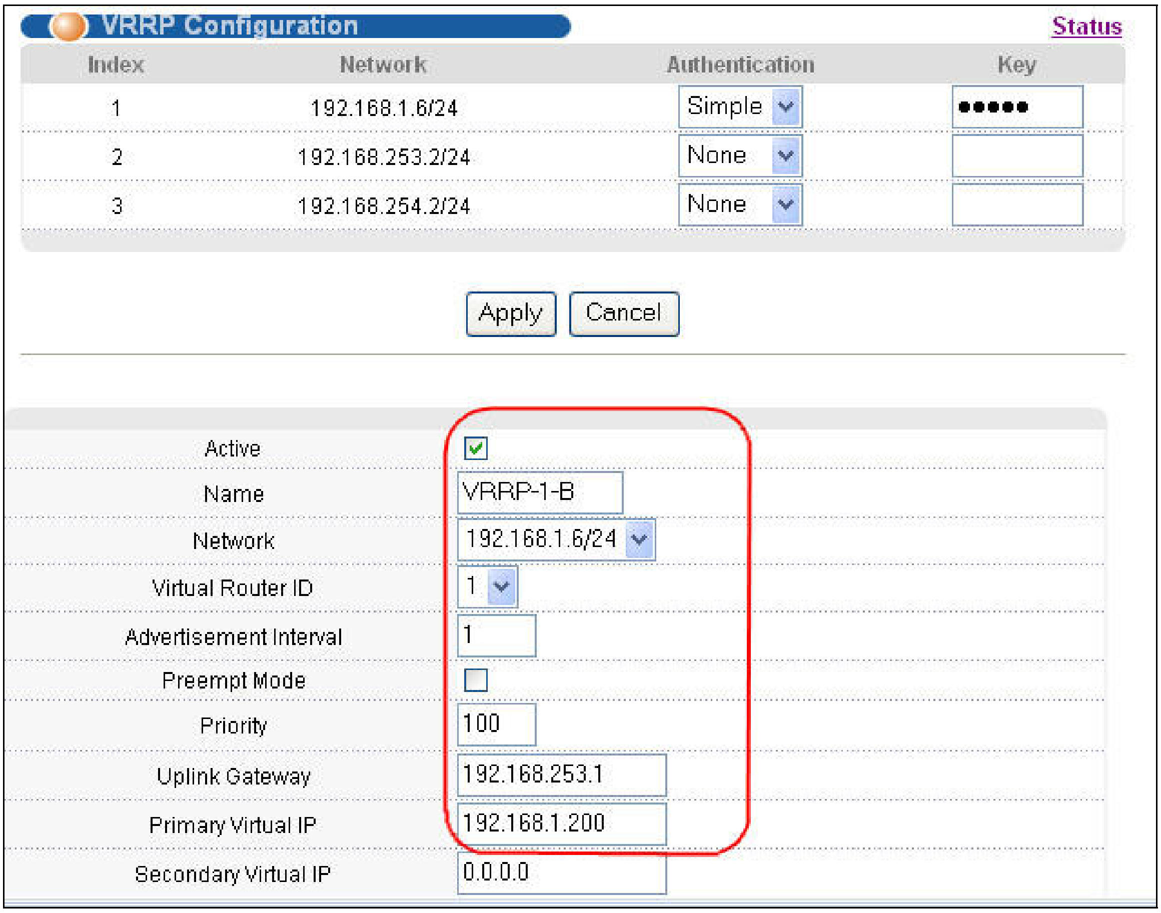


| Index | IP Address | IP Subnet Mask | VID | Delete |
|---|---|---|---|---|
| 1 | 192.168.1.6 | 255.255.255.0 | 1 | □ |
| 2 | 192.168.253.2 | 255.255.255.0 | 3 | □ |
| 3 | 192.168.254.2 | 255.255.255.0 | 2 | □ |

**Step 4.** Setup the switch A's VRRP as the Backup of VRRP group 1.

In the GUI menu **Advanced Application** >> **VRRP**, enter the "**Configuration**" link.

1. authentication: no change
2. key: no change
3. Then input the VRRP information as following figure. Here we use VRRP=1 and use priority=100 to indicate it is the Backup role.



VRRP Configuration

| Index | Network | Authentication | Key |
|---|---|---|---|
| 1 | 192.168.1.6/24 | Simple | ●●●●● |
| 2 | 192.168.253.2/24 | None | |
| 3 | 192.168.254.2/24 | None | |

| | |
|---|---|
| Active | ☑ |
| Name | VRRP-1-B |
| Network | 192.168.1.6/24 |
| Virtual Router ID | 1 |
| Advertisement Interval | 1 |
| Preempt Mode | □ |
| Priority | 100 |
| Uplink Gateway | 192.168.253.1 |
| Primary Virtual IP | 192.168.1.200 |
| Secondary Virtual IP | 0.0.0.0 |

**Step 5.** Setup the switchB's VLAN to apply the environment. Refer to Step2 for the same setting.

**Step 6.** Add one more interface info for the switch B's IP. Similar as switch A's setting at Step3, but different IP address as following.

Configure Switch B's IP setting via GUI menu **Basic Setting** >> **IP Setup**.

- Default Gateway: no change
- Add 3rd IP address for another uplink interface: 192.168.253.3/24 with VID=3

**Step 7.** Setup the switch B as the Master role of VRRP group 1. Please note to use

1. authentication: no change
2. key: no change
3. same 'Virtual Router ID" (=1 in this example)
4. lower priority (=254 in this example) to be a Master role
5. uplink gateway: 192.168.253.1
6. primary virtual IP: 192.168.1.200

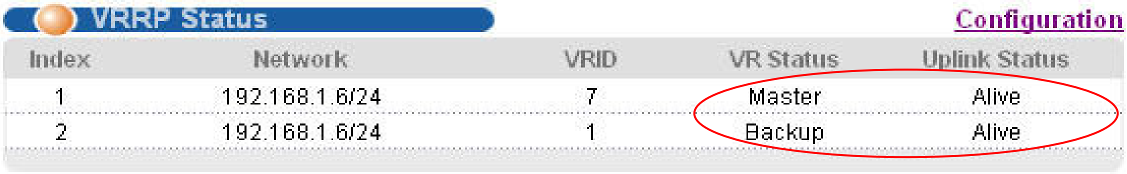
Note: The design of authentication and key is for the authentication between Master and Backup. It only takes effect to configure for downlink network.

**Step 8.** Make sure uplink is ok to be ping. (Otherwise, the uplink status will stay at 'Init'.

Note: The redundancy works when it detects uplink gateway can be ping and other VRRP group members are not available or the switch is with the highest priority among VRRP switches alive.

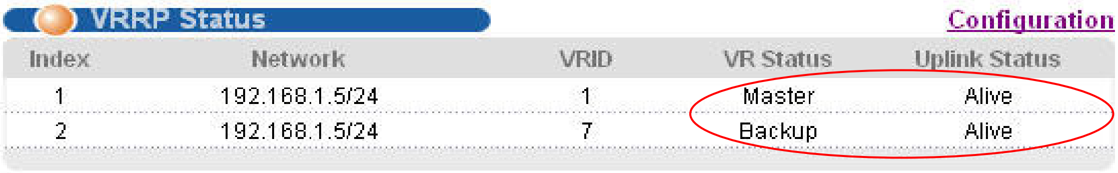
**Step 9.** Check the VRRP status via GUI. Both Master and Backup switches should be alive as following.

For Master,



| Index | Network | VRID | VR Status | Uplink Status |
|---|---|---|---|---|
| 1 | 192.168.1.6/24 | 7 | Master | Alive |
| 2 | 192.168.1.6/24 | 1 | Backup | Alive |

For Backup,



| Index | Network | VRID | VR Status | Uplink Status |
|---|---|---|---|---|
| 1 | 192.168.1.5/24 | 1 | Master | Alive |
| 2 | 192.168.1.5/24 | 7 | Backup | Alive |

# CLI for VRRP

### no ip vrrp authentication-key

- Description: Resets the VRRP authentication settings

### ip vrrp authentication-key <k>

- Description: Sets the VRRP authentication key in the routing domain.
- Ex: ip vrrp authentication-key 12345

### router vrrp network <ip>/<mask-bits> vr-id <1-7> uplink-gateway <ip>

- Description: Set VRRP detail information.
- Ex: router vrrp network 192.168.1.5/24 vr-id 7 uplink-gateway 192.168.254.1

```
name VRRP-7-B

primary-virtual-ip 192.168.1.100

no inactive

no preempt
```

# Centralized Management

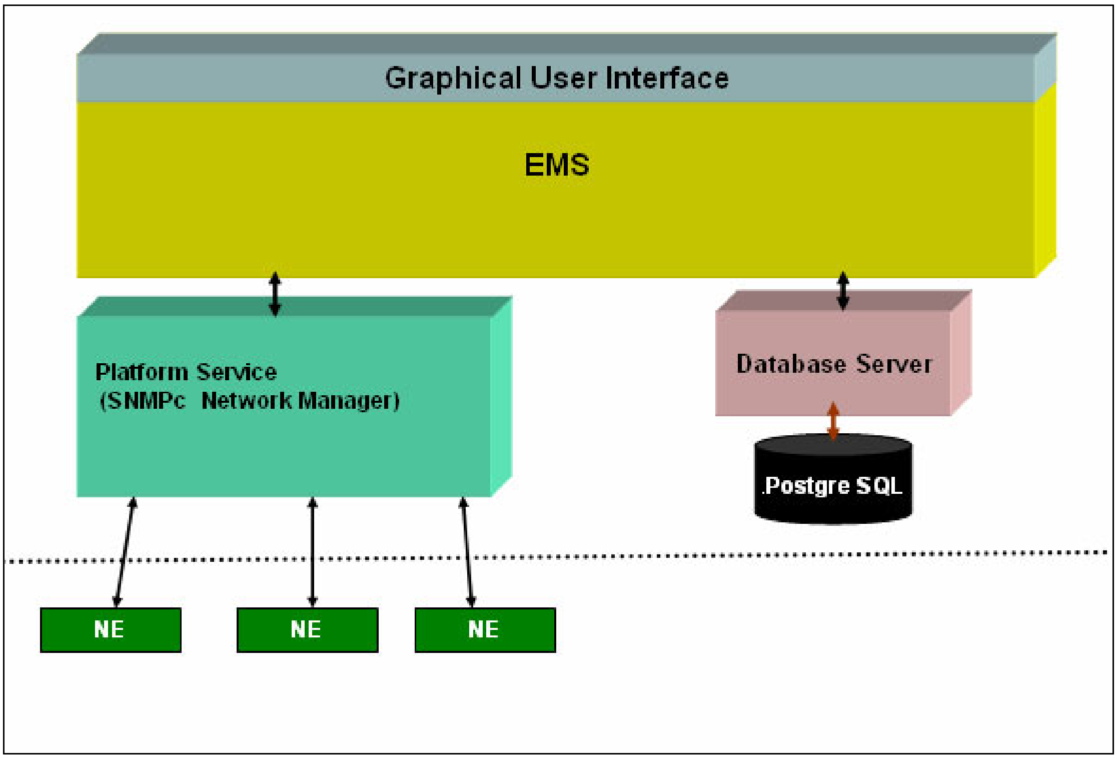
**** Current version of NetAtlas does not support ES-4024A Series***

## Introduction of SNMPc and NetAtlas

With the number of network device increase, the demand to detect and respond to the network failure or external event in a very short time posts a great challenge to network administrator. How to easily manage and monitor network devices across networks becomes more and more important in network management.

Figure 1 presents main elements of the system architecture. Element Management System (EMS), NetAtlas provides a centralized remote management platform and acts as SNMPc manager to perform network configuration, system management, event/alarm management, performance management and security for all ZyXEL's Ethernet Switch solutions. SNMPc is network management software produced by Castle Rock that constantly probe the network element (NE) and collect information of those NE for EMS. Underneath the EMS is Postgres SQL, the enterprise relational database system, provides query for EMS

**Figure 1 System Architecture**

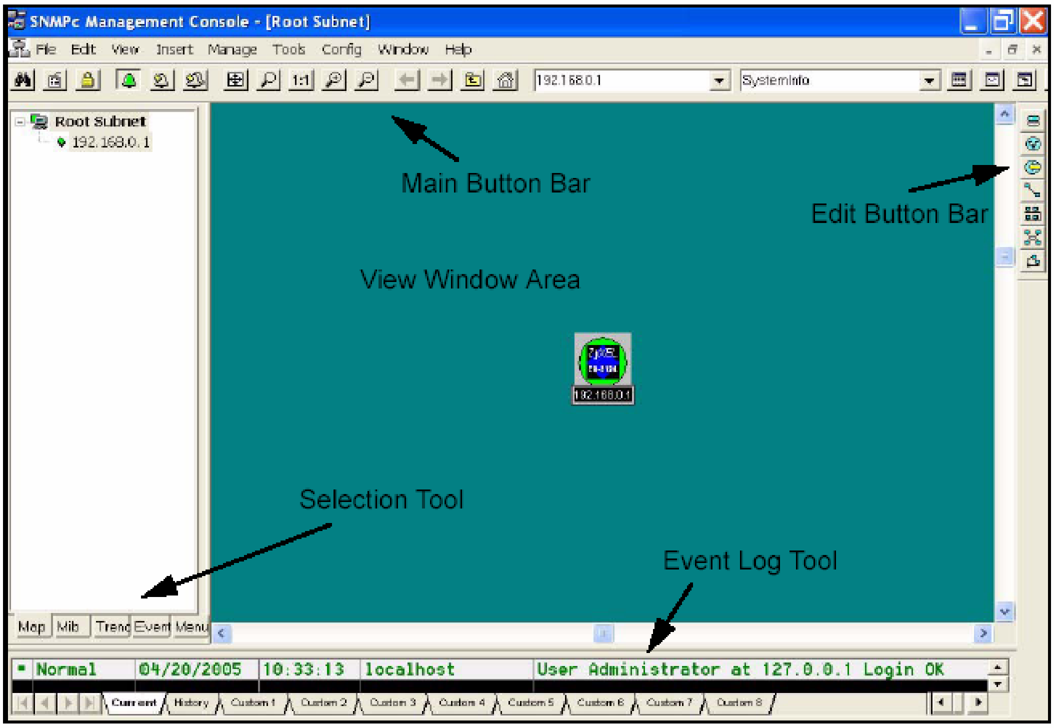


## Overview of SNMPc

The following diagram shows the main elements of SNMPc. SNMPc includes the following function

- **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**


SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
192.168.0.1
SystemInfo
Root Subnet
192.168.0.1
Main Button Bar
Edit Button Bar
View Window Area
Selection Tool
Event Log Tool
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8

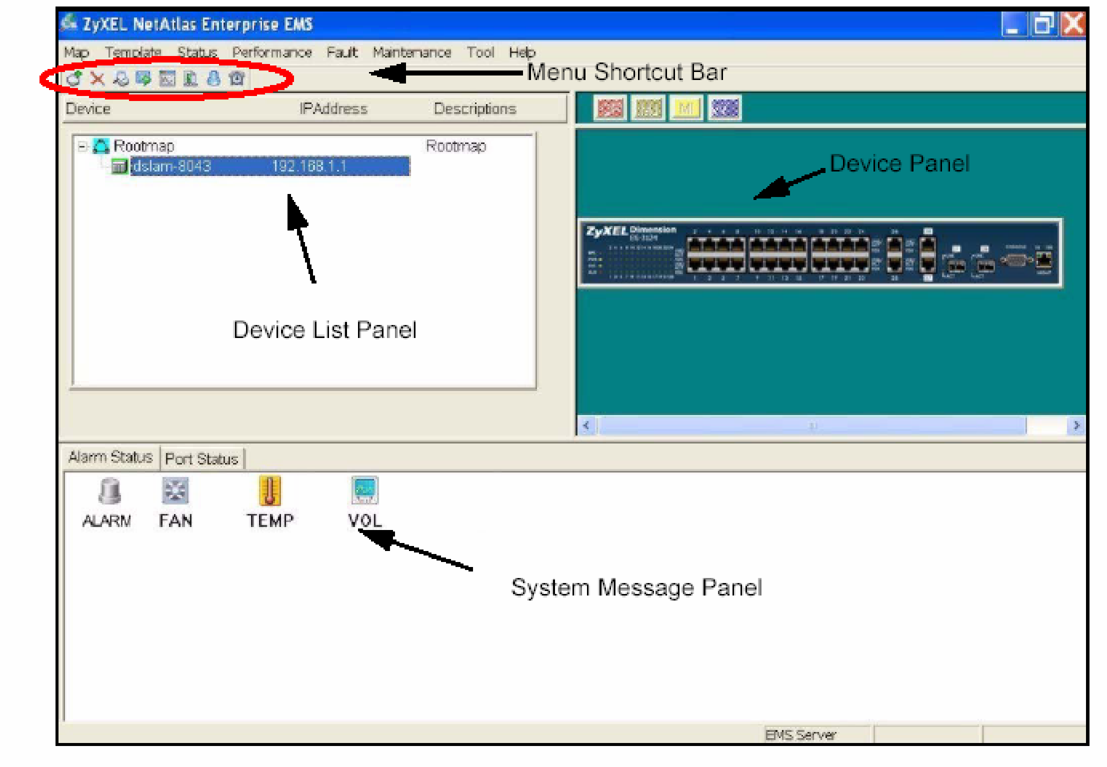
```
Normal  04/20/2005  10:33:13  localhost  User Administrator at 127.0.0.1 Login OK
```

## Overview of EMS

The following diagram illustrates the main elements in EMS. EMS contains the four main functions.

- **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 is working and Rd is no response from the device.
- **System message Panel**: View the alarm Status and port status of the selected switch.

**Figure 3 Overview of EMS**

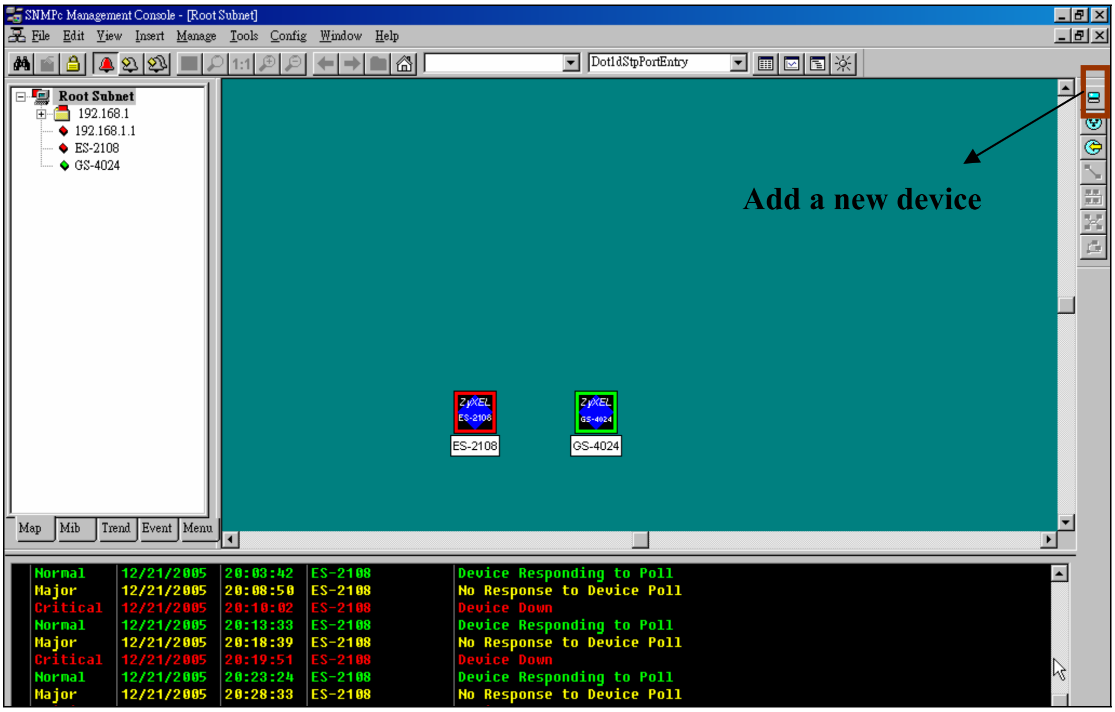


## Configuration of adding a new device via SNMPc

In the following example, we will illustrate how to get started with SNMPc and Netatlas with adding a new device. Follow the procedures from Step 1 to Step 11.

**Step 1**: In the edit button bar shown in the Figure 4 where you may select the icon to insert a new element.

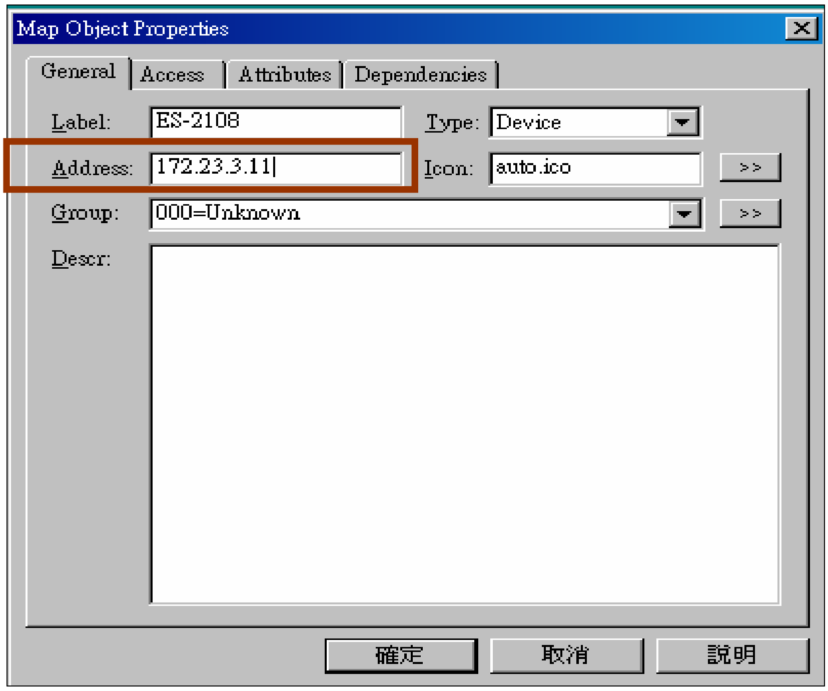
**Figure 4 Adding a new Device**



```
Normal    12/21/2005 20:03:42 ES-2108      Device Responding to Poll
Major     12/21/2005 20:08:50 ES-2108      No Response to Device Poll
Critical  12/21/2005 20:10:02 ES-2108      Device Down
Normal    12/21/2005 20:13:33 ES-2108      Device Responding to Poll
Major     12/21/2005 20:18:39 ES-2108      No Response to Device Poll
Critical  12/21/2005 20:19:51 ES-2108      Device Down
Normal    12/21/2005 20:23:24 ES-2108      Device Responding to Poll
Major     12/21/2005 20:28:33 ES-2108      No Response to Device Poll
```

**Step 2:** In the map object properties, give the label name and enter the IP address of the selected device. In this example, we configure 172.23.3.11 as its IP address of your Switch as shown in Figure 5

**Figure 5 Map Object Properties**



Label: ES-2108

Type: Device

Address: 172.23.3.11

Icon: auto.ico

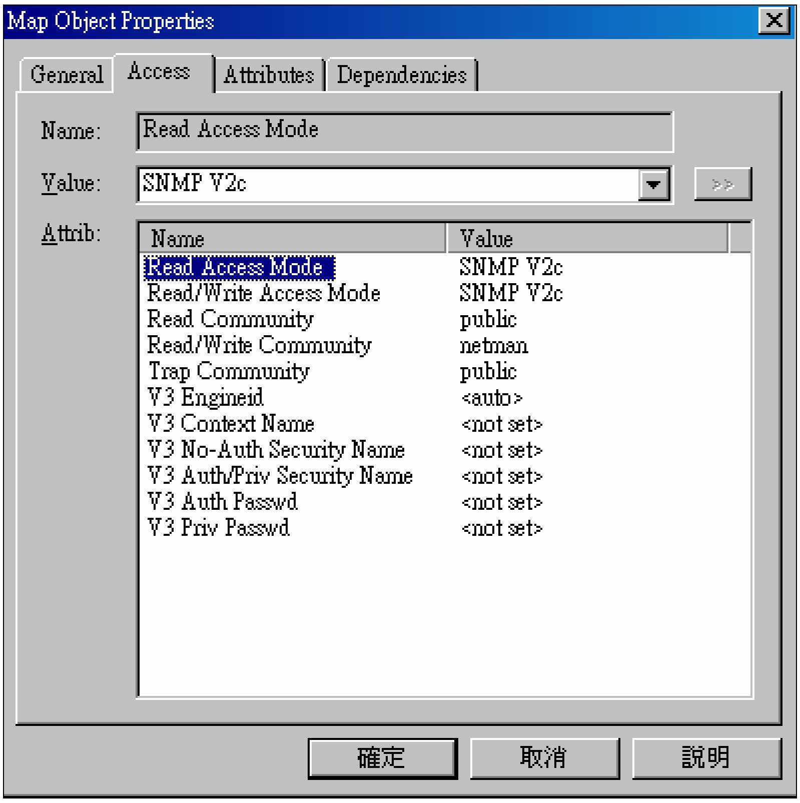
Group: 000=Unknown

Descr:

**Step 4:** In the map object properties, select **Access** tab to set the parameters of Read Access Mode to SNMP V2c shown in Figure 6. Change the value of

Read Access Mode to SNMP V2c.

**Figure 6 Read Access mode**



Map Object Properties

Name: Read Access Mode

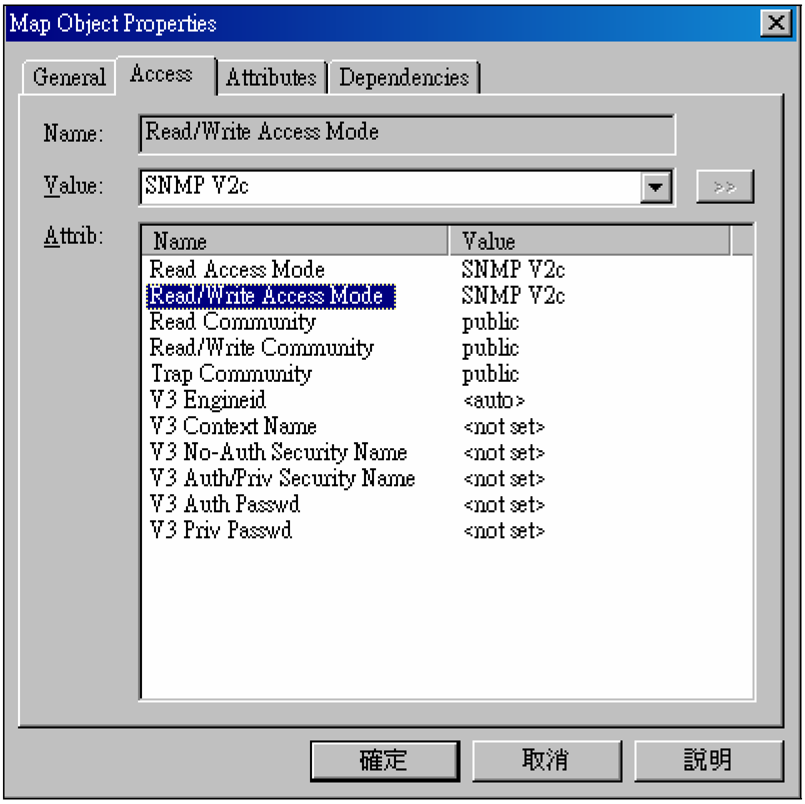
Value: SNMP V2c

Attrib:

| Name | Value |
|---|---|
| Read Access Mode | SNMP V2c |
| Read/Write Access Mode | SNMP V2c |
| Read Community | public |
| Read/Write Community | netman |
| Trap Community | public |
| V3 Engineid | <auto> |
| V3 Context Name | <not set> |
| V3 No-Auth Security Name | <not set> |
| V3 Auth/Priv Security Name | <not set> |
| V3 Auth Passwd | <not set> |
| V3 Priv Passwd | <not set> |

**Step 5:** In the map object properties, select **Access** tab to set the parameters of Read /Write Access Mode to SNMP V2c shown in Figure 7. Change the value of Read/write Access Mode to SNMP V2c.

**Figure 7 Read/Write Access Mode**



Map Object Properties

Name: Read/Write Access Mode

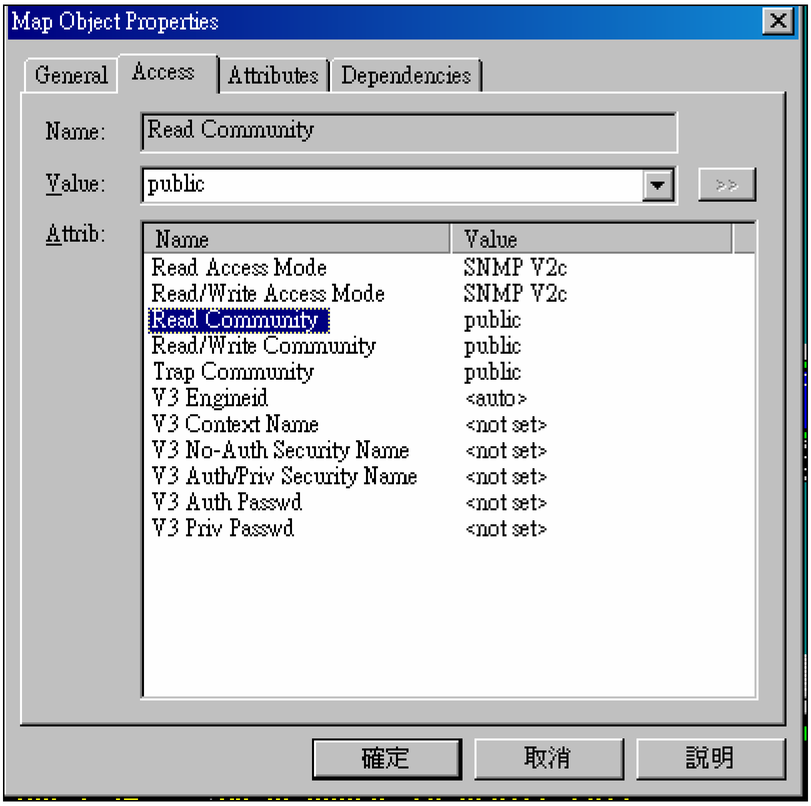
Value: SNMP V2c

Attrib:

| Name | Value |
|---|---|
| Read Access Mode | SNMP V2c |
| Read/Write Access Mode | SNMP V2c |
| Read Community | public |
| Read/Write Community | public |
| Trap Community | public |
| V3 Engineid | <auto> |
| V3 Context Name | <not set> |
| V3 No-Auth Security Name | <not set> |
| V3 Auth/Priv Security Name | <not set> |
| V3 Auth Passwd | <not set> |
| V3 Priv Passwd | <not set> |

**Step 6:** In the map object properties, select **Access** tab to set the parameters of Read community to public as shown in Figure 8.

**Figure 8 Read Community**



Map Object Properties

Name: Read Community

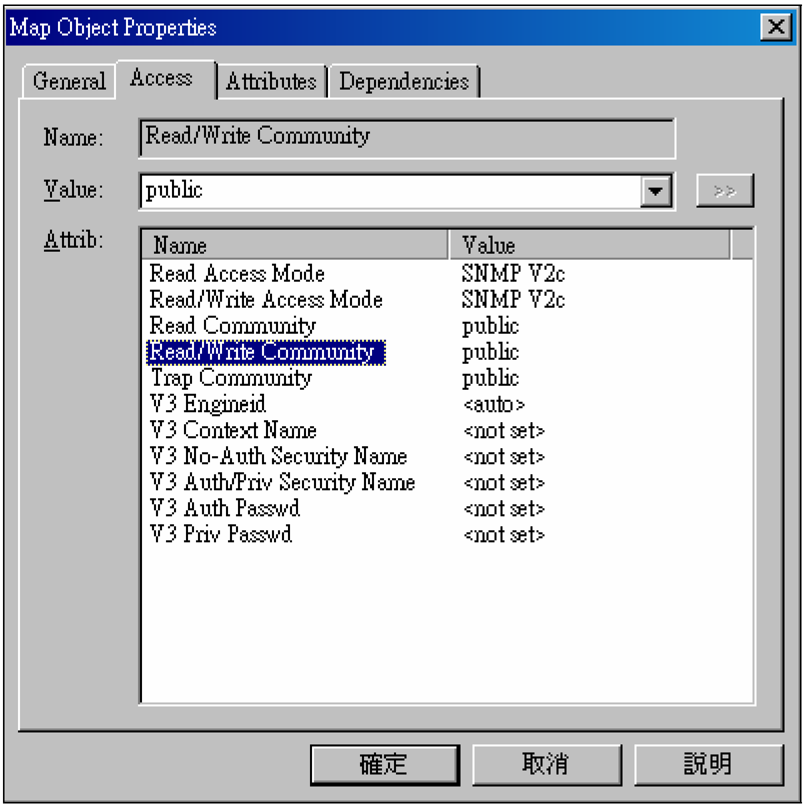
Value: public

Attrib:

| Name | Value |
|---|---|
| Read Access Mode | SNMP V2c |
| Read/Write Access Mode | SNMP V2c |
| Read Community | public |
| Read/Write Community | public |
| Trap Community | public |
| V3 Engineid | <auto> |
| V3 Context Name | <not set> |
| V3 No-Auth Security Name | <not set> |
| V3 Auth/Priv Security Name | <not set> |
| V3 Auth Passwd | <not set> |
| V3 Priv Passwd | <not set> |

**Step 7:** In the map object propeies, select **Access** tab to set the parameters of Read community to public in Figure 9. Change the value of Read//write Community to Public.

**Figure 9 Read/write Community**



Name: Read/Write Community

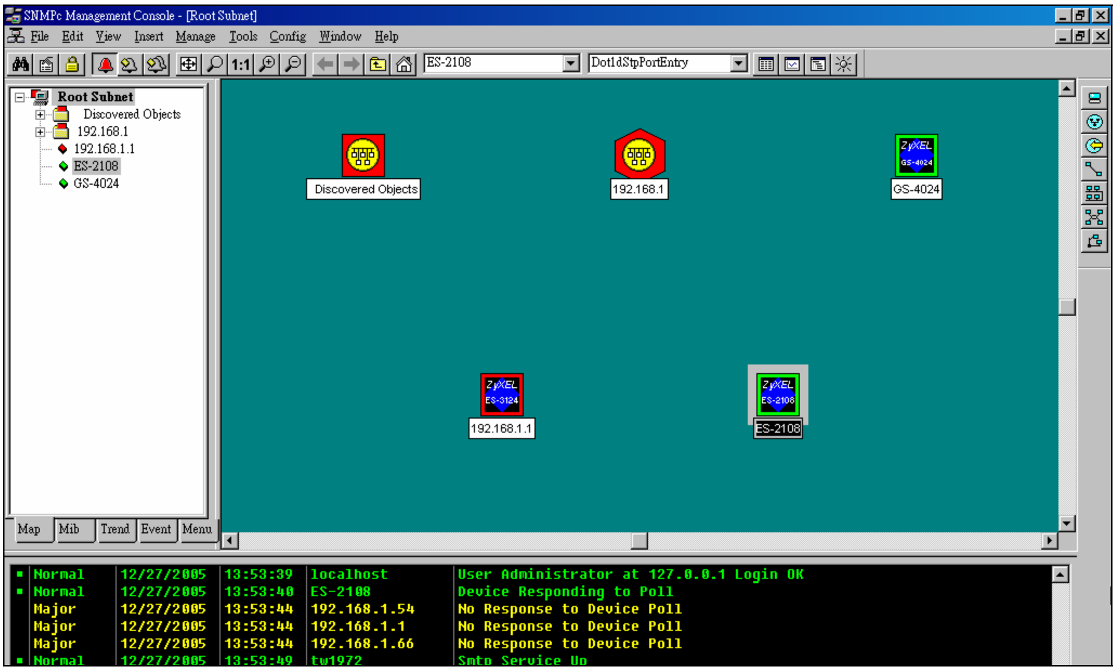
Value: public

Attrib:

| Name | Value |
|---|---|
| Read Access Mode | SNMP V2c |
| Read/Write Access Mode | SNMP V2c |
| Read Community | public |
| Read/Write Community | public |
| Trap Community | public |
| V3 Engineid | <auto> |
| V3 Context Name | <not set> |
| V3 No-Auth Security Name | <not set> |
| V3 Auth/Priv Security Name | <not set> |
| V3 Auth Passwd | <not set> |
| V3 Priv Passwd | <not set> |

**Step 8:** In the Selection tool menu, Click the name of your Switch to manage the device.

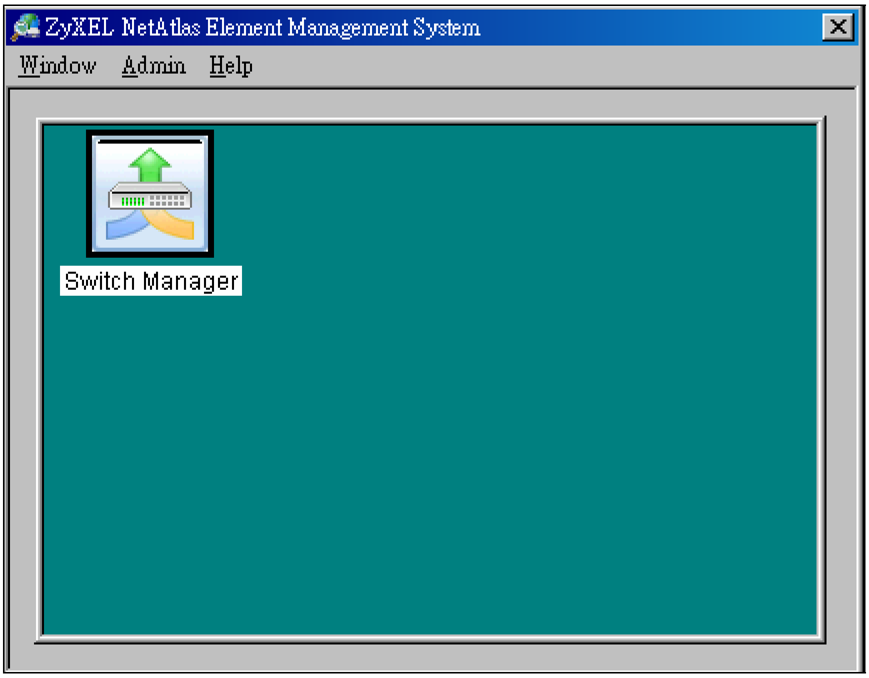
**Figure 10 Device Selection**



```
Normal  12/27/2005  13:53:39  localhost      User Administrator at 127.0.0.1 Login OK
Normal  12/27/2005  13:53:40  ES-2108        Device Responding to Poll
Major   12/27/2005  13:53:44  192.168.1.54   No Response to Device Poll
Major   12/27/2005  13:53:44  192.168.1.1    No Response to Device Poll
Major   12/27/2005  13:53:44  192.168.1.66   No Response to Device Poll
Normal  12/27/2005  13:53:49  tw1972         Smtp Service Up
```

**Step 9:** After the selection, a pop-up menu will display the NetAtlas switch manager diagram. Click the **Switch Manager** to enter the EMS Mapping shown in Figure 11

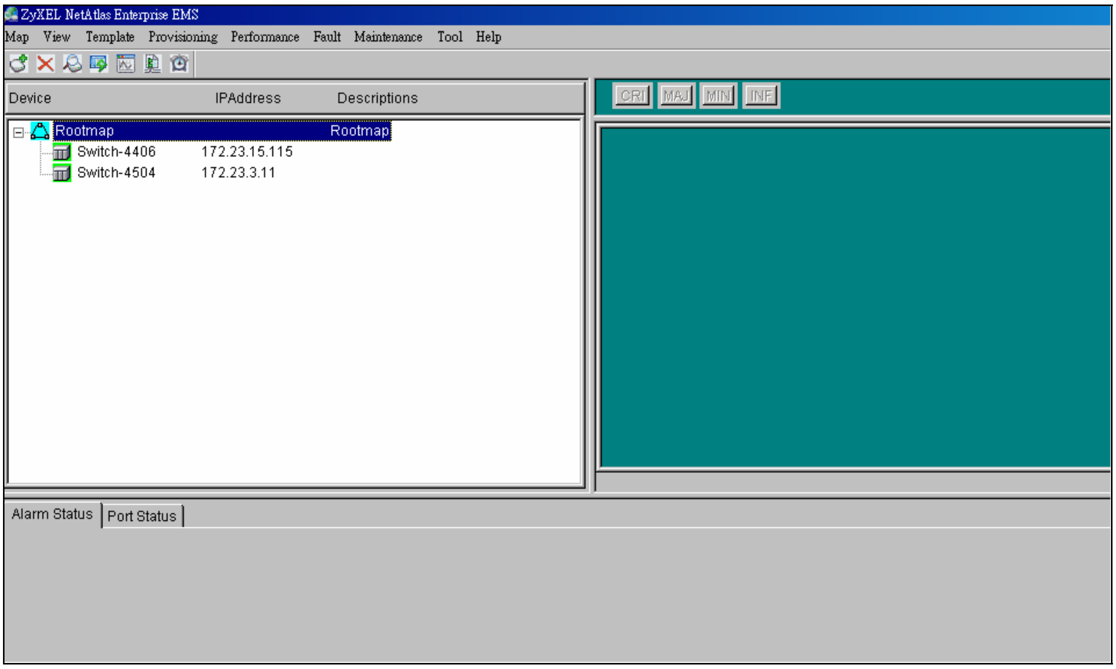
**Figure 11 Device Selection**



**Step 10:** In the EMS mapping, it display a logical hierarchy for the device. In the device list, you may see the devices are added in the Rootmap shown in

Figure 12.

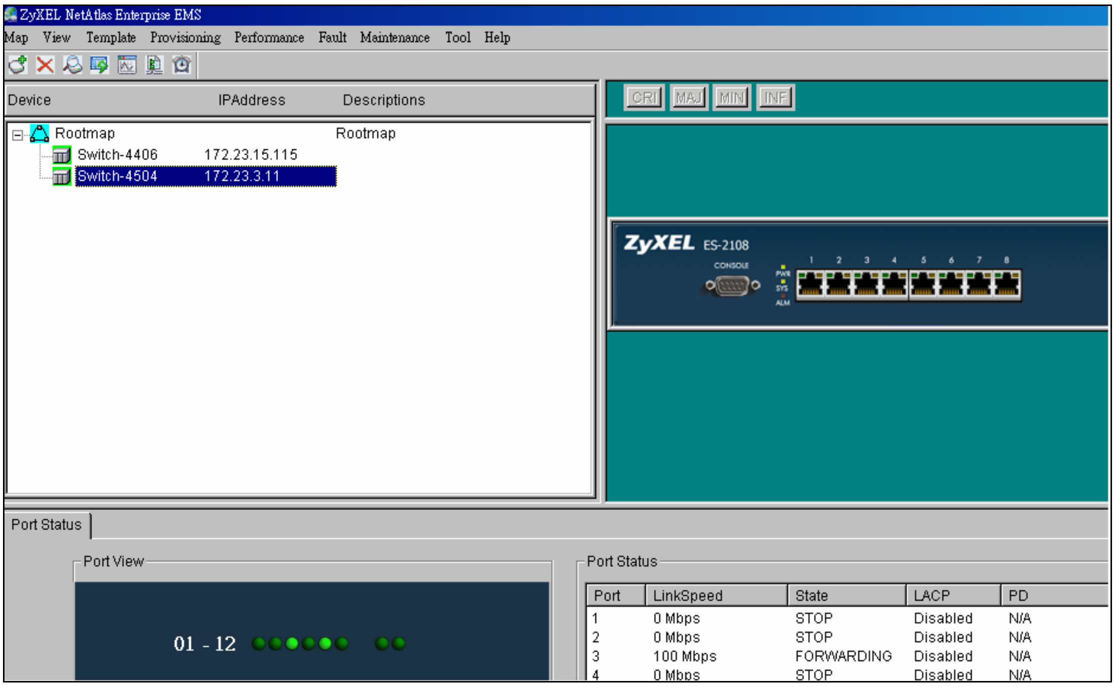
### Figure 12 Rootmap


ZyXEL NetAtlas Enterprise EMS
Map View Template Provisioning Performance Fault Maintenance Tool Help
CRI MAJ MIN INF
Alarm Status
Port Status

| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| Switch-4406 | 172.23.15.115 | |
| Switch-4504 | 172.23.3.11 | |

**Step 11:** Click the your Switch to configure the device shown in Figure 13.

### Figure 13 Device mapping


ZyXEL NetAtlas Enterprise EMS
Map View Template Provisioning Performance Fault Maintenance Tool Help
CRI MAJ MIN INF
ZyXEL ES-2108
CONSOLE
PWR
SYS
ALM
1 2 3 4 5 6 7 8
Port Status
Port View
01 - 12

| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| Switch-4406 | 172.23.15.115 | |
| Switch-4504 | 172.23.3.11 | |

Port Status

| Port | LinkSpeed | State | LACP | PD |
|---|---|---|---|---|
| 1 | 0 Mbps | STOP | Disabled | N/A |
| 2 | 0 Mbps | STOP | Disabled | N/A |
| 3 | 100 Mbps | FORWARDING | Disabled | N/A |
| 4 | 0 Mbps | STOP | Disabled | N/A |

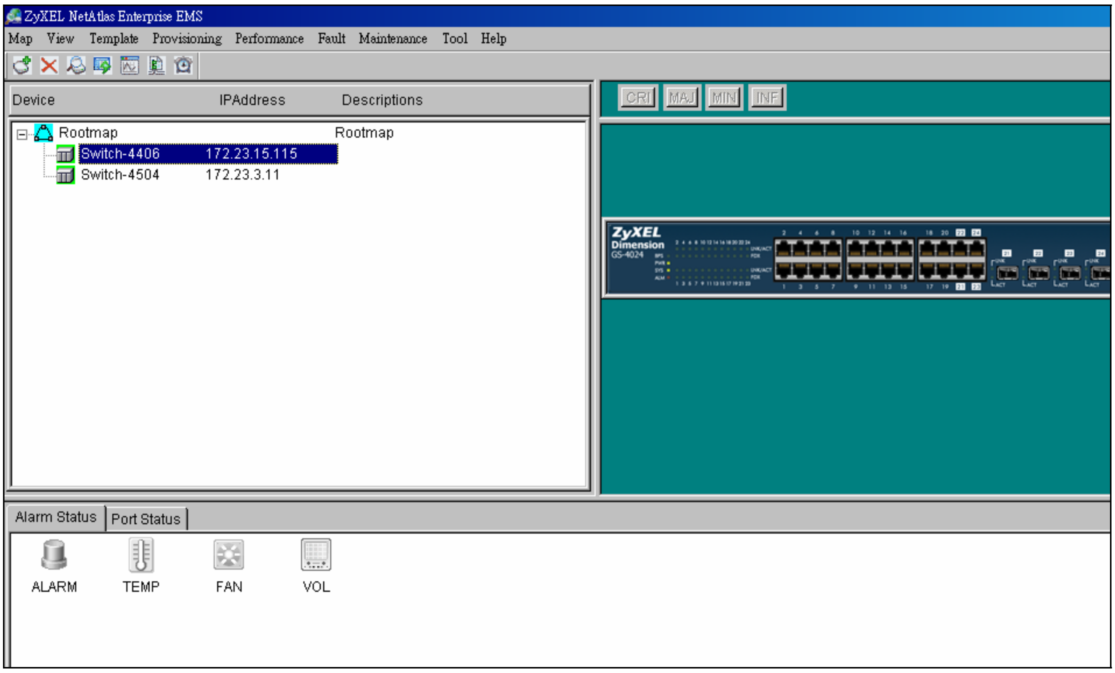
## VLAN Configuration via EMS

In this section, we will give an example to illustrate how to use EMS to create a VLAN2 in GS-4024. Here are the procedures.

Step 1: In the device panel list shown in Figure 12, right-click **Configuration**, **Switch Configuration** and then **Switch Setup** tab as shown in Figure 12 and Figure 13.

Step 2: Define the VLAN type, there are two types of VLAN, one is **802.1Q** and the other is **Port-based VLAN**. Select **802.1Q** as the VLAN type and click Apply in the Figure 14.

**Figure 12 Device panel list**



| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| Switch-4406 | 172.23.15.115 | |
| Switch-4504 | 172.23.3.11 | |

**Figure 13 Switch Configuration**

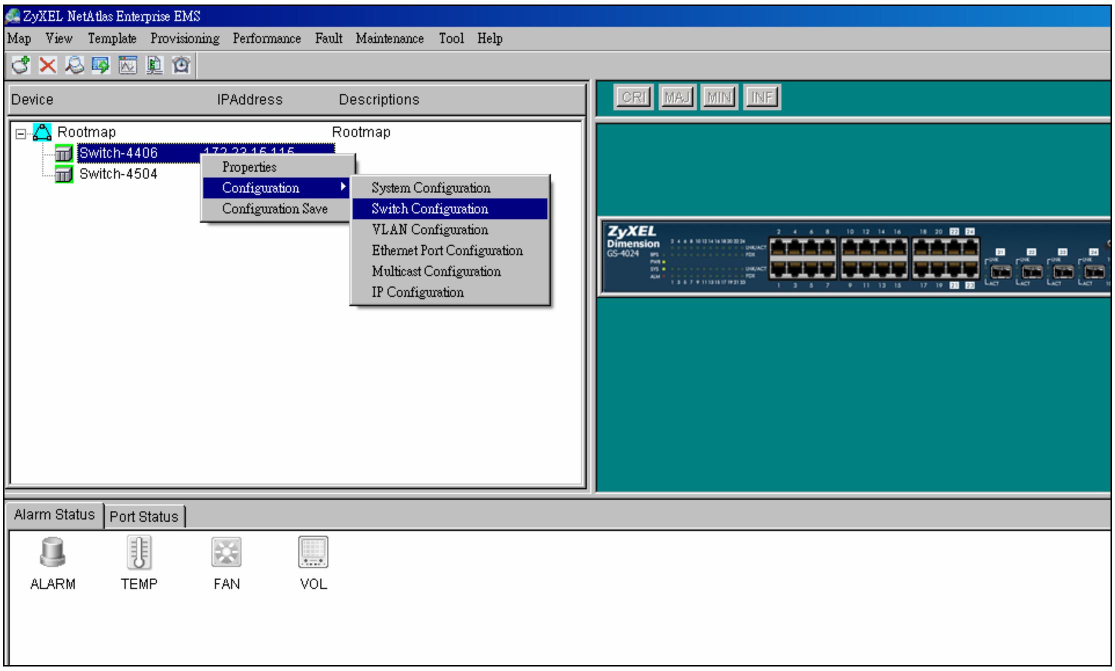
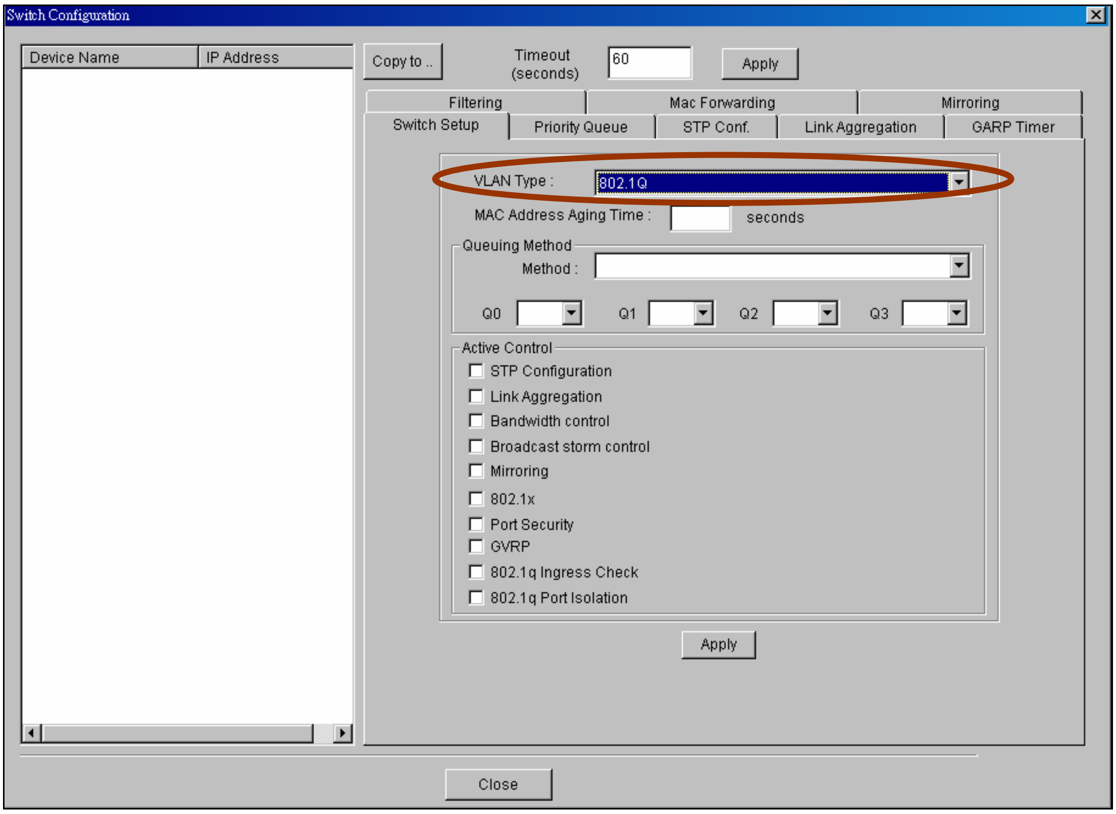


**Figure 14 Selecting a VLAN Type**



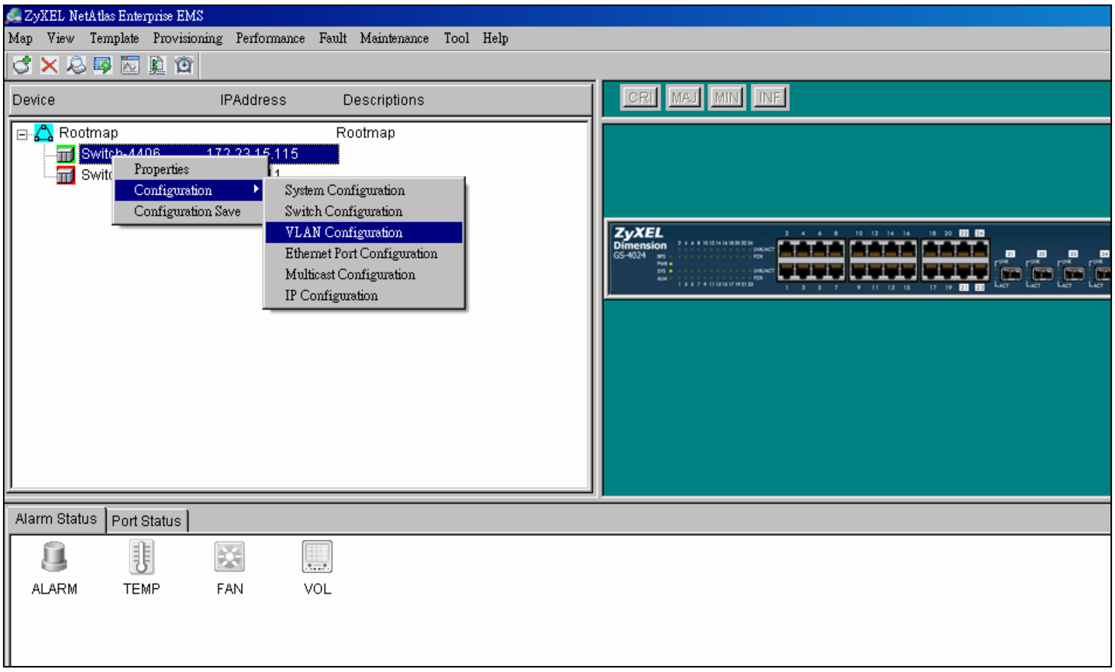
Timeout (seconds): 60

VLAN Type : 802.1Q

After the VLAN type selection, a pop-up window indicates that you have finished the configuration. Then after we have defined the VLAN type to be the 802.1Q, go back to click the Configuration and then VLAN configuration in

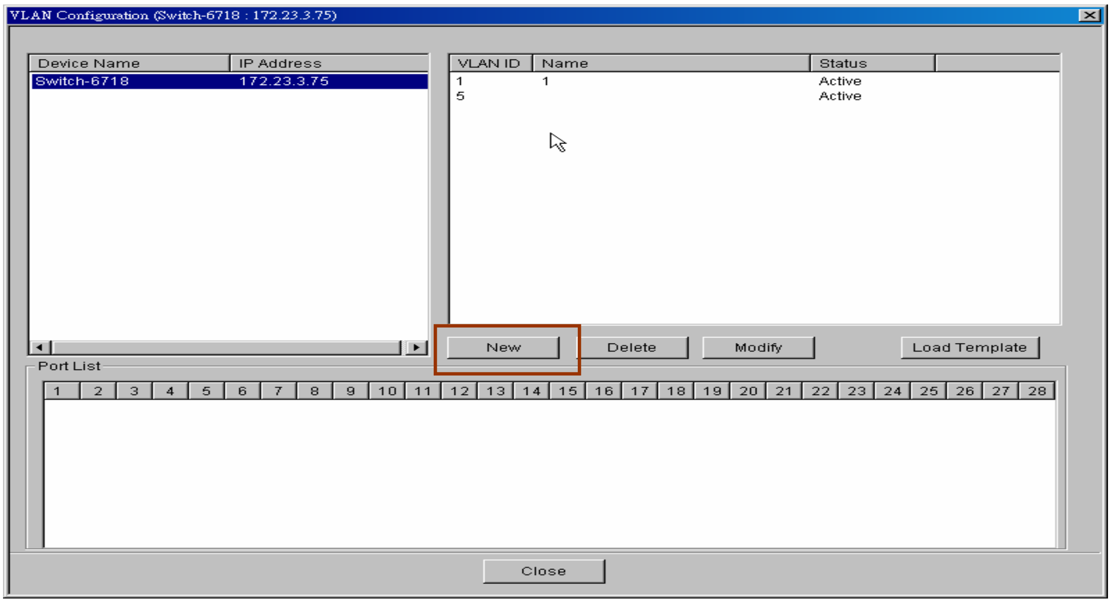
Figure 15.

## Figure 15 VLAN Configuration



Click the New button to create a new VLAN ID in Figure 16.

## Figure 16 Creating a new VLAN ID

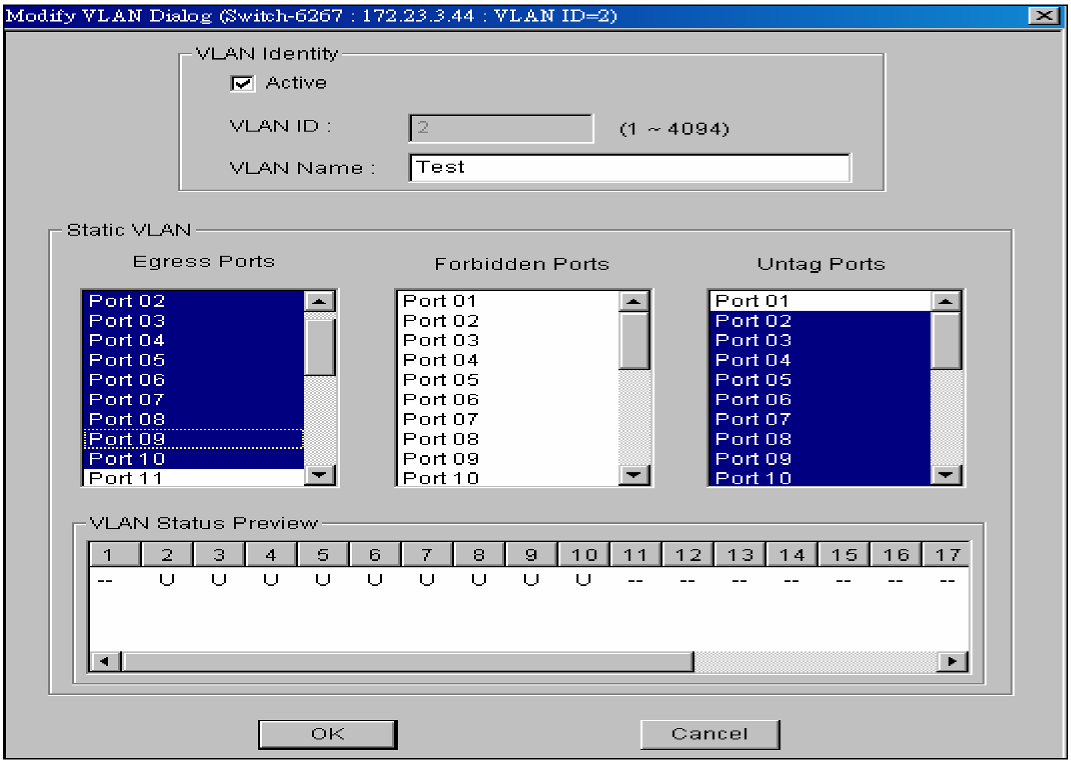


| Device Name | IP Address |
|---|---|
| Switch-6718 | 172.23.3.75 |

| VLAN ID | Name | Status |
|---|---|---|
| 1 | 1 | Active |
| 5 | | Active |

Selecting Egress ports and defines them to be tagged or untagged in Figure 17

## Figure 17 Selecting the ports



Modify VLAN Dialog (Switch-6267 : 172.23.3.44 : VLAN ID=2)

VLAN Identity

☑ Active

VLAN ID : 2 (1 ~ 4094)

VLAN Name : Test

Static VLAN

| Egress Ports | Forbidden Ports | Untag Ports |
|---|---|---|
| Port 02 | Port 01 | Port 01 |
| Port 03 | Port 02 | Port 02 |
| Port 04 | Port 03 | Port 03 |
| Port 05 | Port 04 | Port 04 |
| Port 06 | Port 05 | Port 05 |
| Port 07 | Port 06 | Port 06 |
| Port 08 | Port 07 | Port 07 |
| Port 09 | Port 08 | Port 08 |
| Port 10 | Port 09 | Port 09 |
| Port 11 | Port 10 | Port 10 |

VLAN Status Preview

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -- | U | U | U | U | U | U | U | U | U | -- | -- | -- | -- | -- | -- | -- |

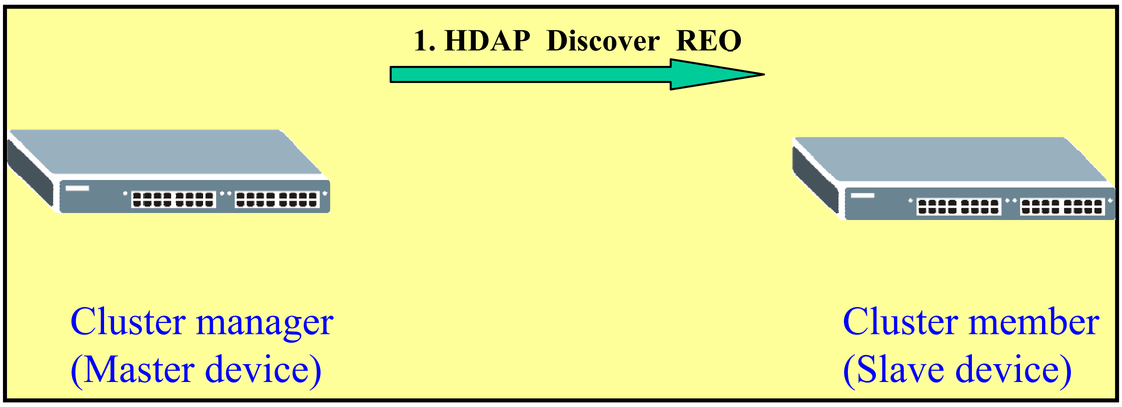
For more information, reference the user guide of NetAtlas.

## Cluster Management Overview

Cluster Management allows you to manage up to 24 switches through a single IP to manage up to 24 switches simultaneously in the same broadcast domain and the same VLAN group ID. The cluster manager which can manage other switches is called the master device. The other terminology we use for cluster management is “istacking”.

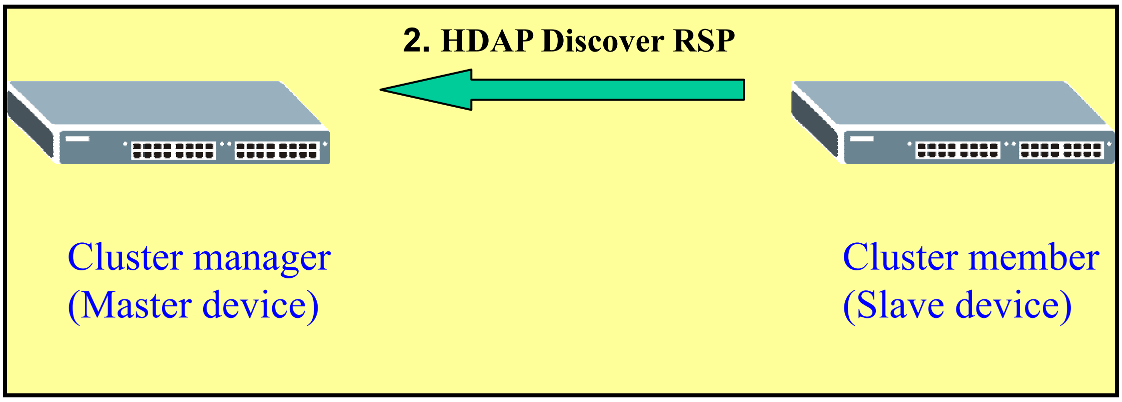
- **How Cluster Management works**

Step 1:



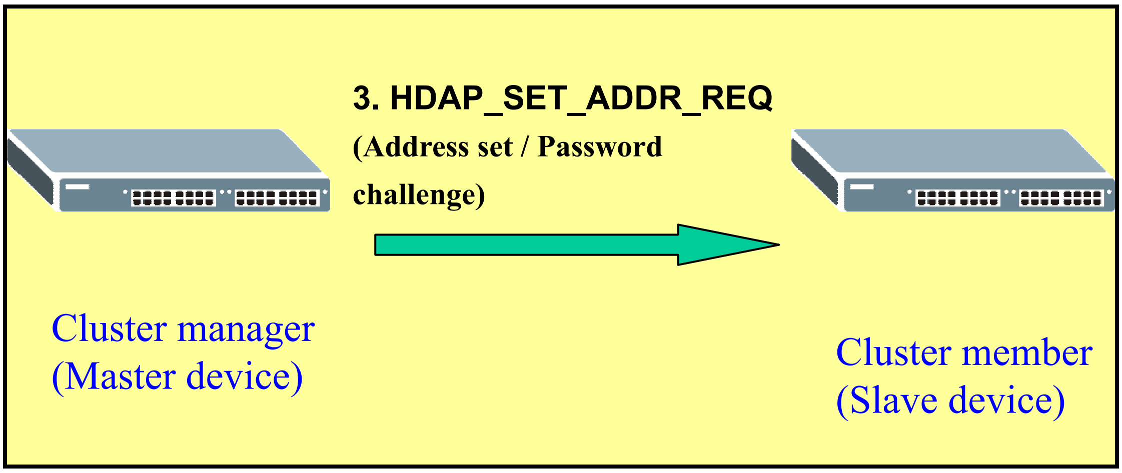
To discover the clustering members, the clustering Manager broadcasts a HDAP (Host Discovery and Address assignment Protocol) Discover request.

Step 2:



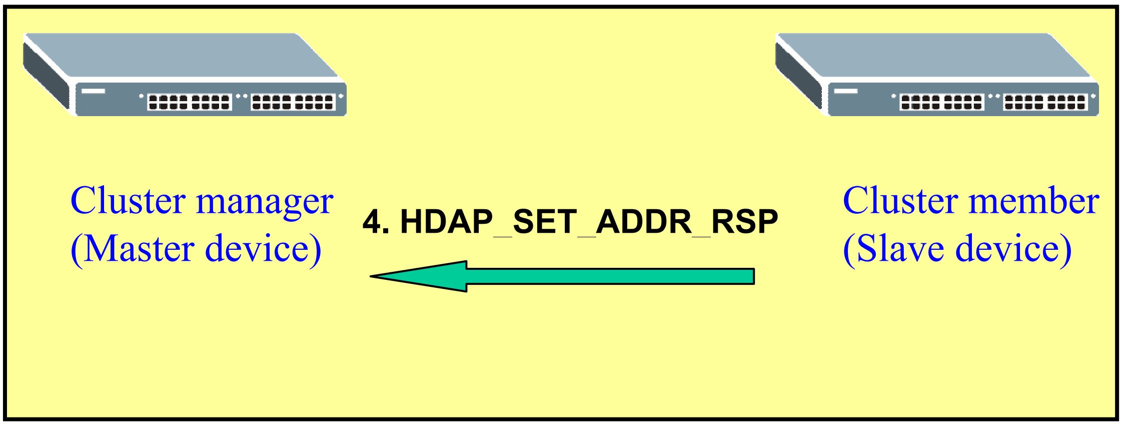
A clustering member listens on UDP port 263. When a clustering member receives a request with the matching signature, it answers with a HDAP Discover Response. In the response, the clustering member provides identity information about itself.

Step 3:



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

Step 4:

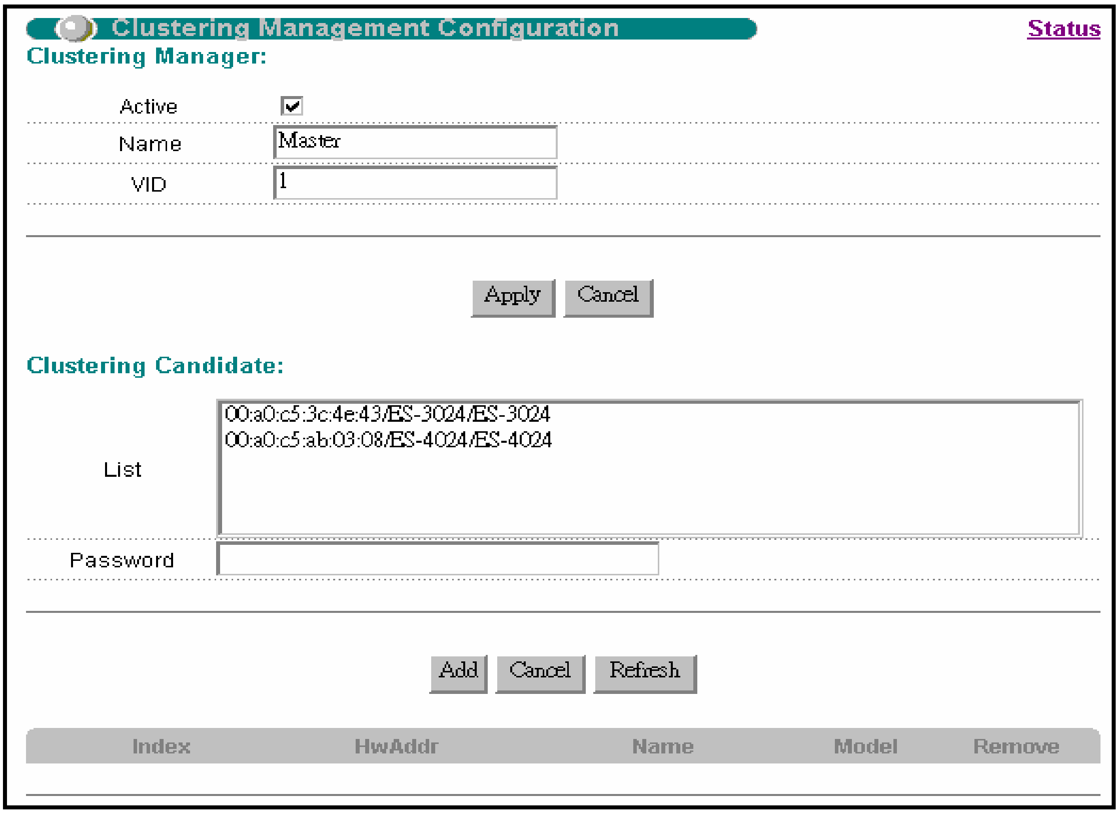


HDPA_SET_ADDR_RSP (Slave device) packet response is for a clustering member to acknowledge a "Set Address" request. The hardware address uniquely identifies the sender of this response.

After the processes are done, the cluster master will be able to manage the slave switch.

- **How to set up Cluster Management in switch**

Step 1:



Clustering Management Configuration

Clustering Manager:

|  |  |
|---|---|
| Active | ☑ |
| Name | Master |
| VID | 1 |

Clustering Candidate:

List:
00:a0:c5:3c:4e:43/ES-3024/ES-3024
00:a0:c5:ab:03:08/ES-4024/ES-4024

Password

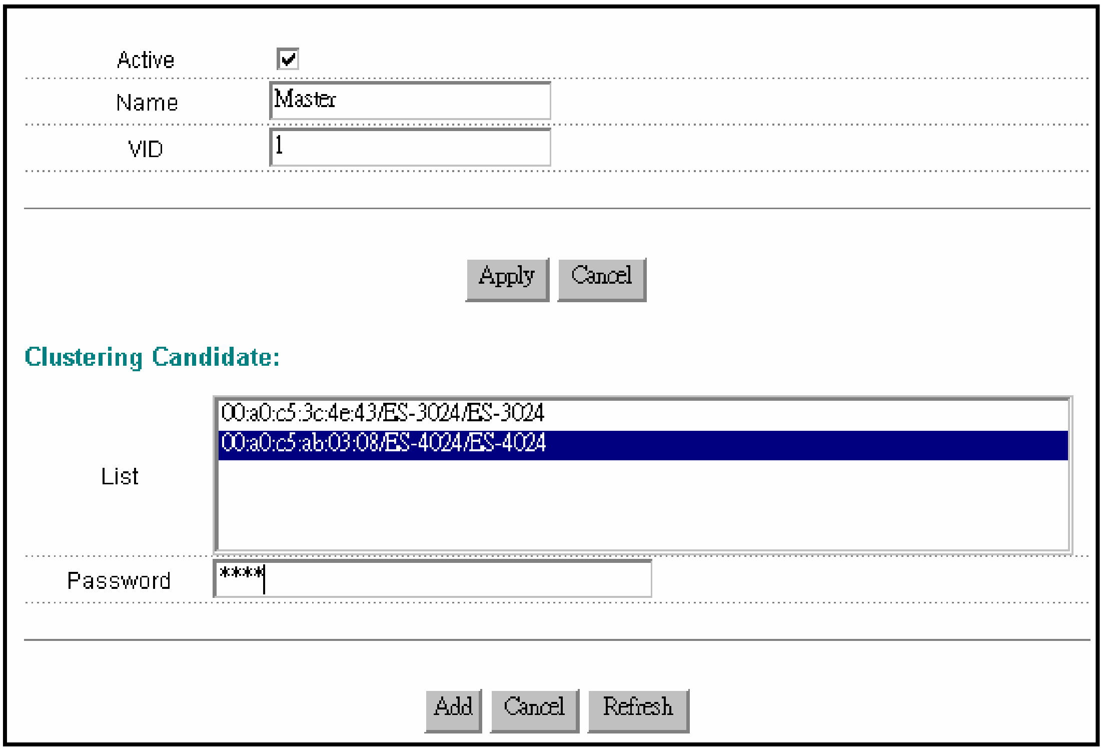
| Index | HwAddr | Name | Model | Remove |
|---|---|---|---|---|

Go to menu: “Management” → ”Cluster Management” → ”Clustering Management Configuration”

In “Clustering Management Configuration” pages, check the “Active” check box to enable Cluster Manager.

In the middle of this page, there is a table shows all the clustering candidates which can be selected and added as the clustering members.

Step 2:



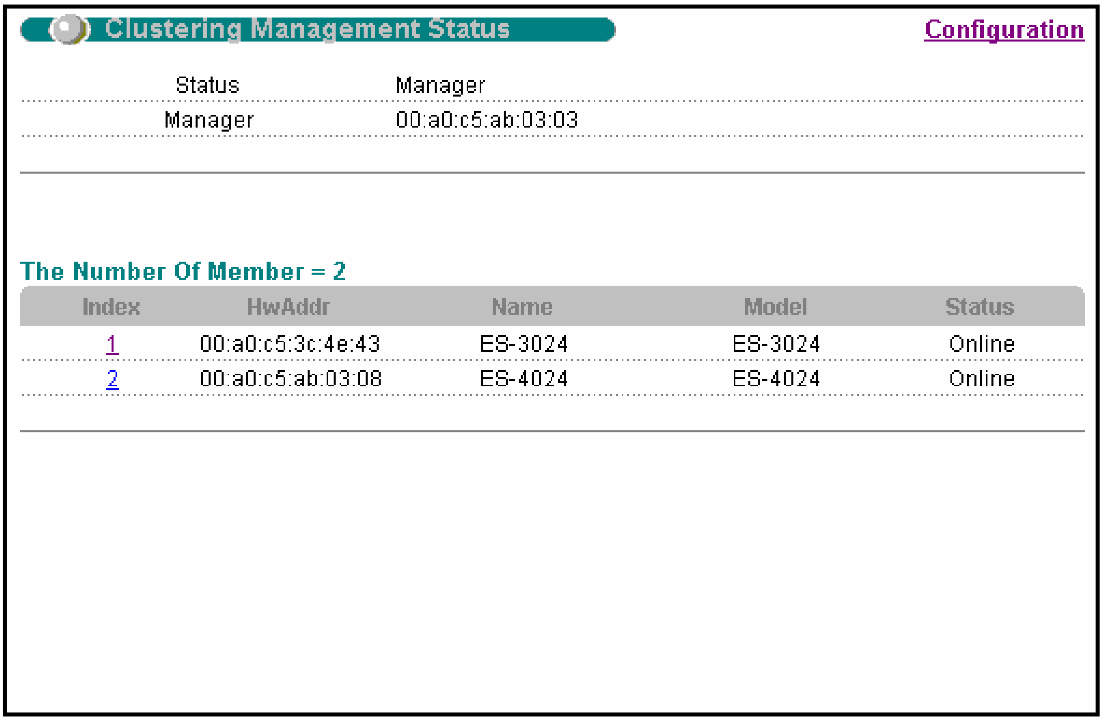
| | |
|---|---|
| Active | ☑ |
| Name | Master |
| VID | 1 |

Clustering Candidate:

| | |
|---|---|
| List | 00:a0:c5:3c:4e:43/ES-3024/ES-3024<br>00:a0:c5:ab:03:08/ES-4024/ES-4024 |
| Password | **** |

Select a device in the Clustering Candidate table and enter the password which is the admin password for the candidate device to add the clustering member.

Step 3:



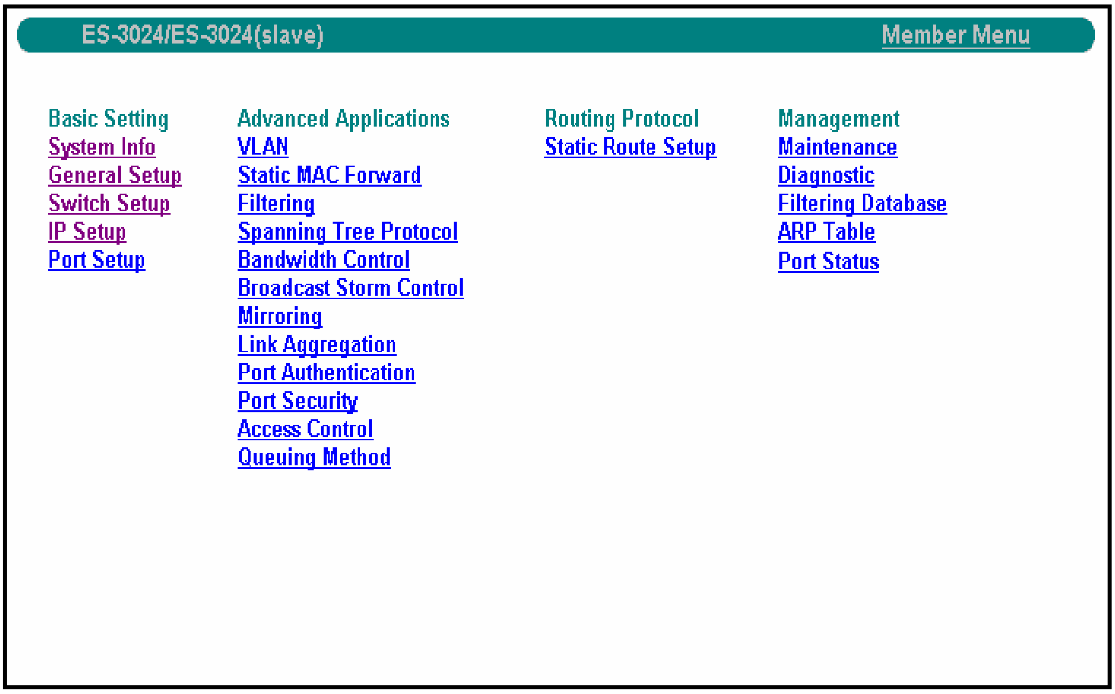
| Status | Manager |
|---|---|
| Manager | 00:a0:c5:ab:03:03 |

The Number Of Member = 2

| Index | HwAddr | Name | Model | Status |
|---|---|---|---|---|
| 1 | 00:a0:c5:3c:4e:43 | ES-3024 | ES-3024 | Online |
| 2 | 00:a0:c5:ab:03:08 | ES-4024 | ES-4024 | Online |

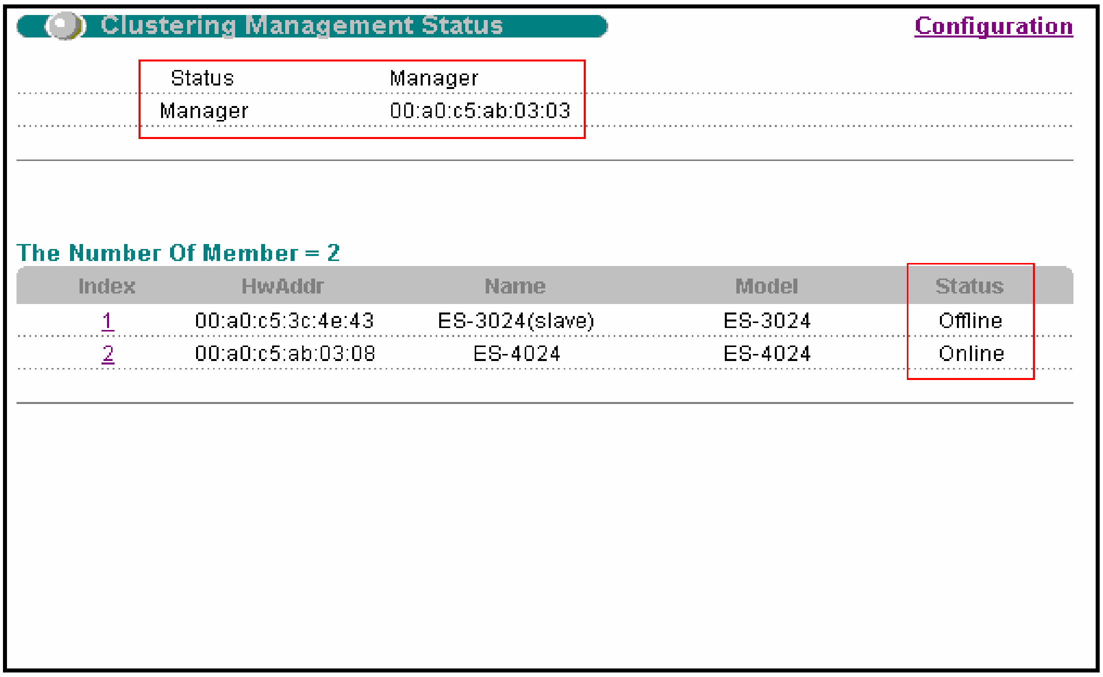
Click on the index number to manage the selected clustering member.

Step 4:



In "**Member Menu**" pages, you can change any setting of the clustering member, except **Cluster Management, Firmware Upgrade and Restore Configuration.**

Step 5:



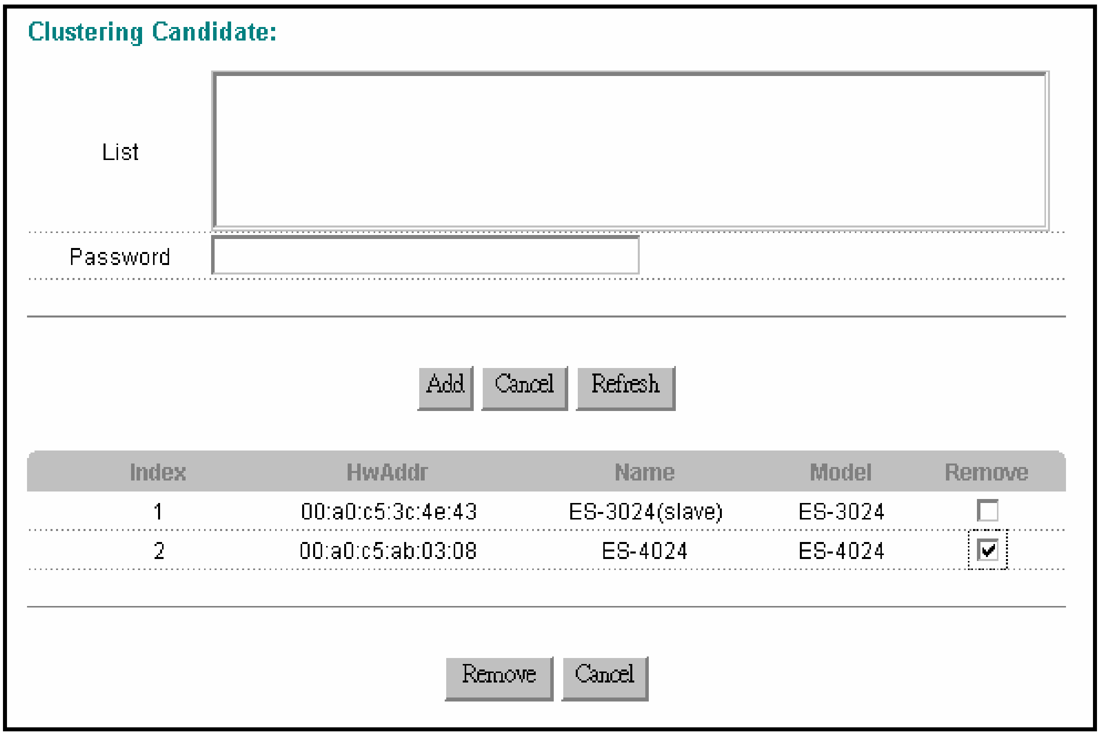
| Status | Manager |
|---|---|
| Manager | 00:a0:c5:ab:03:03 |

The Number Of Member = 2

| Index | HwAddr | Name | Model | Status |
|---|---|---|---|---|
| 1 | 00:a0:c5:3c:4e:43 | ES-3024(slave) | ES-3024 | Offline |
| 2 | 00:a0:c5:ab:03:08 | ES-4024 | ES-4024 | Online |

Enter "**Management**"->"**Cluster Management**"->"**Clustering Management Status**:" In "**Clustering Management Status**" pages, you can check the status for each member.

Step 6:


Clustering Candidate:

| | |
|---|---|
| List | |
| Password | |

| Index | HwAddr | Name | Model | Remove |
|---|---|---|---|---|
| 1 | 00:a0:c5:3c:4e:43 | ES-3024(slave) | ES-3024 | ☐ |
| 2 | 00:a0:c5:ab:03:08 | ES-4024 | ES-4024 | ☑ |

Enter "**Management**"->"**Cluster Management**"->"**Clustering Management Configuration**:" In "**Clustering Management Configuration**" pages , by checking the remove checkbox and then, click on the **Remove** button to remove a cluster member.

## Overview of RMON

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

RMON was originally developed to address the problem of managing LAN segments and remote sites from a central location. The RMON specification, which is an extension of the SNMP MIB, is a standard monitoring specification. Within an RMON network monitoring data is defined by a set of statistics and functions and exchanged between various different monitors and console systems. Resultant data is used to monitor network utilization for network planning and performance-tuning, as well as assisting in network fault diagnosis.

RMON solutions are comprised of two components: a probe (or an agent or a monitor), and a client, usually a management station. Agents store network information within their RMON MIB and are normally found as embedded software on network hardware such as routers and switches although they can be a program running on a PC. Agents can only see the traffic that flows through them so they must be placed on each LAN segment or WAN link that is to be monitored. Clients, or management stations, communicate with the RMON agent or probe, using SNMP to obtain and correlate RMON data.

Now, there are a number of variations to the RMON MIB. For example, the Token Ring RMON MIB provides objects specific to managing Token Ring networks. The SMON MIB extends RMON by providing RMON analysis for switched networks.

## RMON Groups

RMON delivers information in nine RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements. Each group is optional so that vendors do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly. Table 1 summarizes the nine monitoring groups specified in the RFC 1757 Ethernet RMON MIB.

Table 1: RMON Monitoring Groups

| **RMON 1 MIB Group** | **Function** | **Elements** |
|---|---|---|
| Statistics | Contains statistics measured by the probe for each monitored interface on this device. | Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes. |
| History | Records periodic statistical samples from a network and stores for retrieval. | Sample period, number of samples, items sampled. |
| Alarm | Periodically takes statistical samples and compares them with set thresholds for events generation. | Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold. |
| Host | Contains statistics associated with each host discovered on the network. | Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets. |
| HostTopN | Prepares tables that describe the top hosts. | Statistics, host(s), sample start and stop periods, rate base, duration. |

| | | |
|---|---|---|
| Matrix | Stores and retrieves statistics for conversations between sets of two addresses. | Source and destination address pairs and packets, bytes, and errors for each pair. |
| Filters | Enables packets to be matched by a filter equation for capturing or events. | Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters. |
| Packet Capture | Enables packets to be captured after they flow through a channel. | Size of buffer for captured packets, full status (alarm), number of captured packets. |
| Events | Controls the generation and notification of events from this device. | Event type, description, last time event sent |

## Groups of RMON MIB

The objects are arranged into the following groups:

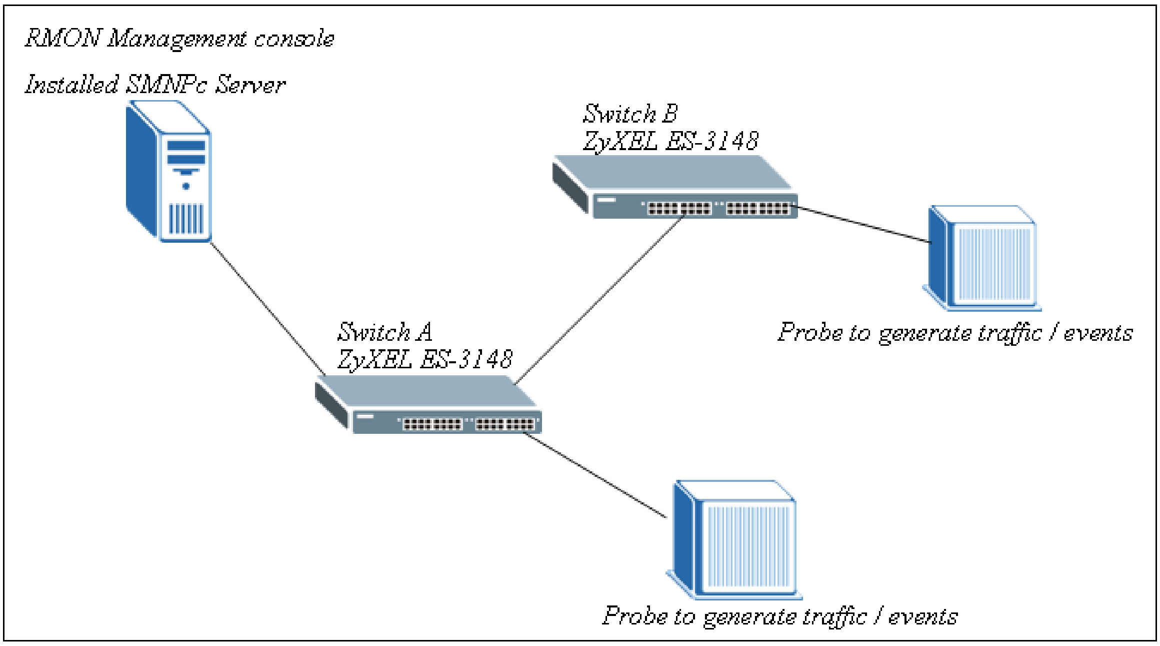
Statistics
(iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).statistics(1))

| | |
|---|---|
| History | (1.3.6.1.2.1.16.2) |
| Alarm | (1.3.6.1.2.1.16.3) |
| Hosts | (1.3.6.1.2.1.16.4) |
| hostTopN | (1.3.6.1.2.1.16.5) |
| Matrix | (1.3.6.1.2.1.16.6) |
| Filter | (1.3.6.1.2.1.16.7) |
| Capture | (1.3.6.1.2.1.16.8) |

Event (1.3.6.1.2.1.16.9)

All groups in this MIB are optional. (MIB-II is **mandatory**)

## Scenario (ES-4024A Series supports RMON 1.2.3.9)



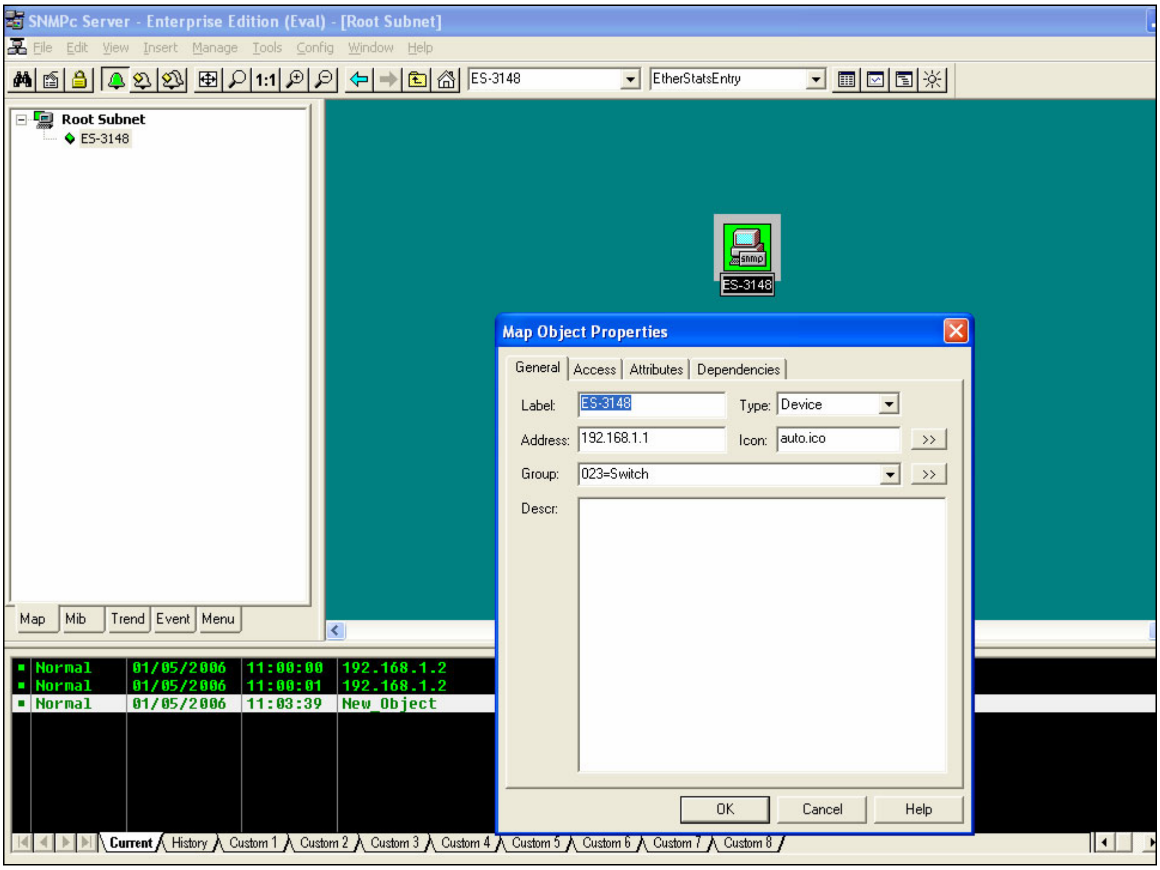
In this illustration, SNMPc Enterprise Edition Version 5.1.6c is installed on the PC. And this PC is defined as “RMON management console”. This PC can ping both ZyXEL ES-3148 (both Switch A & Switch B). And there are some probes / networking devices to generate the traffic to the ZyXEL Switches in order to verify the RMON result. Since the work flow and the technology of RMON on the two switches are the same, only one of the ZyXEL ES-3148 Switch will be demonstrated at this time.

Since RMON is an extension of the SNMP, SNMP must be enabled first in the ZyXEL ES-3148. By default SNMP is enabled and it has set Community (Get,Set,Trap) to “public”. And Trap Destination to 0.0.0.0; It is not mandatory to change the default value in order for SNMP & RMON to work. Therefore, modification is not necessary in this case.

In this scenario, we are going to monitor the Broadcast Packets by using the RMON MIB. The following will demonstrate the steps to monitor the Broadcast Packets by using SNMPc Enterprise Edition Version 5.1.6c.

## 1. Methodology of Scenario Verification

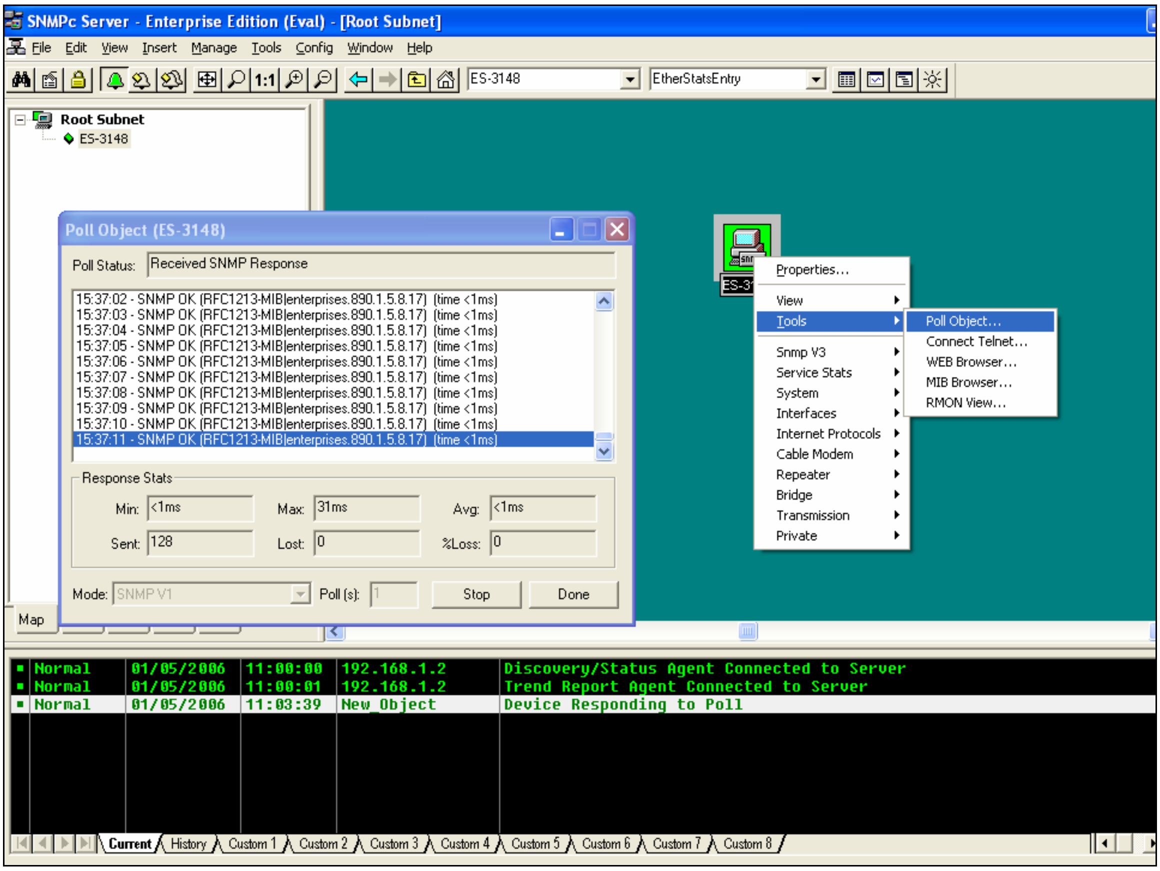
1.Open your SNMPc program first, then pick the ZyXEL-3148 Switch (it is first named as device "root") and give it the correct IP information to get the SNMP information. Also, you can rename it to whatever you want.


SNMPc Server - Enterprise Edition (Eval) - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
ES-3148
EtherStatsEntry
Root Subnet
ES-3148
Map Mib Trend Event Menu
ES-3148
Map Object Properties
General Access Attributes Dependencies
OK Cancel Help
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8

Label: ES-3148
Type: Device
Address: 192.168.1.1
Icon: auto.ico
Group: 023=Switch
Descr:

```
Normal  01/05/2006  11:00:00  192.168.1.2
Normal  01/05/2006  11:00:01  192.168.1.2
Normal  01/05/2006  11:03:39  New_Object
```

You can verify if your configuration is correct by using the "Poll Object" option. Just right click our mouse on the ES-3148 icon and it is located inside the "Tools".



Poll Status: Received SNMP Response

```
15:37:02 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:03 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:04 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:05 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:06 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:07 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:08 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:09 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:10 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
15:37:11 - SNMP OK (RFC1213-MIB|enterprises.890.1.5.8.17)  (time <1ms)
```

Response Stats

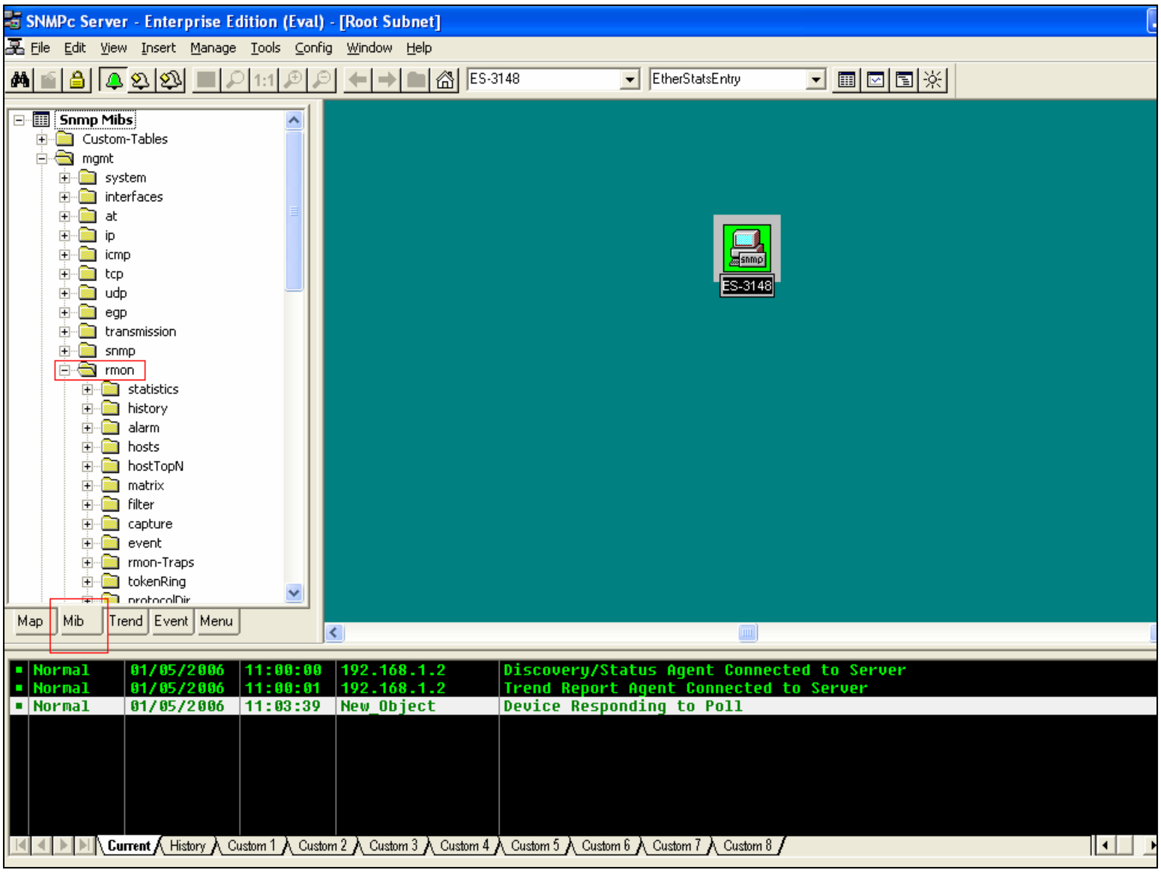
Min: <1ms  Max: 31ms  Avg: <1ms

Sent: 128  Lost: 0  %Loss: 0

Mode: SNMP V1  Poll (s): 1

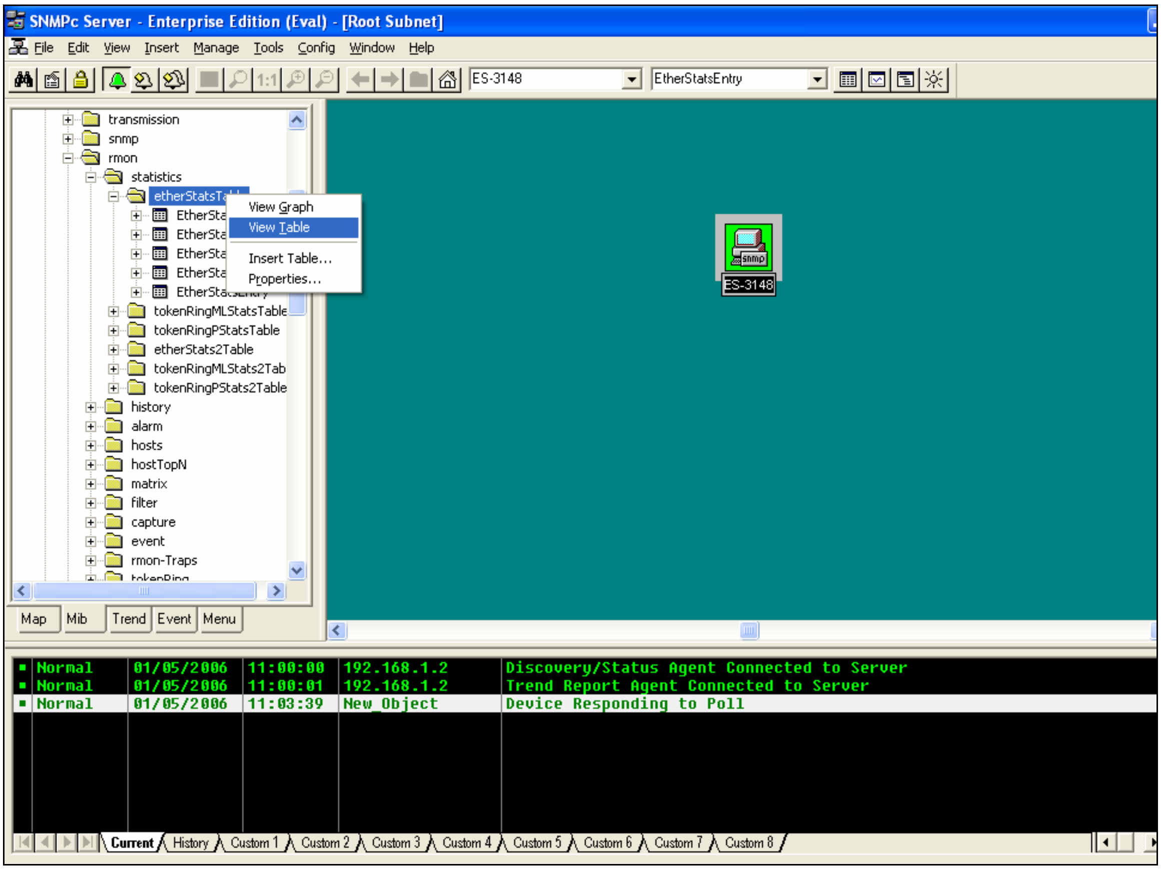
```
Normal   01/05/2006   11:00:00   192.168.1.2   Discovery/Status Agent Connected to Server
Normal   01/05/2006   11:00:01   192.168.1.2   Trend Report Agent Connected to Server
Normal   01/05/2006   11:03:39   New_Object    Device Responding to Poll
```

2. Secondly, click on the “Mib” tab and expend the SNMP Mibs’ tree. You will find that there is an “rmon” group over there and again you can expend its sub-tree.



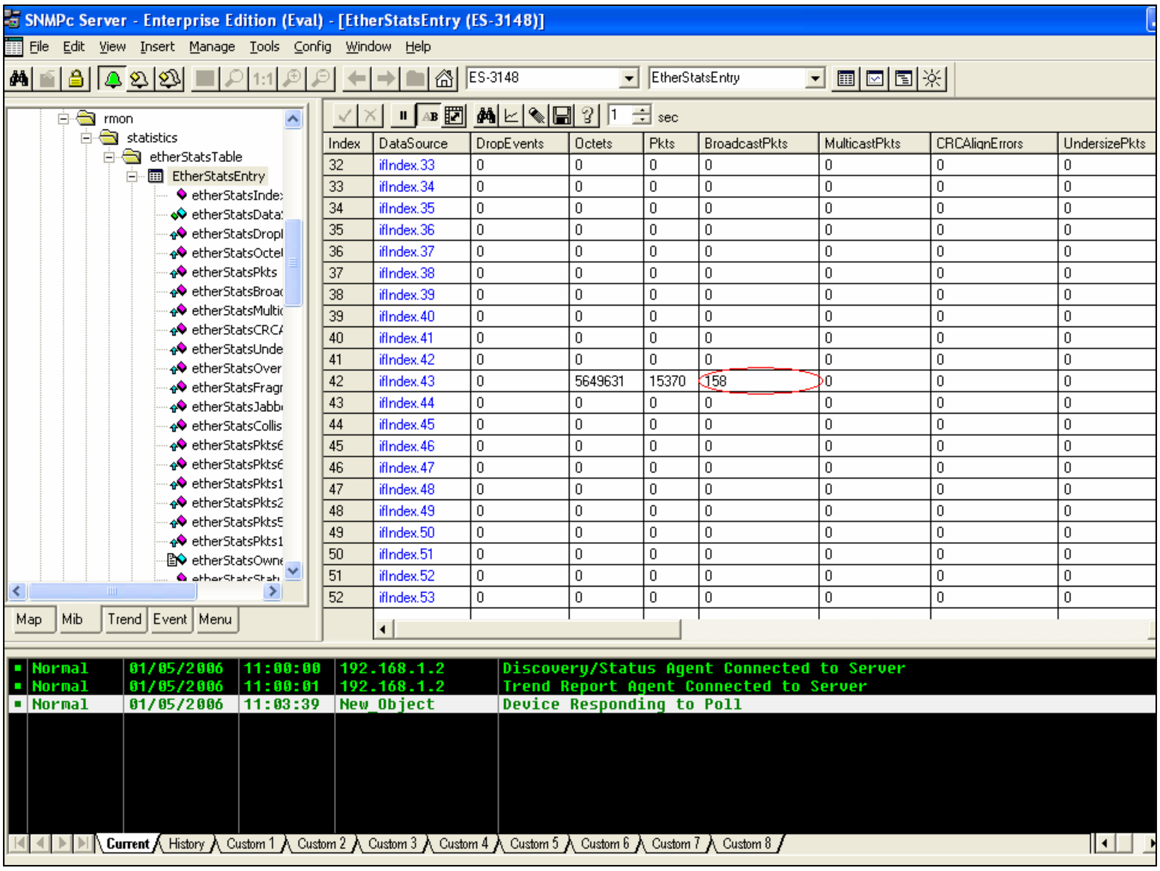
```
Normal  01/05/2006  11:00:00  192.168.1.2  Discovery/Status Agent Connected to Server
Normal  01/05/2006  11:00:01  192.168.1.2  Trend Report Agent Connected to Server
Normal  01/05/2006  11:03:39  New_Object   Device Responding to Poll
```

3. Right click the “etherStatsTable” and choose “View Table”



```
Normal    01/05/2006  11:00:00  192.168.1.2  Discovery/Status Agent Connected to Server
Normal    01/05/2006  11:00:01  192.168.1.2  Trend Report Agent Connected to Server
Normal    01/05/2006  11:03:39  New_Object   Device Responding to Poll
```

4. Find the interface or port that you are looking for. And you can look at the corresponding field and therefore find the value that you want to monitor. In this case, we are looking for the Broadcast Packets.

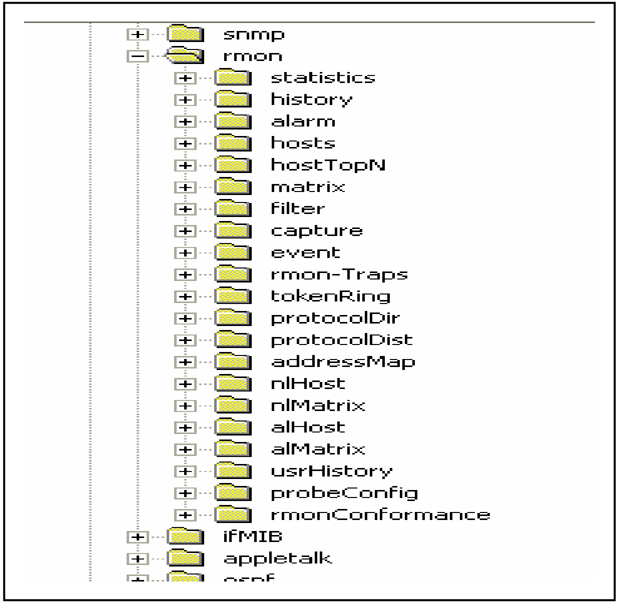


| Index | DataSource | DropEvents | Octets | Pkts | BroadcastPkts | MulticastPkts | CRCAlignErrors | UndersizePkts |
|---|---|---|---|---|---|---|---|---|
| 32 | ifIndex.33 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 33 | ifIndex.34 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 34 | ifIndex.35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 35 | ifIndex.36 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 36 | ifIndex.37 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 37 | ifIndex.38 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 38 | ifIndex.39 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 39 | ifIndex.40 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 40 | ifIndex.41 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 41 | ifIndex.42 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 42 | ifIndex.43 | 0 | 5649631 | 15370 | 158 | 0 | 0 | 0 |
| 43 | ifIndex.44 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 44 | ifIndex.45 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 45 | ifIndex.46 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 46 | ifIndex.47 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 47 | ifIndex.48 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 48 | ifIndex.49 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 49 | ifIndex.50 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 50 | ifIndex.51 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 51 | ifIndex.52 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 52 | ifIndex.53 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

```
Normal  01/05/2006  11:00:00  192.168.1.2  Discovery/Status Agent Connected to Server
Normal  01/05/2006  11:00:01  192.168.1.2  Trend Report Agent Connected to Server
Normal  01/05/2006  11:03:39  New_Object   Device Responding to Poll
```

Try to generate some broadcast traffic from the probe or your network device, then you should see the BroadcastPkts increasing.

5. In conclusion, if the Switch supports RMON, then you can get the values from the Switch in the RMON Group(s), otherwise, it will return 0 and always stays 0. Without the supporting of RMON, then it is impossible to monitor those elements in the RMON MIB Group



# FAQ

**What is the default setting of the IP parameters?**

IP address: 192.168.1.1
Subnet: 255.255.255.0

**What is the default login Name and Password of 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, which has terminal emulation software configured to the follow parameters:
Terminal emulation: VT100
Baud rate: 9600 bps
Data bits: 8
Parity: none
Stop bit: 1
Flow control: none

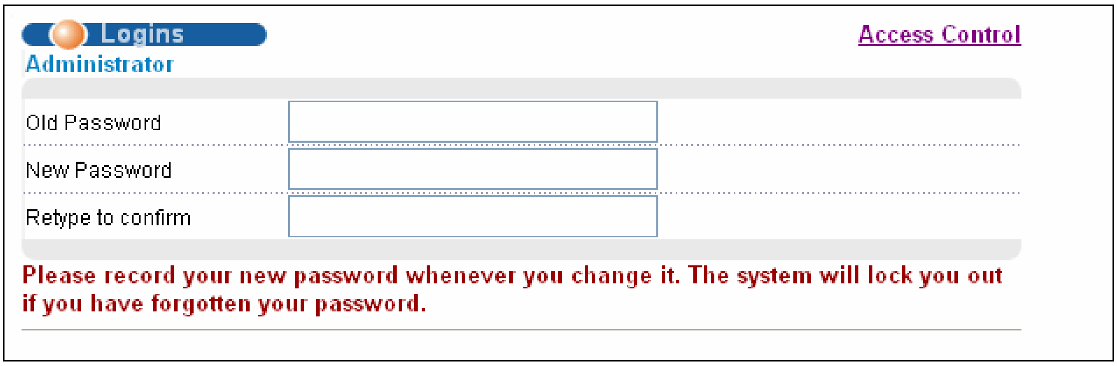
**What is default login password of the console, telnet, and FTP?**

Password: 1234

### How to change the password?

Web Configurator is the only place you can change the password. After you log in for the first time, it is recommended you change the default administrator password.

**From Web Configurator:** Click Advanced Application, Access Control, and then Logins to display the next screen.



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

From there you can change a new password.

### How to access the Command Line Interface?

There are two ways to access the Command Line Interface. One is "Telnet to the switch" and another is "Connect a computer to the console port and use the terminal emulation software." Please check "How to access the Switch through the console port?" to set up the parameters.

### If you forget the password, how to reset the password to default?

If you forget the password, you will need to reload the factory default configuration. Please be aware that you will lose all previous configurations.

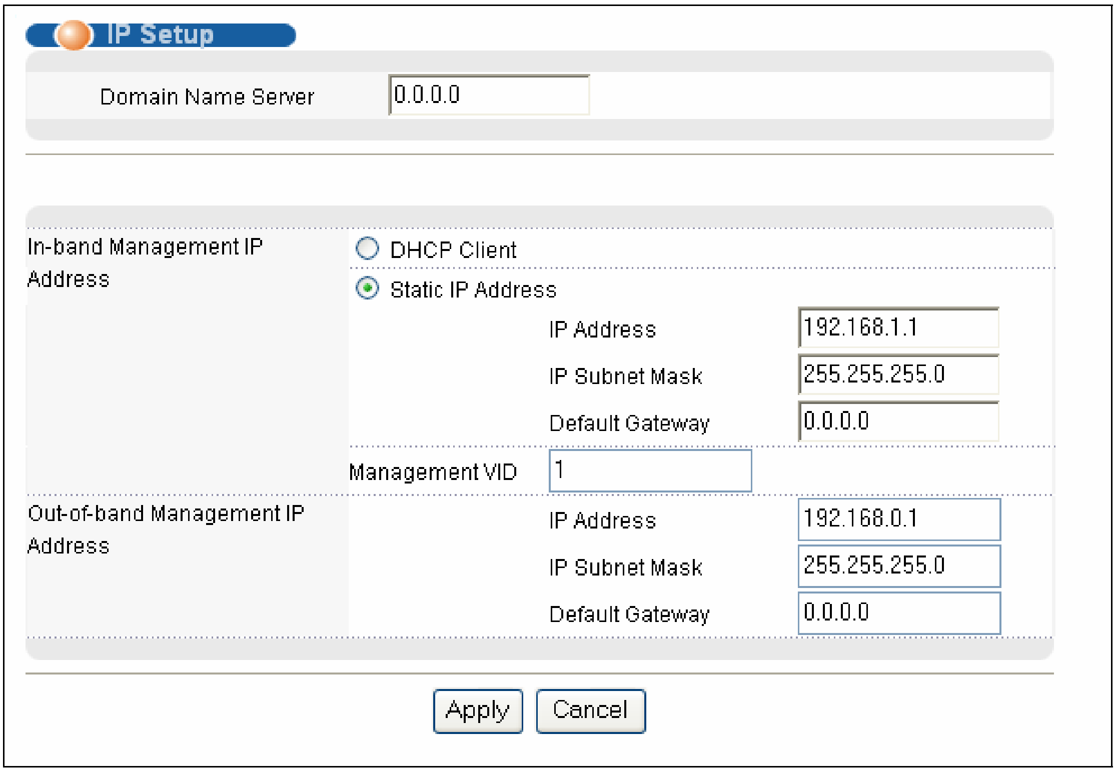
1. Connect the console cable to your computer and open the terminal emulation software.

2. Power off and then power on the Switch, and press any key to enter the debug mode when the screen shows "Press any key to enter Debug Mode within 3 seconds."
3. Type "atlc" and press the enter key
4. When the message "starting XMODEM upload" appears, do XMODEM upload of the default rom file to the Switch
5. After it is done uploading the rom file successfully, type "atgo" to leave the debug mode.
6. The system will be restarted automatically. After the system is up, you should be able to log in with the default password "1234" and the IP address is now 192.168.1.1.

## How do I configure an IP address?

### From Web Configurator:

Click Basic Setting and then IP Setup to display the next screen.



IP Setup

Domain Name Server: 0.0.0.0

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
Management VID: 1

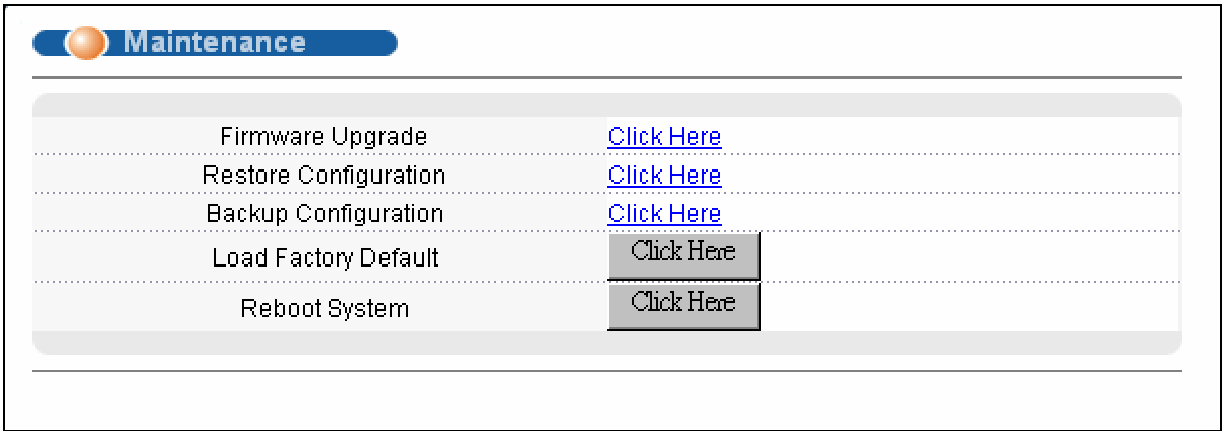
Out-of-band Management IP Address:
IP Address: 192.168.0.1
IP Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0

### Is Online Help available on the Web Configurator?

Yes, the Web Configurator's Online Help is available. Clicking on the Help link will bring up a description of the online help of that screen.

### How to restart device from Web?

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



Maintenance

| | |
|---|---|
| Firmware Upgrade | Click Here |
| Restore Configuration | Click Here |
| Backup Configuration | Click Here |
| Load Factory Default | Click Here |
| Reboot System | Click Here |

2. Click on the "Click Here" button next to the Reboot System will restart the Switch.

### How to check the current running firmware version?

From console, issuing a command, "show system-information" will return the information of the firmware version installed on the switch.

### Is the mini GBIC transceiver hot-swappable?

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

### What is so called "Dual-Personality interface" in Ethernet Switching?

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