ZyXEL ES-3100 Series

(ES-3124/ES-3124PWR/ES-3148/ES-3124-4F)

Ethernet Switch

Support Notes

Version 3.60 September 2006



INDEX

How to manage & maintain your Switch?

Firmware Upgrade Restore a Configuration File Backing Up a Configuration File Load Factory Defaults

Physical Switch connection

Connecting two switches via Fiber Channel

General Networking

DHCP option 82 (Relay Agent Information Option)

Separating a physical network into many virtual networks

Introduction to Virtual LAN Port Based Virtual LAN Setting up Port Based VLAN IEEE 802.1Q Tag-based VLAN Setting up Tag-based VLAN Setting up VLAN Trunking How to configure GVRP

IP Multicasting

IGMP Snooping Multicast VLAN Registration (MVR)

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

Introduction to Spanning Tree Protocol How does Spanning Tree Protocol Work?

Switching security

MAC freeze Setting up 802.1x Radius Authentication Classifier & Policy Rule (ACL)

Centralized Management

Introduction of SNMPc and NetAtlas *NetAtlas v1.00 supported ES-3124 / ES-3124PWR *NetAtlas v1.03 and newer releases will support ES-3148 and some new features with ES-3124/ ES-3124PWR Cluster Management -- iStacking Remote Monitoring (RMON)

<u>FAQ</u>

What is the default setting of the IP parameters? 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:

<u>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.</u>

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.

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	<u>Maintenance</u>
To upgrade the internal switch firmware, browse to the location of the binary button.	(.BIN) file and click Apply
File Path Browse	
Upgrade	

- 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.

🔵 Re	store Configuration Maintenance
To restore t Restore but	the device's configuration form a file, browse to the location of the configuration file and click tton.
File Path	Browse
	Restore

- 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.

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	<u>Maintenance</u>
This page allows you to back up the device's current configuration to your v Backup button.	vorkstation. Now click the
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.

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?".



- 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:

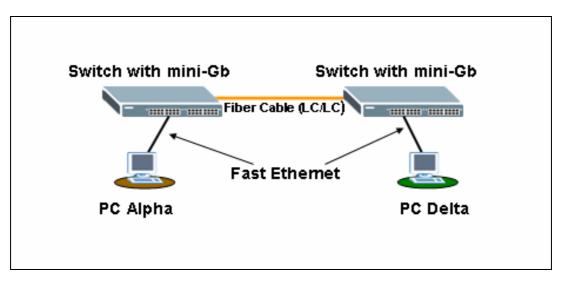
- 1. Connect to the console port and open the Terminal Emulation Software.
- Type in the correct password to bring up the prompt.
 Type "erase run" to load the factory default configurations.

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.

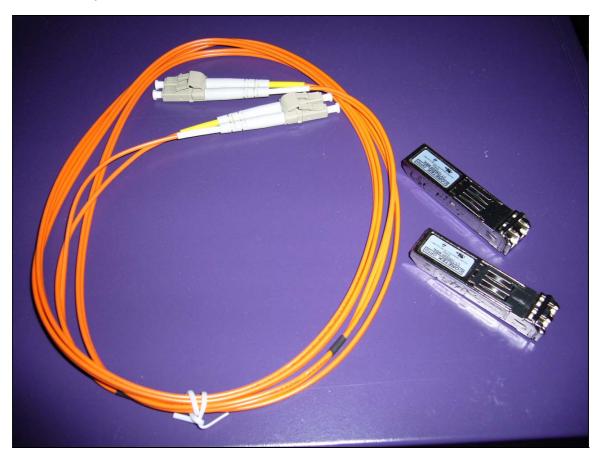
Scenario



In this scenario, two Switch with mini-Gb port connected together via its mini-GB Port with a LC/LC Fiber cable (62.5/125MM). PC "Alpha" is connected to the Switch on the left and another PC "Delta" is connected to the Switch on the right via the RJ45 Port (Cat 5 cable).

What you need here to complete this scenario:

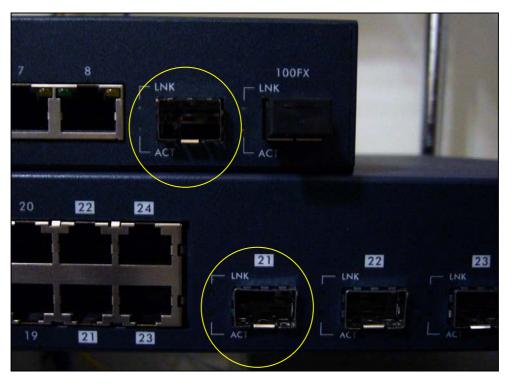
•	ZyXEL Switch with Mini-GB port	<u>x2</u>
	(note: Each ES-3100 Series Switch of	comes with 2 Mini-GB Port)
•	SFP-SX Transceiver	<u>x2</u>
•	LC/LC Fiber Cable (62.5/125MM)	x1



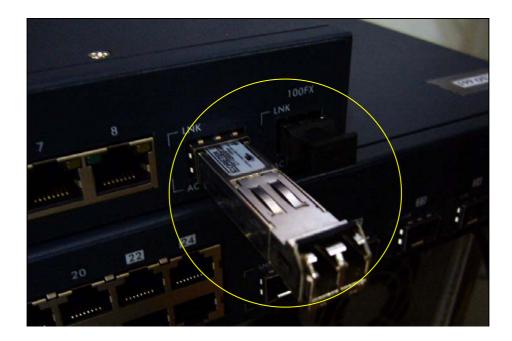
Here is the photo of the SFP-SX Transceiver & the LC/LC Fiber Cable.

Steps to complete this scenario

1. Find both Mini-GB ports on your Switch first.



2. Get one transceiver and plug it into the Mini-GB Port of your Switch



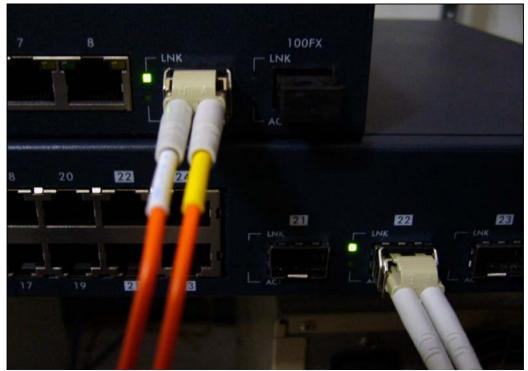
3. Plug another transceiver into the Mini-GB Port of the other Switch



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



5. Plug the LC/LC Fiber Cable into the transceivers on both Switch.



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

- 6. Now, connect the first PC "Alpha" to the Switch on the left and the second PC "Delta" to the Switch on the right via the regular Ethernet cable.
- 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)
- 8. 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
```

9. 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:

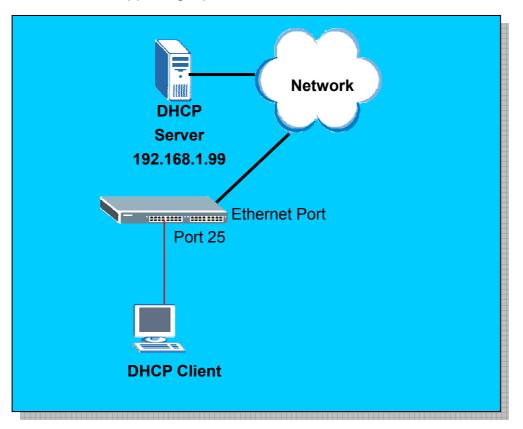
Minimum = 5ms, Maximum = 28ms, Average = 11ms
```

10. Now you can confirm that the network connection between these two Switch 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 <u>READ ONLY</u> here and it is the same as the host name of the Switch.

8.1.99
ion 82
3-3012
-

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".

🛪 Incognito Management Console			
<u>File Edit Service View Import Export Wi</u>	zards <u>T</u> ools <u>R</u> eports Help		
	🗈 - 🔍 🔇 🦻		
P Connect New Service P Con	nmander		
IP Commander / Client Revision Copyright c 199 Incognito Softw	8 - 2004		
			; 🖮 🛛 🗘
🛃 開始 🚺 🐚 temp	Doc1 - Microsoft Word	🧠 Incognito Managemen	 33 33

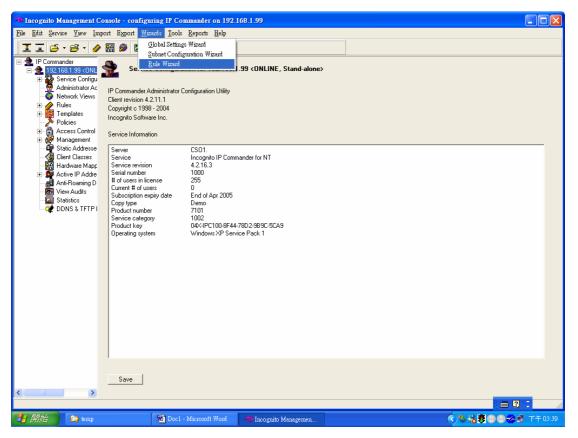
Input the DHCP IP address or domain name and click "ok". Our IP is 192.168.1.99.

🤿 Incognito M	lanagement Console				
<u>File E</u> dit Serv	ice <u>V</u> iew <u>I</u> mport E <u>x</u> port <u>W</u>	izards <u>T</u> ools <u>R</u> eports <u>H</u> elp			
IIG	• 🕼 • 🍙 🔚 🏚 🖾	🖹 - 🔍 🤄 🦻			
	ander 🔬 IP Co	mmander Administrator Configuration Utility 4.2.11.1 38 - 2004 vare Inc. Select Server	name of the server with the IP Commander a age: OK	Service you Cancel	
🐉 開始	🐢 Incognito Managemen	📓 文件1 - Microsoft Word			📢 🛃 🍓 🛃 🛞 🌺 🛞 🥪 下午 03:28

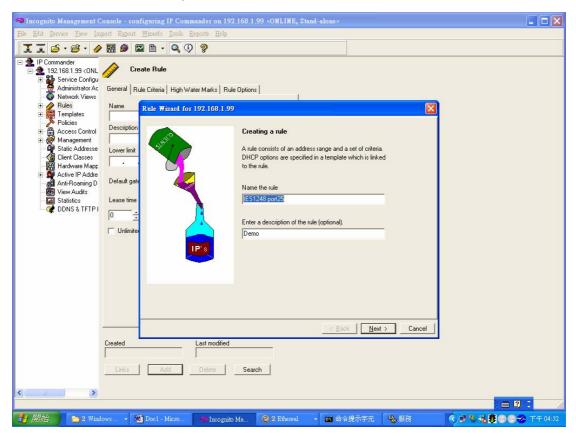
Input user name and password. The default user name is "administrator" and password is "incognito".

🦈 Incognito M	anagement (Console						
<u>File E</u> dit Servi	ce <u>V</u> iew <u>I</u> r	nport Export <u>W</u> izards <u>T</u> ool	s <u>R</u> eports <u>H</u> elp					
IIG	• 🖾 • 🖌	• 🖬 🌒 🗖 🖻 • 🔍	٩ 🦻					
- 2 IP Comma		IP Commander Administrator Client Revision 4.2.11.1 Copyright c 1998 - 2004 Incognito Software Inc.	Configuration Utility	sing an IP Commander ser t a Winnt or Unix user acc	vice administrat	tor account on		
🦺 開始 💧	🔄 temp	Doc1	- Microsoft Word	👒 Incognito Manage	men		<	👌 🗾 下午 03:38

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".

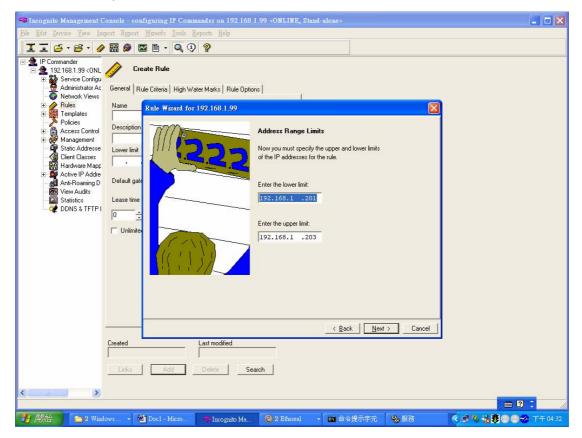


Give a name and description to the new rule.



All contents copyright (c) 2006 ZyXEL Communications Corporation.

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.



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

🛪 Incognito Management Console - configuring IP Commander on 192.168.1.99	
Eile Edit Service Yiew Import Export Wizards Icols Reports Help	
II 🖆 · 🖆 · 🔌 🎛 🌌 🖹 · 🔍 🤄 💡	
Promoved in the initial and in the initial and in the initial and in the initial and i	
Save	
🔰 🎆 🏠 🍃 temp 📓 Docl - Microsoft Word 👒 Incognito Managemen	() 14 ···································

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.

🛪 Incognito Management Console - configuring IP Commander on 192.168.1.99 <online, stand-alone=""></online,>	
Ele Edit Service Yiew Import Export Wizards Icols Reports Help	
II 🖆 · 🗃 · 🖉 🗃 🛍 🖿 · 🔍 🕄 💡	
I 12: 103. 139 (ONL) Create Rule Interview Interview	
< >	
📑 開始 📄 2 Windows • 📓 Docl - Micro 👒 Incognito Ma 😮 2 Ethereal 🔹 前令提示字元 👒 服務 🔍 🕫 修 🦂 👰 🛞 🛞	🌽 下午 04:34

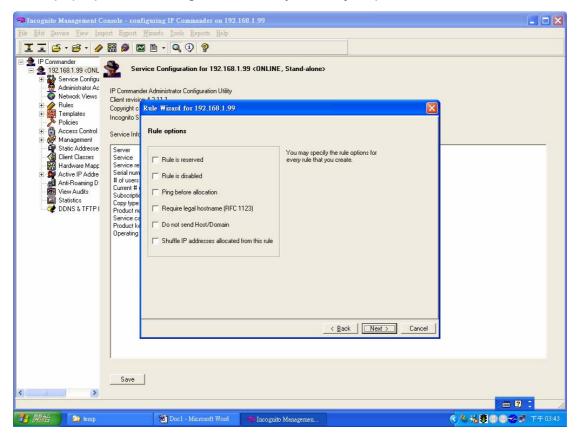
After you finish above step, you will see the following figure.

🛪 Incognito Management C	ionsole - confi	guring IP Comn	ander on 192.16	58.1.99 <online, s<="" th=""><th>Stand-alone></th><th></th><th></th></online,>	Stand-alone>		
<u>File Edit Service View Im</u>	port E <u>xp</u> ort <u>W</u>	<u> I</u> izards <u>T</u> ools <u>R</u>	eports <u>H</u> elp				
II 6 · 6 · 🤌	🔛 🔗 🖾	🖻 • 🔍 🤅	2				
IP Commander IP Commander IP 2168 1.39 (ONL Service Configu Administrator Ac Network Views P Rules P Rul	General Rule	te Rule Criteria High Wa Crite Wizard for Create the m Select rule crit in the operator Keywords: DHCP Option Rule criteria	ter Marks Rule Op 192.168.1.99 ule criteria eria from the keywor s list. Use paranthes	ds list, and link them us les to specify the order Operators:			
	Created Links	Add	Last modified	Search	<u>sack</u>	Next > Cancel	
							:
🐉 開始 🔰 🛅 2 Wind	lows 🔸 🔟	Doc1 - Micro	🤫 Incognito Ma	🙆 2 Ethereal	- 🔹 命令提示	字元 🧠 服務	🔇 🖻 🌯 👬 🕃 💿 💿 🥪 下午 04:34

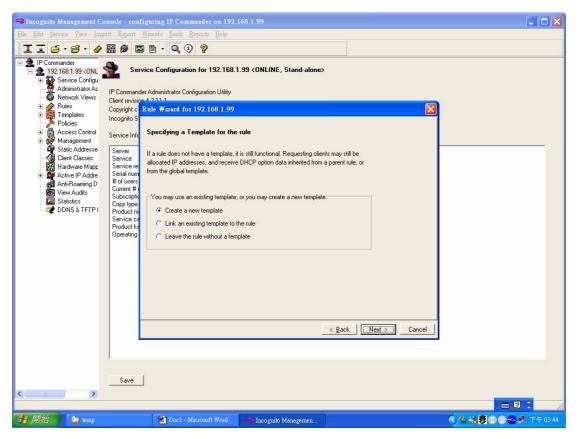
All contents copyright (c) 2006 ZyXEL Communications Corporation.



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



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



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

🛪 Incognito Management Console - configuring IP Commander on 192.168.1.99	
Eile Edit Service View Import Export Wizards Tools Reports Help	
II 🖆 • 🚔 • 🔌 🖼 🕬 🖾 🖹 • 🔍 🔇 💡	
P Commander 1921881.139 (CNL Administrator AA Administrator A Network Views Ruds Templates Policies Access Control Access Control Access Control Access Control Access Control Service Inc Service Service Inc Service Inc Service Inc Service In	
Save	
🛃 🕅 🏠 😰 temp 🛛 🕲 Docl - Microsoft Word 🔷 Incognito Managemen) 🌭 🍓 🖲 💿 🥪 🕑 下午 03:44

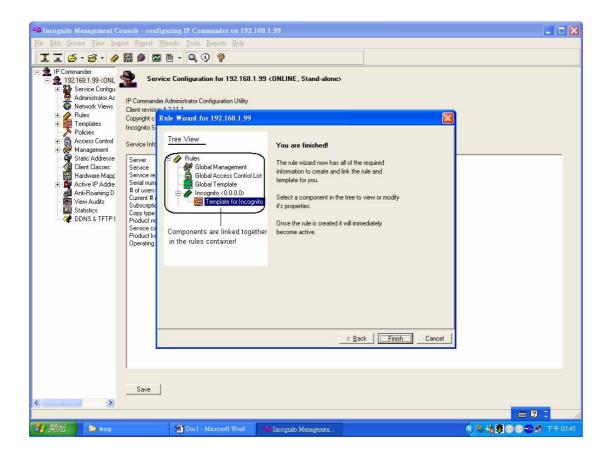
All contents copyright (c) 2006 ZyXEL Communications Corporation.



You can apply DDNS service to DHCP server or not.

🖘 Incognito Management Consol	- configuring IP Commander on 192.168.1.99	
<u>File Edit Service View Import I</u>	ixport <u>Wizards Iools Reports H</u> elp	
II 6 · 6 · 🔗 🖼	🔎 🖾 🖻 - 🔍 🔇 🦻	
Network Views Clier Pules Construction Pules Templates Incc Policies Construct Policies Ser Static Addresse Se Static Addresse Se Anti-Roaming D L Active IP Addre Se Statis Addresse Se Anti-Roaming D L C Statis C Statis C Statis C Ser Se	Service Configuration for 192.168.1.99 <online, stand-alone=""> ommander Administrator Configuration Utility trevision 4.2111 revision 4.211 revis</online,>	
	Save	
× >		
🦺 開始 🛛 🐚 temp	🐻 Docl - Microsoft Word 🛛 👒 Incognito Managemen	🔇 🌯 🝓 🕄 🕲 🥪 🔊 🏹 T 🕂 03:44

The rule creation has been finished.



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.

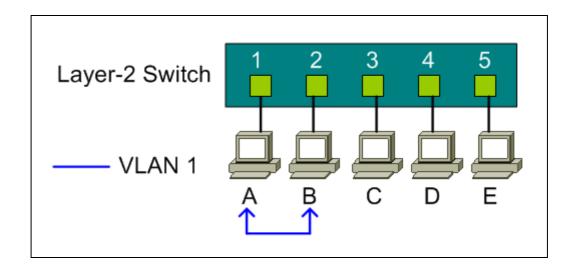
There are two most popular VLAN implementations, Port-based VLAN and IEEE 802.1q Tagged VLAN. ES-3100 series supports both VLAN implementations. The most difference between both VLAN implementations is Tagged VLAN can across Layer-2 switch but Port-based VLAN cannot.

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.

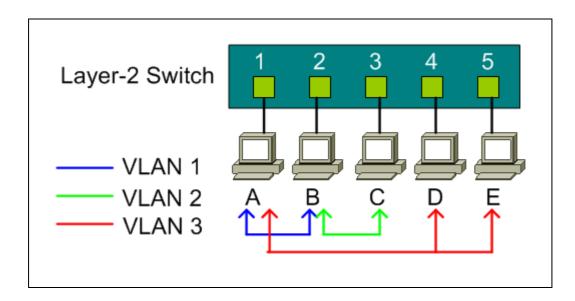
Case 1: Host A and Host B can talk to each other, because they are in the same VLAN group. But Host A and Host B can't talk to Host C, D, and E.



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.

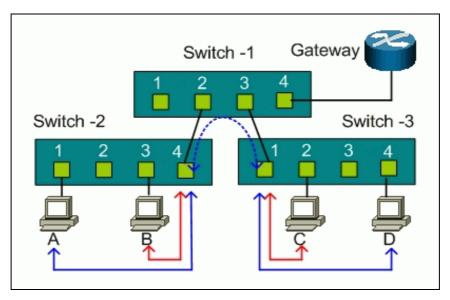


Port-based VLAN definition:

- 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.

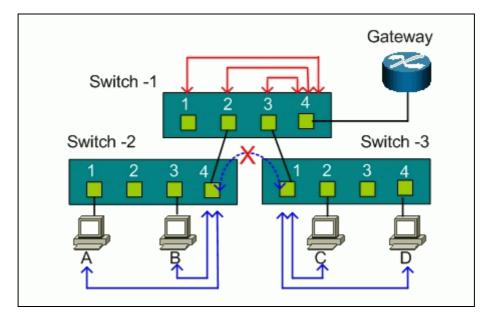
- Switch-2 VLAN 1 member port: port 1 and port 4
- Switch-2 VLAN 2 member port: port 2 and port 4
- Switch-2 VLAN 3 member port: port 3 and port 4

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.



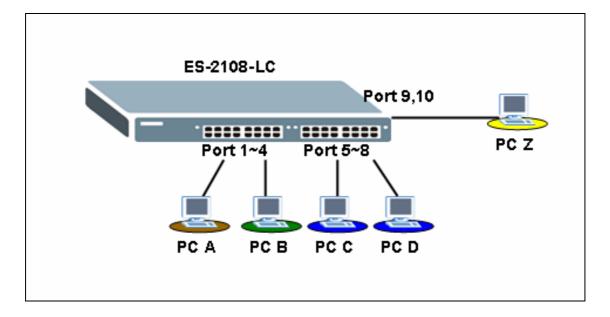
For Switch-1, port 1, port2, and port 3 are allowed to communicate back and forth with uplink port 4, but not with other ports.

- 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 <u>http://192.168.1.1</u> 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.

MENU										
Basic Setting		Status								
Advanced Application	-	Up Time: 22:35:		0110110100			in the second			
P Application	Port	Link	State	LACP	TxPkts	RxPkts		Tx KB/s		
Aanagement	1	100M/F	FORWARDING	Disabled	3313	4581	0	0.0	0.0	22:2
nanagement	2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	3	Down	STOP	Disabled		0	0	0.0	0.0	0:00
	4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	<u>6</u>	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	<u>7</u>	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	8	Down	STOP	Disabled	U	0	0	0.0	0.0	0:00
	<u>9</u>	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	<u>10</u>	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00
	Poll Inte	erval(s) 40	Set Interval	Stop						

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.

ZyXEL					
					🖻 Status 🗎 Lo
Basic Setting	🔿 🔘 Switch Setup				
Advanced Application P Application	VLAN Type	 802.1Q Port Based 	>		
Management	IGMP Snooping	Active			
	MAC Address Learning	Aging Time	300	seconds	
System Info		Join Timer	200	milliseconds	
General Setup Switch Setup	GARP Timer	Leave Timer	600	milliseconds	
IP Setup		Leave All Timer	10000	milliseconds	
Port Setup	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.

ZyXEL													
												6	🛿 Status 🗎 Logout 🖬 Help
MENU Basic Setting													
Advanced Application		Sett	ing Wiza	ard	Port is	olation	~	App	dy				
IP Application	1												
Management			_					Incomi	ng			-	_
		/	1	2	3	4	5	6	7	B	9	10	
VLAN Static MAC Forwarding		1		~		V							1
Filtering		2	V	~		V							2
Spanning Tree Protocol		3	V	~		V							3
Bandwidth Control Broadcast Storm Control		4	V	~	V	V							4
Mirroring		5					V						5
Link Aggregation	Outgoing	б						v	V				б
Port Authentication		1						~		~	V	~	7
Port Security Queuing Method		В						~	V	~	V	V	В
watering wethod	$\langle \rangle$	9				V		~	V	~	V		9
	\sim	10				V		~	v	~	V	V	10
	\sim	CPU		V		V		~	V	~	V	V	CPU
	\langle		1	2	3	4	s	б	7	B	9	10	
		1											
								Apply	Cancel)	_	/	
													© Copyright 1995-2005 by ZyXEL Comm

- 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).

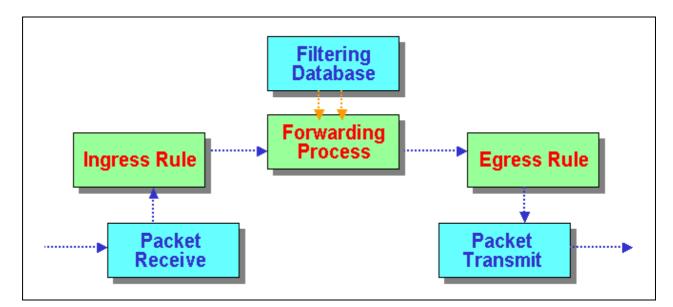
6 bytes	6 bytes	2 byt	es		variable			
Dest.	Src.	Length /	Туре		Data		Stand	lard frame
•			·····		·····			
Dest.	Src.	TPID	тсі	L /	т	Data		Tagged frame
		2 bytes			*******			I
			Priority		VID			
			3 bits	1 bit	12 bits			

- **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 (2³) 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.

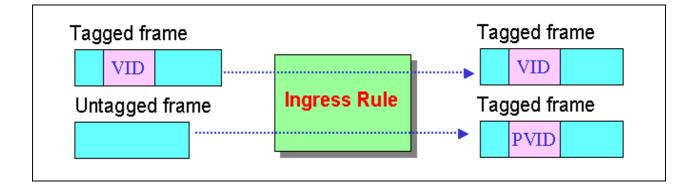


1. Ingress Process:

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	<u>Normal</u>	UnTag
20	1	Fixed	Tag
20	5	Fixed	UnTag

Filtering Database

VID	Egress Port
10	1
10	2
20	3

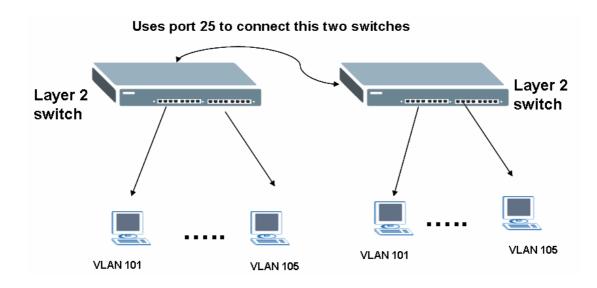
Dynamic VLAN (DVLAN) table

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
I	1	U	U	U	U	U	U	U	U	U	U	U	U	U	0.01.49	otatit
2	101	U	-	-	-	-	-	-	-	-	-	-	-	-	0:01:49	Static
2	101	U	U	-	-	-	-	-	-	-	-	-	-	-	0.01.49	otatic
3	102	-	U	U	-	-	-	-	-	-	-	-	-	-	0:01:49	Static
J	102	-	-	U	-	-	-	-	-	-	-	-	-	-	0.01.43	Static
4	103	-	-	-	U	U	-	-	-	-	-	-	-	-	0:01:49	Static
4	103	-	-	-	U	U	-	-	-	-	-	-	-	-	0.01.45	otatic
5	104	-	-	-	-	-	-	-	-	-	-	-	U	-	0:01:49	Static
5	104	-	-	-	-	-	-	-	-	-	-	-	U	-	0.01.49	otatic
6	105	-	-	-	-	-	U	U	-	-	-	-	-	-	0:01:49	Static
U	105	-	-	-	-	-	U	U	-	-	-	-	-	-	0.01.49	Static
7	106	-	-	-	-	-	-	-	U	-	-	-	-	-	0:01:49	Static
(100	-	-	-	-	-	-	-	U	U	-	-	-	-	0.01.49	otatic
8	107	-	-	-	-	-	-	-	-	U	U	-	-	-	0:01:48	Static
0	107	-	-	-	-	-	-	-	-	-	U	U	-	-	0.01.40	Static

2. Configuration of VLAN on switch B

+ Number Of VLAN = 6

							Por	t Num	iber							
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	0:02:25	Static
1		U	U	U	U	U	U	U	U	U	U	U	U	U	0.02.23	Jtalit
2	101	U	U	-	-	-	-	-	-	-	-	-	-	-	0:02:25	Static
2	101	U	U	U	-	-	-	-	-	-	-	-	-	-	0.02.25	otatit
3	102	-	-	U	U	U	-	-	-	-	-	-	-	-	0:02:25	Static
3	102	-	-	-	U	U	-	-	-	-	-	-	-	-	0.02.25	Static
4	103	-	-	-	-	-	U	U	-	-	-	-	-	-	0:02:25	Static
4	103	-	-	-	-	-	U	U	-	-	-	-	-	-	0.02.25	Static
5	104	-	-	-	-	-	-	-	U	U	-	-	-	-	0:02:25	Static
U	104	-	-	-	-	-	-	-	U	U	-	-	-	-	0.02.25	atatic
6	105	-	-	-	-	-	-	-	-	-	U	U	-	-	0:02:25	Static
0	105	105 -	-	-	-	-	-	-	-	-	U	U	U	-	0.02.25	Static

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")

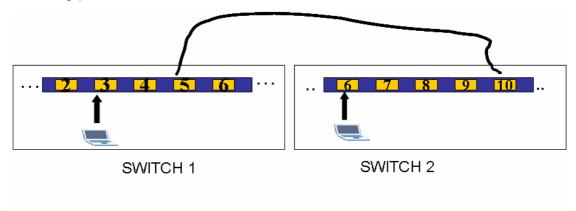
VID:102 (port 6,7,8,9,10,"25 TAG") VID:103 (port 11,12,13,14,"25 TAG") VID:104 (port 15,16,17,18,"25 TAG") VID:105 (port 19,20,21,23,22"25 TAG) Clients in same VLAN on both switches can communicate each other. PVID:

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

Set PVID on switch 2: Port 1, 2, 3, 4 : <u>101</u> Port 6, 7, 8, 9, 10, : <u>102</u> Port 11, 12, 13, 14, : <u>103</u> Port 15, 16, 17, 18: <u>104</u> Port 19, 20, 21, 22, 23: <u>105</u> 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:

VLA	in Fort Setting				VLAN Status
	GVRP				
P	ort 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

O VLA	N Port Setting				VLAN Status
	GVRP				
Р	ort 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	Π

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

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

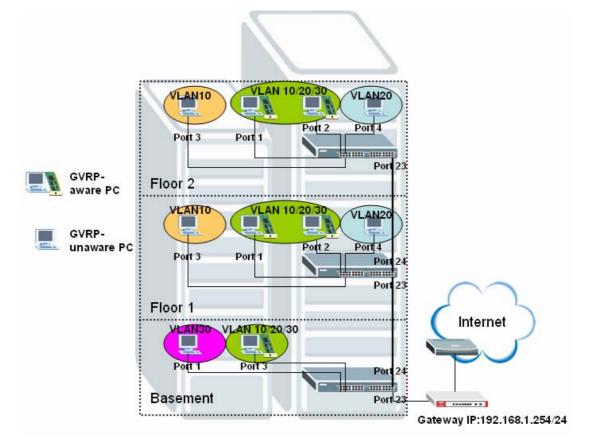
The switch 1 IP address: 192.168.1.31

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.

C:\WINDOWS\System32\cmd.exe - ping 192.168.1.21 -t	
Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms 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	-

How to configure GVRP?



Description:

In this scenario, PCs belong to different divisions within a single corporation can not communicate with each other, and we leave some ports of switches for GVRP-aware PC and others for VLAN-unaware PC. So network administrator can manage and configure VLAN smartly based on different devices and requirements. For switches on floor 1 and 2, PC connecting to port 3 joins VLAN 10 statically; PC connecting to port 4 joins VLAN 20 statically; and PCs connecting to port 1&2 can join VLAN 10/20/30 which determined by its configuration on GVRP-aware NIC dynamically. For switch on basement, PC connecting to port 1 joins VLAN 30 while PC connecting to port 3 can join VLAN10/20/30 dynamically. Please Note: all clients connecting to switches in this scenario should be located in the same subnet (in this example, the subnet is 192.168.1.0/24)

How to configure this scenario:

1. For Switch A on Floor 2:

Please enter VLAN setting under Advanced Application menu and click "static VLAN" to bring up the following screen, adding VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging".

					🖬 Status 🗎 Logo	ut 🛿 Help
MENU Basic Setting	🔵 Static	VLAN			VLAN Status	
Advanced Application		ACTIVE				
Routing Protocol				VLAN 10		
Management		Name				
		VLAN Group ID		10		
VLAN						
Static MAC Forwarding	Port		Contro		Tagging	
Filtering	1	Normal	O Fixed	O Forbidden	Tx Tagging	
Spanning Tree Protocol	2	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Bandwidth Control	- 3	Normal	Fixed	O Forbidden	Tx Tagging	
Broadcast Storm Control	4	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Mirroring	5	Normal	O Fixed	O Forbidden	Tx Tagging	
Link Aggregation	ĥ	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Port Authentication	7	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Port Security DHCP	8	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Access Control	9	 Normal 	O Fixed	O Forbidden	Tx Tagging	
DiffServ	10	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Queuing Method	11	 Normal 	O Fixed	O Forbidden	Tx Tagging	
VRRP	12	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	13	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	14	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	15	 Normal 	Fixed	O Forbidden	Tx Tagging	

Add VLAN 20 to this switch, VLAN 20: port 4, fixed, untag; port 23, fixed, Tx tagging.

					🖬 Status 🗎 Log	jout 🛿 Help
MENU Basic Setting	🔘 Static	VLAN			VLAN Status	
Advanced Application				_		
Routing Protocol		ACTIVE				
Vanagement		Name		VLAN 20		
management		VLAN Group ID		20		
VLAN	Devit		01		The second second	
Static MAC Forwarding	Port	-	Contro		Tagging	
Filtering Spanning Tree Protocol	1	Normal	O Fixed	O Forbidden	Tx Tagging	
Bandwidth Control	2	Normal	Fixed	O Forbidden	Tx Tagging	
Broadcast Storm Control	3	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Mirroring	4	🔘 Normal	💿 Fixed	🔘 Forbidden	Tx Tagging	
Link Aggregation	5	💿 Normal	🔘 Fixed	🔘 Forbidden	💌 Tx Tagging	
Port Authentication	6	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Port Security	7	Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
DHCP	8	Normal	Fixed	Forbidden	Tx Tagging	
Access Control	9	Normal	Fixed	O Forbidden	Tx Tagging	
DiffServ	10	 Normal 	O Fixed	O Forbidden	V Tx Tagging	
Queuing Method	11	 Normal 	O Fixed	O Forbidden	Tx Tagging	
VRRP	12	Normal	O Fixed	O Forbidden	Tx Tagging	
	13	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	14	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	14	 Normal Normal 	Fixed	O Forbidden	Tx Tagging	

Please click VLAN port setting to bring up the following screen, setup **PVID 10** for port 3, **PVID 20** for port 4, and enable GVRP on the top of the screen and port 1, port 2, port 23.

							🖸 Status 🗎 Logou	: 🛛 Help
MENU Basic Setting		N Port Settin	q				VLAN Status	
Advanced Application		OVRP						
Routing Protocol			V					
Management	F	ort isolation						
VLAN	Port	Ingress Chec	k PVID	GVRP	Acceptable	Frame Type	VLAN Trunking	
Static MAC Forwarding	1		1	Image: A start of the start	All	*		
Filtering	2		1		All	~		
Spanning Tree Protocol	3		10		All	~		
Bandwidth Control			20		All			
Broadcast Storm Control	4		20			*		
Mirroring	5		1		All	~		
Link Aggregation	6		1		All	~		
Port Authentication	7		1		All	~		
Port Security			1		All	~		
DHCP Access Control	8		1					
DiffServ	9		1		All	*		
Queuing Method	10		1		All	*		
VRRP	11		1		All	*		
	12		1		All	*		
	13		1		All	~		
	14		1		All	~		

2. For Switch B on Floor 1:

Please follow the same steps to adding VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging; port 24, fixed, Tx tagging".

ZyXEL						
MENU					🖾 Status 🗎 Logout	: 2 Help
Basic Setting	🔵 🌖 Static	VLAN			VLAN Status	
Advanced Application		ACTIVE		v		
Routing Protocol		Name		VLAN 10		
Management						
		VLAN Group ID		10		
VLAN						
Static MAC Forwarding	Port		Contro	bl	Tagging	
Filtering	1	Normal	O Fixed	O Forbidden	Tx Tagging	
Spanning Tree Protocol	2	Normal	O Fixed	O Forbidden	Tx Tagging	
Bandwidth Control	3	O Normal	Fixed	O Forbidden	Tx Tagging	
Broadcast Storm Control	4	Normal	O Fixed	Forbidden	Tx Tagging	
Mirroring	5	 Normal 	Fixed	O Forbidden	Tx Tagging	
Link Aggregation	6	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Port Authentication Port Security	7	 Normal 	O Fixed	O Forbidden	Tx Tagging	
DHCP	8	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Access Control	9	 Normal 	O Fixed	O Forbidden	Tx Tagging	
DiffServ	10	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Queuing Method	11	 Normal 	O Fixed	O Forbidden	Tx Tagging	
VRRP	12	Normal	O Fixed	O Forbidden	Tx Tagging	
	13	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	14	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	15	 Normal 	Fixed	O Forbidden	Tx Tagging	
	1.		~ Tixed			

Add VLAN 20 to this switch, VLAN 20: port 4, fixed, untag; port 23, fixed, Tx tagging; port 24, fixed, Tx tagging.

					Status	🛾 🛛 Logout 🖻 Help	
MENU							
Basic Setting	🔵 Statio	: VLAN			VLAN Status		
Advanced Application		ACTIVE					
Routing Protocol		Name		VLAN 20			
Management							
		VLAN Group ID		20			
VLAN							
Static MAC Forwarding	Port		Contro	d	Tagging		
Filtering	1	Normal	O Fixed	O Forbidden	Tx Tagging		
Spanning Tree Protocol	2	 Normal 	O Fixed	O Forbidden	Tx Tagging		
Bandwidth Control	- 3	 Normal 	O Fixed	O Forbidden	Tx Tagging		
Broadcast Storm Control		Normal	Fixed	O Forbidden	Tx Tagging		
Mirroring	5	 Normal 	O Fixed	O Forbidden	Tx Tagging		
Link Aggregation	5 6	 Normal 	O Fixed	O Forbidden	Tx Tagging		
Port Authentication	7	 Normal 	O Fixed	O Forbidden	Tx Tagging		
Port Security DHCP		 Normal 	O Fixed	O Forbidden	Tx Tagging		
Access Control	9	 Normal 	Fixed	Forbidden	Tx Tagging		
DiffServ	10	 Normal 	Fixed	O Forbidden	Tx Tagging		
Queuing Method	10	 Normal 	Fixed	O Forbidden	Tx Tagging		
VRRP	12	 Normal Normal 	Fixed	Forbidden			
	12	 Normal Normal 	Fixed	O Forbidden	Tx Tagging		
	13		Fixed	O Forbidden	Tx Tagging		
		Normal			Tx Tagging		
	15	 Normal 	O Fixed	O Forbidden	🗹 Tx Tagging		

Please click VLAN port setting to bring up the following screen, setup **PVID 10** for port 3, **PVID 20** for port 4, and enable GVRP on the top of the screen and port 1, port 2, port 23, port 24.

ZyXEL								-
IENU							🖬 Status 🛢 Logout	2 Help
Basic Setting	🔿 VLA	N Port Setting	a 🔹				VLAN Status	
Advanced Application		GVRP						
Routing Protocol		Port isolation						
- Nanagement	- F	onisolation						
VLAN	Port	Ingress Check	C PVID	GVRP	Acceptable I	Frame Type	VLAN Trunking	
Static MAC Forwarding	1		1		All	*		
Filtering	2		1		All	~		
Spanning Tree Protocol	3		10		All	~		
Bandwidth Control			20		 All			
Broadcast Storm Control	4		20			*		
Mirroring	5		1		All	*		
Link Aggregation	6		1		All	*		
Port Authentication	7		1		All	~		
Port Security	8		1		All	~		
DHCP Access Control			-					
DiffServ	9		1		All	*		
Queuing Method	10		1		All	*		
VRRP	11		1		All	*		
	12		1		All	~		
	13		1		All	~		
	14		1		All	~		

3. For Switch C on Basement:

Please set static VLAN 10: port 23, fixed, untag.

ZyXEL					🖾 Status 🗎 Logou	t 🖬 Help
MENU Basic Setting	C (a) Stati	e VLAN			VLAN Status	
Advanced Application						
Routing Protocol		ACTIVE				
		Name		VLAN10		
flanagement		VLAN Group ID		10		
VLAN						
Static MAC Forwarding	Port		Control		Tagging	
Filtering	1	 Normal 	Fixed	O Forbidden	🗹 Tx Tagging	
Spanning Tree Protocol Bandwidth Control	2	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Bandwidth Control Broadcast Storm Control	3	📀 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Mirroring	4	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Link Aggregation	5	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Port Authentication	6	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Port Security	7	💿 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Access Control	8	📀 Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Queuing Method	9	Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging	
Classifier	10	Normal	Fixed	🔘 Forbidden	🗹 Tx Tagging	
Policy Rule	11	Normal	Fixed	🔘 Forbidden	🗹 Tx Tagging	
/LAN Stacking	12	Normal	O Fixed	🔘 Forbidden	🗹 Tx Tagging	
OHCP Relay	13	Normal	O Fixed	O Forbidden	Tx Tagging	
	14	Normal	Fixed	O Forbidden	Tx Tagging	
	15	 Normal 	O Fixed	O Forbidden	Tx Tagging	

Please set static VLAN 20: port 23, fixed, untag.

ZyXEL						
					🖸 Status	🖻 Logout 😰 Help
MENU Basic Setting	🔵 🔘 Stati	c VLAN			VLAN Status	
Advanced Application				_		
Routing Protocol		ACTIVE				
/lanagement		Name		VLAN20		
wanagement		VLAN Group II)	20		
VLAN						
Static MAC Forwarding	Port		Contro	1	Tagging	
Filtering	1	Normal	O Fixed	O Forbidden	🗹 Tx Tagging	
Spanning Tree Protocol	2	Normal	O Fixed	O Forbidden	Tx Tagging	
Bandwidth Control	3	Normal	O Fixed	O Forbidden	Tx Tagging	
Broadcast Storm Control	4	Normal	O Fixed	O Forbidden	Tx Tagging	
Mirroring	5	Normal	O Fixed	O Forbidden	Tx Tagging	
Link Aggregation	- 6	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Port Authentication Port Security	7	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Access Control	8	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Queuing Method	9	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Classifier	10	 Normal 	O Fixed	O Forbidden	Tx Tagging	
Policy Rule	11	 Normal 	O Fixed	O Forbidden	Tx Tagging	
VLAN Stacking	12	 Normal 	O Fixed	O Forbidden	Tx Tagging	
DHCP Relay	13	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	14	 Normal 	O Fixed	O Forbidden	Tx Tagging	
	15	 Normal 	O Fixed	O Forbidden	Tx Tagging	
			~ 10.60			

Please add VLAN 30: port 1, fixed, untag; port23, fixed, untag; port 24, fixed, Tx tagging.

VE

ZyXEL					🗟 Status	🛙 Logout 🖬 Help	
MENU Basic Setting	Statio	VLAN			VLAN Status		
Advanced Application Routing Protocol		ACTIVE		VLAN30			
Management		Name VLAN Group ID		30			
VLAN							
Static MAC Forwarding	Port		Contro	bl	Tagging		
Filtering	1	🔘 Normal	Fixed	🔘 Forbidden	Tx Tagging		
Spanning Tree Protocol	2	Normal	Fixed	🔘 Forbidden	🗹 Tx Tagging		
Bandwidth Control	3	Normal	🔘 Fixed	🔘 Forbidden	🗹 Tx Tagging		
Broadcast Storm Control	4	Normal	Fixed	🔘 Forbidden	🗹 Tx Tagging		
Mirroring	5	Normal	O Fixed	Forbidden	🗹 Tx Tagging		
Link Aggregation Port Authentication	6	Normal	Fixed	Forbidden	🗹 Tx Tagging		
Port Security	7	Normal	O Fixed	O Forbidden	✓ Tx Tagging		
DHCP	8	Normal	O Fixed	O Forbidden	Tx Tagging		
Access Control	9	Normal	O Fixed	O Forbidden	Tx Tagging		
DiffServ	10	Normal	O Fixed	O Forbidden	Tx Tagging		
Queuing Method	11	Normal	Fixed	O Forbidden	Tx Tagging		
VRRP	12	Normal	O Fixed	O Forbidden	Tx Tagging		
	13	 Normal 	O Fixed	O Forbidden	Tx Tagging		
	14	 Normal 	Fixed	O Forbidden	Tx Tagging		
	15	 Normal 	Fixed	O Forbidden	Tx Tagging		
	13						

Please setup PVID 30 for port 1 and enable GVRP on port 3 and port 24.

ZyXEL							🖻 Status 🗎 Logout	2 Help
IENU Jasic Setting	C 🌖 VLA	N Port Settir	ng 📄				VLAN Status	
dvanced Application		GVRP						
louting Protocol	F	Port isolation						
lanagement								
	Port	Ingress Chec	k PVID	GVRP	Acceptable I	Frame Type	VLAN Trunking	
/LAN	1		30		All	v		
Static MAC Forwarding	2		1		All	~		
Spanning Tree Protocol			1		All			
Bandwidth Control	3		1			*		
Broadcast Storm Control	4		1		All	*		
lirroring	5		1		All	*		
ink Aggregation	6		1		All	~		
Port Authentication	7		1		All	~		
Port Security			-		All	• •		
OHCP Access Control	8		1					
DiffServ	9		1		All	*		
Queuing Method	10		1		All	*		
/RRP	11		1		All	*		
	12		1		All	*		
	13		1		All	*		
	14		1	7	All	~		

Then, this scenario is done here.

IP Multicasting

How to setup IGMP snooping in your switch?

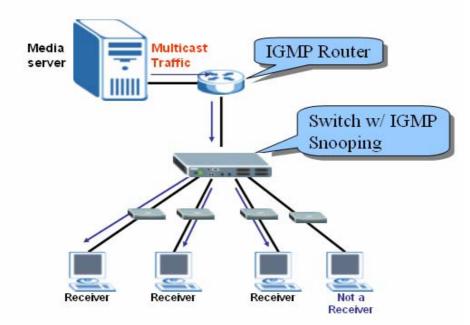


Figure 1: IGMP and IGMP snooping

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.

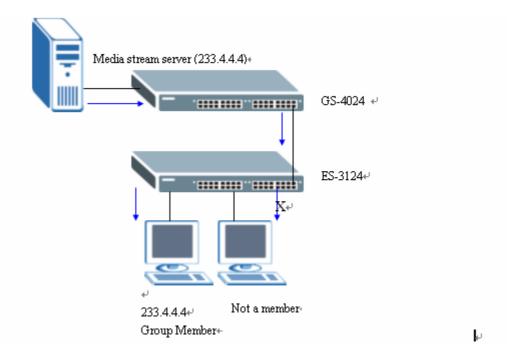


Figure 2: IGMP snooping Example

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

ZyXEL				🗈 Status 🖸 Logout 🖬 Helj
MENU Basic Setting Advanced Application IP Application	Active	2		
Management Static Routing	Index 1	Network 192.168.1.1/24	Version None	
RIP OSPF [OMP] DVMRP		Ар		
IP Multicast DiffServ DHCP &				
VRRP				

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

					🖬 Status	🗈 Logout	E He
Basic Setting	🔇 🍥 Switch Setup						
Advanced Application Routing Protocol	VLAN Type	● 802.1Q○ Port Based					
Management	IGMP Snooping	Active					
	MAC Address Learning	Aging Time	300	seconds			
System Info	GARP Timer	Join Timer	200	milliseconds			
General Setup		Leave Timer	600	milliseconds			
Switch Setup IP Setup		Leave All Timer	2000	milliseconds			
Port Setup	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.

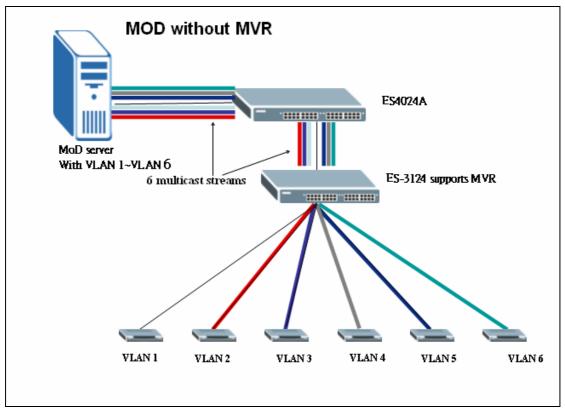
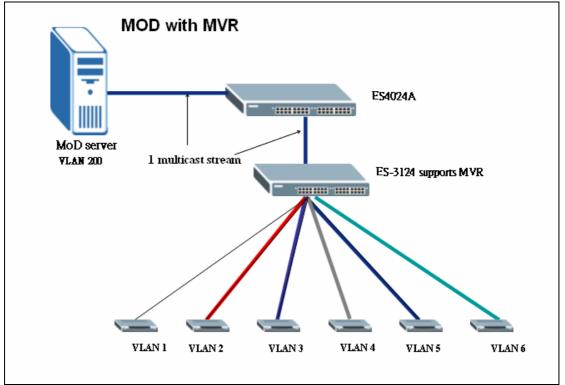


Figure 1





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.

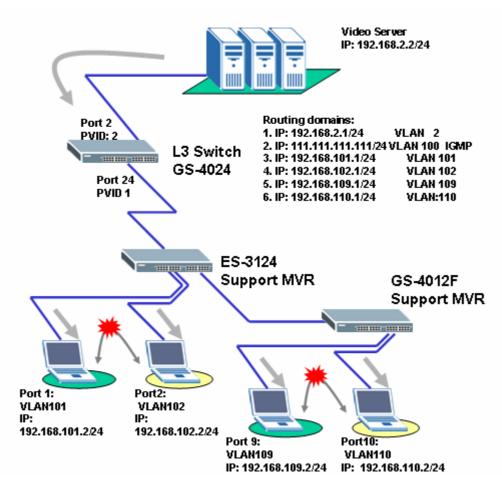
Immediate Leave Operation

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 media stream from the media servers will be transmitted from port 24 of GS-4024 (as an IGMP Router) to ES-3124 (L2 edge Switch) and GS-4012F.(work as L2 edge Switch). On Switch ES-3124 and GS4012F, we enabled the MVR function to allocate the multicast traffic from GS-4024 to separate VLAN hosts located on ES-3124 and GS-4012F. Moreover, we created a dummy ip interface for the multicast VLAN (VLAN100) on GS-4024. VLAN100 will be the Multicast VLAN in this scenario.

Illustration of this scenario



Static VLAN

Configuration via Web [GS-4024]

1. First of all, you need to create all those IP domains on the GS-4024 Switch. Once you completed those VLANs, your VLAN status should looks like the same as below.

VLAN Port Setting

🔵 🔘 VLAN Status
The Number Of VLAN = 7

							Port N	umbei	r						
Index	VID	2	4	6	8	10	12	14	16	18	20	22	24	Elapsed Time	Status
		1	3	5	7	9	11	13	15	17	19	21	23		
1	1	U	U	U	U	U	U	U	U	U	U	U	U	0:00:38	Static
	1	U	U	U	U	U	U	U	U	U	U	U	U	0.00.38	otatic
2	2	U	-	-	-	-	-	-	-	-	-	-	-	0:00:38	Static
2	2	-	-	-	-	-	-	-	-	-	-	-	-	0.00.30	
3	100	-	•	-	-	-	-	-	-	-	-	-	Т	0:00:37	Static
5	100	-	-	-	-	-	-	-	-	-	-	-	-	0.00.37	otatic
4	101	-	-	-	-	-	-	-	-	-	-	-	Т	0:00:37	Static
4	101	-	-	-	-	-	U	-	-	-	-	-	-	0.00.37	olalit
5	102	-	-	-	-	-	U	-	-	-	-	-	Т	0:00:37	Static
5	102	-	-	-	-	-	-	-	-	-	-	-	-	0.00.37	otatic
6	109	-	-	-	-	-	-	-	-	-	-	-	Т	0:00:37	Static
U	109	-	-	-	-	U	-	-	-	-	-	-	-	0.00.37	oldiit
7	110	-	-	-	-	U	-	-	-	-	-	-	Т	0:00:37	Static
(110	-		-	-		-	-	-	-	-	-	-	0:00:37	Static

2. Below are their related PVID settings.

🔵 VLA	N Port Setting				VLAN Status
	GVRP				
P	ort isolation				
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1		1		All 🗸	
2		2		All 🔽	
3		1		All 🗸	
4		1		All 🗸	
5		1		All 🗸	
6		1		All 🗸	
7		1		All 🗸	
8		1		All 🗸	
9		109		All 🗸	
10		110		All 🗸	
11		101		All 🗸	
12		102		All 🗸	
13		1		All 🔽	

3. Right after the VLAN, you should add the IP domains to the related VLANs.

Basic Setting	IP Address	192.168.0.1		
P Application	IP Subnet Mask	255.255.255.0		
Management	Default Gateway	0.0.0.0		
System Info General Setup Switch Setup		(Apply) Cancel		
IP Setup	P Interface			
Port Setup	IP Address	0.0.0.0		
	IP Subnet Mask	0.0.0.0		
	VID	Add) Cancel		
[VID Index IP Addr		VID	Delete
		ess IP Subnet Mask	VID 100	Delete
	Index IP Addr	ess IP Subnet Mask 11.111 255.255.255.0		
	Index IP Addr 1 111.111.1	IP Subnet Mask 11.111 255.255.255.0 3.1.1 255.255.265.0	100	
	Index IP Addi 1 111.111.1 2 192.16	IP Subnet Mask 11.111 255.255.265.0 3.1.1 255.255.265.0 3.2.1 255.255.265.0	100 1	
	Index IP Addit 1 111.111.1 2 192.16 3 192.16	IP Subnet Mask 11.111 255.255.255.0 3.1.1 255.255.255.0 3.2.1 255.255.255.0 101.1 255.255.255.0	100 1 2	
	Index IP Addr 1 111.111.1 2 192.16i 3 192.16i 4 192.16i	IP Subnet Mask 11.111 255.255.255.0 3.1.1 255.255.255.0 3.2.1 255.255.255.0 101.1 255.255.255.0 102.1 255.255.255.0	100 1 2 101	
	Index IP Addr 1 111.111.1 2 192.167 3 192.167 4 192.168 5 192.168	ess IP Subnet Mask 11.111 255.255.255.0 31.1 255.255.255.0 32.1 255.255.255.0 101.1 255.255.255.0 102.1 255.255.255.0 109.1 255.255.255.0	100 1 2 101 102	

4. Since this GS-4024 works as an IGMP Router, you need to enable IGMP V2 on the multicast ip interface (which is the dummy interface). Please notice that since GS-4024 works here as an IGMP Router, you cannot enable IGMP Snooping on the same time because IGMP Snooping is a L2 feature.

				🖸 Statu
C () IGMP				
0.45.4				
Active				
Index	Network	Version	1	
1	111.111.111.111/24	-		
2	192.168.1.1/24	None	~	
3	192.168.2.1/24	None	~	
4	192.168.101.1/24	None	*	
5		None	~	
			~	
		None	~	
	Active Index 1 2 3 4 5 6	Active ▼ Index Network 1 111.111.111.111/24 2 192.168.1.1/24 3 192.168.2.1/24 4 192.168.101.1/24 5 192.168.102.1/24	Index Network Version 1 111.111.111.111/24 IGMP-v2 2 192.168.1.1/24 None 3 192.168.2.1/24 None 4 192.168.101.1/24 None 5 192.168.102.1/24 None 6 192.168.109.1/24 None	Active Version 1 111.111.111.111/24 IGMP-v2 • 2 192.168.1.1/24 None • 3 192.168.2.1/24 None • 4 192.168.101.1/24 None • 5 192.168.102.1/24 None • 6 192.168.109.1/24 None •

Here we have done everything we need on the IGMP Router <GS-4024>.

Configuration via Web [ES-3124]

 At the very beginning, you can create your MVR VLAN First (which is VLAN100). To create this multicast VLAN, we do it in another way. First, access to the GUI of your Switch. Then click "Advanced Application" on the left and choose "Multicast". Finally, you should click MVR on the right frame to setup your Multicast VLAN.

					🖾 Status 🗎 Log	out 🛛 I
ENU asic Setting		Multicast Settir	Ig	Multicast S	Status IGMP Filtering Profile	MVR
dvanced Application		IGMP Sno	oping	Active 🔽		
outing Protocol		IGMP Site				
lanagement		Unknown Multi		Active	-	
		UNKNUWN MUIU	cast Frame	Uro	þ	
(LAN						
Static MAC Forwarding						
iltering	Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	
panning Tree Protocol	1			0	Default 😽	
andwidth Control	2			n	Default 🗸	
roadcast Storm Control						
irroring	3			0	Default 🚩	
ink Aggregation	4			0	Default 😽	
ort Authentication	5			0	Default 🔽	
ort Security	6			0	Default 🗸	
ccess Control	_					
ueuing Method	7			0	Default 💌	
lassifier	8			0	Default 🛩	
olicy Rule	9			0	Default 🗸	
LAN Stacking	10			<u> </u>	Default 🗸	
ulticast						
HCP Relay	11			0	Default 🛩	
	12			0	Default 🗸	

2. Give a name to this Multicast VLAN following by its VLAN ID. Active this VLAN; Pick port 1 and 2 as the receiver ports; Pick port 27 and 28 as the Source Port. In this scenario, we need to make the source ports remain the VLAN "tag". Thus, we come out the following setting. Click "add" to create this VLAN. When the VLAN is set, we keep going and click "Group Configuration" on the upper right corner to create our Multicast Groups.

		Multicast Setting	Group Configuration
Active	<u> </u>		
Name	100		
Multicast VLAN ID	100		
Mode	💿 Dynamic 🔘 Con	npatible	

Port	Source Port	Receiver Port	None	Tagging
1	0	۲	0	
2	0	۲	0	
3	0	0	۲	
4	0	0	۲	
5	0	0	۲	
6	0	0	۲	
7	0	0	۲	
27	۲	0	0	✓
28	۲	0	0	
		Add Cancel		

3. First of all, please choose the Multicast VLAN ID that we just created (which is VLAN100). Then give a name to this group, as long as you can understand. Place the range of Multicast groups here with the start address and End address. Finally, click "Add" to create this group. (In this scenario, we use 224.10.10.0 ~ 224.10.10.50)

🔇 🥥 Group Configuration		MVR
Multicast VLAN ID	100 💌	
Name	Start Address	End Address
224.10.10.0	224.10.10.0	224.10.10.50
	Add Cancel	

4. At this point we go back to the "Multicast Setting" page, enable "IGMP Snooping" here. (Since MVR needs IGMP Snooping). For Unknown Multicast Frame, we prefer "Drop" here in order to avoid any Multicast Video with no subscriber. (No body joining that multicast group). 7.VEI

ZyXEL						🖸 St	atus 🗎 Log	out 🖪
MENU		Multicast Settir			Multicast Status	ICMD Eilte	ring Profile	MVF
Basic Setting		Multicast Setti	<u>N</u>		Mutucast Status	TOWF FILE	IIIIg FIUIIIe	IVI V P
Advanced Application		IGMP Sno	oping	Active [✓			
Routing Protocol		IGMP Filte	ering	Active [
/lanagement		Unknown Multio	cast Frame	🔿 Floodii	ng 💿 Drop			
VLAN								_
Static MAC Forwarding								
Filtering	Port	Immed. Leave	Group Limited	Max Group	Num.	IGMP Filtering	-	
Spanning Tree Protocol	1			0		Default	*	
Bandwidth Control	2			0		Default	~	
Broadcast Storm Control	3			n		Default	~	
Mirroring	3			-			=	
Link Aggregation	4			0		Default	<u>×</u>	
Port Authentication	5			0		Default	*	
Port Security	6			0		Default	~	
Access Control								
Queuing Method	· · · · · · · · · · · · · · · · · · ·			U		Default	=	
Classifier	8			0		Default	*	
Policy Rule	9			0		Default	*	
/LAN Stacking	10			0	1	Default	~	
Multicast DHCP Relay	11			0		Default	=	
	12					Default	=	

5. Right after that you will need to create all other non-Multicast VLANs on this Switch. Once you completed those VLANs, your VLAN status should looks like the same as below.

Number 1	Status Of VLAN = 4									<u>VL</u>	<u>AN P</u>	ort Se	etting		5	Static VLAN	
								Port N	lumbe	er							
Index	VID	2	4	6	8	10	12	14	16	18	20	22	24	26	28	Elapsed Time	Status
		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	1:36:10	Static
I	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	1.30.10	otatit
2	100	U	-	-	-	-	-	-	-	-	-	-	-	-	Т	1:36:10	Other
2	100	U	-	-	-	-	-	-	-	-	-	-	-	-	Т	1.30.10	other
3	101	-	-	-	-	-	-	-	-	-	-	-	-	-	Т	1:36:10	Static
J	101	U	-	-	-	-	-	-	-	-	-	-	-	-	-	1.30.10	ordir
4	102	U	-	-	-	-	-	-	-	-	-	-	-	-	Т	1:36:10	Static
4	102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1.50.10	ordif

6. Below are their related PVID settings.

	GVRP				
F	Port isolation				
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunkin
1		101		All 💌	
2		102		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 🔽	
26		1		All 🖌	
27		1		All 🖌	
28		1		All 🔽	

Apply Cancel

Here we have done everything we need on the Edge Switch <ES-3124>.

Configuration via Web [GS-4012F]

 At the very beginning, you can create your MVR VLAN First (which is VLAN100). To create this multicast VLAN, we do it in another way. First, access to the GUI of your Switch. Then click "Advanced Application" on the left and choose "Multicast". Finally, you should click MVR on the right frame to setup your Multicast VLAN.

ZyXEL						ŵ	Status 🛙 Lo	gout 🛛
MENU Basic Setting		Multicast Settin	a	Multi	cast Status	IGMP F	Filtering Profile	MVR
Advanced Application								
IP Application		IGMP Sno	• •	Active 🗹				
		IGMP Filte	······	Active				
Management		Unknown Multio	cast Frame	🔘 Flooding 🧕) Drop			
VLAN								
Static MAC Forwarding	Port	Immed, Leave	Group Limited	Max Group Num.	IGMP Filtering	Drofilo	IGMP Querier	Mode
Filtering	FUIL	innineu. Leave	oroup Linited	0	Default		Auto	
Spanning Tree Protocol	1							
Bandwidth Control	2			0	Default	~	Auto 💊	•
Broadcast Storm Control	3			0	Default	~	Auto 💊	•
Mirroring	4			0	Default	~	Auto 🗸	
Link Aggregation	4							
Port Authentication	5			0	Default	*	Auto 💊	1
Port Security	6			0	Default	~	Auto 💊	•
Classifier	7			0	Default	~	Auto 🗸	•
Policy Rule				0	Default		Auto 🗸	
Queuing Method	8							
VLAN Stacking	9			0	Default	*	Auto 💊	•
Multicast	10			0	Default	*	Auto 💊	•
	11			0	Default	~	Auto 💊	•
	12			0	Default	~	Auto 💊	•

2. Give a name to this Multicast VLAN following by its VLAN ID. Active this VLAN; Pick port 11 as the receiver port; Pick port 9 and 10 as the Source Port. In this scenario, we need to make the source port remains the VLAN "tag". Thus, we come out the following setting. Click "add" to create this VLAN. When the VLAN is set, we keep going and click "Group Configuration" on the upper right corner to create our Multicast Groups.

🔿 MVR	Multicast Setting	Group Configuration
Active		
Name	100	
Multicast VLAN ID	100	
Mode	💿 Dynamic 🔘 Compatible	

Port	Source Port	Receiver Port	None	Tagging
1	0	0	۲	
2	0	0	۲	
3	0	0	۲	
4	0	0	۲	
5	0	0	۲	
6	0	0	۲	
7	0	0	۲	
8	0	0	۲	
9	0	۲	0	
10	0	۲	0	
11	۲	0	0	✓
12	0	0	۲	
		Add Cancel		

 First of all, please choose the Multicast VLAN ID that we just created (which is VLAN100). Then give a name to this group, as long as you can understand. Place the range of Multicast groups here with the start address and End address. Finally, click "Add" to create this group. (In this scenario, we use 224.10.10.0 ~ 224.10.10.50)

🔵 Group Configuration		MVR
Multicast VLAN ID	100 🗸	
Name	Start Address	End Address
224.10.10.0	224.10.10.0	224.10.10.50
	Add Cancel	

4. At this point we go back to the "Multicast Setting" page, enable "IGMP Snooping" here. (Since MVR needs IGMP Snooping). For Unknown Multicast Frame, we prefer "Drop" here in order to avoid any Multicast

NU					<u></u>	Status 🛾 Logout 🛛 I	пеір
sic Setting		Multicast Settir	ng	Multic	ast Status IGMP Fi	Itering Profile MVR	
vanced Application		IGMP Sno	oping	Active 🔽			
Application		IGMP Filt		Active			
inagement		Unknown Multi		O Flooding	Drop		
AN							
atic MAC Forwarding	Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode	
anning Tree Protocol	1			0	Default 🐱	Auto 🗸	
ndwidth Control	2			0	Default 🗸	Auto 🗸	
oadcast Storm Control	3			0	Default 🗸	Auto 🗸	
roring	4			0	Default 🗸	Auto 🗸	
ik Aggregation rt Authentication	5			Ő	Default 🗸	Auto 🗸	
rt Security	6			0	Default 🗸	Auto 🗸	
assifier				0	Default 🗸	Auto 🗸	
licy Rule	7						
euing Method AN Stacking	8			0	Default 🗸	Auto 🗸	
AN Stacking Iticast	9			0	Default 🖌	Auto 🕶	
a l	10			0	Default 🖌	Auto 🔽	
	11			0	Default 🖌	Auto 🖌	
	12			0	Default 🖌	Auto 👻	

Video with no subscriber. (No body joining that multicast group).

5. Right after that you will need to create all other non-Multicast VLANs on this Switch. Once you completed those VLANs, your VLAN status should looks like the same as below.

The Number O								<u>VLAN P</u>	<u>ort Setting</u>	Static VLAN
				Port N	umbe	r				
Index	VID	2	4	6	8	10	12	Elapsed Time	Status	
		1	3	5	7	9	11			
1	1	U	U	U	U	U	U	0:10:27	Static	
I	1	U	U	U	U	U	U	0.10.27	Otalic	
2	100	-	-	-	-	U	-	0:10:27	Other	
2	100	-	-	-	-	U	Т	0.10.27	Other	
3	109	-	-	-	-	-	-	0:10:27	Static	
3	109	-	-	-	-	U	Т	0.10.27	Otalic	
,	110	-	-	-	-	U	-	0:10:27	Static	
4	110	-	-	-	-	-	Т	0.10.27	oralle	

6. Below are their related PVID settings.

🔘 VLA	N Port Setting					VLAN Status
	GVRP					
P	ort isolation					
Port	Ingress Check	PVID	GVRP	Acceptable F	rame 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		109		All	~	
10		110		All	~	
11		1		All	~	
12		1		All	~	
			Apply Ca	uncel		

Here we have done everything we need on the Edge Switch <GS-4012F>.

Configuration via CLI [GS-4024]

Connect the Switch Console port with your PC or Notebook.

8. Open your Terminal program.(Ex, Hyper Terminal in Windows System)

9. Make sure that your port settings are

bps:9600

Data bits:8

Parity: None

Stop bits:1

Flow control: None:

10. After you connected successfully, give the correct user name and password.

11. Put "en" or "enable" to go into the privileged mode. Then put "config" to go into the configuration mode.

Issue the following commands to setup your Switch in this scenario.

To Create VLAN2 with its related IP domain:

```
vlan 2
name server
normal 1,3-24
fixed 2
forbidden ""
untagged 2
ip address 192.168.2.1 255.255.255.0
exit
```

To Create VLAN100 (Multicast VLAN) with its related IP domain (the dummy interface):

vlan 100 name MVR normal 1-23 fixed 24 forbidden "" untagged "" ip address 111.111.111.111 255.255.255.0 exit

To Create VLAN101 with its related IP domain:

```
vlan 101
name 101
normal 1-10,12-23
fixed 11,24
forbidden ""
untagged 11
ip address 192.168.101.1 255.255.255.0
exit
```

To Create VLAN102 with its related IP domain:

```
vlan 102
name 102
normal 1-11,13-23
fixed 12,24
forbidden ""
untagged 12
ip address 192.168.102.1 255.255.255.0
exit
```

To Create VLAN109 with its related IP domain:

```
vlan 109
name 109
normal 1-8,10-23
fixed 9,24
forbidden ""
untagged 9
ip address 192.168.109.1 255.255.255.0
exit
```

To Create VLAN110 with its related IP domain:

vlan 110

name 110 normal 1-9,11-23 fixed 10,24 forbidden "" untagged 10 ip address 192.168.110.1 255.255.255.0 exit

To enable IGMP Routing:

router igmp exit

To set PVID of Port 2:

interface port-channel 2 pvid 2 exit

To set PVID of Port 9:

interface port-channel 9 pvid 109 exit

To set PVID of Port 10:

interface port-channel 10 pvid 110 exit

To set PVID of Port 11:

interface port-channel 11 pvid 101 exit

To set PVID of Port 12:

interface port-channel 12 pvid 102 exit

To enable IGMP v2 on the dummy IP interface:

interface route-domain 111.111.111.111/24

ip igmp v2

exit

Configuration via CLI [ES-3124]

Connect the Switch Console port with your PC or Notebook.

1. Open your Terminal program.(Ex, Hyper Terminal in Windows System)

2. Make sure that your port settings are

bps:9600

Data bits:8

Parity: None

Stop bits:1

Flow control: None:

3. After you connected successfully, give the correct user name and password.

4. Put "en" or "enable" to go into the privileged mode. Then put "config" to go into the configuration mode.

Issue the following commands to setup your Switch in this scenario.

To Setup VLAN 101:

vlan 101 name Data normal 2-27 fixed 1,28 forbidden "" untagged 1 exit

To Setup VLAN 102:

vlan 102 name Data normal 1,3-27 fixed 2,28 forbidden "" untagged 2 exit

To enable IGMP Sooping with unknown Multicast "Drop":

igmp-snooping igmp-snooping unknown-multicast-frame drop

To set PVID of Port 1:

interface port-channel 1 pvid 101 exit

To set PVID of Port 2:

interface port-channel 2 pvid 102 exit

To create the MVR VLAN 100 with group information:

```
mvr 100
source-port 27-28
receiver-port 1-2
name 100
tagged 27-28
group 224.10.10.0 start-address 224.10.10.0 end-address 224.10.10.50
exit
```

Configuration via CLI [GS-4012F]

Connect the Switch Console port with your PC or Notebook.

1. Open your Terminal program.(Ex, Hyper Terminal in Windows System)

2. Make sure that your port settings are

bps:9600

Data bits:8

Parity: None

Stop bits:1

Flow control: None:

3. After you connected successfully, give the correct user name and password.

4. Put "en" or "enable" to go into the privileged mode. Then put "config" to go into the configuration mode.

Issue the following commands to setup your Switch in this scenario.

To Setup VLAN 109:

vlan 109 name 109 normal 1-8,10,12 fixed 9,11 forbidden "" untagged 9 exit

To Setup VLAN 110:

vlan 110 name 110 normal 1-9,12 fixed 10-11 forbidden "" untagged 10 exit

To enable IGMP Sooping with unknown Multicast "Drop":

igmp-snooping igmp-snooping unknown-multicast-frame drop

To set PVID of Port 9:

interface port-channel 9 pvid 109 exit

To set PVID of Port 10:

interface port-channel 10 pvid 110 exit

To create the MVR VLAN 100 with group information:

```
mvr 100
source-port 11
receiver-port 9-10
name 100
tagged 11
group 100 start-address 224.10.10.0 end-address 224.10.10.50
exit
```

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

What is Spanning Tree Protocol

• Spanning Tree Overview

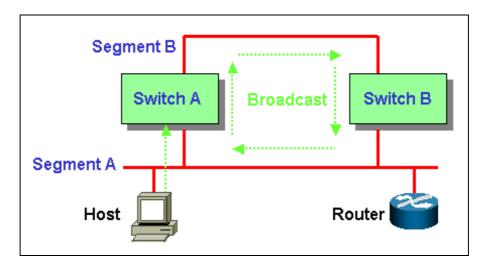
Spanning-Tree Protocol (STP) is a Layer 2 protocol designed to run on bridges and switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops 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.

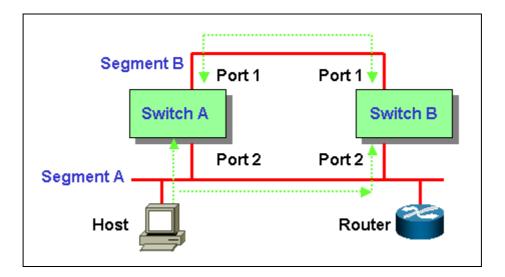
- 1. When Host sends a broadcast frame, like an ARP request to Router, the frame will be received by Switch A.
- Switch A identify the destination MAC address field (broadcast FF:FF:FF:FF:FF:FF) in the frame and determine to flood it onto Segment B.
- 3. When the broadcast frame arrives at Switch B, 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.

- 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".

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.

- 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**.
- 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.

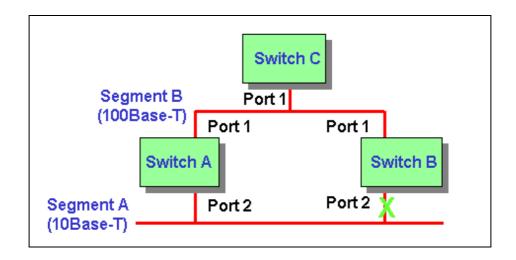
1. How STP works

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.

MAC =	IAC = 00A0C5111111,		MAC =	MAC = 00A0C5222222,			Switch C : MAC = 00A0C5333333 Priority = 1	
	Port 1	Port 2		Port 1	Port 2		Port 1	
Cost	19	100	Cost	19	100	Cost	19	
Priority	128	128	Priority	128	128	Priority -	128	

For example:



- 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.
- 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.
- 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

wfq		Set WFQ method
ES-3124(config)# port-se	curity 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
dd [port:6	vid:1	mac:00:0d:60:8f:1c:80] to static forwarding
dd [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
dd [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

	Active					
	Name					
MA	C Address	s 🚺 :	: :	: ::		
	VID					
	Port	Port 1 💌				
			Add Cancel Clea	ar		
			Add Odnoor Oloc	A1		
Index	Active	Name	MAC Address	VID	Port	Delete
Index	Active Yes	Name 00:02:3f:67:17:be	MAC Address 00:02:3f:67:17:be	VID 1	Port 6	Delete
				VID 1 1		Delete
1	Yes	00:02:3f:67:17:be	00:02:3f:67:17:be	VID 1 1 1	6	Delete
1 2	Yes Yes	00:02:3f:67:17:be 00:02:e3:4a:af:3c	00:02:3f:67:17:be 00:02:e3:4a:af:3c	VID 1 1 1 1 1	6 6	Delete
1 2 3	Yes Yes Yes	00:02:3f:67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00	00:02:3f:67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00	VID 1 1 1 1 1 1 1	6 6 6	Delete
1 2 3 4	Yes Yes Yes Yes	00:02:3f:67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00 00:08:02:1f:da:fe	00:02:3f67:17:be 00:02:e3:4a:af.3c 00:04:80:9b:78:00 00:08:02:1f.da:fe	VID 1 1 1 1 1 1 1 1	6 6 6 6	Delete
2 3 4 5	Yes Yes Yes Yes Yes	00:02:3f:67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00 00:08:02:1f:da:fe 00:0a:e4:13:7d:04	00:02:3f67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00 00:08:02:1f:da:fe 00:0a:e4:13:7d:04	VID 1 1 1 1 1 1 1 1	6 6 6 6	Delete
1 2 3 4 5	Yes Yes Yes Yes Yes Yes	00:02:3f67:17:be 00:02:e3:4a:af3c 00:04:80:9b:78:00 00:08:02:1f:da:fe 00:0a:e4:13:7d:04 00:0a:e4:13:7e:fa	00:02:3f67:17:be 00:02:e3:4a:af:3c 00:04:80:9b:78:00 00:08:02:1f:da:fe 00:0a:e4:13:7d:04 00:0a:e4:13:7e:fa	VID 1 1 1 1 1 1 1 1 1	6 6 6 6 6 6	Delete

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

Ort	Security		
	Activ	e	V
Port	Active	Address Learning	Limited Number of Learned MAC Address
1			O
2			O
3			0
4			0
5			0
6	V		0
7		V	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.

			🗃 Home
MENU Basic Setting			<u>802.</u>
Advanced Application	Enable Authentication Service	/er	
Routing Protocol			
Management	IP address	192.168.1.3	
Config Save	UDP Port	1812 (0-65535)	
	Shared Secret	12345678	
VLAN			
IGMP Snooping		Apply	
Static Multicast	Enable Local Profile Settin	a. (Supprotupto 64 profiles)	
Filtering			
Spanning Tree Protocol	Name		
Port Authentication	Password		
Port Security	Botuno Bocoword to confirm		
DHCP Relay	Retype Password to confirm		
SysLog		Add Cancel	
Access Control		Aud Cancer	
	Index	Name	Delete
	1	admin	
		Delete Cancel	

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.

Basic Setting		802. 1:				RADIUS
Advanced Application	Env	able Auth	entication 🔽			
Routing Protocol	Elle	ible Autri				
Vlanagement				Appl	Cancel	
onfig Save	Port	Enable	Control		Reauthentication	Reauthentication Period(s)
VLAN	1	~	AUTO	*	On 😽	3600 (80~65535)
GMP Snooping	2		AUTO	~	0n 😽	3600 (60~65535)
tatic Multicast	3		AUTO	~	0n 🗸	3600 (60~65535)
iltering Spanning Tree Protocol	4		AUTO	~	0n 🖌	3600 (60~65535)
ort Authentication	5		AUTO	~	0n 🖌	3600 (60~65535)
ort Security	6		AUTO	~	0n 🖌	3600 (60~65535)
HCP Relay	7		AUTO	*	0n 🖌	3600 (80~65535)
vsLog ccess Control	8		AUTO	~	On 🖌	3600 (60~65535)
8	9		AUTO	~	0n 🖌	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.

ZyXEL	
ADVANCED	RADIUS SERVER
RADIUS	
ROOT CA SERVER CERTIFICATE	
RADIUS SERVER	Server Port
MAINTENANCE	Authentication Port: 1812 (1-66535)
MANAGEMENT	Accounting Port : 1813 (1-86535)
	Allowed Access Type
LOGOUT	Allow Any IP Address
	Shared Secret 12345678 (max. 20 characters)
	Allowed Specified IP Address / Network Address Apply
	Allowed IP Address (max. 20)
X	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.

ZyXEL				
ADVANCED	USER ACCOU	INT		
RADIUS ROOT CA SERVER CERTIFICATE RADIUS SERVER USER ACCOUNT MAINTENANCE	User Accou	nt List (max. 200 Accounts) New User		Select All
MANAGEMENT	No.	User Name	Action	Delete
	1	abyss	Change Password	
LOGOUT	2	zyxel	Change Password	
				Delete

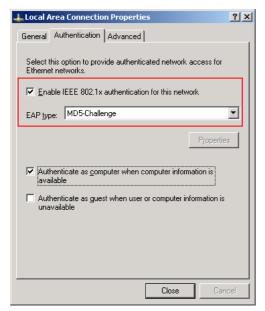
Windows XP(Supplicant) settings:

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

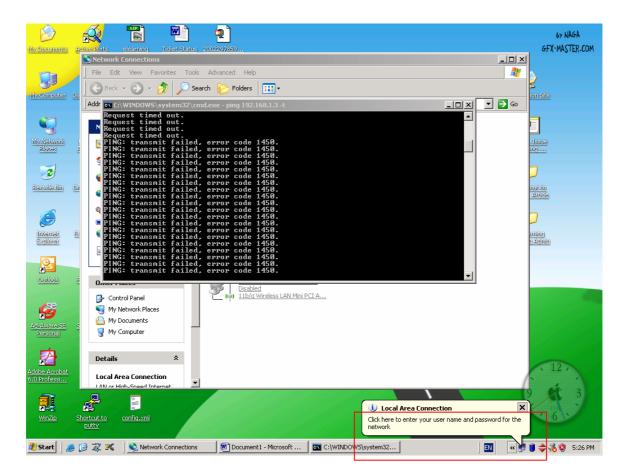
802.1x client as an example here.

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.



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



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.

Local Area Connection	<u>?</u> ×
	N N
User name: zyxel	
Password:	
Logon domain:	
OK Cancel	

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 to perform Access

Control on your Switch

Introduction on ACL

ACL (Access Control List) is the name of a combination of Classifier and Policy Rule. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow. A policy rule ensures that a traffic flow gets the requested treatment in the network. Please be advised that you must first configure a classifier in the Classifier screen before you configure a policy rule.

The relative weight of parameters in ACL

In the classifier, there are a lot of parameters that we can set. Each parameter holds a relative weight. This relative weight is meaningless unless there is a multiple match (or conflict) on the rules.

Here is the order of weight from lowest to the highest:

- 1. [Source-port]
- 2. [Destination-port]
- 3. [Packet-format]
- 4. [Destination-mac]
- 5. [Source mac]
- 6. [Priority]
- 7. [VLAN ID]
- 8. [Ethernet-type]
- 9. [DSCP]
- 10. [IP-Protocol]
- 11. [Source-IP]
- 12. [Destination-IP]
- 13. [Source Socket]
- 14. [Destination Socket]
- 15. [Establish Only]

If you choose a combination of parameters as your rules, the rule with a

higher weight of parameter just gets the highest weight at all. For example, you have defined the first classifier to have "Source Port" plus "Source Socket" as your rule parameters; and your second classifier has only "Destination Socket" as your rule parameter; at this time, since "Destination Socket" has a relative high weight comparing to "Source Port" or "Source Socket", thus the second classifier will have a higher weight.

The higher the weight a classifier has, the higher the priority its related policy rule can apply. A higher priority of policy rule can always overwrite a lower priority of policy rule.

ACCESS CONTROL ACL Flow Example

In general, access control is done by assigning a policy for traffic at-large and a specific policy for a subset. An example is if the network administrator wants to deny all IP traffic originated from the subnet 192.168.3.xx, except for ICMP traffic. The ICMP traffic is a subset of generic IP traffic. To implement this policy, the ACL conflict resolution logic is required to handle this multiple matching scenario.

In this scenario, all IP traffic originating from the 192.168.3.xx subnet is discarded. This is implemented by the **<u>first rule</u>**, with the following:

• Layer 3 protocol type = IP

• IP source address = 192.168.3.0/24

Any packet matched is discarded as specified in ACTION—but if there is ICMP traffic originated from the 192.168.3.xx subnet, they should be forwarded. This is supported by the **second rule**, with the following:

• Layer 3 protocol type = IP

• Layer 4 protocol type = ICMP

• IP source address = 192.168.3.0/24

The action of the second rule is not to discard the packet (Do not drop the matching frame previously marked for dropping).

When two rules match a packet and the resulting actions are conflicting (discard versus not-discard), a higher layer rule has priority over lower layer rule. In this case, the action of the second rule (Layer 4) is carried out because the first rule is only up to Layer 3.

QoS ACL Flow Example

Classifiers	 Policy Rules
Set VLAN=4094	-Replace Priority to 7
Set SrcMAC=00:00:00:00:00:01	Replace Priority to 6
Set SrcPort=1	Replace priority to 5
Set SrcIP=192.168.1.100	Replace priority to 4

Here is another scenario to help you understanding the flow of ACL. There are totally 4 rules.

First rule contains the following:

• When there is traffic from Layer 2 VLAN ID = 4094 Any matched packet will be set the Priority to 7

Second rule contains the following:

•When there is traffic from Layer 2 Source MAC address = 00:00:00:00:00:00:01 Any matched packet will be set the Priority to 6

Third rule contains the following:

•When there is traffic from Layer 2 Source Port = 1 Any matched packet will be set the Priority to 5

Fourth rule contains the following:

•When there is traffic from IP source address = 192.168.1.100/32 Any matched packet will be set the Priority to 4

The above four rules are conflicting together since you can have traffic coming from port 1 and also come with a source IP address of 192.168.1.100. When two or more rules match a packet and the resulting actions are conflicting (Set to different priority value), a higher layer rule has priority over lower layer rule. In this case, the action of the fourth rule (Layer 3) is carried out because the other rules are only up to Layer 2. Although VLAN, MAC, Port are all belonging to Layer two, their carrying out priority would be VLAN>MAC>Port.

In conclusion, every parameter (or rule) in the packet header has a weight. The deeper the parameter in the packet header, the higher the weight is. Further more, the deeper parameter in the packet header has much more higher weight than shallower parameters.

ZyXEL

ACL Scenario

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 the Switch applies its policy rules. We define three rules. Firstly, we define a classifier that is coming from port 2 and its source address is coming from 172.23.3.120; secondly, we specify a classifier that is based on port 2. Finally we specify a classifier for ARP.

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 (do not drop the matching frame previously marked for dropping) only the traffic from port 2 and with the ip address of 172.23.3.120. 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. Moreover, do not forget to apply a policy rule (do not drop the matching frame previously marked for dropping) for our last classifier.

The logic is like this. Since the first rule has a higher weight (layer 3 V.S. layer2) then the second rule and third rule, although the second rule says "drop all from port 2", the first rule will overwrite the action of all other rules since rule one has the higher weight. Therefore, all other traffic from port 2 will be drop, but traffic coming from port 2 with 172.23.3.120 will be forward.

GUI configuration of classifier and policy rule.

Classif	ier 1
---------	-------

 C C 	lassifier	
Active	 Image: A start of the start of	
Name	AllPort2	
Packet Format	All	✓
	VLAN	Any
	Priority	 O ✓
	Ethernet	
Layer 2	Туре	O Others (Hex)
	Source	MAC O Any Address MAC : : : : : : : : : : : : : : : : : : :
		Port Port 2 💌
	L Destination	MAC O Any Address MAC : : : : : : : : : : : : : : : : : : :
	DSCP	Any
	IP Protocol	
		O Others (Dec)
Layer 3	Source	IP Address / 0.0.0.0 / Address Prefix
Layer J		Socket O Any Number
		IP
		Address / n n n n
		© Copyright 1995-2004 by ZyXEL C

Classifier 2

C 🔘 C	lassifier	
Active	V	
Name	Port+IP	
Packet Format	All	
	VLAN	Any
	Priority	 Any 0 v
	Ethernet	● IP
Layer 2	Туре	O Others (Hex)
	Source	MAC O Any Address O MAC : : : : : : : : : : : : : : : : : : :
		Port Port 2 💌
	Destination	MAC Any Address AAC : : : : : : : : : : : : : : : : : :
	DSCP	Any
	IP Protocol	All Establish Only Others (Dec)
Layer 3	Source	IP Address / Address / Address Prefix
Layer J		Socket Oracle Any Number
		IP
		Address / n n n n , , , , , , , , , , , , , , ,
		© Copyright 1995-2004 by ZyXEL C

Classifier 3

C 🔵 C	lassifier	
Active		
Name	ARP	
Packet Format	All	▼
	VLAN	Any
	Priority	 O ▼
	Ethernet	
Layer 2	Туре	O Others (Hex)
	Source	MAC O Any Address MAC : : : : : : : : : : : : : : : : : : :
		Port Port 2 💌
	Destination	MAC O Any Address MAC : : : : : :
	DSCP	Any
	IP Protocol	All Establish Only Others (Dec)
Layer 3	Source	IP Address / 0.0.0.0 / Prefix
201010		Socket Any Number

Policy Rule Configuration

Policy rule on Classifier 1

Active				
Name	DropAllPort2			
Classifier(s)	AllPort2			
	VLAN ID EgressPort	General 1 Port 1	Bandwidth Out-of-Profile DSCP	Metering O Kbps O
Parameters	Outgoing packet format for Egress port Priority DSCP TOS	 Tag ○ Untag ○ ○ ○ ○ 		
г	Forwarding O No change			
L	Discard the packet Do not drop the matching frame previou Priority	isly marked for dropping		
	A bla shanga		@ Cop	rright 1995-2004 by ZvXEL C

Policy rule on classifier 2

🛛 🔘 Policy				
Active				
Name	AllowPort2IP120			
Classifier(s)	Port+IP			
	VLAN ID EgressPort	General 1 Port 1	Bandwidth Out-of-Profile DSCP	Metering O Kbps O
Parameters	Outgoing packet format for Egress port Priority DSCP TOS	 Tag Untag U O O O O O 		
	Forwarding No change Discard the packet Do not drop the matching frame previ Priority	ously marked for dropping		
			© Copy	rright 1995-2004 by ZyXEL Co

Policy rule on classifier 3

🔵 🕘 Policy		_		
Active				
Name	AllowARP			
Classifier(s)	ARP			
		General		Metering
	VLAN ID	1	Bandwidth	0 Kbps
	EgressPort	Port 1 💌	Out-of-Profile DSCP	0
Parameters	Outgoing packet format for Egress po	rt 💿 Tag 🔘 Untag		
	Priority	0 🕶		
	DSCP	0		
	TOS	0 🕶		
	Forwarding			
	🔘 No change			
-	O Discard the packet			
	O not drop the matching frame preserved and the second	reviously marked for dropping		
	Priority			
	A No shongo		@ Copy	rright 1995-2004 by ZyXEL C

CLI configuration of classifier and policy rule.

Please logon to the Switch by either telnet, SSH or Console. Step into the configuration mode and put the follow commands:

Classifier 1 Switch(config)#classifier AllPort2 source-port 2

Classifier 2 Switch(config)#classifier ARP ethernet-type arp source-port 2

Classifier 3 Switch(config)#classifier Port+IP ethernet-type ip source-port 2 source-ip 172.23.3.120 mask-bits 32

Policy rule on classifier 1

Switch(config)#policy AllowARP classifier ARP vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action forward

Policy rule on classifier 2

Switch(config)#policy AllowPort2IP120 classifier Port+IP vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action forward

Policy rule on classifier 3

Switch(config)#policy DropAllPort2 classifier AllPort2 vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action drop

Verifying your result

Connect a PC "A" to the Switch on port2. Connect another PC "B" to the Switch on port10 with IP 172.23.3.191. First set the IP of PC "A" to 172.23.3.120. At this time, PC "A" can ping PC "B". However, if you set the IP of PC "A" to another IP besides 172.23.3.120, it can no longer ping PC "B".

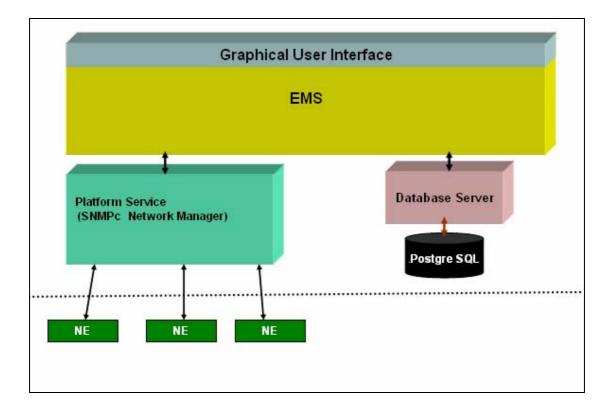
Centralized Management

4 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

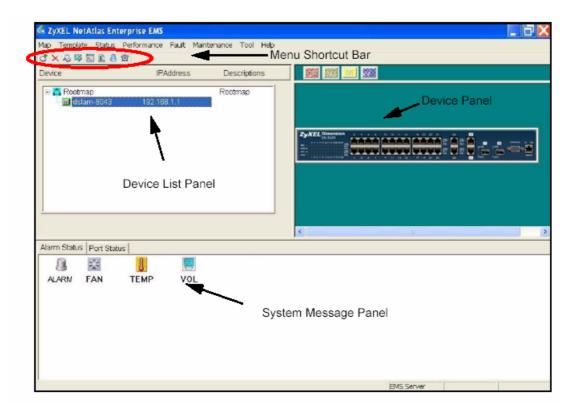
SNMPc Management Co		
🚠 File Edit View Insert f	Manage Tools Config Window Help	- 6 ×
M 🖻 🎒 📮 🔊 🔊	E P 1:1 P P ← → E @ 1921680.1 ▼ Systeminto	
■ Root Subnet	Main Button Bar Edit But	■●●●ア調業日 tton Bar
	View Window Area	<u>a</u>
	Selection Tool	
-	Event Log Tool	v 1
Map Mib Trend Event Menu		>
Normal 04/20/2 Gurrent Hidery		in OK

4 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

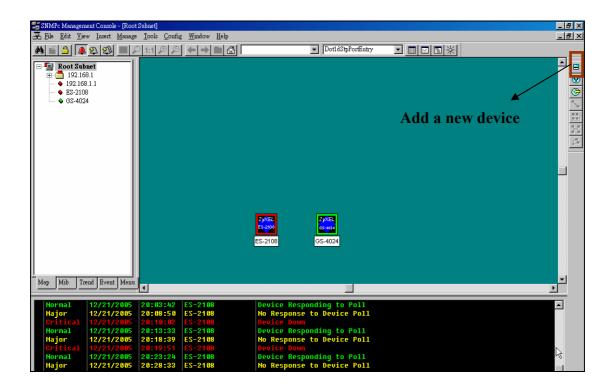


Configuration of adding a new device via SNMPc

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



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

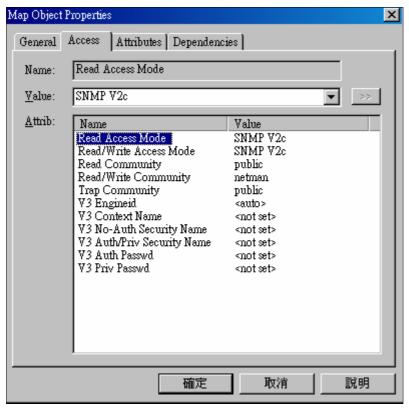
Figure 5 Map Object Properties

Map Object Properties							
General A	.ccess Attributes Deper	ndencies					
<u>L</u> abel:	ES-2108	Type: Device	•				
<u>A</u> ddress:	172.23.3.11	Icon: auto.ico	>>				
<u>G</u> roup:	000=Unknown	-	▼ >>				
Descr:							
			28 08				
	確況	2 取消					

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
--------	--------	--------	------



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		×
General	Access Attributes Dependen	cies	
Name:	Read/Write Access Mode		
<u>V</u> alue:	SNMP V2c		▼ >>
<u>A</u> ttrib:	Name Read Access Mode Read/Write Access Mode Read/Write Community Trap Community V3 Engineid V3 Context Name V3 No-Auth Security Name V3 Auth/Priv Security Name V3 Auth/Priv Security Name V3 Auth Passwd V3 Priv Passwd	Value SNMP V2c SNMP V2c public public <auto> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not></auto>	
	確定	取消	說明

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	t Properties		×							
General	Access Attributes Depende	ccess Attributes Dependencies								
Name:	Read Community									
<u>V</u> alue:	public		▼ >>							
<u>A</u> ttrib:	Name Read Access Mode Read/Write Access Mode Read/Write Community Trap Community V3 Engineid V3 Context Name V3 No-Auth Security Name V3 Auth/Priv Security Name V3 Auth/Priv Security Name V3 Auth Passwd V3 Priv Passwd	Value SNMP V2c SNMP V2c public public vauto> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not>								
	確定	取消	說明							

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.

Map Object	Map Object Properties 🛛 🗙								
General	General Access Attributes Dependencies								
Name:	Read/Write Community								
<u>V</u> alue:	public		>>						
<u>A</u> ttrib:	Name Read Access Mode Read/Write Access Mode Read Community Read/Write Community Trap Community V3 Engineid V3 Context Name V3 No-Auth Security Name V3 No-Auth Security Name V3 Auth/Priv Security Name V3 Auth Passwd V3 Priv Passwd	Value SNMP V2c SNMP V2c public public <auto> <not set=""> <not set=""></not></not></not></not></not></not></not></not></auto>							
	確定	取消	說明						

Figure 9 Read/write Community

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

Figure 10 Device Selection

🚟 SNMPc Management Console - [Root Subnet]					_ 8 ×
Ā File Edit View Insert Manage Icols Con					_ 8 ×
🙈 🖆 🔔 & 🕸 🕀 🔎 1:1 🗩 🖇	D ← → 🗈 🗥 ES-2108	 Dot1dStpPortEntry 	- III 🖂 🖾 💥		
Root Subat ⊕ Discovered Objects ⊕ 192.168.1 ● 192.168.1 ● ES-2108 ● GS-4024	Discovered Objects	152.188.1		2 /024 02-004 CS-4024	 □ ③ ④ ~ #3 % 4 ▲
	2002 1921681) 1	2444 25-210		
Map Mib Trend Event Menu					▼
 Normal Normal 12/27/2005 13:53:39 Normal 12/27/2005 13:53:44 Hajor 12/27/2005 13:53:44 Hajor 12/27/2005 13:53:44 Hajor 12/27/2005 13:53:44 Hajor 12/27/2005 13:53:45 13:53:45 13:53:45 13:53:45 13:53:45 	ES-2108 Device 192.168.1.54 No Resp 192.168.1.1 No Resp 192.168.1.6 No Resp	ministrator at 127.0.0 Responding to Poll onse to Device Poll onse to Device Poll onse to Device Poll rvice Ho	.1 Login OK		

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

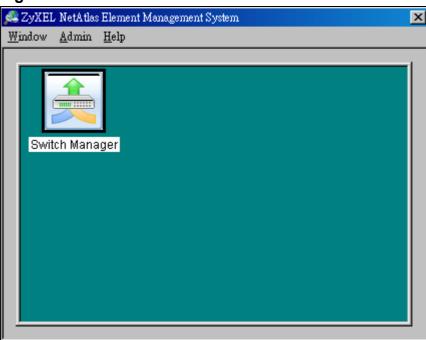


Figure 11 Device Selection

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 EM				
Map View Template Provisio	oning Performance	Fault Maintenance	Tool Help	
් 🗙 😣 📭 🖾 🚊 🖄				
Device	IPAddress	Descriptions		CRI MAJ MIN INF
Contrap Switch-4406 Switch-4504	172.23.15.115 172.23.3.11	Rootmap		
Alarm Status Port Status				

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

Figure 13 Device mapping

🕵 ZyXEL NetAtlas Enterprise E	10							
Map View Template Provis		Fault Maintenance	Tool Help					
J 🗙 💫 噚 🔯 🚊 🕯		Total Production	Tool Holp					
						-1		
Device	IPAddress	Descriptions			RI MAJ MIN IN			
🖃 🔼 Rootmap		Rootmap		1—				
Switch-4406	172.23.15.115							
Switch-4504	172.23.3.11							
					YXEL ES-2108			
				111 -		1234		
					e 📖 e		***	*
						LM		_
Port Status								
Port View				Port Sta	us			
				Port	LinkSpeed	State	LACP	PD
				1	0 Mbps	STOP	Disabled	N/A
0	01 - 12			2	0 Mbps	STOP	Disabled	N/A
, i i i i i i i i i i i i i i i i i i i				3	100 Mbps	FORWARDING	Disabled	N/A
				14	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.

yXEL NetAtlas Enterprise EMS ng Perfor View Template Provis Fault Maintenance Tool Help Мар ් 🗙 💫 噚 🔯 🚊 😭 RI MAJ MIN INF Device IPAddress Descriptions 🖃 🔼 Rootmap - Switch-4406 Rootmap 172.23.15.115 172.23.3.1 ZyXEL Alarm Status Port Status ł X ALARM TEMP EAN VOL

Figure 12 Device panel list

Figure 13 Switch Configuration

ing Performance Fault Ma	intenance Tool Help	
IPAddress Desci	riptions	ICRI MAJ MIN INF
172 20 46 446 Properties Configuration Configuration Save 1	System Configuration Switch Configuration VLAN Configuration Ethemet Port Configuration Multicast Configuration	
FAN VOL		
	ing Performance Fault Me IPAddress Desc Rootr T222215115 Properties Configuration Configuration Save	ing Performance Fault Maintenance Tool Help IPAddress Descriptions Rootmap Properties Configuration Configuration System Configuration ULAN Configuration Ethemet Port Configuration IP Configuration IP Configuration

Figure 14 Selecting a VLAN Type

witch Configuration		
Device Name	IP Address	Copy to Timeout (seconds) 60 Apply Filtering Mac Forwarding Mirroring Switch Setup Priority Queue STP Conf. Link Aggregation
		VLAN Type : 802.1Q MAC Address Aging Time : seconds Queuing Method Method : Q0 Q1 Q2 Q3 Active Control
		STP Configuration Link Aggregation Bandwidth control Broadcast storm control Mirroring 802.1x Port Security
		GVRP 802.1q Ingress Check 802.1q Port Isolation Apply
I		Close

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

🕵 ZyXEL NetAtlas Enterprise EMS	
Map View Template Provisioning Performance Fault Maintenance Tool Help	
Device IPAddress Descriptions	ICRI MAJ MIN INF
Rootmap Switch 4406 T2 2315 Properties Configuration Configuration Save VLAN Configuration Wilch Configuration WLAN Configuration Rethemet Port Configuration Multicest Configuration IP Configuration	
Alarm Status Port Status	
ALARM TEMP FAN VOL	

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

Figure 16 Creating a new VLAN ID

۷	LAN Configuration (Switch-671	18 : 172.23.3.75)						×
Γ								
L	Device Name	IP Address	VLAN ID	Name		Status		
L	Switch-6718	172.23.3.75	1	1		Active		
L			5			Active		
L				•				
L				\square				
L								
L								
L								
L								
L								
L								
L								
L								
L	Port List		New	┛┢	Delete Modify	Lo	ad Template	
L		F	- r - r	┯┛				
L	1 2 3 4 5	6 7 8 9 10 11	12 13 1	4 15	16 17 18 19 20 21	22 23 24 25	5 26 27 28	
L								
L								
L								
L								
L								
			6	lose	1			
L								

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

Figure 17 Selecting the ports

Modify VLAN Di	alog (Sv	witch-	6267	: 172	.23.3.	44 : V	'LAN	ID=2)							×
	R	N Ide Z Act LAN	ive		2				(1 ~	409	4)			1		
	V	'LAN	Nam	e:	Tes	st										
Static VLA	.N															
Egr	ess Po	orts			F	orbid	den I	Ports			ι	Jntag	Port	з		
Port 02 Port 03 Port 04 Port 05 Port 06 Port 07 Port 08 Port 09 Port 10 Port 11	tatus F	Previe			Port Port Port Port Port Port Port Port	02 03 04 05 06 07 08 09			•		Port Port Port Port Port Port Port Port	02 03 04 05 06 07 08 09				
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								
			ок							Car	ncel					

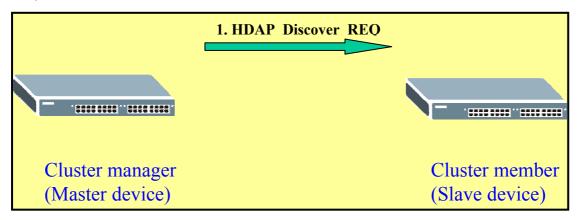
For more information, reference the user guide of NetAtlas.

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".

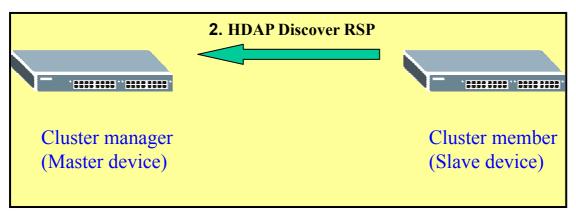
How Cluster Management works

Step 1:



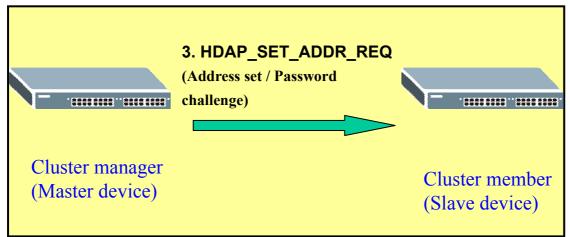
To discover the clustering members, the clustering Manager broadcasts a HDAP (Host Discovery and Address assignment Protocol) Discover request.

Step 2:



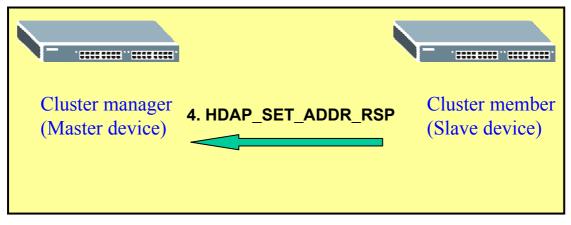
A clustering member listens on UDP port 263. When a clustering member receives a request with the matching signature, it answers with a HDAP Discover Response. In the response, the clustering member provides identity information about itself.

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	
Slep	1	

Clustering Mana	ing Management Confi ager:	iguration		<u>Status</u>
Active	V			
Name	Master			
VID	1			
Clustering Cand	_			
Password				
Index	Add	Cancel Refresh Name	Model	Remove

Go to menu: "Management" \rightarrow "Cluster Management" \rightarrow "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			
		Apply	Cancel	
Clustering Cand	lidate:			
	00:a0:c5:3c:4e:43/	ES-3024/ES-3024		
	00:a0:c5:ab:03:08/	ES-4024/ES-4024		
List				
Password	****			
		Add Canc	el Refresh	

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:

Clust	tering Manageme	ent Status		<u>Configura</u>
	Status	Manager		
	Manager	00:a0:c5:ab:03:03		
Number	Of Member = 2			
Index	HwAddr	Name	Model	Status
<u>1</u>	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:

ES-3024/ES-	3024(slave)		<u>Member Menu</u>
Basic Setting System Info General Setup Switch Setup IP Setup Port Setup	Advanced Applications <u>VLAN</u> <u>Static MAC Forward</u> <u>Filtering</u> <u>Spanning Tree Protocol</u> <u>Bandwidth Control</u> <u>Broadcast Storm Control</u> <u>Mirroring</u> <u>Link Aggregation</u> <u>Port Authentication</u> <u>Port Security</u> <u>Access Control</u> <u>Queuing Method</u>	Routing Protocol <u>Static Route Setup</u>	Management Maintenance Diagnostic Filtering Database ARP Table Port Status

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

Step 5:

) Clus	tering Manageme	ent Status		<u>Configu</u>
Γ	Status	Manager		
	Manager	00:a0:c5:ab:03:03		
umbe	r Of Member = 2			
ndex	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
<u> </u>	00.40.05.40.03.06	E3-4024	E0-4024	Unine

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

Step 6:

Clustering Cand	idate:			
List				
Password				
Index	Add Can	oel Refresh	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	N
	Remov	e Cancel		

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.

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.

Table 1: RMON Monitoring Groups

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	matched by a filter	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))

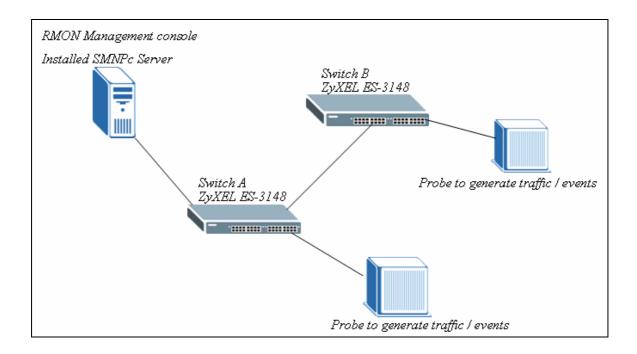
History	(1.3.6.1.2.1.16.2)
Alarm	(1.3.6.1.2.1.16.3)
Hosts	(1.3.6.1.2.1.16.4)
hostTopN	(1.3.6.1.2.1.16.5)
Matrix	(1.3.6.1.2.1.16.6)
Filter	(1.3.6.1.2.1.16.7)
Capture	(1.3.6.1.2.1.16.8)

All contents copyright (c) 2006 ZyXEL Communications Corporation.

Event (1.3.6.1.2.1.16.9)

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

Scenario (ES-3100 Series supports RMON 1.2.3.9)



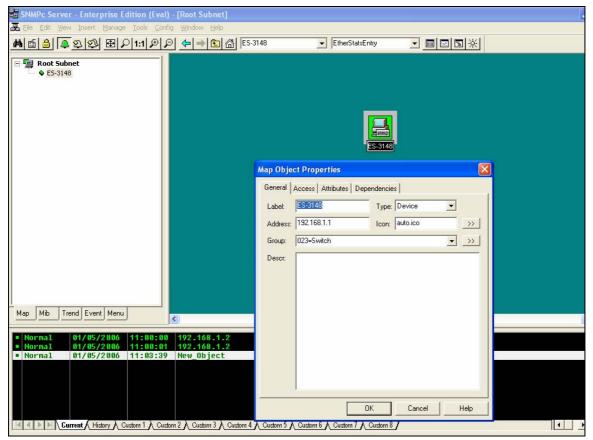
In this illustration, SNMPc Enterprise Edition Version 5.1.6c is installed on the PC. And this PC is defined as "RMON management console". This PC can ping both ZyXEL ES-3148 (both Switch A & Switch B). And there are some probes / networking devices to generate the traffic to the ZyXEL Switches in order 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.



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".

🖥 SNM	Pc Server	- Enterpr	rise Editi	on (Eval) - [Root Subr	iet]					
亮 Eile	<u>E</u> dit <u>V</u> iew	Insert M	<u>l</u> anage <u>T</u>	ools <u>C</u> oni	fig <u>W</u> indow <u>H</u> i	elp					
#		2 20 1	⊞ ₽ ′	l:1 ⊕ ∫	₽ 	ES-314	3	▼ EtherStatsEntry		3 ×	
	Root Subne Science Subne ES-3148	et									
	Poll Obje	ct (ES-31									
	Poll Status:	Receive	d SNMP R	esponse					Properties		
	15:37:03 15:37:04 15:37:05 15:37:06 15:37:08 15:37:09 15:37:09 15:37:09 15:37:10 15:37:11 Response Min Sen	SNMP OK SNMP OK	(RFC1213 (RFC1213 (RFC1213 (RFC1213 (RFC1213 (RFC1213 (RFC1213 (RFC1213 (RFC1213	MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter; MIBjenter;		7) [time <1ms] 7) [time <1ms] 8 Avg: <1n %Loss: 0			View Iools Snmp V3 Service Stats System Interfaces Interrat Protocols Cable Modem Repeater Bridge Transmission Private	Poll Object Connect Telnet WEB Browser MIB Browser RMON View	
 Map	Mode: SN	MP V1		Ŧ	Poll (s): 1	Stop	Done				
					<u><</u>						
 Nor Nor 	mal ()1/05/2)1/05/2)1/05/2	006 1 ⁻	1:00:00 1:00:01 1:03:39	192.168.	1.2 T	rend Report	atus Agent Conn Agent Connecte Inding to Poll			
	🕨 🕨 🔪 Curr	ent / Histor	ry 👌 Custo	m 1 👌 Cus	tom 2 👌 Custom 3	λ Custom 4 λ (Custom 5 👌 Custo	n 6 <u>)</u> Custom 7 <u>)</u> Custom	18 /		

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.

🖥 SNMPc Server - Enterprise Edition (Ev	al) - [Root Subnet]			
🛃 File Edit View Insert Manage Tools 🖸	onfig <u>W</u> indow <u>H</u> elp			
🗛 🖆 📮 🎗 🕸 🔳 🔎 1:1 🗩	Ø ← → ● ▲ ES-3148	EtherStatsEntry		
Snmp Mibs Custom-Tables System Sy				
	<			
Normal 01/05/2006 11:00: Normal 01/05/2006 11:00: Normal 01/05/2006 11:00:	01 192.168.1.2 Tre	covery/Status Agent Conne nd Report Agent Connected ice Responding to Poll	ected to Server d to Server	
Current & History & Custorn 1 & C	Suctors 2 & Outburs 3 & Outbur 4 & Out	nna 5 à Cuctora 6 à Cuctora 7 à Cuctora	8.1	4

3. Right click the "etherStatsTable" and choose "View Table"

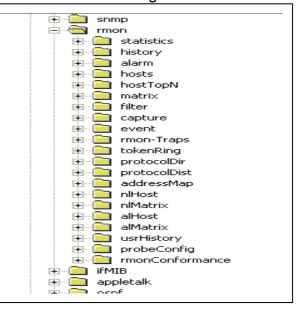
🖶 SNMPc Server - Enterprise Edition (Eval) - [Root Subnet]	
R Elle Edit View Insert Manage Tools Config Window Help	
	5-3148 🗸 EtherStatsEntry 🔽 🔟 🖂 🛞
Itransmission Itransmission Issues Image: Statistic Image: Statistic	
 Normal 01/05/2006 11:00:00 192.168.1.2 Normal 01/05/2006 11:00:01 192.168.1.2 Normal 01/05/2006 11:03:39 New_Object 	Discovery/Status Agent Connected to Server Trend Report Agent Connected to Server Device Responding to Poll
Custom 1 Custom 2 Custom 3 Custom	4) Custom 5) Custom 6) Custom 7) Custom 8 /

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.

SNMPc Server - Enterprise Edition (I	ival) - [Eth	erStatsEntry	(ES-3148)]						
Eile Edit View Insert Manage Tools	<u>C</u> onfig <u>W</u> in	dow <u>H</u> elp							
# ≦ ≜ & & Ø ■ ₽ 1:1 #	● 🔎 🔶	→■☆	ES-3148	•	EtherSt	atsEntry _		<u>*</u>	
🖃 🚔 rmon 🛛	T 🔽	🛛 🗉 🗛 🌠		121	÷ sec				
🖃 🚖 statistics	Index	DataSource	DropEvents	Octets	Pkts	BroadcastPkts	MulticastPkts	CBCAlignErrors	UndersizePkts
🚊 🚖 etherStatsTable	32	ifIndex.33	0	00000		0	Mulucastrics		0 0
EtherStatsEntry	33	ifIndex.33	0	0	0	0	0	0	0
🔷 🗣 etherStatsInde	34	ifIndex.34	0	0	0	0	0	0	0
🛶 🔷 etherStatsData	35	ifIndex.35	0	0	0	0	0	0	0
💀 etherStatsDropl			0	-	-	0	-	-	-
+ etherStatsOctel	36	ifIndex.37	-	0	0	-	0	0	0
↔ etherStatsPkts	37	ifIndex.38	0	0	0	0	0	0	0
↔ etherStatsBroad	38	ifIndex.39	0	0	0	0	0	0	0
••••••••••••••••••••••••••••••••••••••	39	ifIndex.40	0	0	0	0	0	0	0
→ → etherStatsUnde	40	ifIndex.41	0	0	0	0	0	0	0
↔ etherStatsOver	41	ifIndex.42	0	0	0	0	0	0	0
🚸 etherStatsFragr	42	ifIndex.43	0	5649631	15370	158	>0	0	0
🛶 🚸 etherStatsJabb	43	ifIndex.44	0	0	0	0	0	0	0
🛶 松 etherStatsCollis	44	ifIndex.45	0	0	0	0	0	0	0
🚽 松 etherStatsPkts6	45	ifIndex.46	0	0	0	0	0	0	0
🛶 松 etherStatsPkts6	46	ifIndex.47	0	0	0	0	0	0	0
💠 etherStatsPkts1	47	ifIndex.48	0	0	0	0	0	0	0
↔ etherStatsPkts2	48	ifIndex.49	0	0	0	0	0	0	0
↔ etherStatsPkts5	49	ifIndex.50	0	0	0	0	0	0	0
↔ etherStatsPkts1	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
Map Mib Trend Event Menu			1	l	ľ,	ľ	ľ	ľ	+
		•							
	- 00 - 400		D. t. and and				ha Carrier		
Normal 01/05/2006 11:00 Normal 01/05/2006 11:00 Normal 01/05/2006 11:00		.168.1.2	UISCOV Trend	ery/stat Renort A	us Hge nont C	nt Connected onnected to S	to Server		
Normal 01/05/2006 11:03		Object		Respond			oet vet		
				in a point.					
Current History Custom 1	Custom 2	Custom 3 🚶 Cus	tom 4 👌 Custom 5	Custom 6	Custom	7 Custom 8			•

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



<u>FAQ</u>

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.

Access Control

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.

0.0.0 HCP Client atic IP Address IP		
atic IP Address		
atic IP Address		
atic IP Address		
IP		
	Address	192.168.1.1
IP	Subnet Mask	255.255.255.0
De	efault Gateway	0.0.0.0
ement VID 1]
IP	Address	192.168.0.1
IP	Subnet Mask	255.255.255.0
De	efault Gateway	0.0.0.0
	ement VID 1 IP IP Di	Default Gateway ement VID 1 IP Address IP Subnet Mask Default Gateway

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.

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.