IES1248

Support Notes

March 2006

ZyXEL
Unleash Networking Power

Index

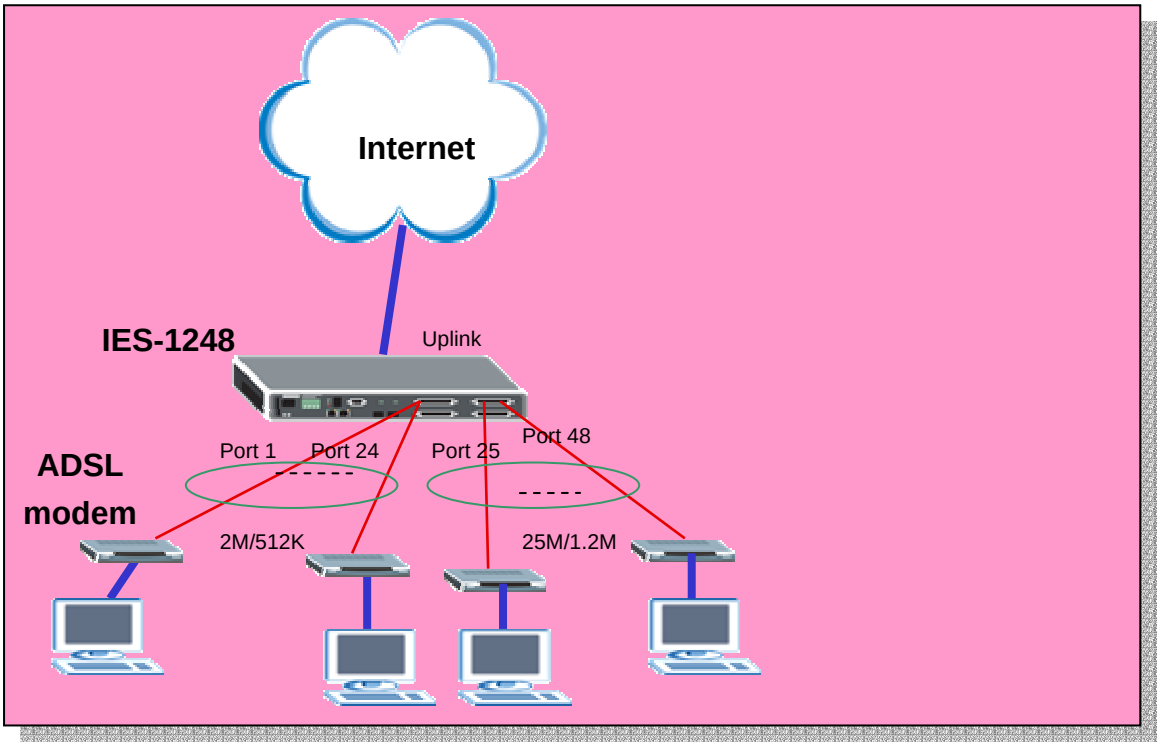
Application Notes **4**
Provide Different DSL Port Speeds to different subscribers 4
How to apply the profile to ports 4
How to configure 802.1Q VLAN 10
How to set up a VLAN environment. 11
Triple play Application 14
How to set up a Multiple PVCs environment. 15
802.1x Application 23
How to set up an 802.1x environment. 23
Setting up the Syslog Server 28
How to set up a Syslog server. 28
Setting up the Ring Environment 30
How to set up a Ring Environment. 31
Setting up the IGMP Snooping/IGMP Filtering 37
How to set up IGMP snooping/IGMP filtering 38
Static Multicast 40
How to configure Static Multicast filter 42
Limit the users behind the certain DSL port 46
How to set up MAC Filter/Port Security 47
DHCP Relay Option 82 Application 49
How to set up DHCP Relay Option 82 Environment 50
Filter Some Certain Packet 60
How to Filter Some Specific Packet 60
Cascade two IES1248 (Daisy chain mode) 62
How to setup Daisy-chain mode 62
VLAN Application 63
How to configure VLAN: 64
FAQ **80**
What is the maximum line rate of IES1248 ? 80
How many management instances can access IES-1248 at the same time? 80
What is the difference between IES1248-71 and IES1248-73 ? 80
What is the power requirement of IES- 1248? 80
What kind of the DSL standard does IES1248 compliant ? 80
What is the ADSL chipset of IES1248? 80
What is the Network Processor of IES1248 ? 80
How many Flash memory and SDRAM that IES 1248 supports? 80
What kind of the features that IES 1248 supports ? 81

What is the default console rate of IES1248 ? 81
How many static VLAN entries can IES1248 support ? 81
How many VLANs can each ADSL port of IES1248 join ? 81
How many VLANs can each ADSL port of IES1248 join ? 81
What kinds of profiles can IES1248 supprot? 81
Trouble Shooting 83
If my computer can't access the DSLAM by WEB/Telnet/Ping from Ethernet port, only console screen can access successfully, what can I do? 83
If DHCP Relay Option 82 can't work, for example, PC can not get desired IP address from DHCP server, what can I do? 85
How to reset this device as factory default? 85
xDSL link fail? 90
Which new version I should upgrade? 90
I forgot the Password, how do I recover it? 91
I can not access the DSLAM via console port. What should I do? 91
There is no traffic could be transmitted through the DSLAM, what should I do? 92
Alarm Led is always on, what should I do? 92

Application Notes

Provide Different DSL Port Speeds to different subscribers

An ISP may provide different Line speeds for each DSL port. In our IES-1248 have an easy way to configure the line speed for each port. It can create some profiles which can set different parameters to meet the different users' requirement.
In this application, we will set up two profiles. One is for low speed requirement with upstream/downstream is 2M/512Kbps and the other is for high speed requirement with upstream/downstream is 25M/1.2Kbps. We suppose there are general subscribers from port 1 to port 24 with a low speed profile and some enterprise users from port 25 to port 48 with high speed profile.



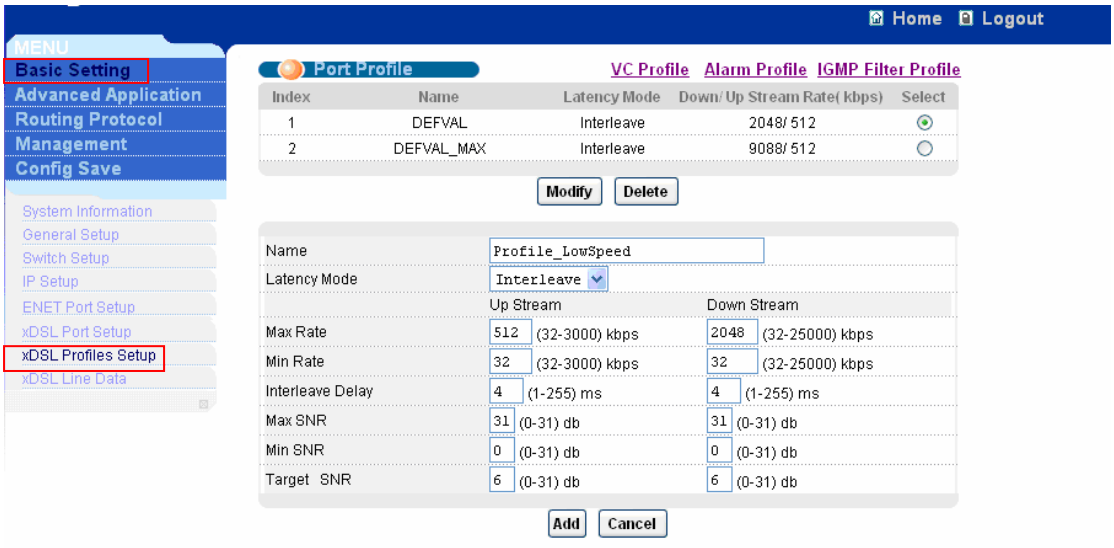
How to apply the profile to ports

In this application, we need to configure IES1-1248 and ADSL CPE. We use ZyXEL Prestige 660R-61 CPE here.

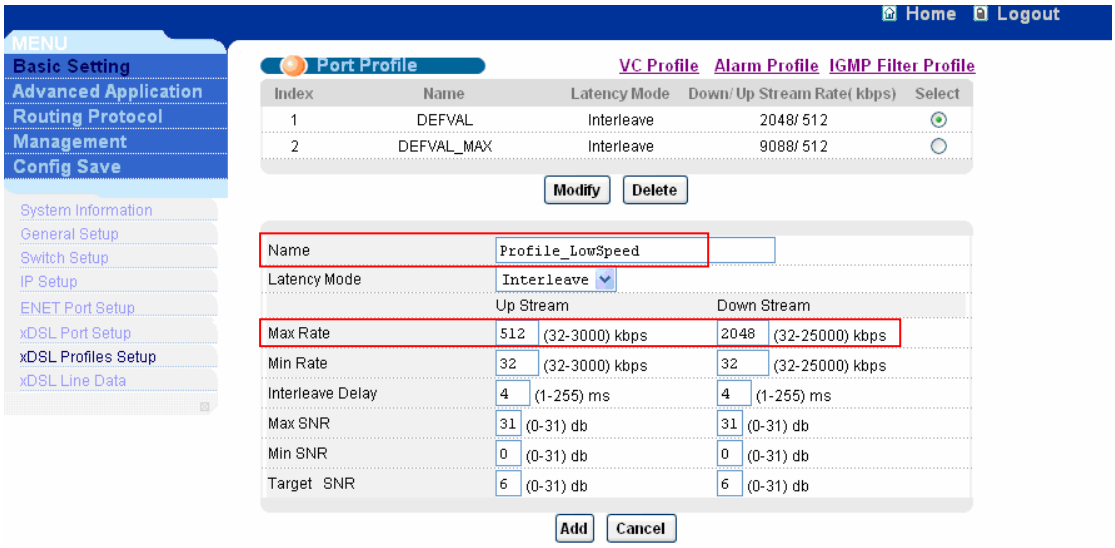
1. IES-1248 Settings

1.1 Profiles settings

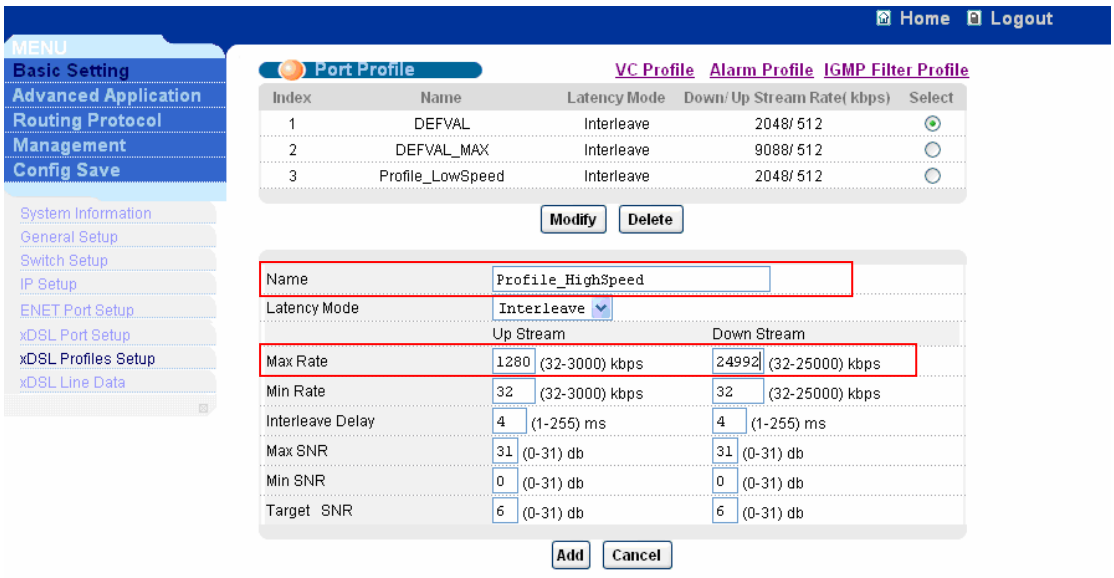
Click Basic Setting, xDSL Profiles Setup in the navigation panel to display configuration screen as shown.



Set up Low Speed Profile. Give this profile a name like Profile_LowSpeed and input the MaxRate for Up Stream and Down Stream. In this case, we set 512Kbps and 2048Kbps for Up Stream and Down Stream.

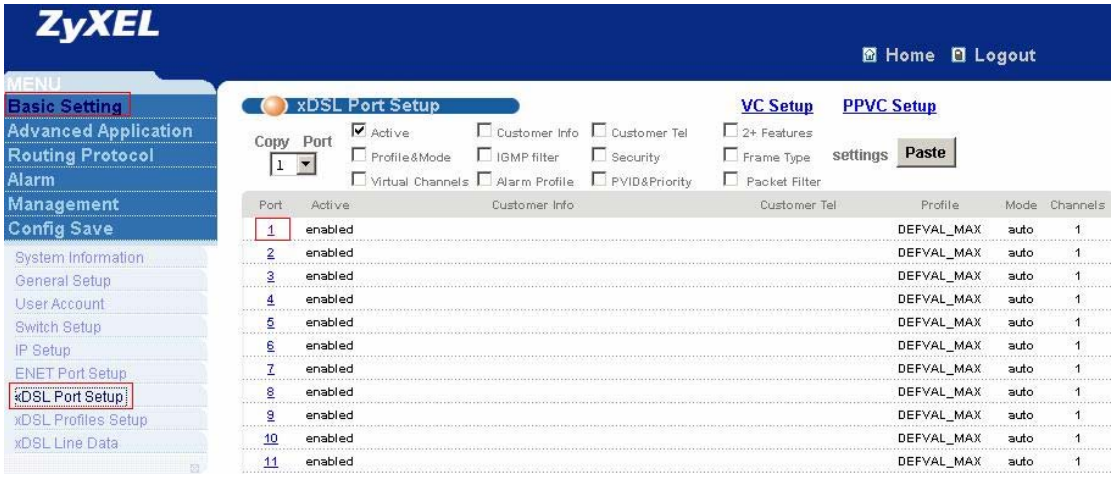


Set up High Speed Profile. Give this profile a name like Profile_HighSpeed and input the MaxRate for Up Stream and Down Stream. In this case, we set 1280Kbps and 24992Kbps for Up Stream and Down Stream.

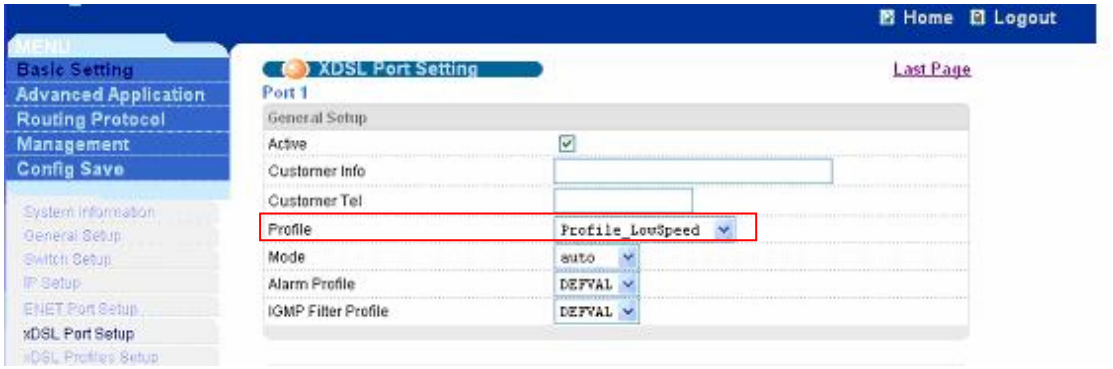


1.2 Profile Assignment

Click **Basic Setting**, **xDSL Port Setup** in the navigation panel to display configuration screen as shown.

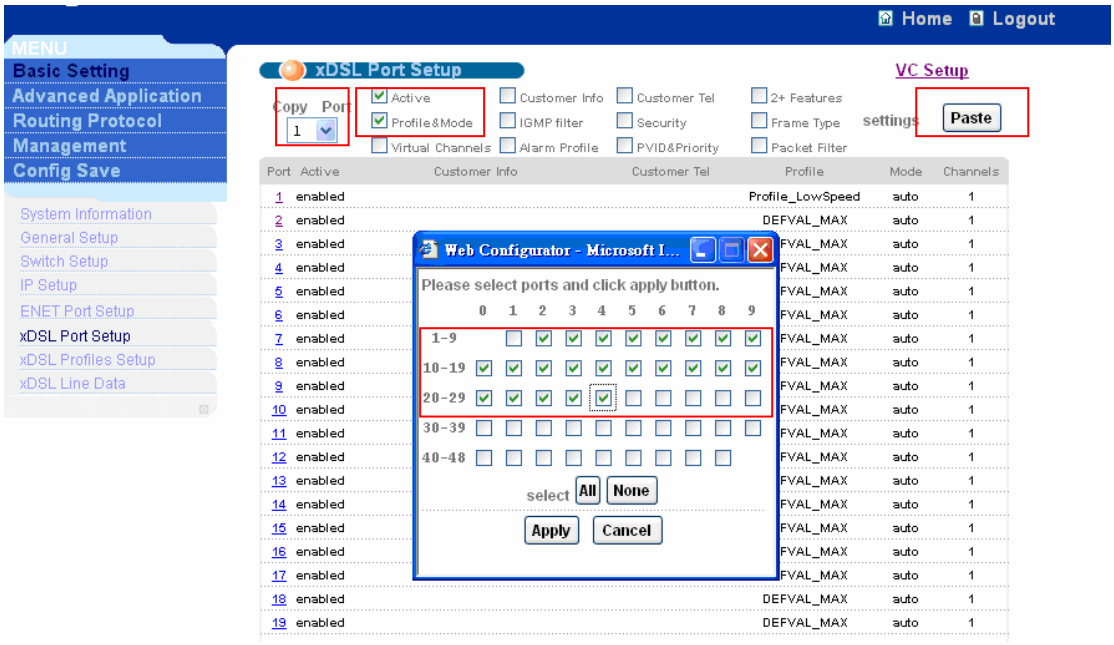


Assign Profile_LowSpeed to port 1. Click a number **1** in the Port index field to enter Port setup screen. Select the Profile_LowSpeed profile and press **Apply** button.

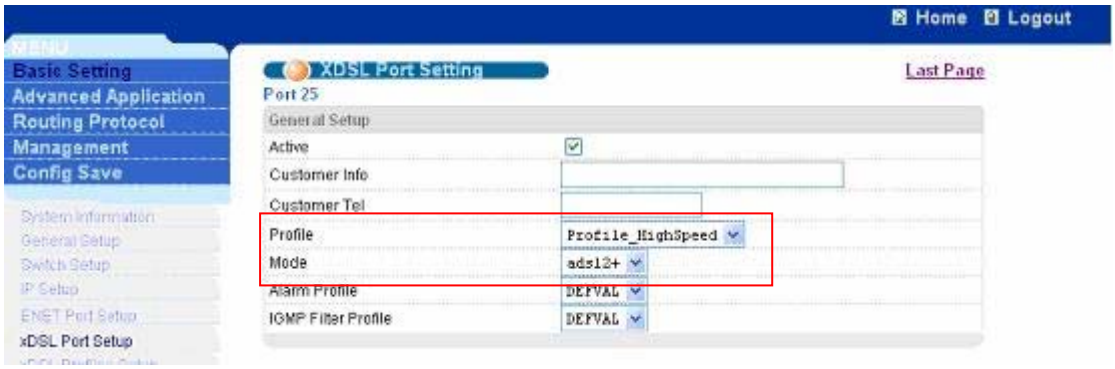


Copy the settings of port 1 to the ports from 2 to 24. After finishing port 1 setting, the screen will be back to the xDSL port Setting screen. Select port 1 in **Copy Port**

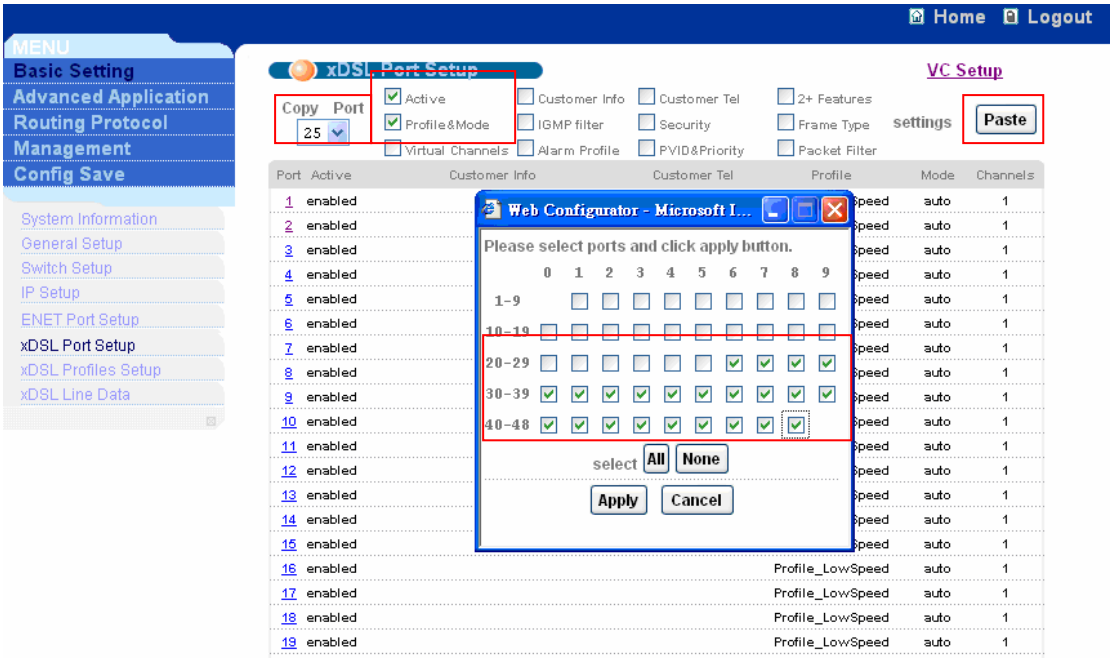
combobox. Check the **Active** and **Profile&Mode**. After press the **Paste** button. It will pop up a screen to select the ports. Select the ports you want to copy the configuration to and press **Apply** button. The settings of port 1 will be copied to other ports.



For the high speed profile, you can set the Profile_HighSpeed to port 25. You also can select ADSL2+ mode in **Mode** combobox. That will fix the mode on ADSL2+ mode.



Copy the settings of port 25 to the ports from 26 to 48. You can follow the same procedures as port 1.

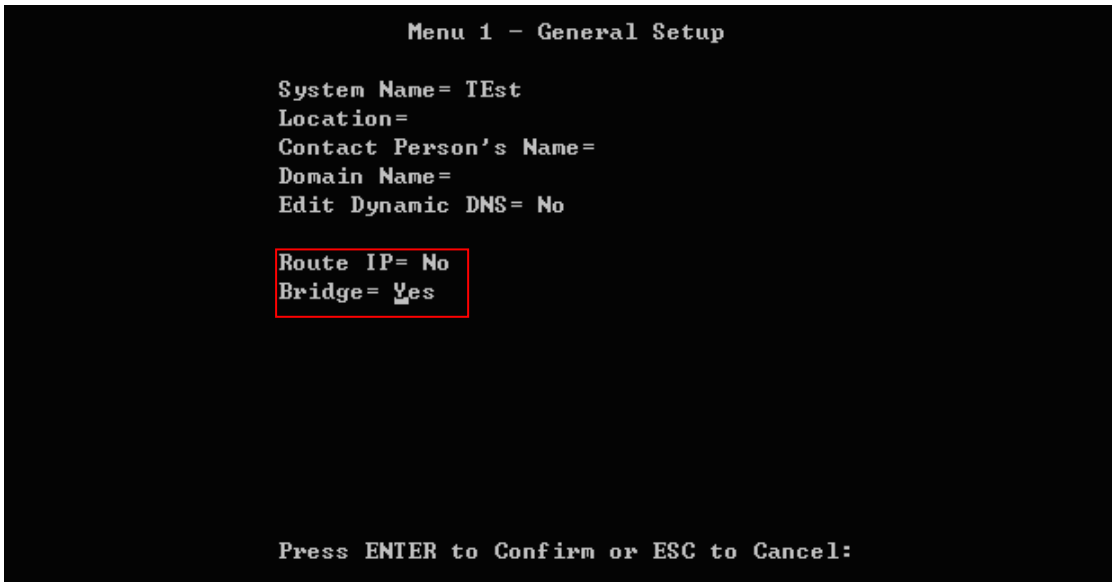


2. Prestige 660R-61 Settings

We configure Prestige 660R-61 as bridge mode. The default VPI/VCI of IES-1248 is 0/33. So we need to set up such values. Prestige 660R-61 has a Telnet server inside. We need to configure it via Telnet.

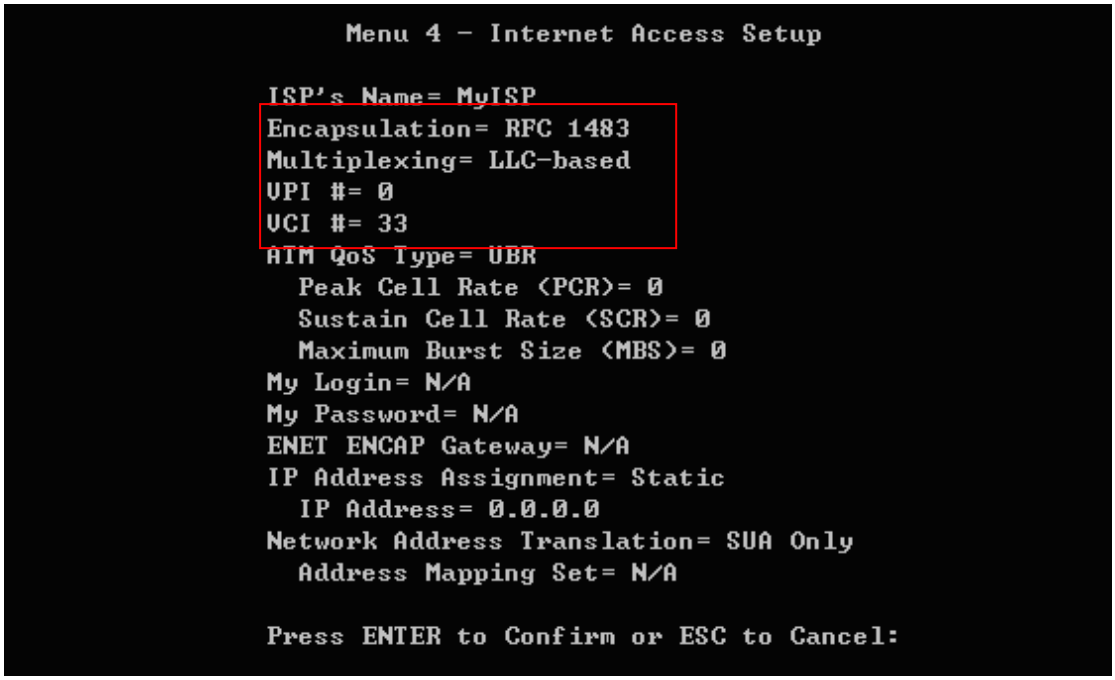
2.1 Menu1: General Setup

Go to Menu 1. In this menu, we must set “Rout IP = NO” and “Bridge = YES”.



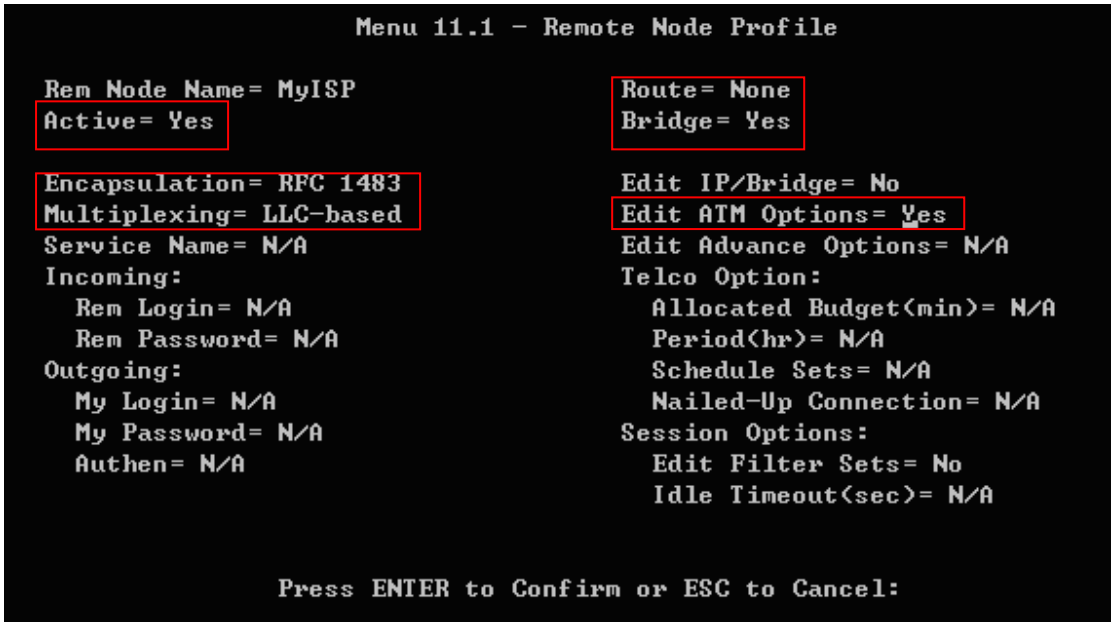
2.2 Menu4: Internet Access Setup

The encapsulation must be RFC 1483 for bridge mode. The Multiplexing should be the same as IES-1248. The LLC-based is default mode of IES1248. Additionally, we must check if the VPI/VCI is the same as IES-1248. The default VPI/VCI of IES1248 is 0/33.



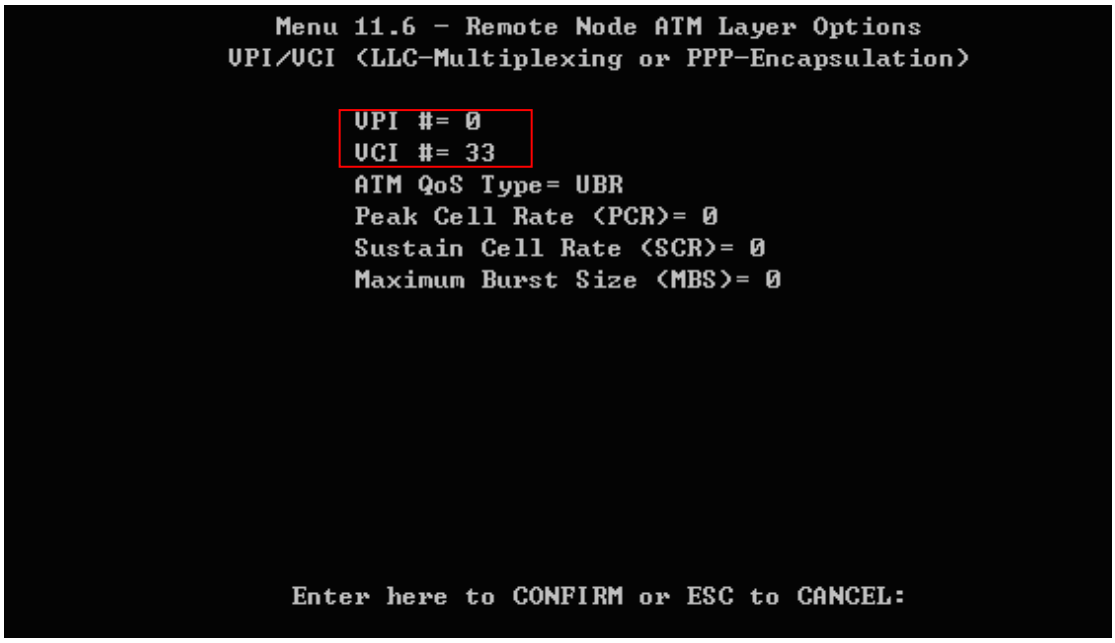
2.3 Menu11.1: Remote Node Profile

In menu11.1, we should activate this profile with "Active= Yes". The Encapsulation and the Multiplexing are the same as the menu 4. Setting "Edit ATM Options=Yes" will enter Menu 11.6.

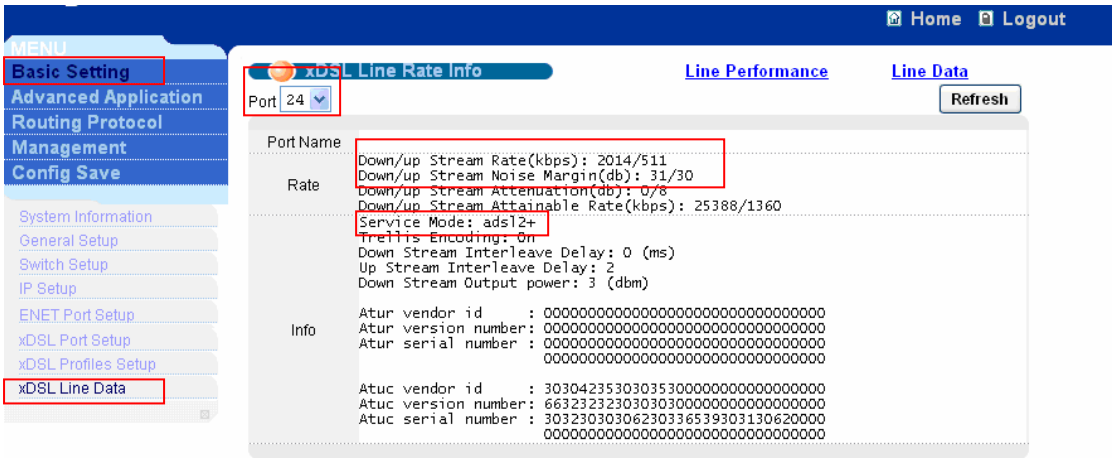


2.4 Menu11.6: Remote Node ATM Layer Options

Check the values above are the same as the IES-1248.



You can click **Basic Setting** and **xDSL Line Data** in navigation Panel to display configuration screen as shown. Select the port connected to the IES-1248. You will see the link speed and link mode.

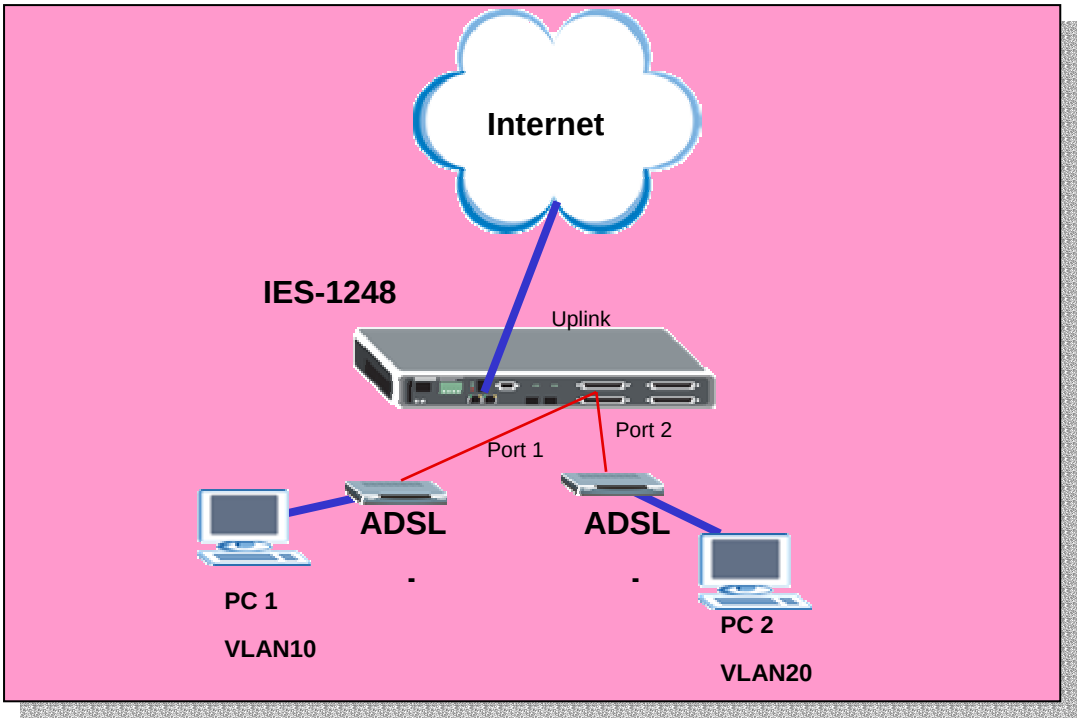


How to configure 802.1Q VLAN

A VLAN (Virtual 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 groups.

We want to deploy VALN environment in this application. The following figure shows the VLAN example. Two PCs connect to the port 1 and port 2 of the line card

and belong to different VLAN. One is VLAN 10 and the other is VLAN 20. So they can't communication with each other. But both PC 1 and PC 2 can connect to Internet.



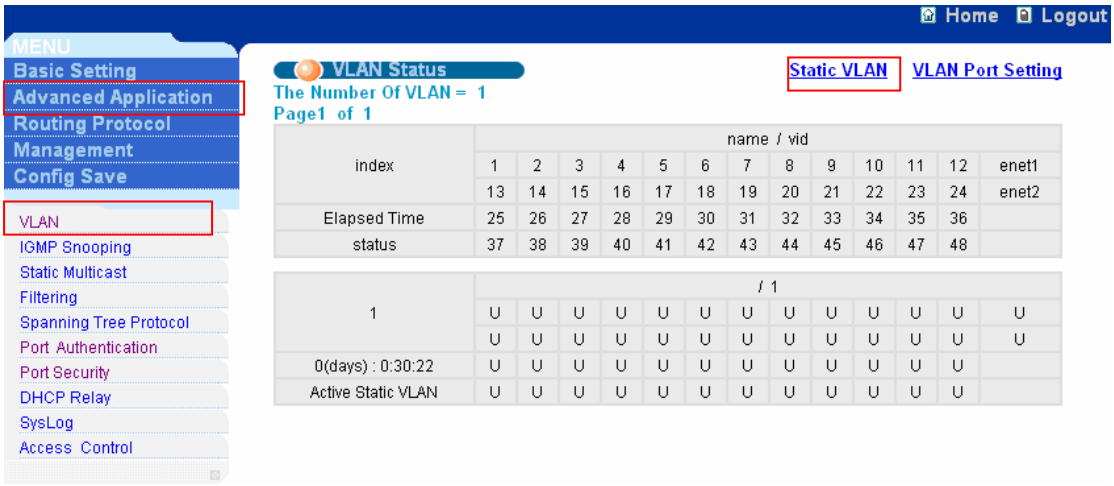
How to set up a VLAN environment.

In this application, we need to configure IES1-1248 and ADSL CPE. We use ZyXEL Prestige 660R-61 CPE here. Because the two ports belong to different VLAN want to go to the Internet via Uplink port of IES1248, we need to set up an extra VLAN and let the two ports be members of this VLAN.

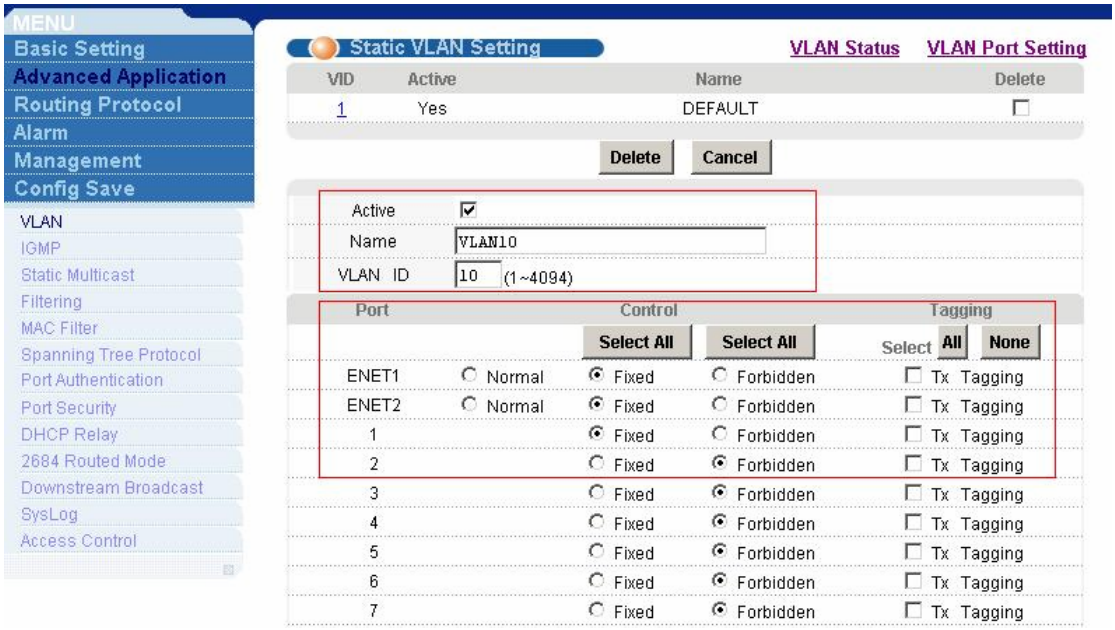
1. IES-1248 Settings

1.1 VLAN settings

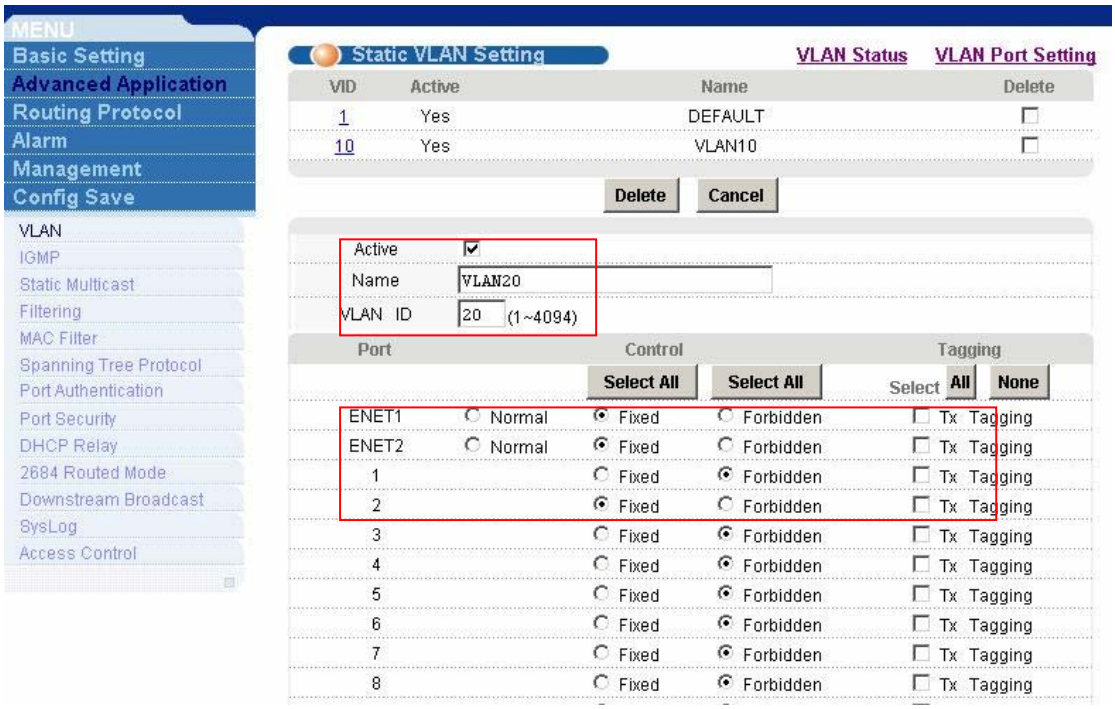
Click **Advanced Application**, **VLAN** in the navigation panel to display configuration screen as shown. Click **Static VLAN** to set the VLAN parameters.



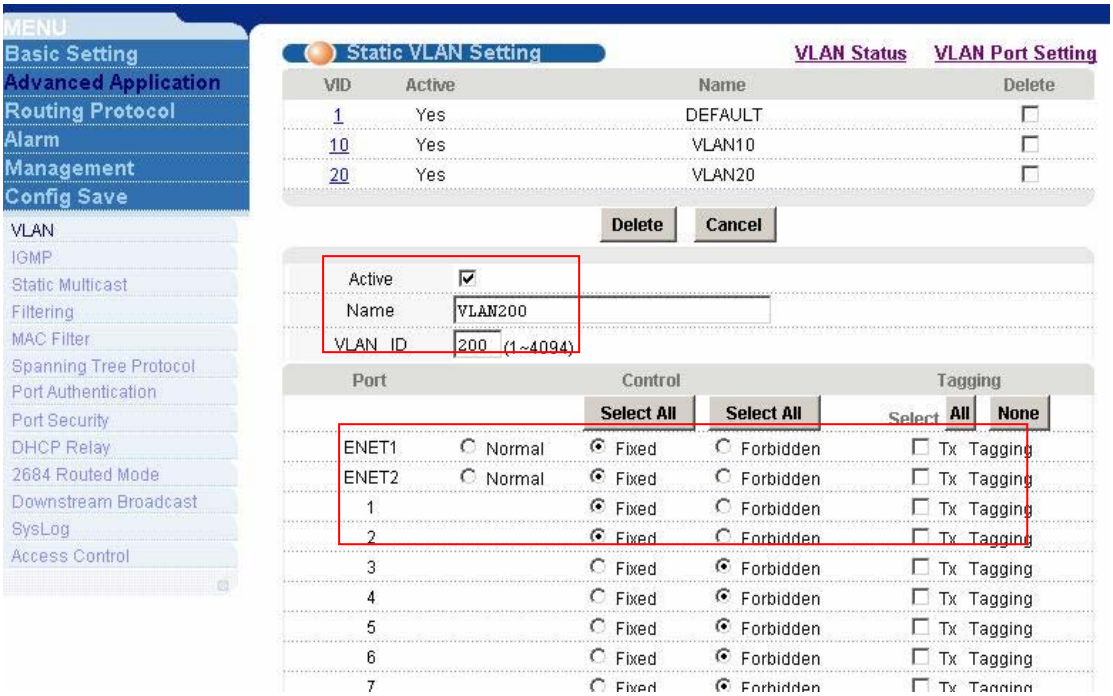
Add VLAN10. Assign Port 1, ENET1 and ENET2 to be members of VLAN10 as shown.



Add VLAN20. Assign Port 2, ENET1 and ENET2 to be members of VLAN20 as shown.

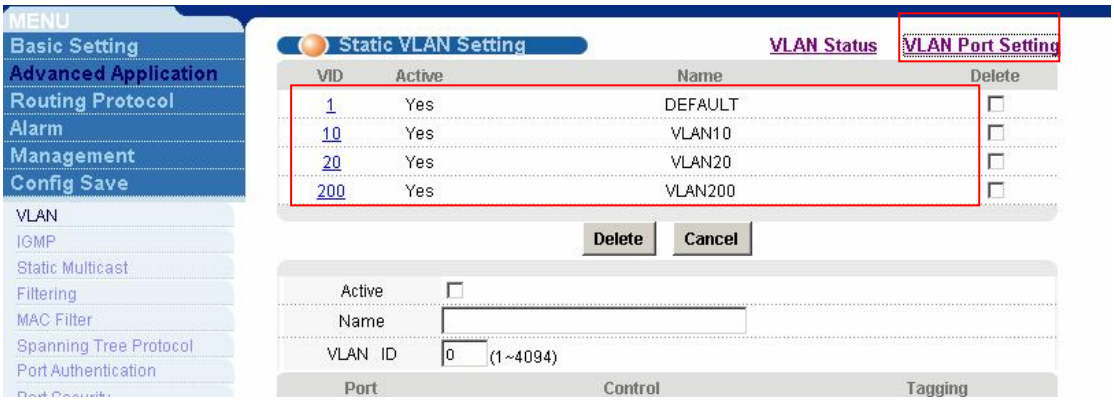


Add VLAN200. Assign Port 1, Port2, ENET1 and ENET2 to be members of VLAN200 as shown.

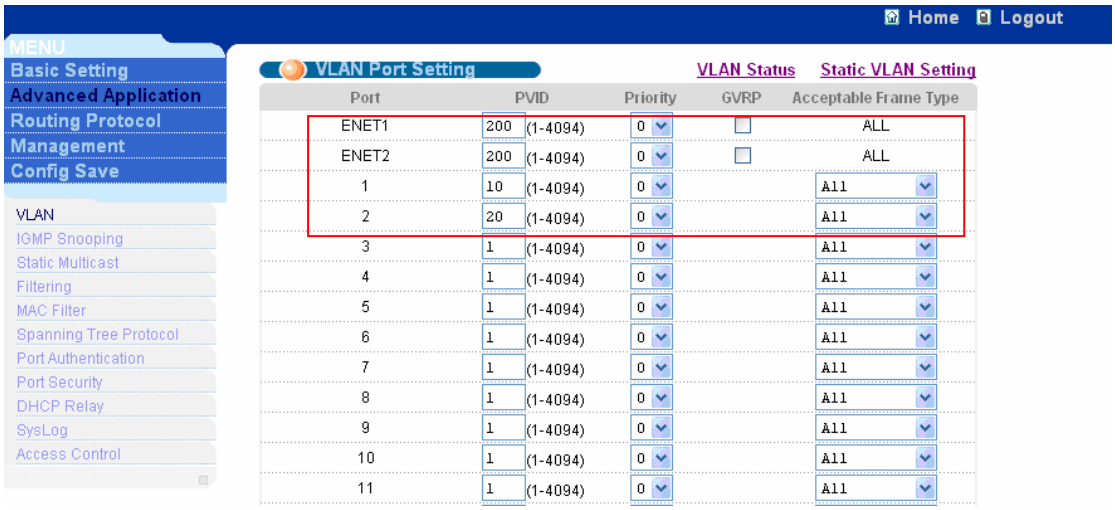


1.2 PVID settings

After set up the three VLAN, we can see Vlan10, Vlan20 and Vlan200 as shown. Now, click **VLAN Port Setting** to set the PVID.

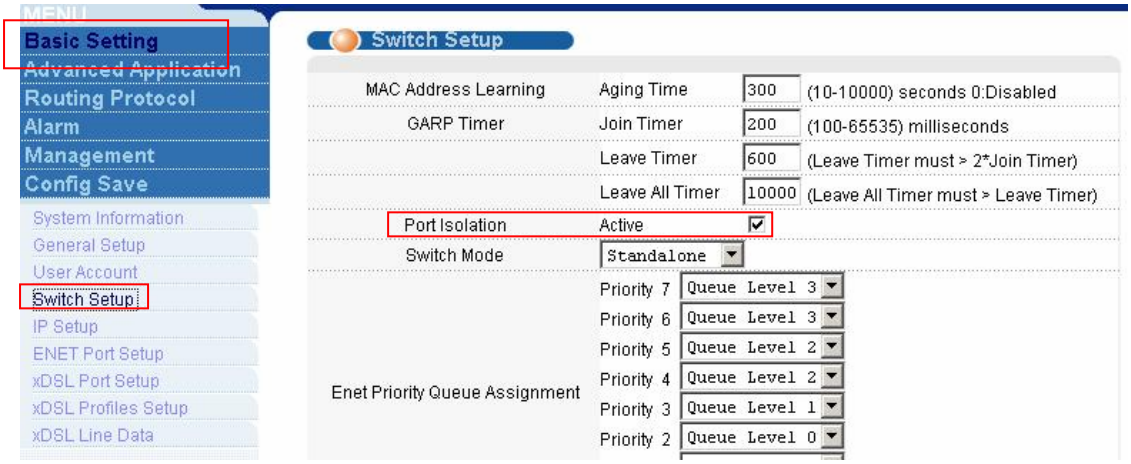


We assign VLAN 200(PVID) to ENET1, ENET2. Also, we assign VLAN 10 and VLAN 20 to Port1 and port2, respectively as shown.



1.3 Port Isolation

If we just want to isolate ports of IES-1248 and don't want to set any VLAN, there is another easy way to do this. Click **Basic setting**, **Switch Setup** in navigation panel to display configuration screen as shown. Check **Port isolation Active** check box.



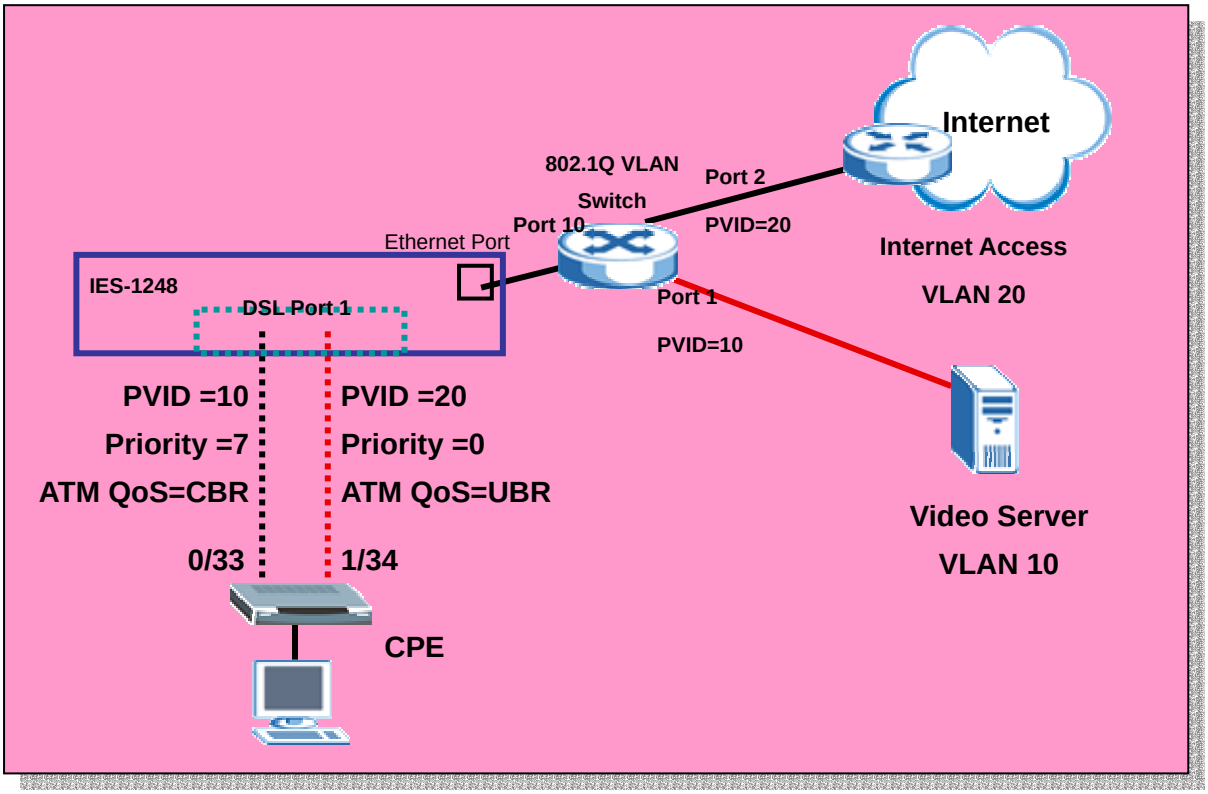
2. Prestige 660R-61 Settings

Please refer to the procedures in previous application.

Triple play Application

The IES-1248 allows you to use different channels(also called Permanent Virtual Circuits or PVCs) for different services. Define channels on each DSL port for different services and assign each channel a priority, a VLAN and ATM Quality of Service (QoS). The ATM QoS allows you to regulate the average rate and fluctuations of data transmission. This helps eliminate congestion to allow transmission of real time data (such as audio and video).

In this application, we demonstrate how to set up the multiple PVCs environment. From the figure below, the PC wants to access the two kinds of network services. One is the Internet service (data service) and the other is Video service. Because we hope we can see the video smoothly, we need to set the video service higher priority. In IES-1248, we can set the two services with different VLANs and assign the PVCs with different VLAN, priority and ATM QoS. That will make the video traffic get the higher priority than data traffic. We also can expand this application to triple play environment.



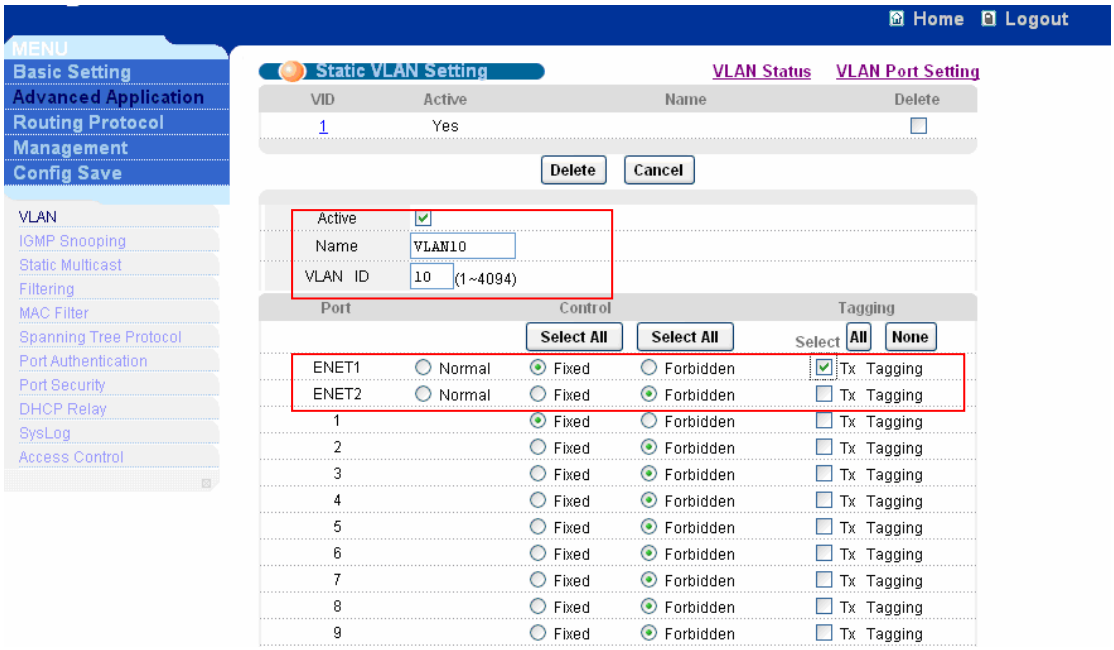
How to set up a Multiple PVCs environment.

Following procedures will introduce the settings of IES-1248, VLAN-aware switch and ADSL CPE. We use ZyXEL ES-2024 and Prestige 660R-61 as VLAN-aware switch and ADSL CPE, respectively.

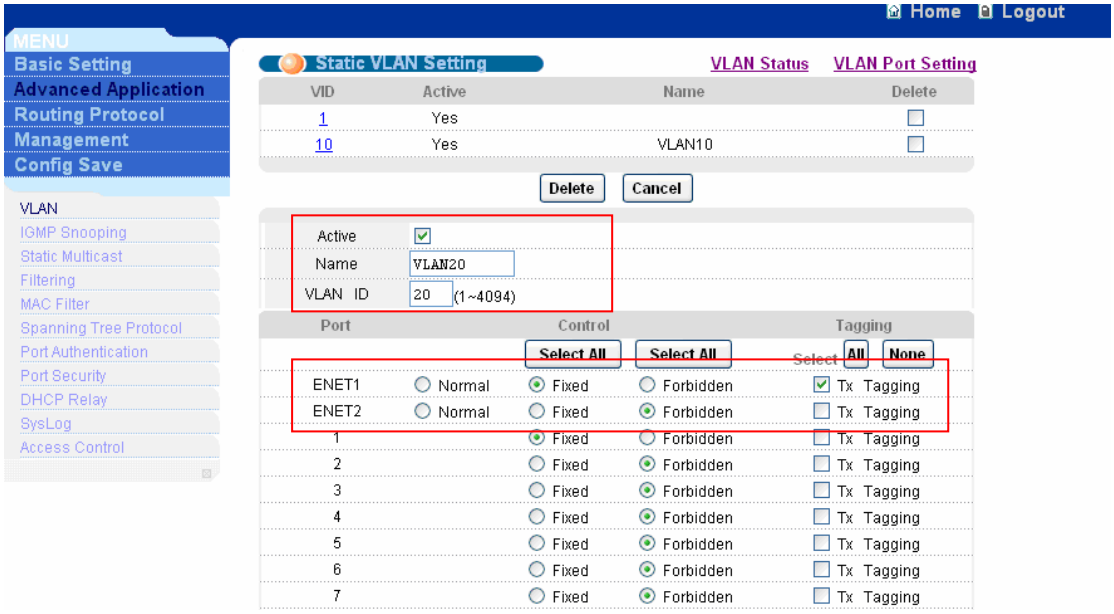
1. IES-1248 Settings

1.1 VLAN setup

We can set up VLAN like procedure described in VLAN application. Add VLAN10. Assign Port 1, ENET1 to be members of VLAN10 as show. We need to check the **Tx Tagging** on ENET1.

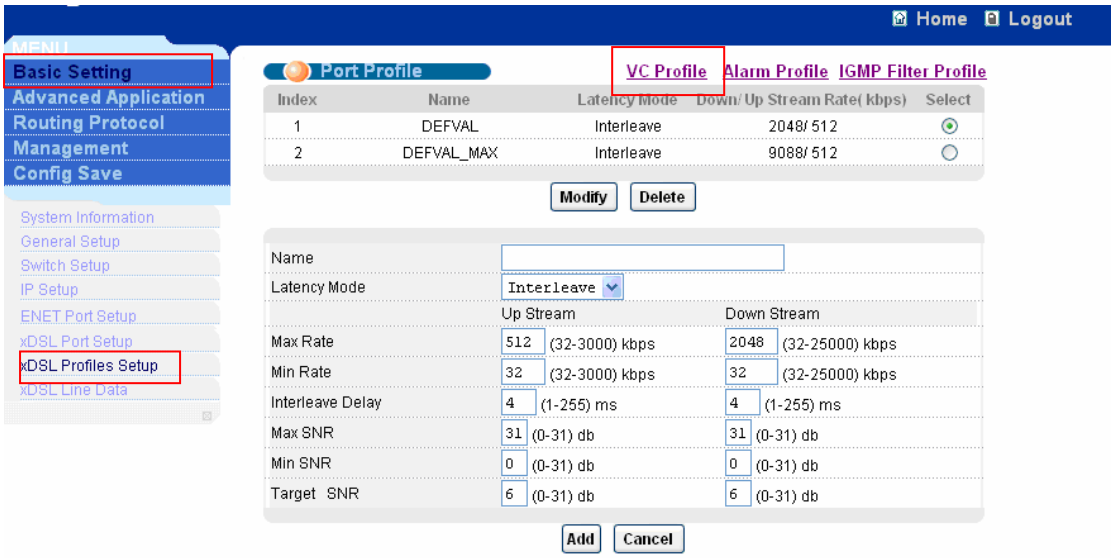


Add VLAN20. Assign Port 1, ENET1 to be members of VLAN20 as show. We need to check the **Tx Tagging** on ENET1.

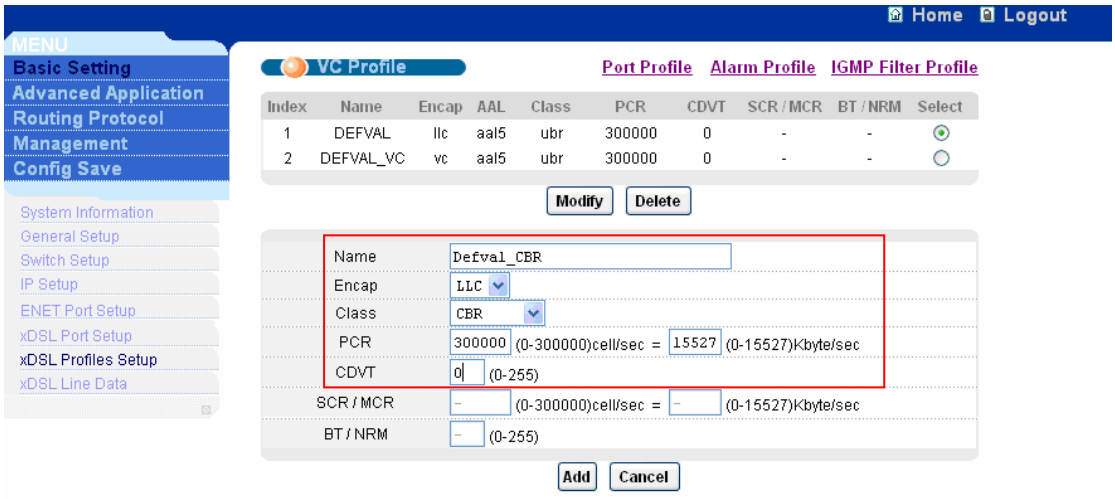


1.2 VC profile setup

Click **Basic Setting** and **xDSL Profile Setup** in navigation panel to display the configuration screen as shown. Click VC profiles in this screen.

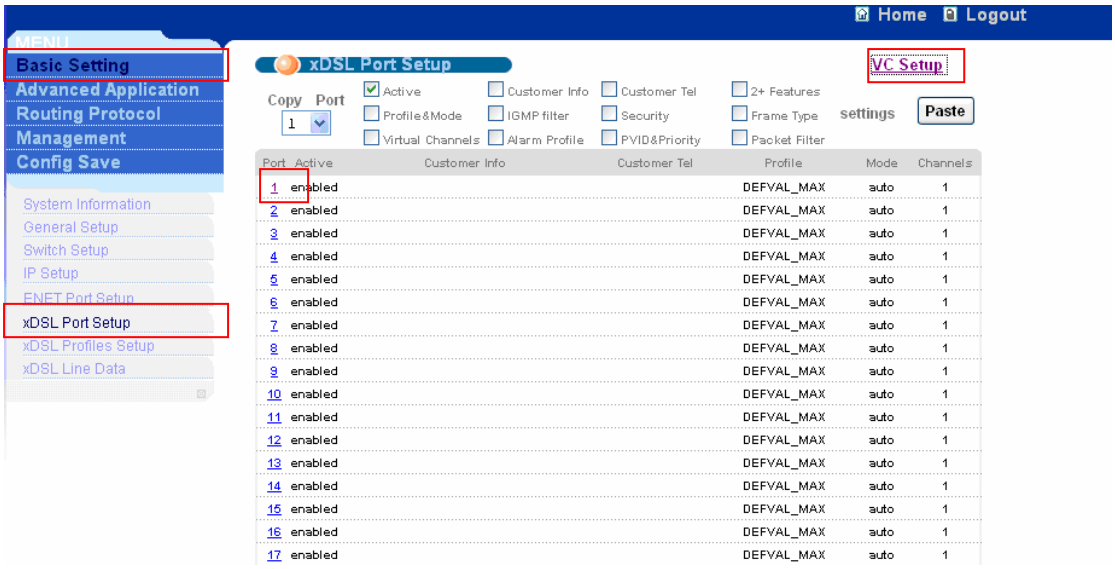


Add Defval_CBR VC profile. Set up Encap, Class, PCR and CDVT as shown. **Encap** should be LLC the same as IES-1248. **Class** should be CBR which has higher priority in ATM QoS.

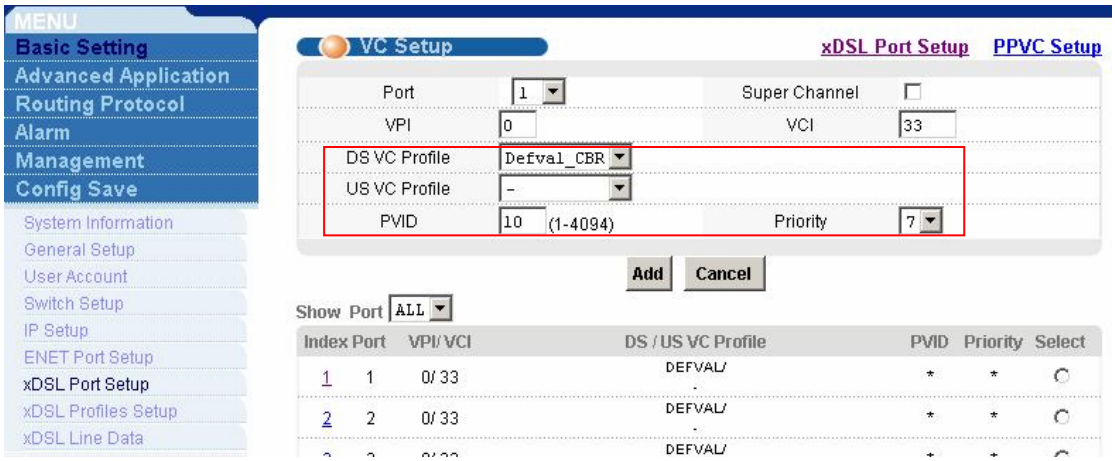


1.3 Multiple PVCs setup

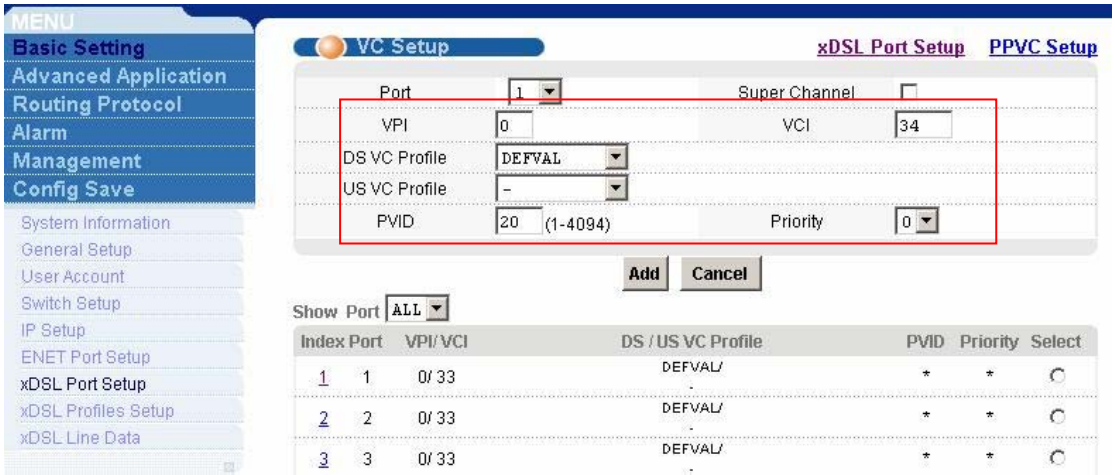
Click **Basic Setting** and **xDSL Port Setup** in navigation panel to display the configuration screen as shown. Click **VC Setup** in this screen.



We hope VPI/VCI with 0/33 get the higher priority. We should modify this VPI/VCI with Defval_CBR profile which we created before. Press **Apply** button to make it take effect.



Then we add the VPI/VCI with 0/34. We apply the DEFVAL profile to this channel.



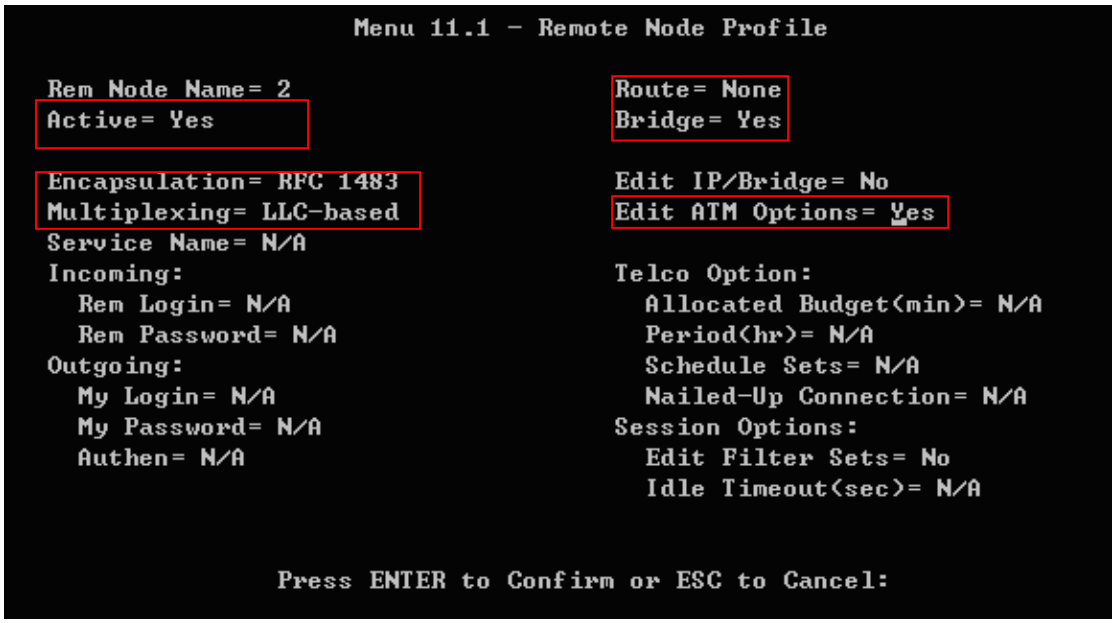
2. Prestige 660R-61 Settings

We need to set two channels. One is 0/33 and the other is 0/34. From former

application, we already knew how to set up CPE with one channel (0/33). We just demonstrate how to set up second channel.

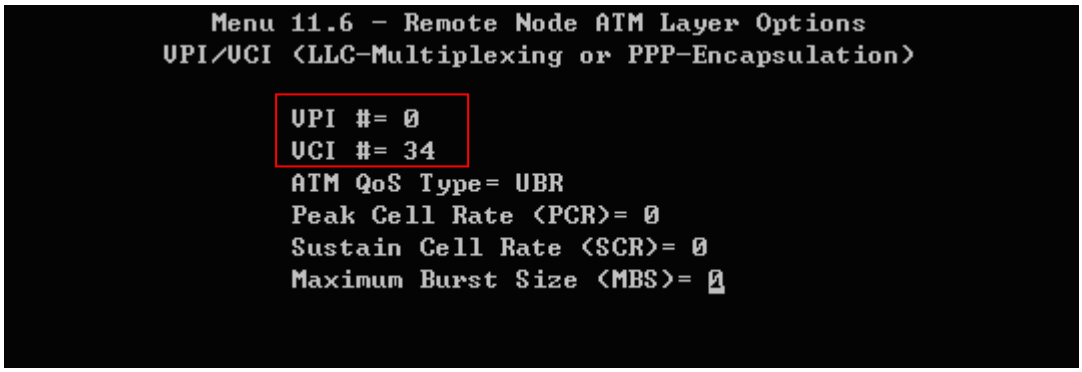
2.1 Menu11.1: Remote Node Profile

In menu11.1, we should activate this profile with “Active= Yes”. The Encapsulation and the Multiplexing are the same as the menu 4. Setting “Edit ATM Options=Yes” will enter Menu 11.6.



2.2 Menu11.6: Remote Node ATM Layer Options

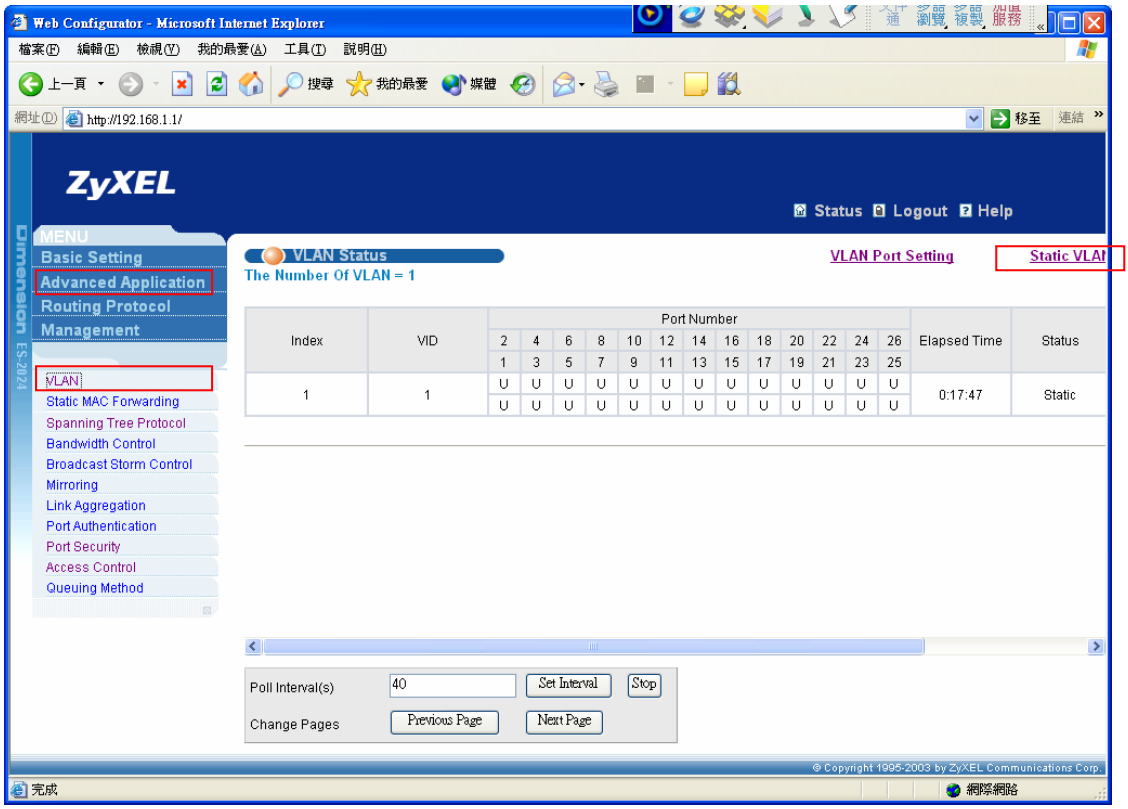
We should set up another VPI/VCI with 0/34 the same as the IES-1248.



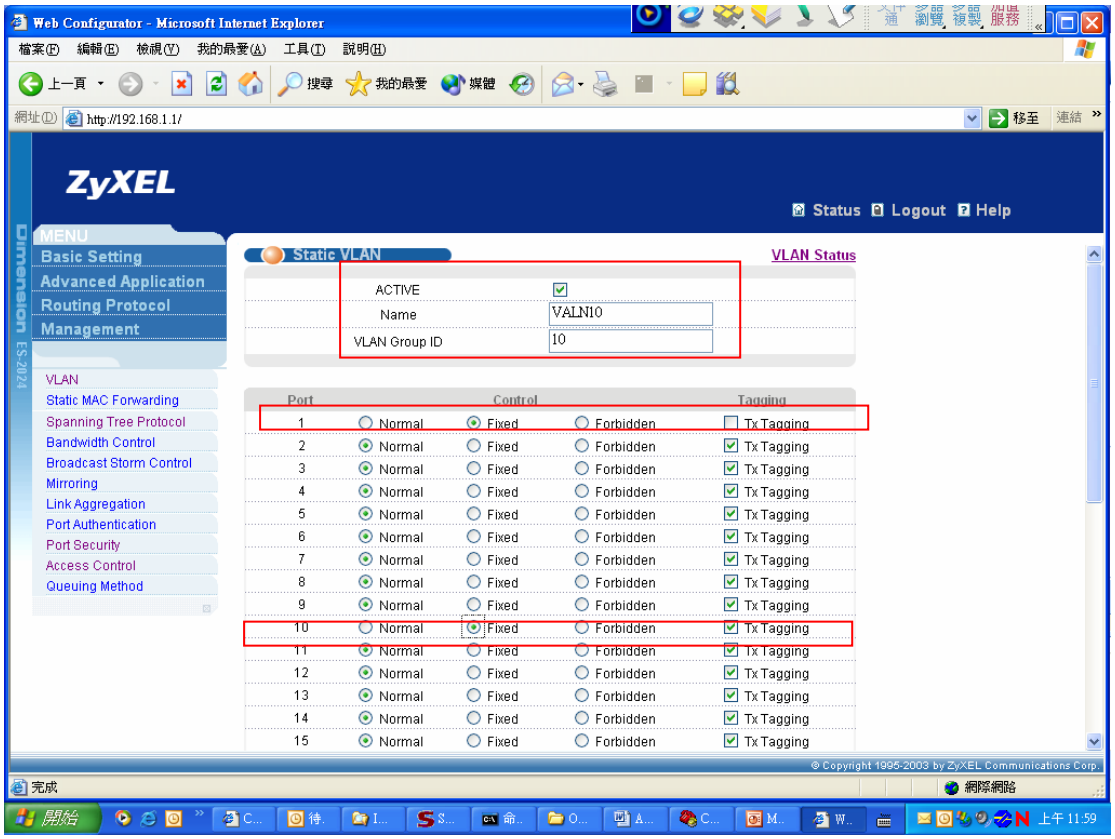
3. ES-2024 settings

3.1 VALN

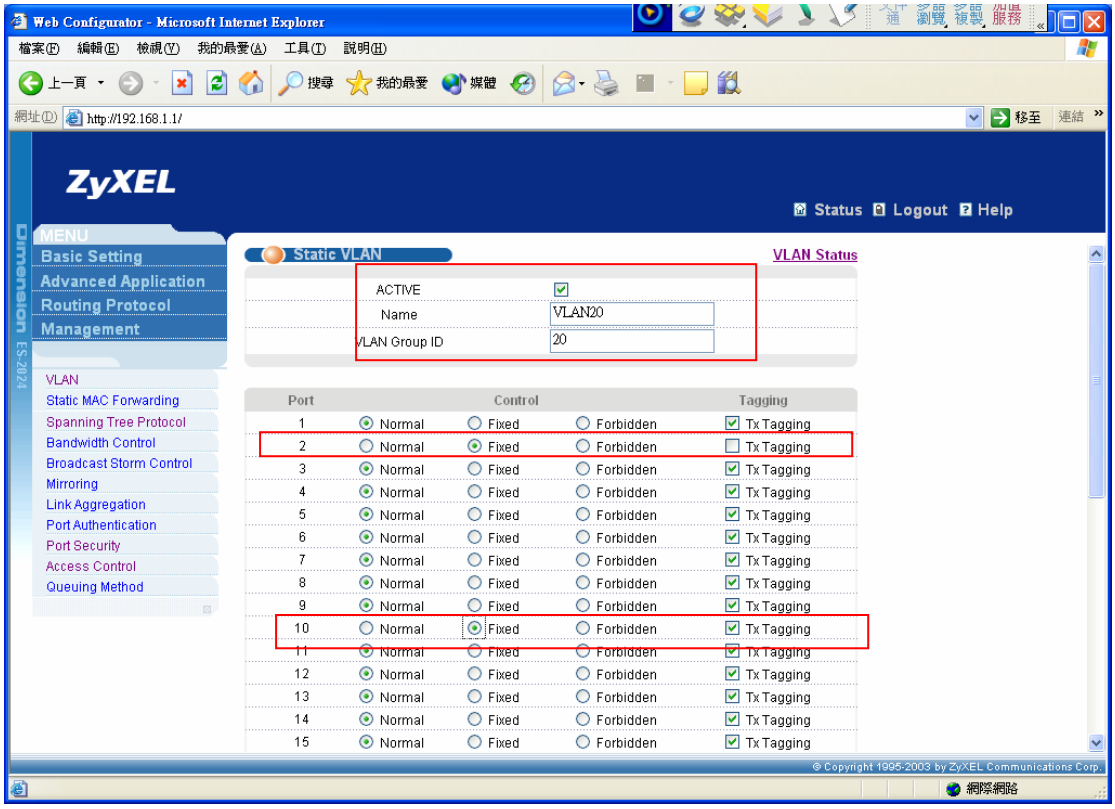
Click **Advanced Application** and **VLAN** in navigation panel to display configuration screen as shown. Click **Static VLAN** to show VLAN setup screen.



Add VLAN10. Assign Port 1, Port 10 to be members of VLAN10 as show. We need to check the **Tx Tagging** on Port 10.

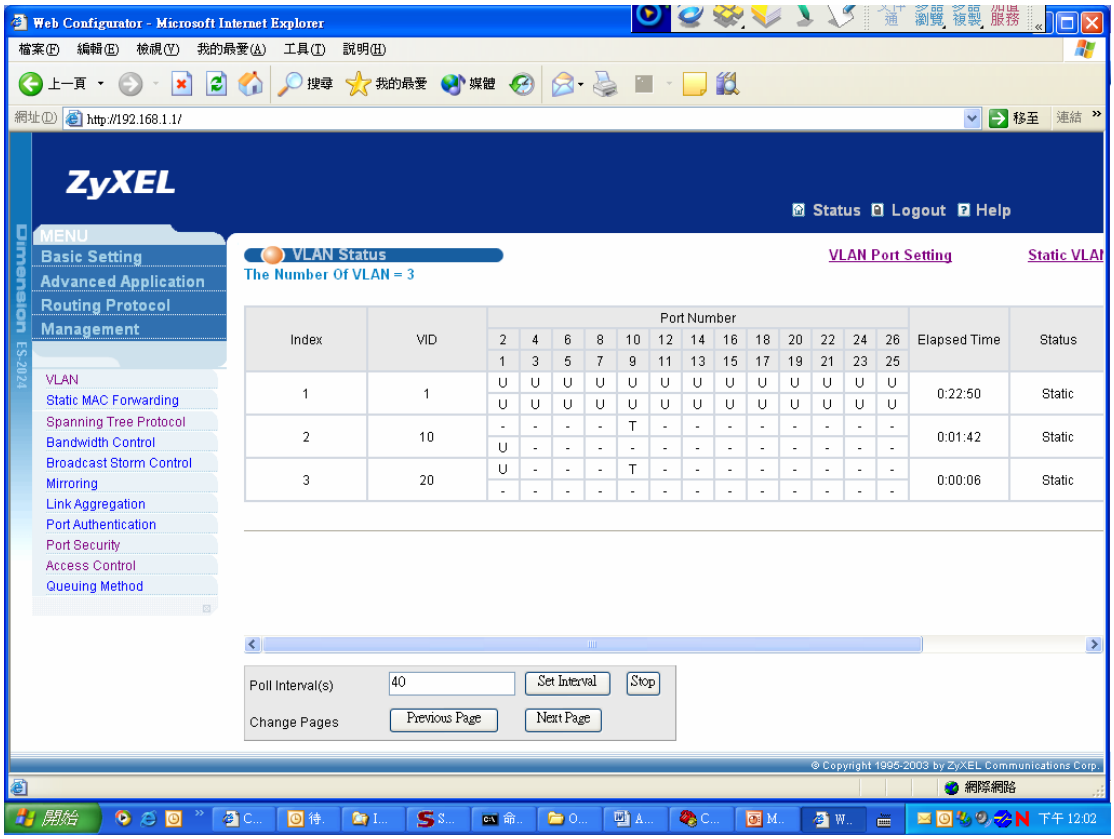


Add VLAN20. Assign Port 2, Port 10 to be members of VLAN20 as show. We need to check the **Tx Tagging** on Port 10.

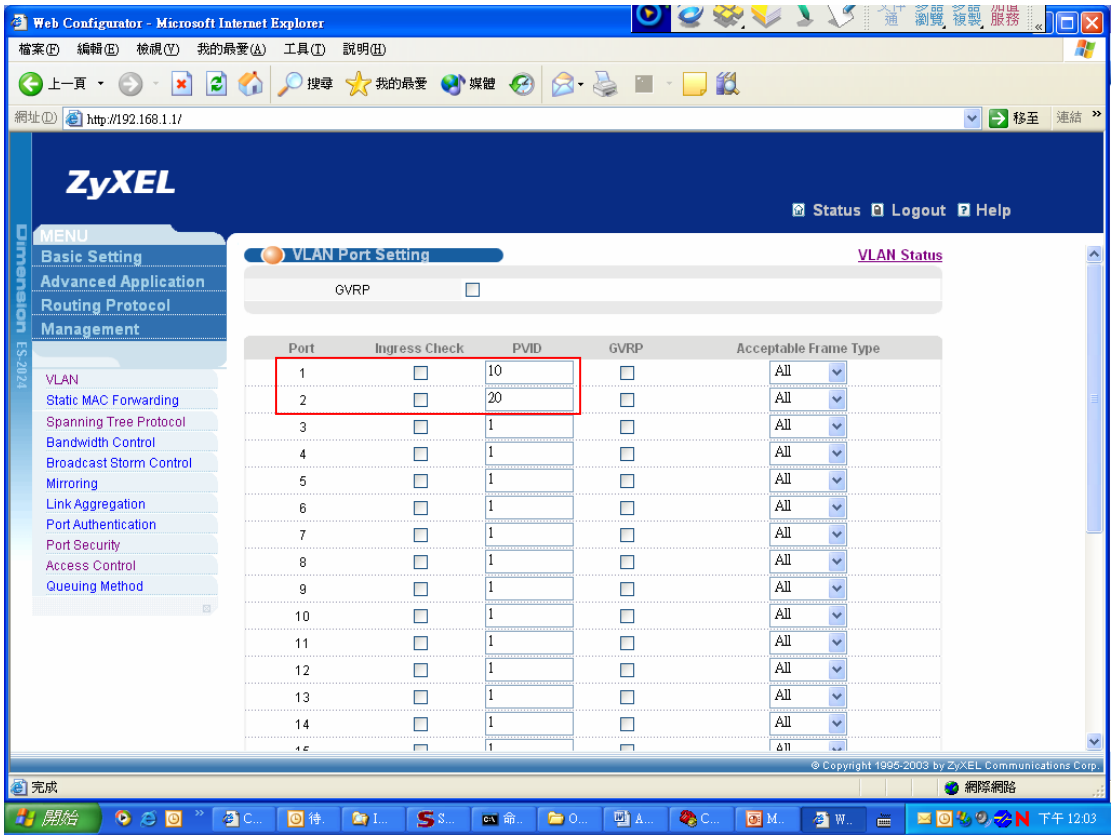


3.2 PVID setup

Click **Advanced Application** and **VLAN** in navigation panel to display configuration screen as shown. Click **VLAN Port Setting** to show PVID setup screen.



Let 10 be the PVID of Port 1 and 20 be the PVID of Port 2.



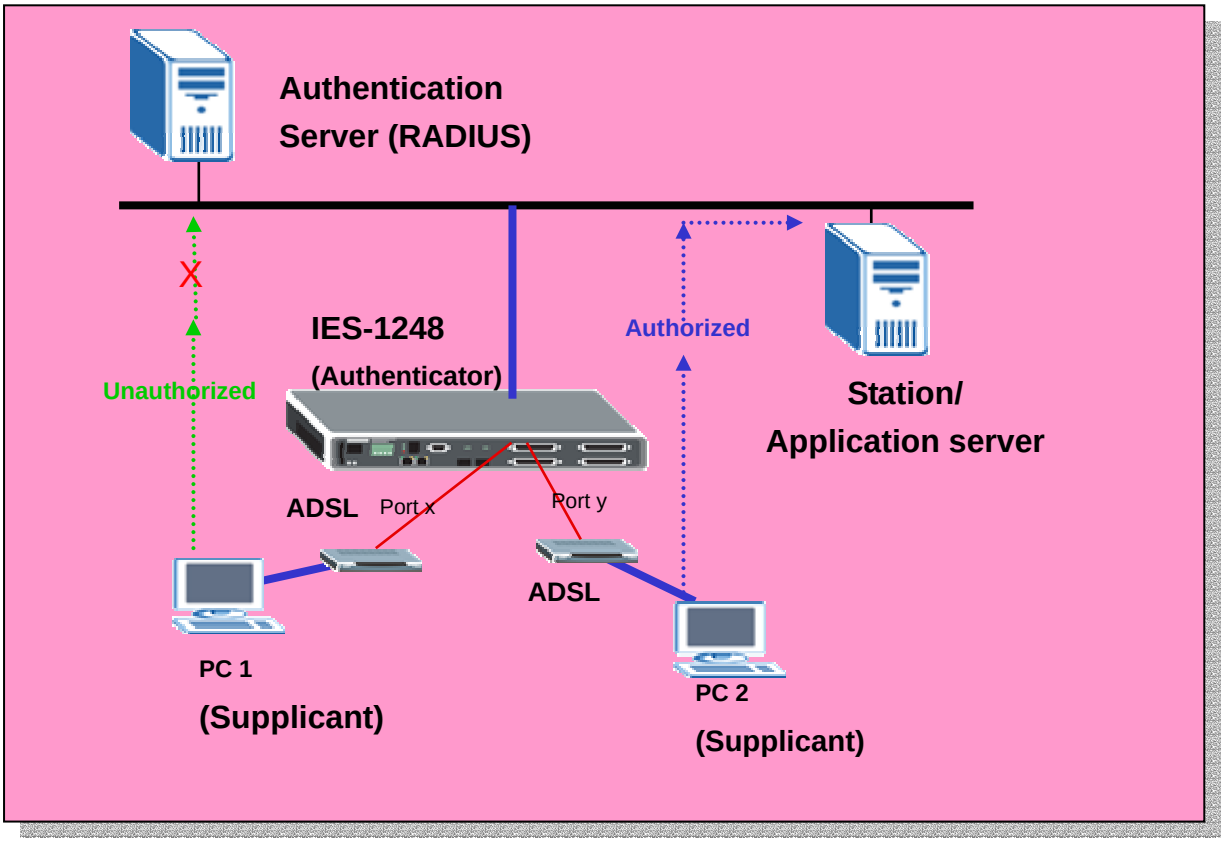
In this application, you will see the video traffic will go via 0/33 and data traffic

will go via 0/34. And the 0/33 get the higher priority. The video traffic will go first when the two traffics arrive at the same time.

802.1x Application

IEEE 802.1x port-based authentication is desired to prevent unauthorized ports (clients) from gaining access to the network. It is an extended authentication protocol that allows support of RADIUS (Remote Authentication Dial in User Service, RFC2138, 2139) for centralized user profile management on a network RADIUS server.

We want to deploy 802.1x environment in this application. The following figure shows the 802.1x example. PC1(supplicant) and PC2(supplicant) want to access to the application server. If PC1 is not unauthorized, the traffic from PC1 to application server will be blocked. If PC2 is an authorized client, then it can access to the application server. From the figure, IES1248 acts as an authenticator.



How to set up an 802.1x environment.

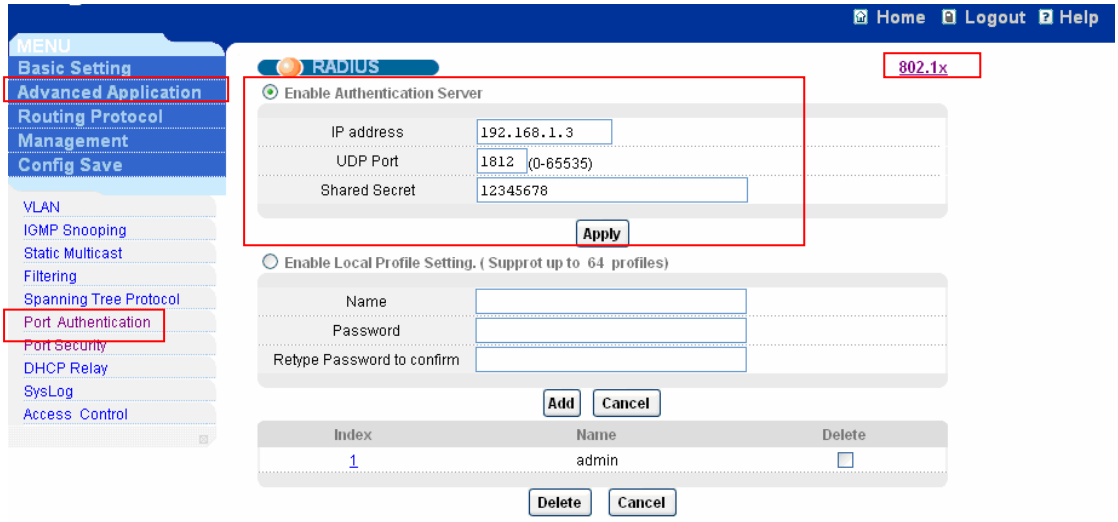
We should configure Authenticator, RADIUS and Supplicant three parts in 802.1x

environment. The Microsoft 802.1x client and ZyXEL Vantage 50 will be used as supplication and RADIUS, respectively. Following sections will describe the detailed procedure to set up the environment.

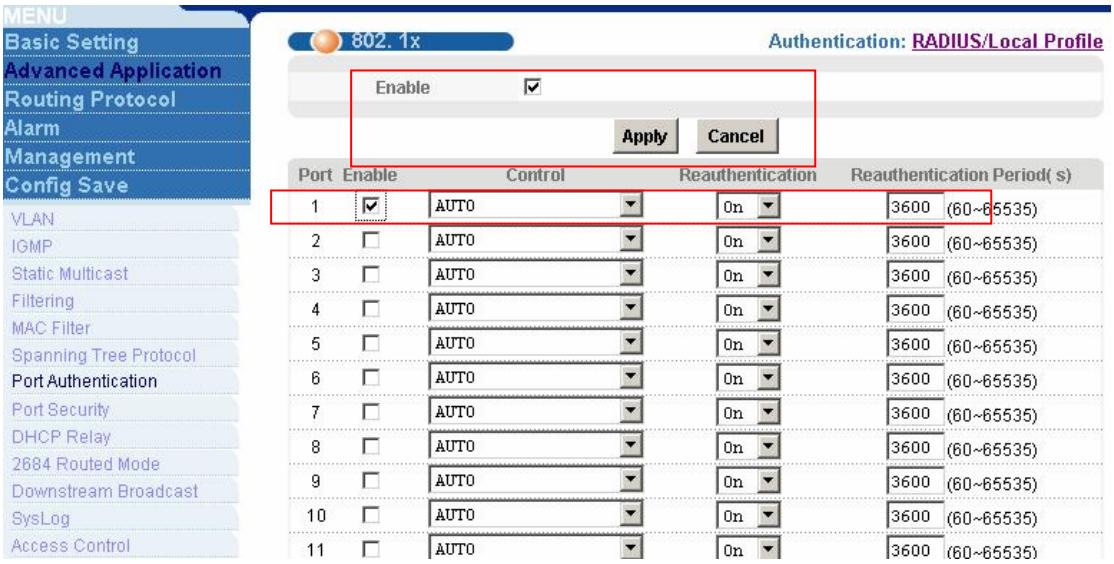
1. IES-1248 (Authenticator) settings:

1.1 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.



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.

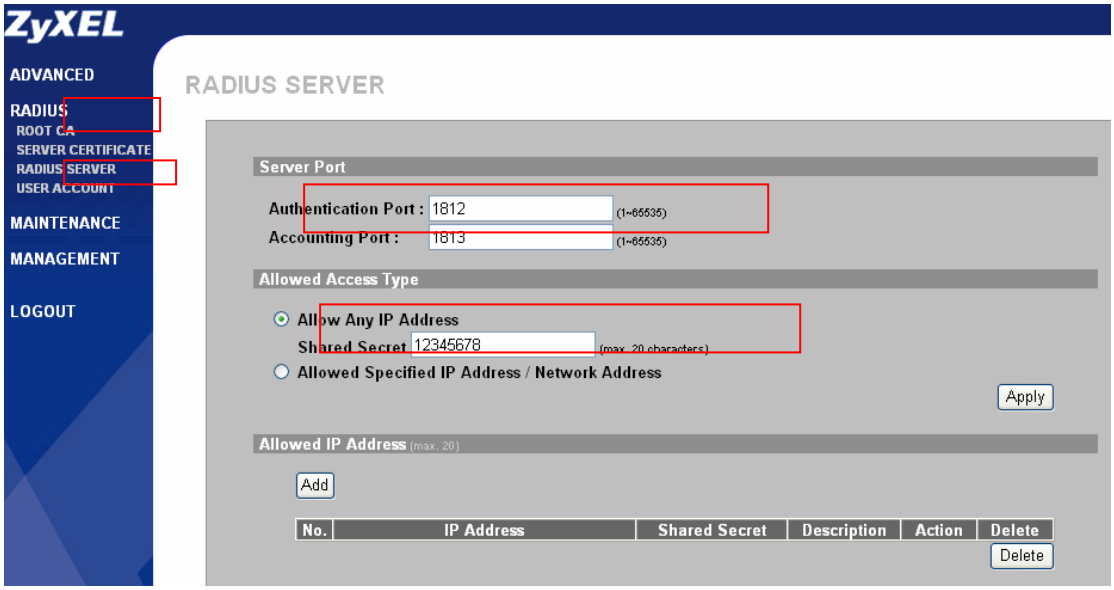


2. Vantage 50(RADIUS) settings:

We use Vantage 50 as the RADIUS server. It's a one of ZyXEL's product. Of course, you can use other RADIUS server like Funk Steel-Belted RADIUS, Cisco Access Control Server, MeetingHouse Aegis server and so on. You can configure it by WEB GUI and its default IP is 192.168.1.3.

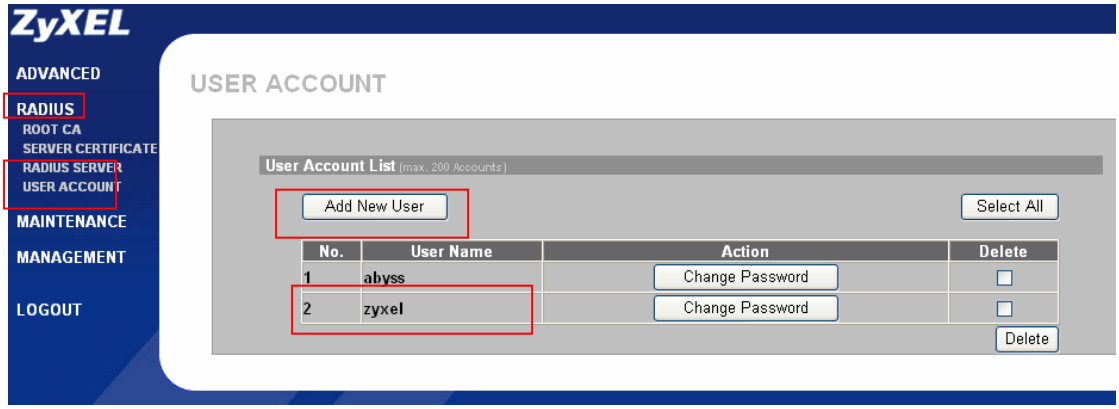
2.1 RADIUS server setup

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.



2.2 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.

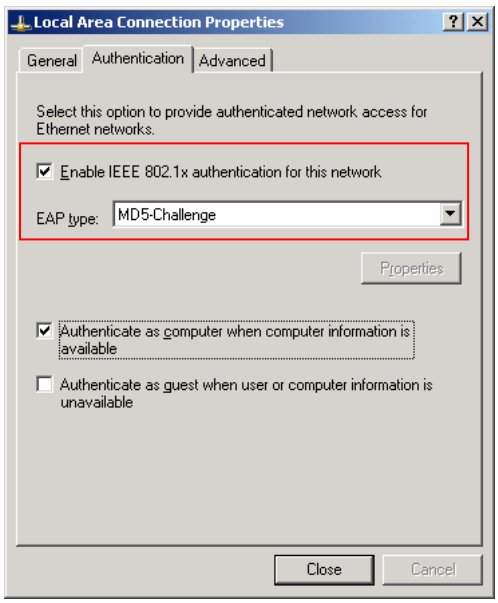


3. Windows XP(Supplicant) settings:

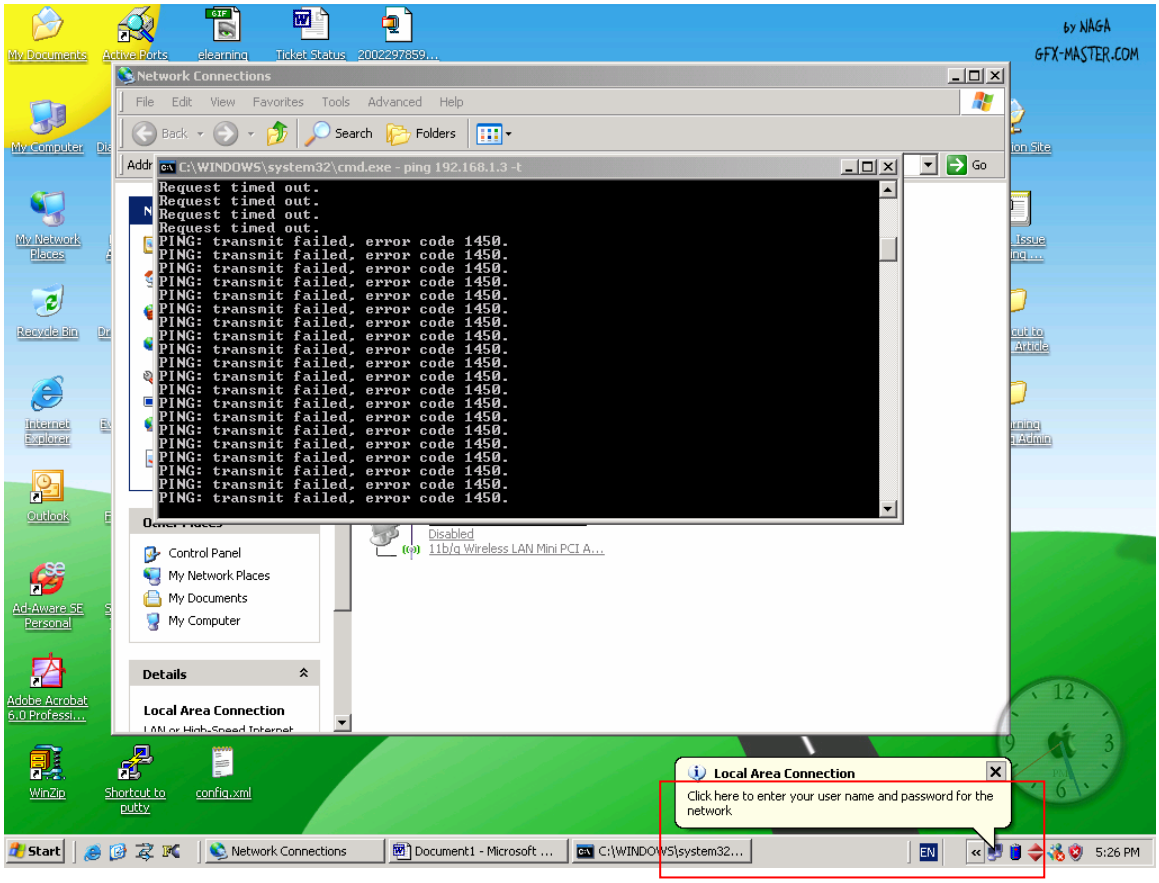
There are many supplicants we can choose like MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client. We take Microsoft 802.1x client as an example here.

3.1 802.1x/MD5-challenge setup

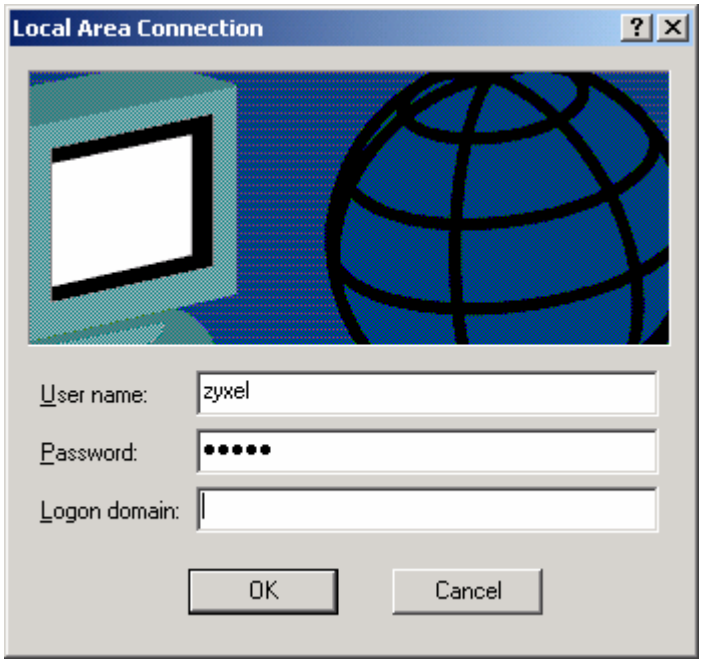
Open the **Local Area connection Properties**, and then click **Authentication** page. Check the **Enable IEEE 802.1x authentication for this network** and select the **MD5-challenge** in EAP type combobox. Please see the following figure.



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.



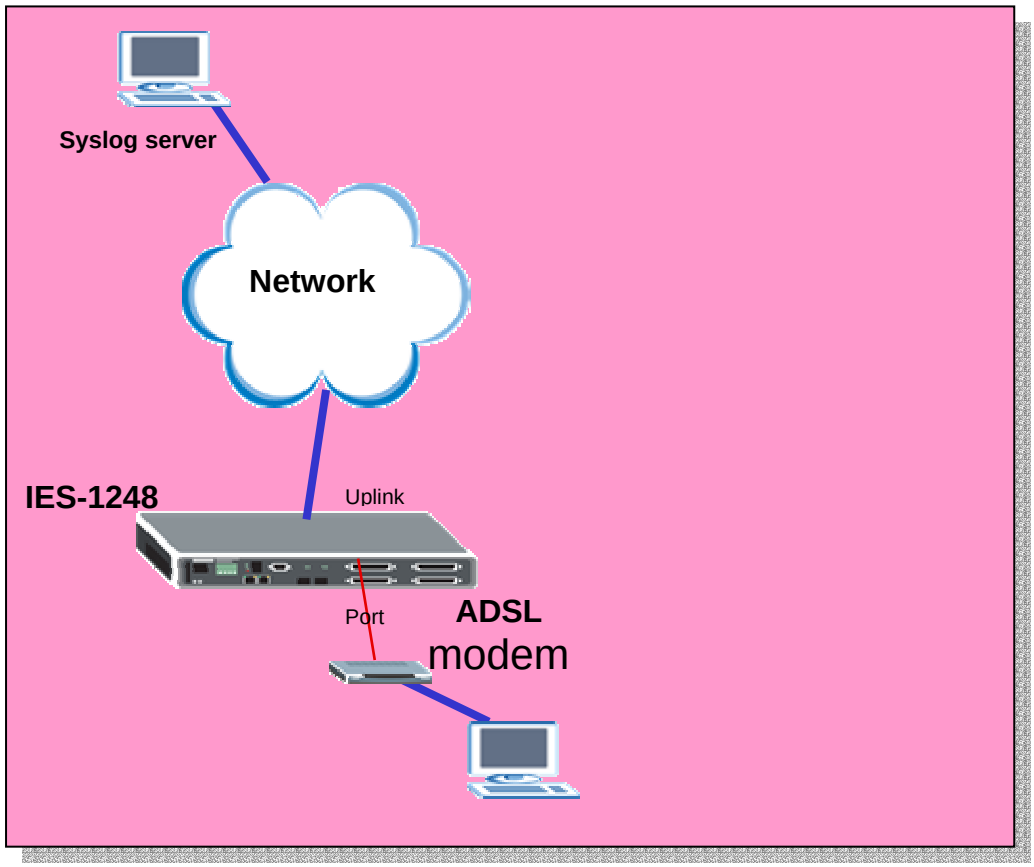
After above procedure, we can allow the authenticated port the access the server. If the DSL port doesn't be authenticated, the PCs behind the port can't access the network.

4. Prestige 660R-61 Settings

Please refer to the procedures in previous application.

Setting up the Syslog Server

ZyXEL products are able to send system log to a Syslog deamon such as Unix Syslogd and Kiwi's Syslog Daemon (http://www.kiwisyslog.com/). When DSL or Ethernet ports are linked up/down, IES-1248 sends a record to Syslog server. The Syslog server can be placed on the network, which IES-1248 can access.

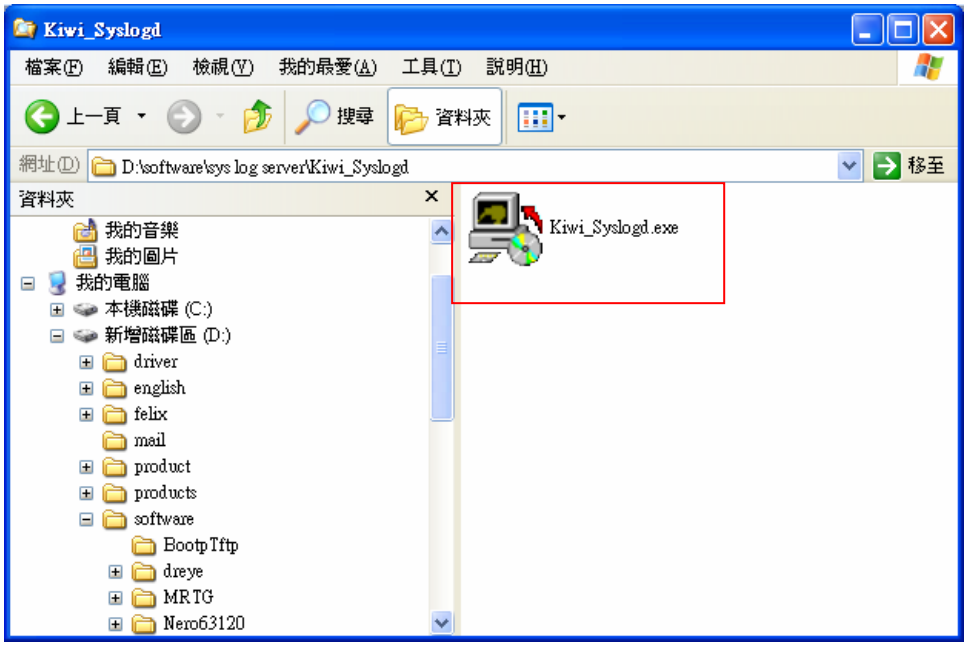


How to set up a Syslog server.

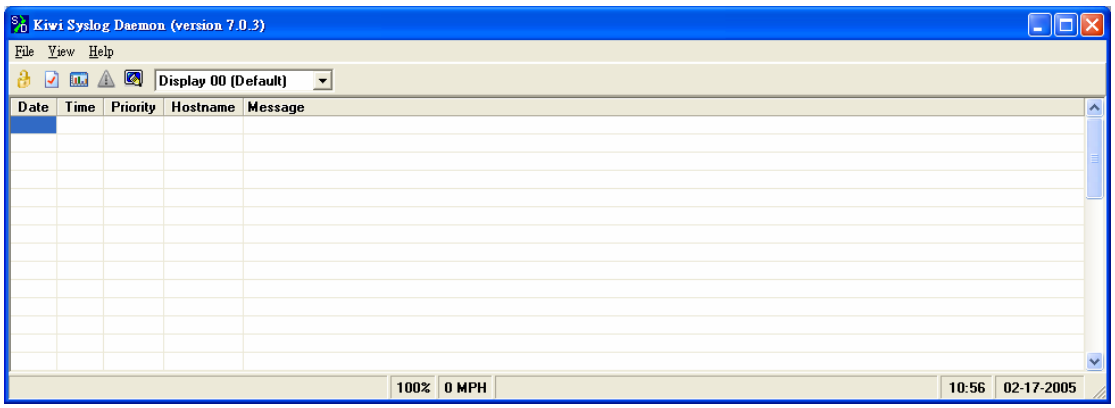
We should configure IES-1248 and Syslog server in this application. Here, we use the Kiwi's Syslog Daemon as an example. Following sections will describe the detailed procedures to set up the environment.

1. Install and Run Kiwi's Syslog Server

Double Click the Kiwi's Syslog Server installing program. It is very easy to install it.

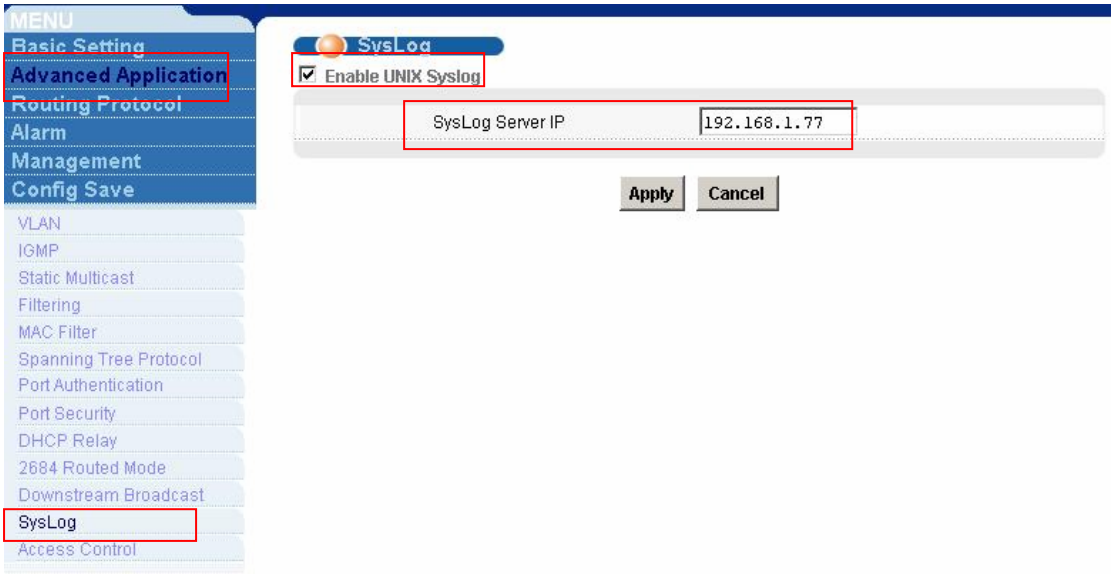


After finishing the installation, you can run it from the Start Menu. And you will see following dialog. And the Server's IP is 192.168.1.77.

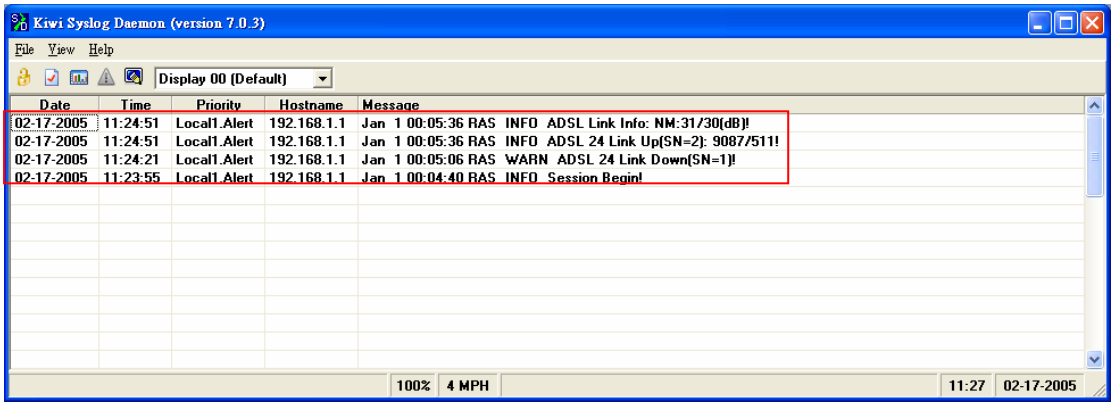


2. IES-1248 settings

Click **Advanced Application**, **SysLog** in the navigation panel to display configuration screen as shown. Check the **Enable UNIX Syslog**. Assign the UNIX Syslog Server IP, 192.168.1.77 in this case. Then press the **Apply** button and the setup is complete.

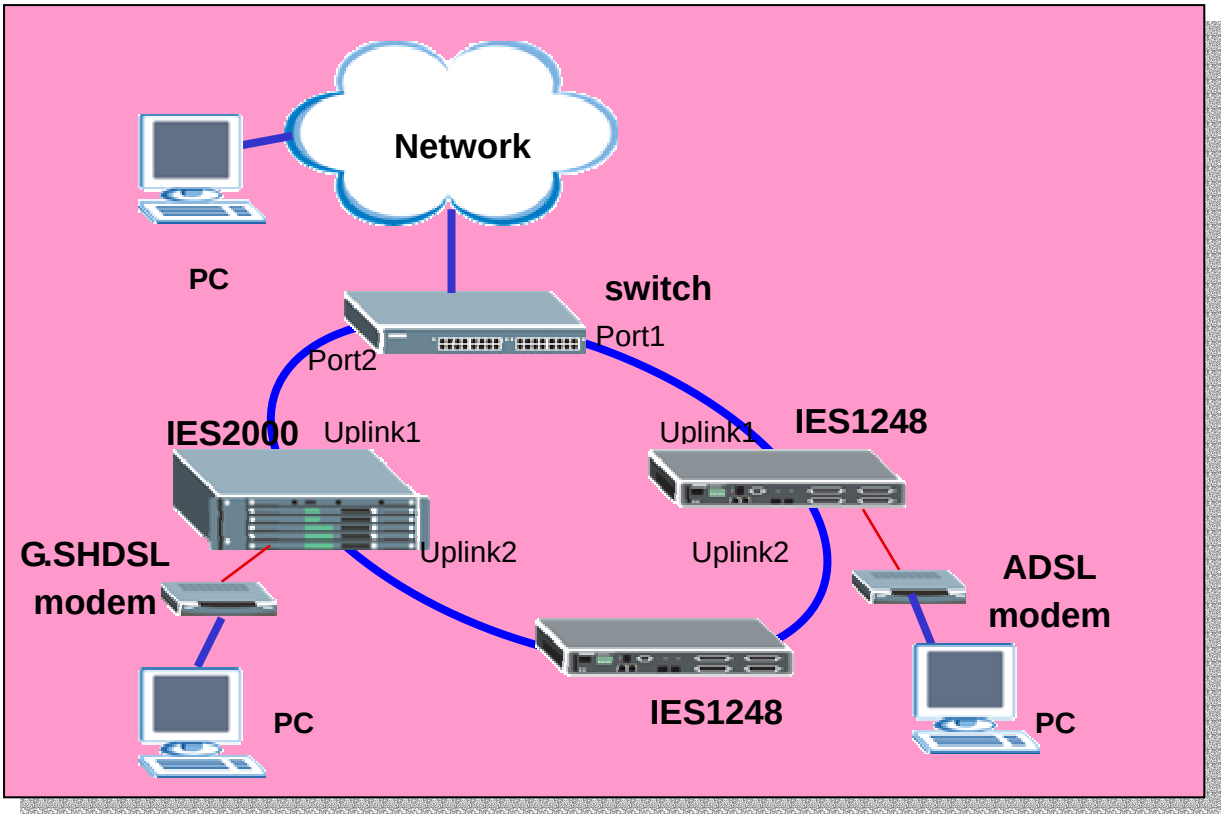


When DSL ports are linked up/down, IES-1248 sends a record to Syslog server. We can see these logs in Kiwi's Syslog server.



Setting up the Ring Environment

The Ring topology is used to guarantee the network being normal even if one link between two device broken. So, in ring topology, the network will work well if one link is broken. In Ring Topology, you must enable RSTP/STP to prevent the loop issue.



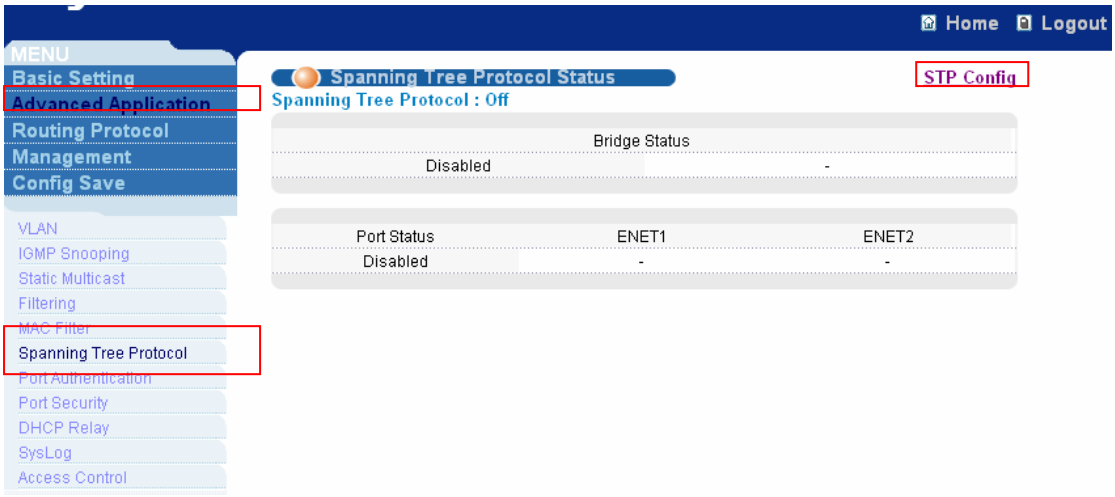
How to set up a Ring Environment.

We set up Ring environment with one IES1248, one IES2000 and one ES4024. A PC behind IES can connect the PC in the network even one of the links broken. Following sections will describe the detailed procedures to set up the environment.

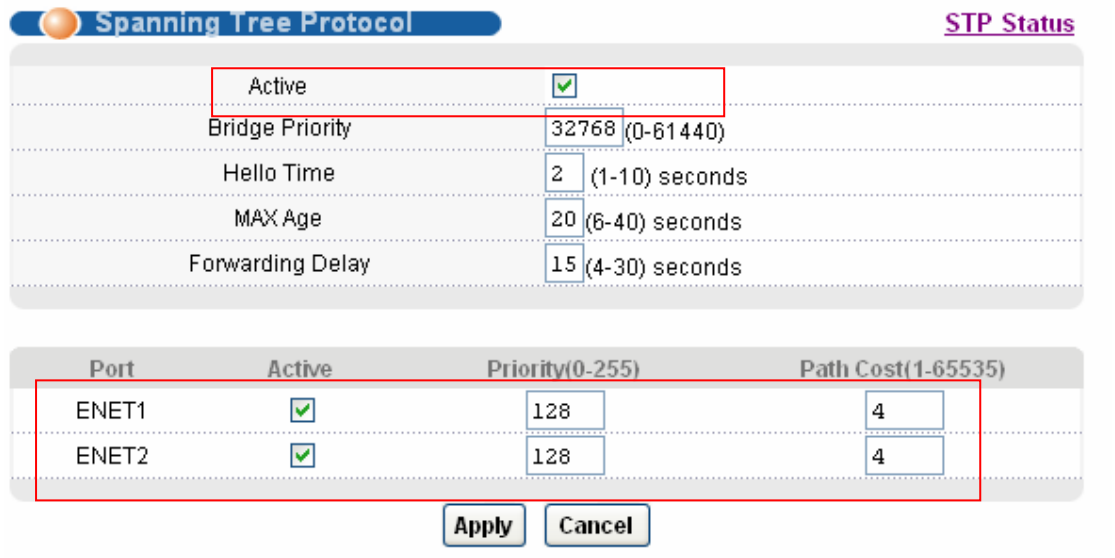
1. IES-1248 settings

1.1 Enable Spanning Tree protocol on Ethernet ports

Click **Advanced Application**, **Spanning Tree Protocol** in the navigation panel to display configuration screen as shown. You will see the **Spanning Tree Protocol Status** page. Click **STP config** to configure panning tree protocol settings.



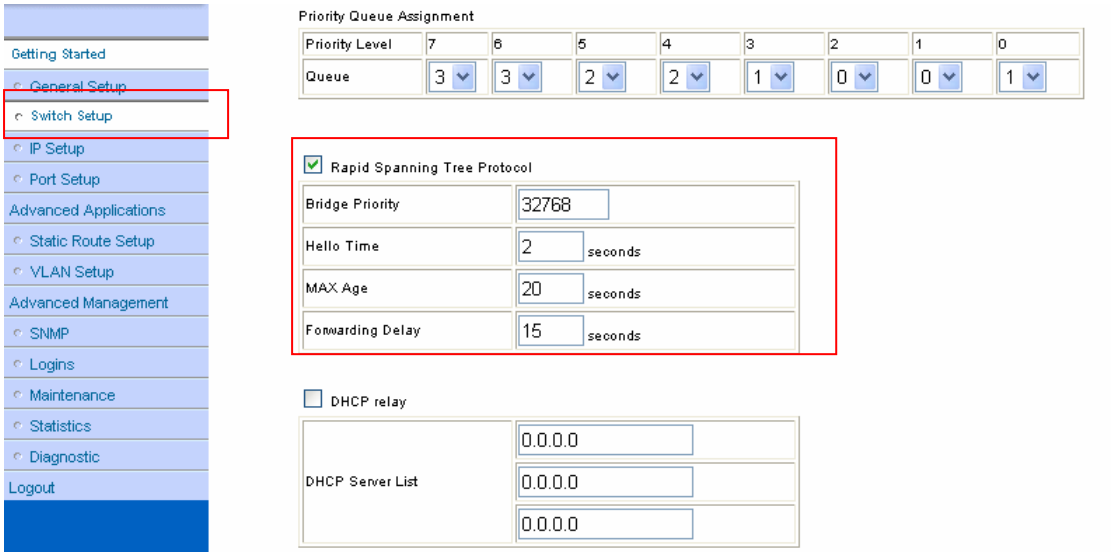
Click **Active** to enable Spanning Tree Protocol. Then enable it on **ENET1** port and **ENET2** port.



2. Setup IES2000

2.1 Enable Spanning Tree protocol

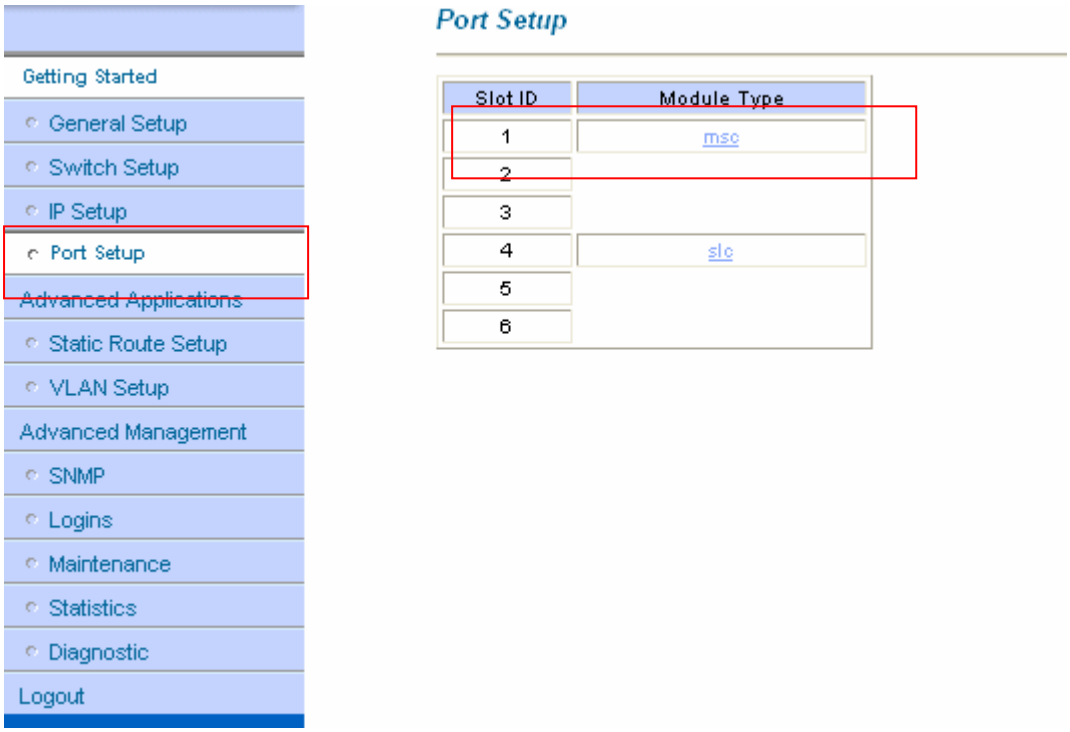
Click **Switch Setup** in the navigation panel to display configuration screen as shown. Then check **Spanning Tree Protocol** to enable it.



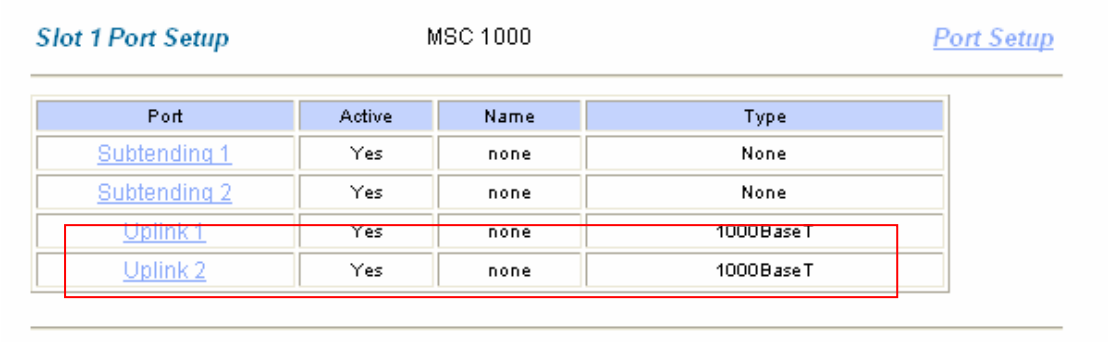
2.2 Enable Spanning Tree protocol on Ethernet ports

Click **Port Setup** in the navigation panel to display configuration screen as shown.

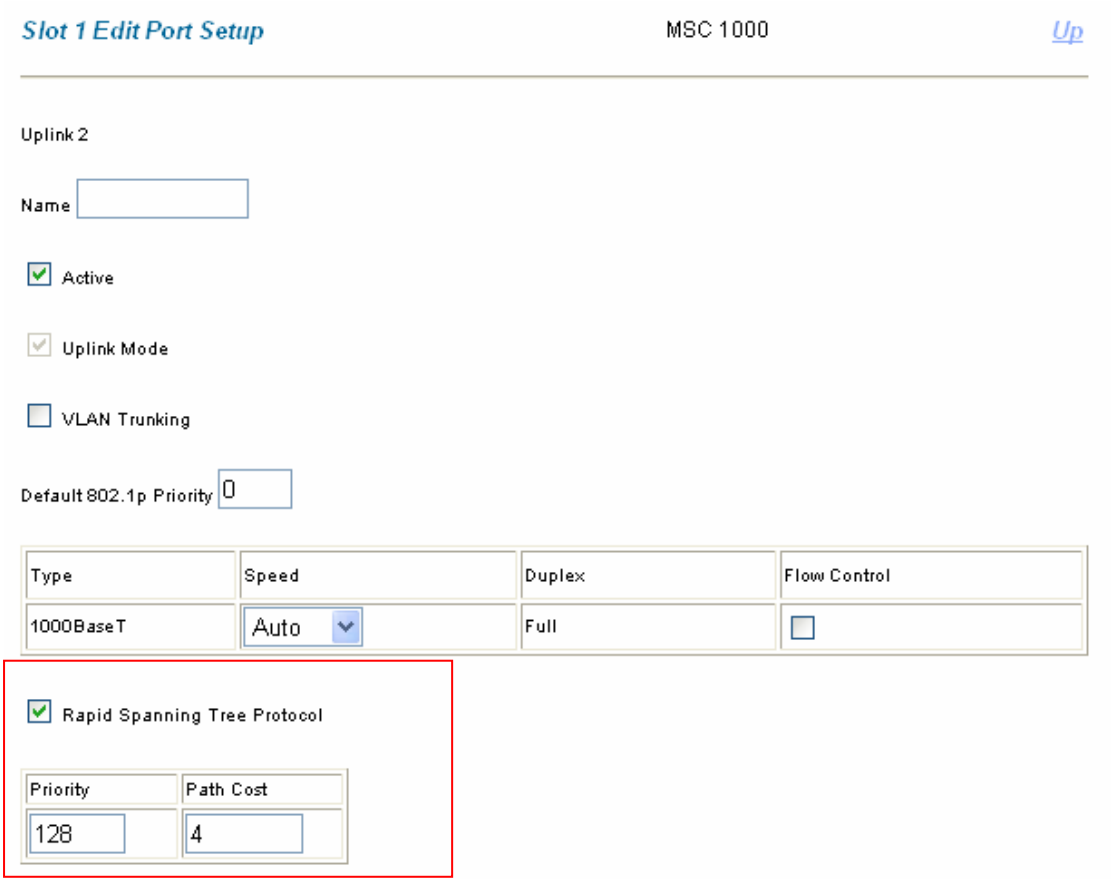
Click **msc** to display MSC card Port setup.



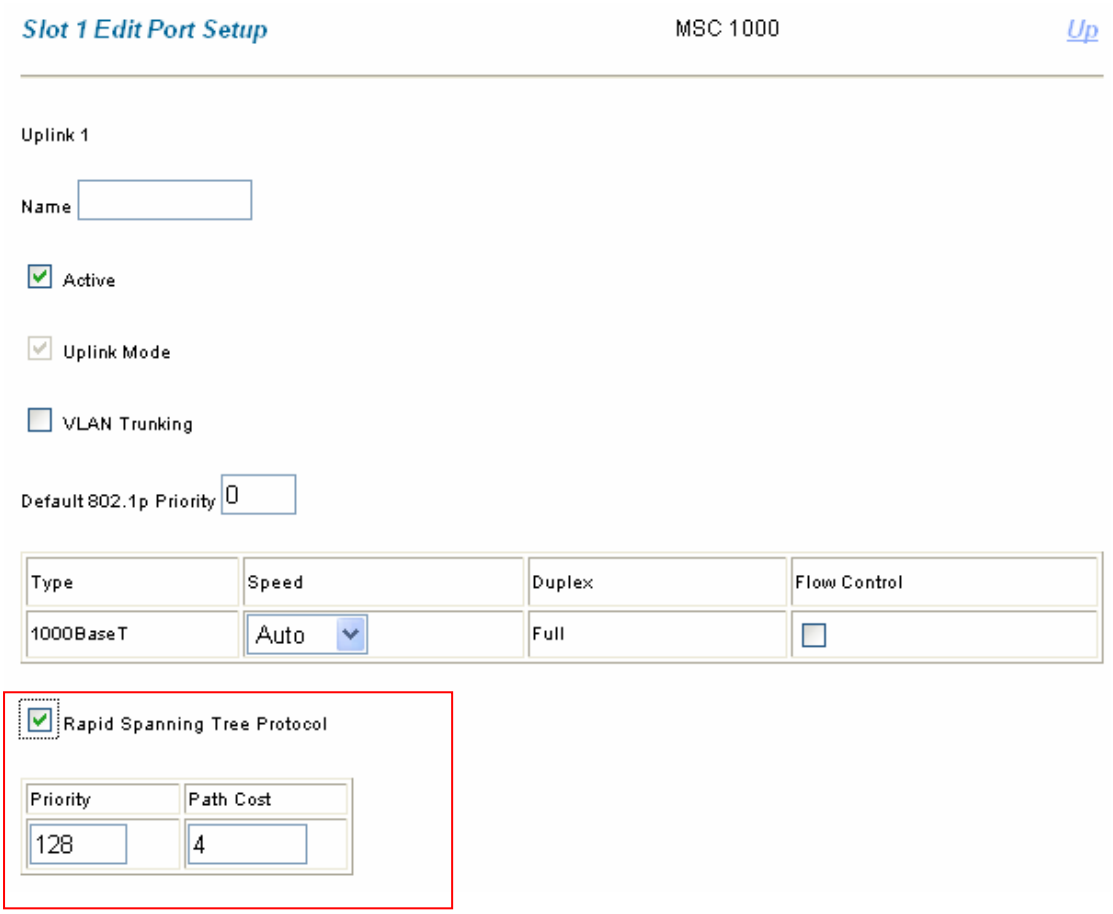
Click **Uplink2** to set up this port.



Check **Spanning Tree Protocol** to enable it.



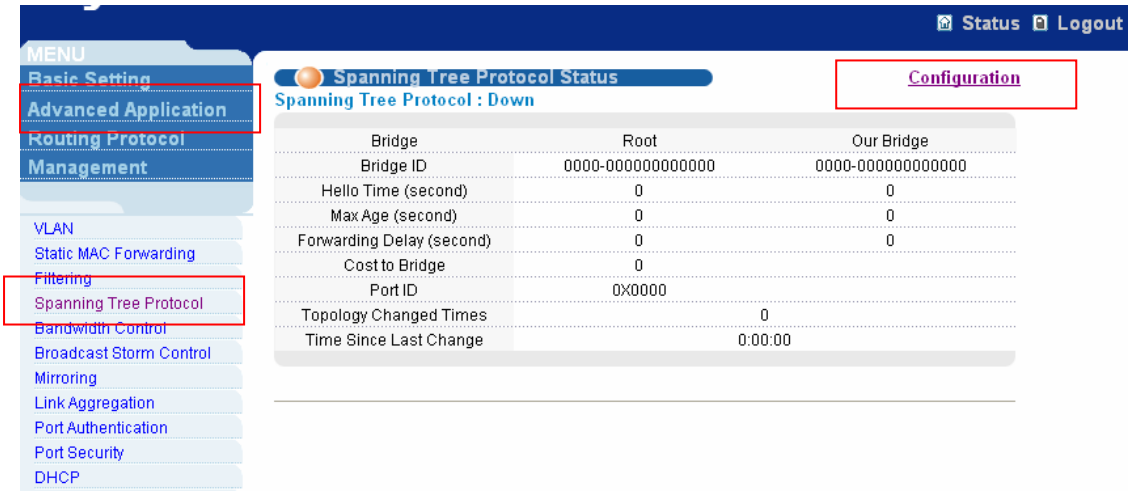
Take the same procedures with Uplink1. Please see the following figure.



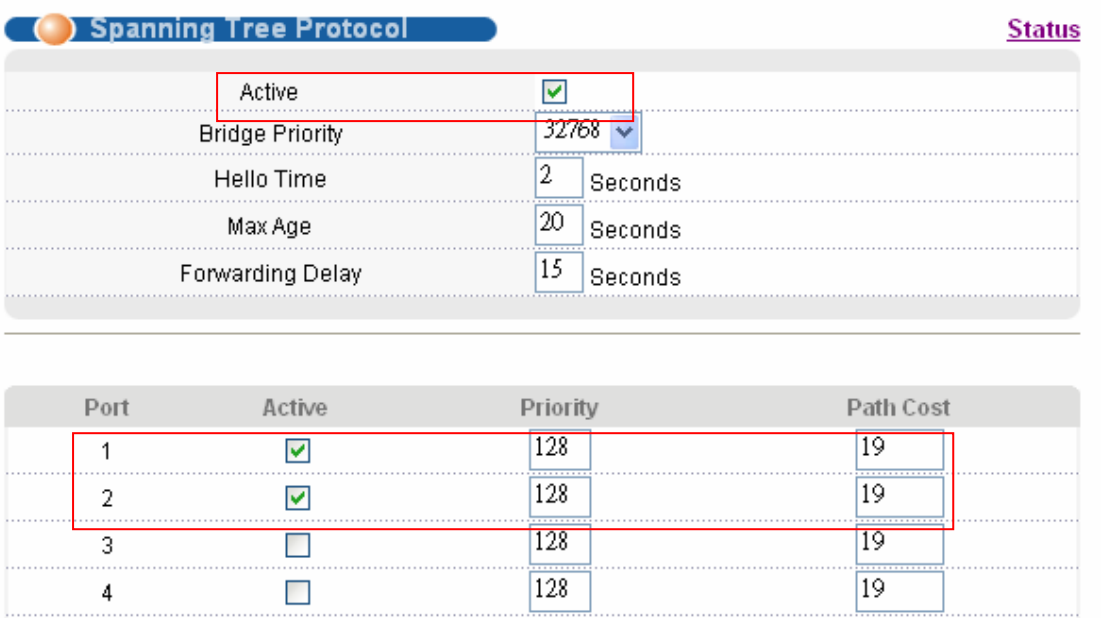
3. Setup ES4024

3.1 Enable Spanning Tree protocol on Ethernet ports

Click **Advanced Application**, **Spanning Tree Protocol** in the navigation panel to display configuration screen as shown. You will see the **Spanning Tree Protocol Status** page. Click **Configuration** to configure panning tree protocol settings.

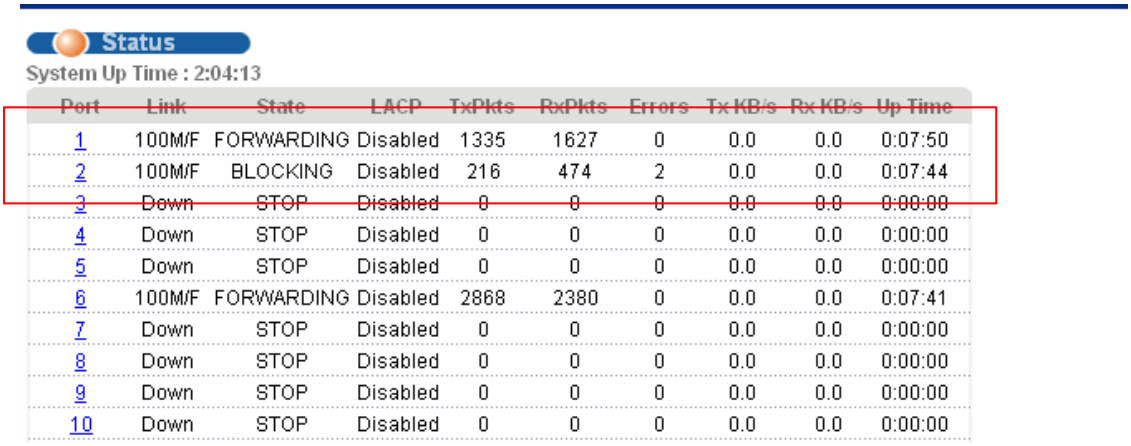


Click **Active** to enable Spanning Tree Protocol. Then enable it on **Port 1** and **Port 2**.



4. Results

We can see the link between port 2 of ES4024 and Uplink1 of IES2000 will be blocked as shown after we connect.



After we remove the cable between port 1 of IES1248 and port 1 of ES4024, the connection still exists. We can remove any one of the cable. That will not affect the connection. You can see the blocking port will become forwarding port.

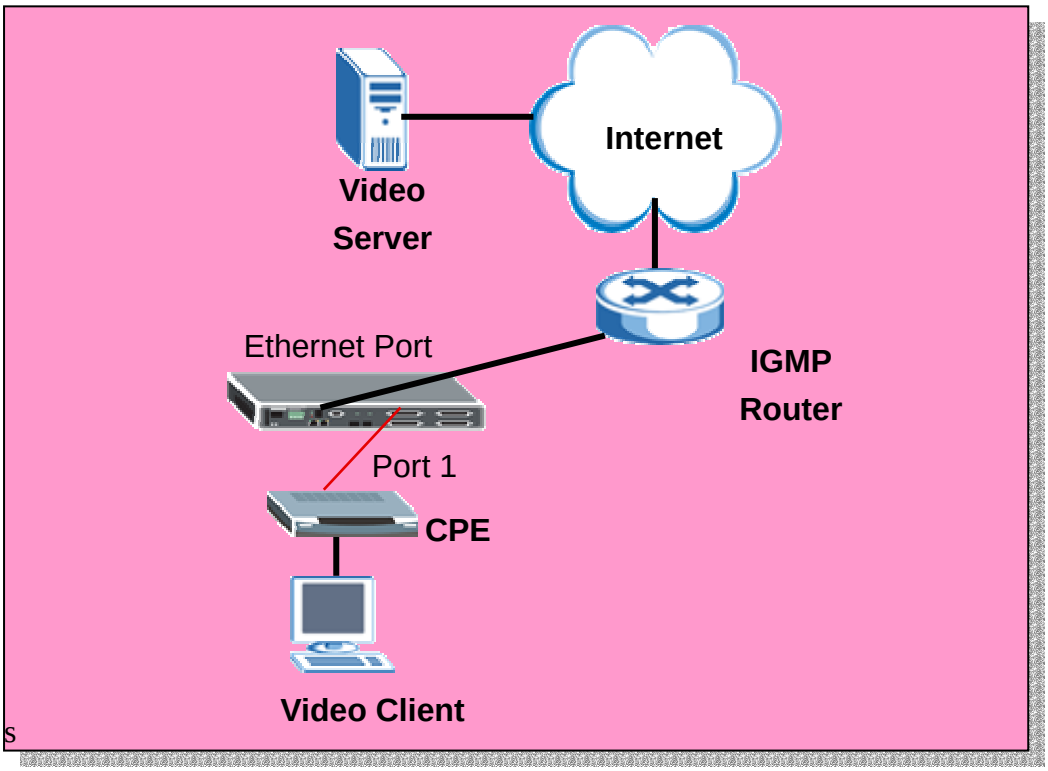
Status

System Up Time : 2:11:04

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2	100M/F	FORWARDING	Disabled	217	683	2	0.0	0.0	0:01:44
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6	100M/F	FORWARDING	Disabled	3278	2698	0	0.0	0.0	0:14:32
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Setting up the IGMP Snooping/IGMP Filtering

Without IGMP snooping multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all port. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through the IP-DSLAM. IGMP filtering is for allowing a port to join some specific IGMP groups. This can be applied in Video service providers. They can only open some specific channels (groups) to specific ports.



S

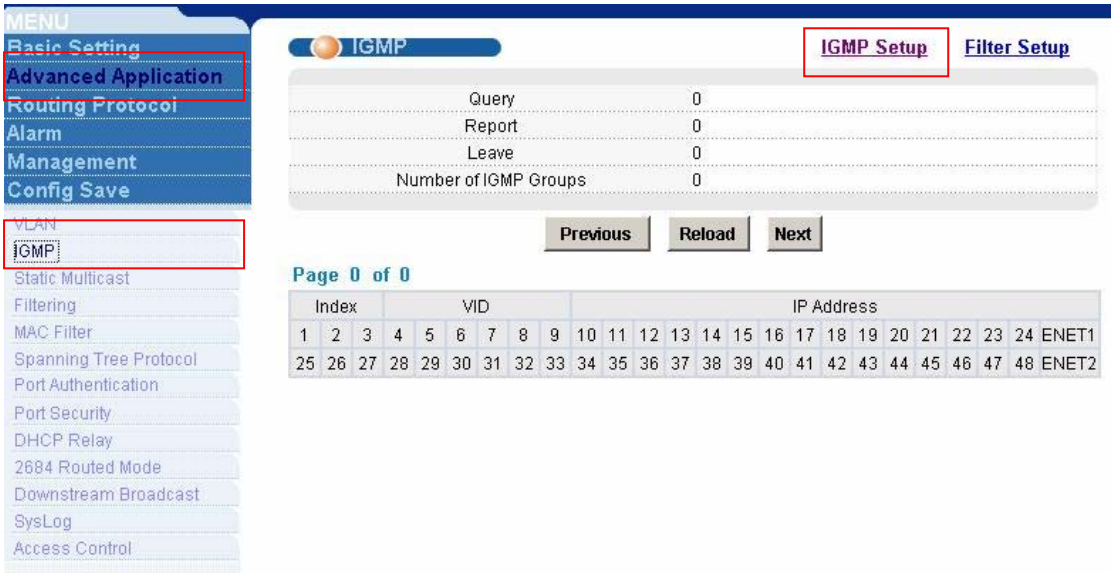
How to set up IGMP snooping/IGMP filtering

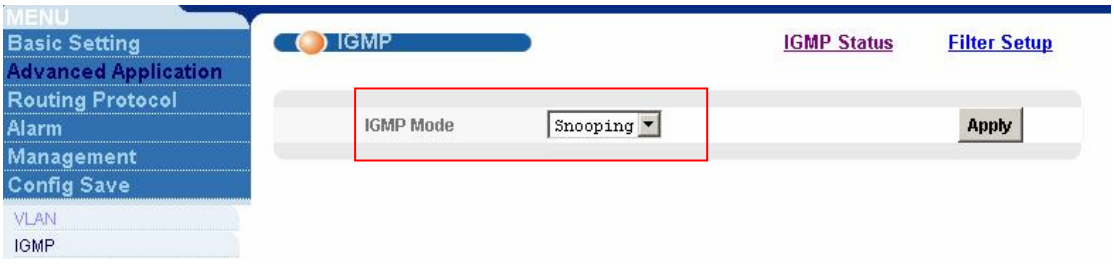
Here, we only set up the IES1248 to support IGMP snooping and IGMP filtering. Please refer to the user guide of the Video Server and the subscriber device. We assume the video server provides three channels, movie 1 on 240.10.10.8 group, movie 2 on 240.10.10.9 group and movie 3 on 240.10.10.10 group. And we assume the subscriber want to subscribe two channel, movie 1 and movie 2. If we don't enable the IGMP snooping, every one can see all movies. If we don't set the IGMP filtering on the port, the subscriber behind the port will receive all movies.

1. IES-1248 settings

1.1 Enable IGMP Snooping

Click **IGMP setup** on IGMP Snooping page and enable the IGMP snooping. After a while, you will see the number of **Query** will increase when IES-1248 receives the query packet from IGMP router.

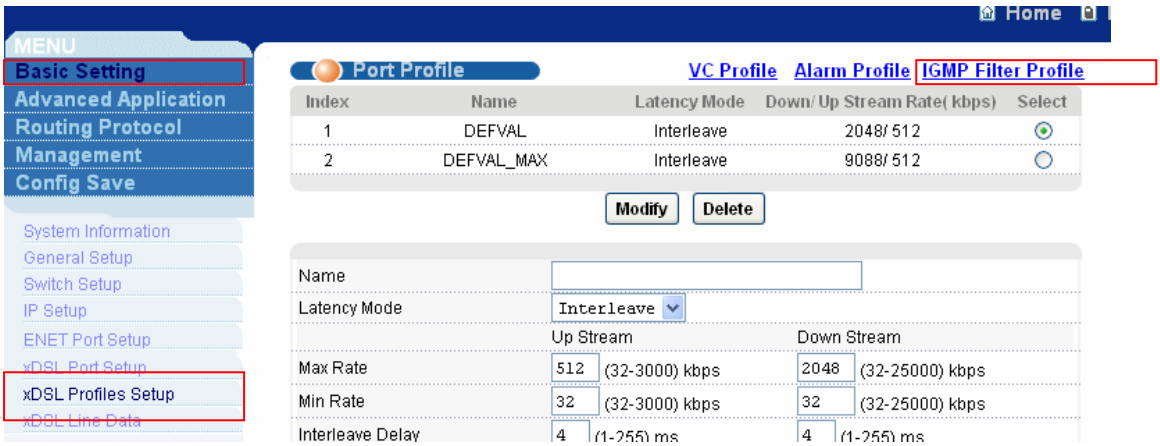




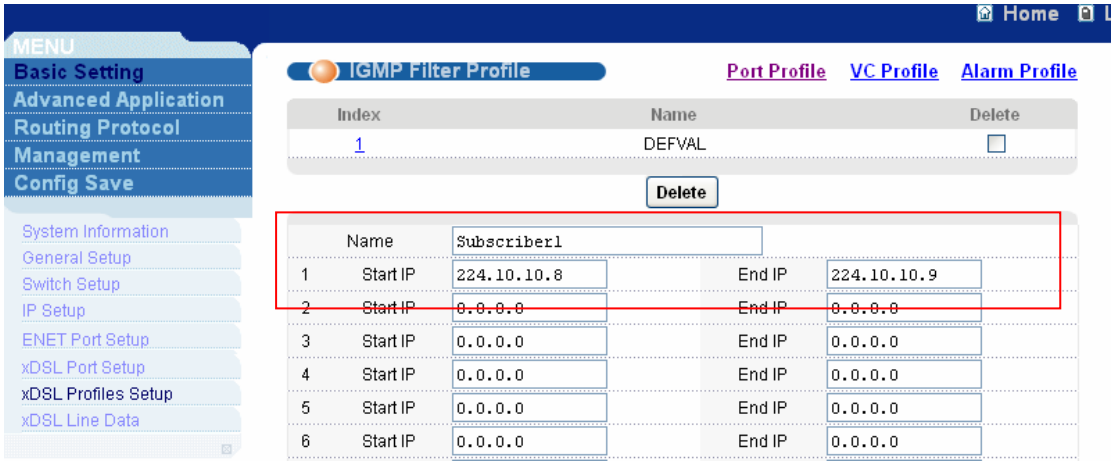
Meanwhile, if the subscriber sends the join packet, we can see the number of **Report** will increase and the IGMP table will be created.

1.2 Set up IGMP Filtering

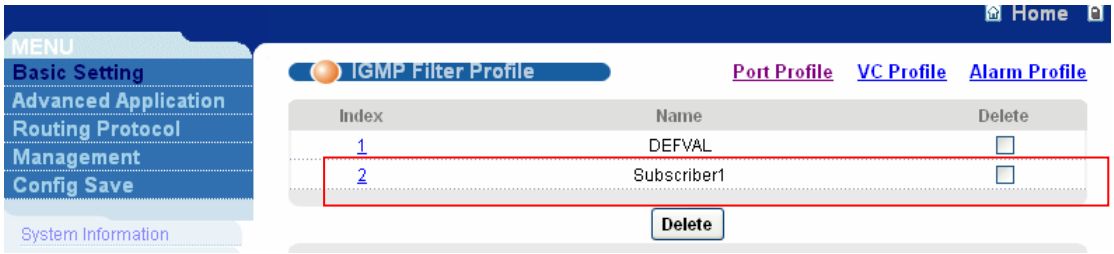
If we don't set up IGMP filtering, the subscriber will receive all the movies. We set up a IGMP filter Profile and apply it to specific port to limit the channels subscriber can see. Click **Basic Setting**, **xDSL Profiles Setup** in the navigation panel to display configuration screen as shown. And click the **IGMP Filter Profile** to show the setup page.



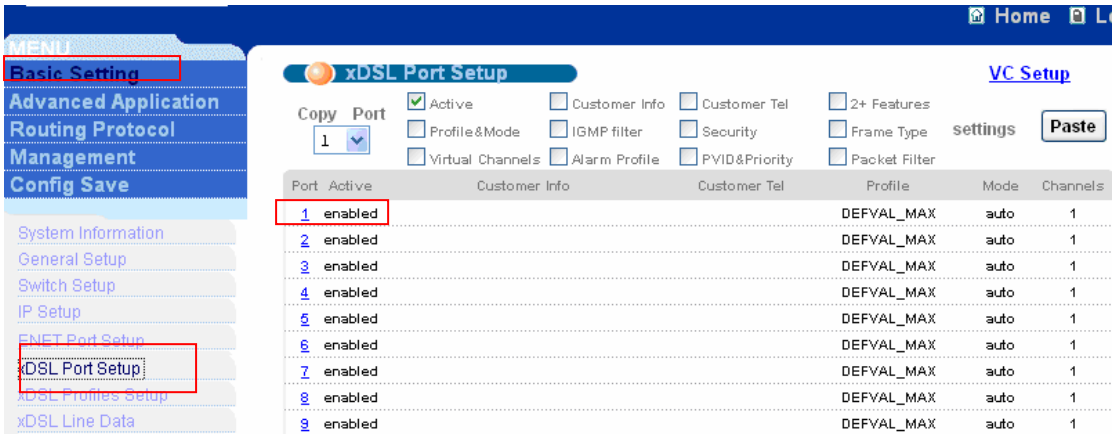
In this case we only allow the subscriber to join movie 1 and movie 2. That means only the groups 240.10.10.8 and 240.10.10.9 can be forwarded this subscribed port.



After create this profile, there is a new profile added in the list.



Then we need to apply the profile to port 1. Click **Basic Setting**, **xDSL Profiles Setup** in the navigation panel to display configuration screen as shown. Click the port index **1** to set up this port.



We select the **Subscriber1** in **IGMP Filter Profile** Combobox. And click **Apply** to let the setting take effect.

Go back to check the IGMP Snooping table. We will see only two channels allowed to be forwarded to port 1.

Static Multicast

What is Static Multicast Filter?

Static Multicast Filter allow network administrator to configure multicast group consisting of one or more ranges of MAC multicast addresses. An administrator can control multicast traffic per-switch-port basis with static multicast filter. By default, all multicast traffic are dropped without static multicast filter setup or IGMP snooping which cause some routing protocol such as RIPv2 and OSPF can not be passed through IP DSLAM. So administrator must do any configuration of static multicast filter to pass such routing protocol and other related application smoothly.

Some Well-known multicast group address:

224.0.0.1---------all systems on this subnet

224.0.0.2---------all routers on this subnet

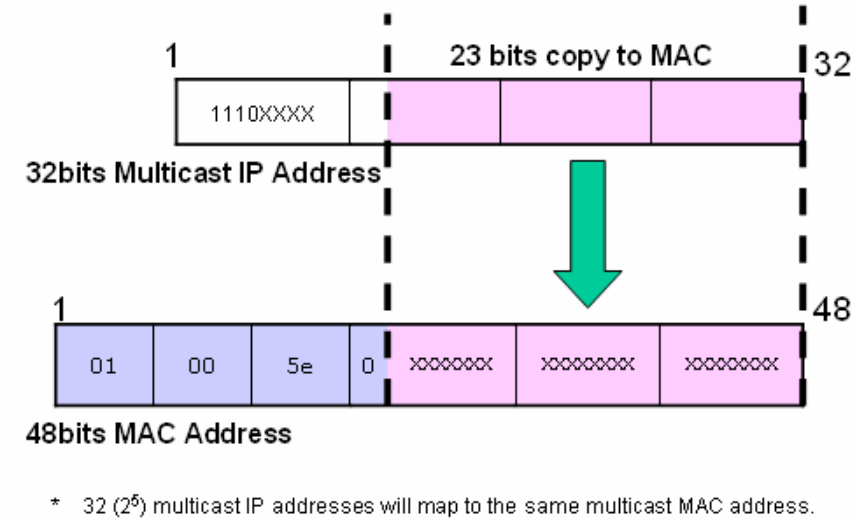
224.0.0.5---------all routers running OSPF

224.0.0.6---------all Designed Routers running OSPF

224.0.0.9---------for RIPv2

224.0.1.1---------for NTP

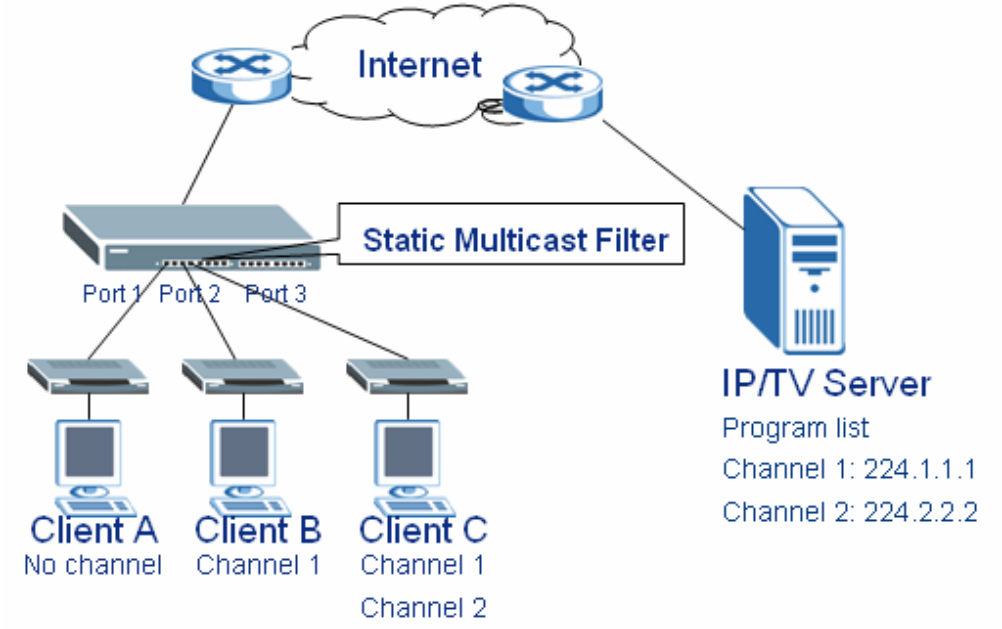
Before using static multicast filter, you must mapping Multicast IP address to Multicast MAC address because IES IPDSLAM using Multicast MAC address to forwarding multicast traffic.



This feature can also be combined with IGMP Snooping feature to make ports know multicast traffic that are not learned by IGMP Snooping or forbid specified ports to receive multicast traffic learned by IGMP Snooping.

Application Scenario

Scenario Description



An ISP wants to provide multicast video service to end user and subscribes who with different pay enjoy different programs.

Client A (connect to ADSL port 1) is a normal subscribe, so he has no authority to access movie resource.

Client B (connect to ADSL port 2) is a pay subscribe, he has authority to access limited movie resource (for example, just only channel 1).

Client C (connect to ADSL port 3) is a VIP subscribe, so he has the highest authority to access all movie resource (for example, both channel 1 and 2)

Static Multicast Filters can specify which video channels (based on multicast MAC addresses) are allowed or denied to be received by each subscribe.

The Multicast traffic MAC address of different channels as follows

IGMP Query: 01:00:5E:00:00:01 (224.0.0.1)

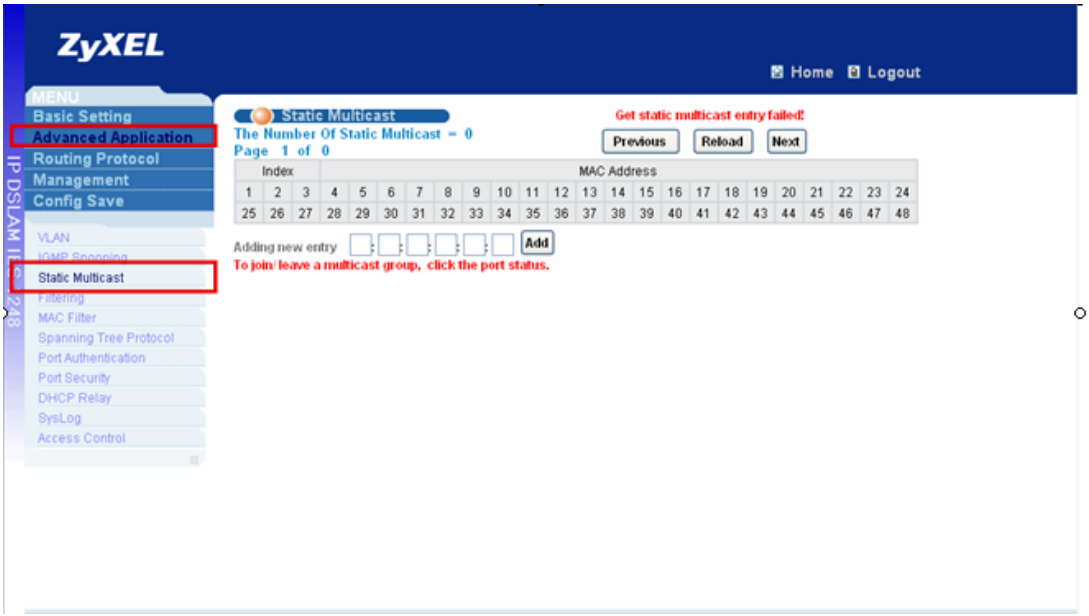
IGMP Report: 01:00:5E:00:00:02 (224.0.0.2)

Channel 1 multicast MAC address: 01:00:5E:01:01:01 (224.1.1.1)

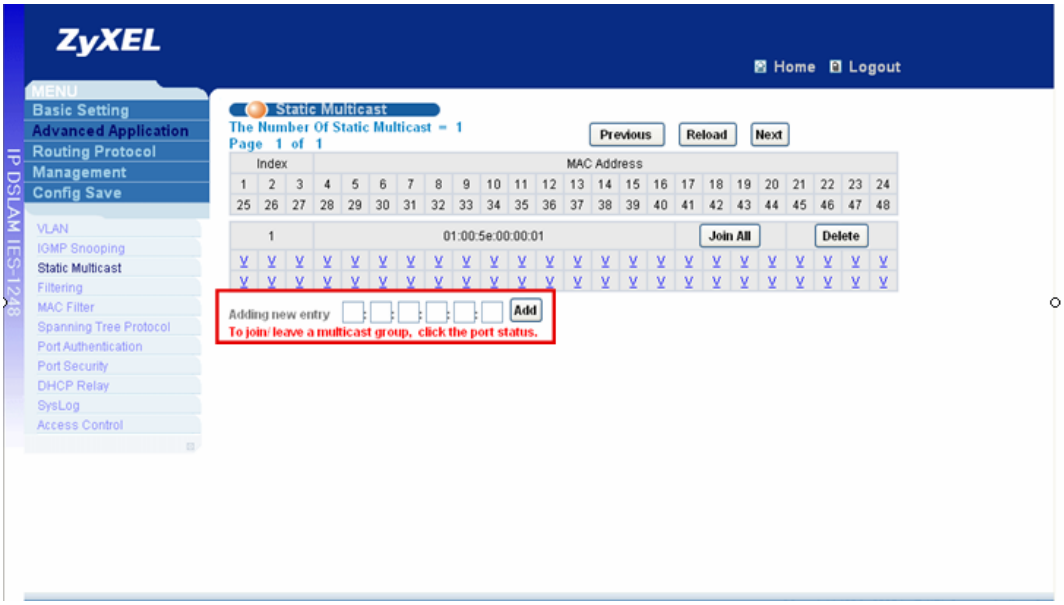
Channel 2 multicast MAC address: 01:00:5E:02:02:02 (224.2.2.2)

How to configure Static Multicast filter

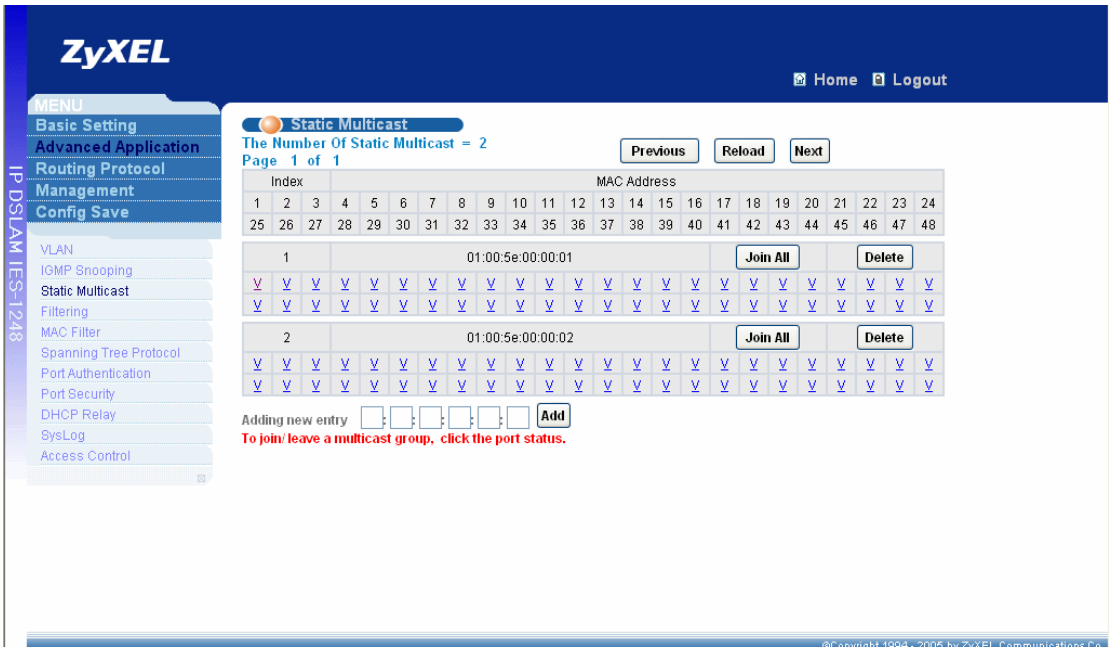
1. Please click “Advanced Application” first and then click “Static multicast” to bring up the following screen.



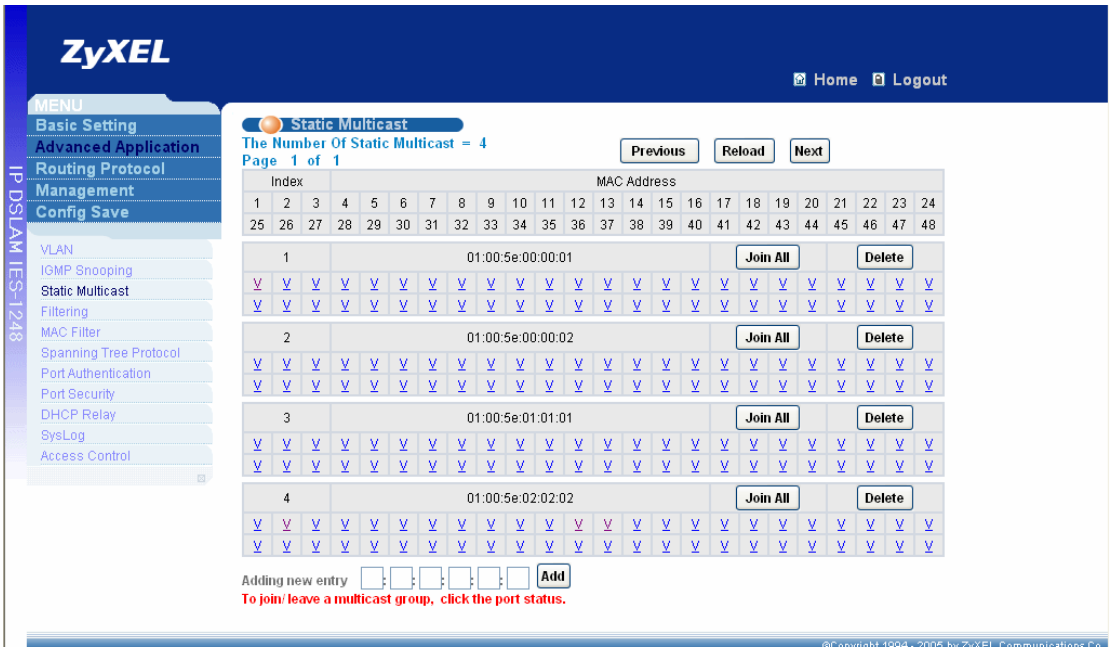
2. Please key in “01:00:5e:00:00:01” in the “Adding new entry” and click “Add” to bring up the following screen. “**V”** displays for member and **“-”** displays for non-member.



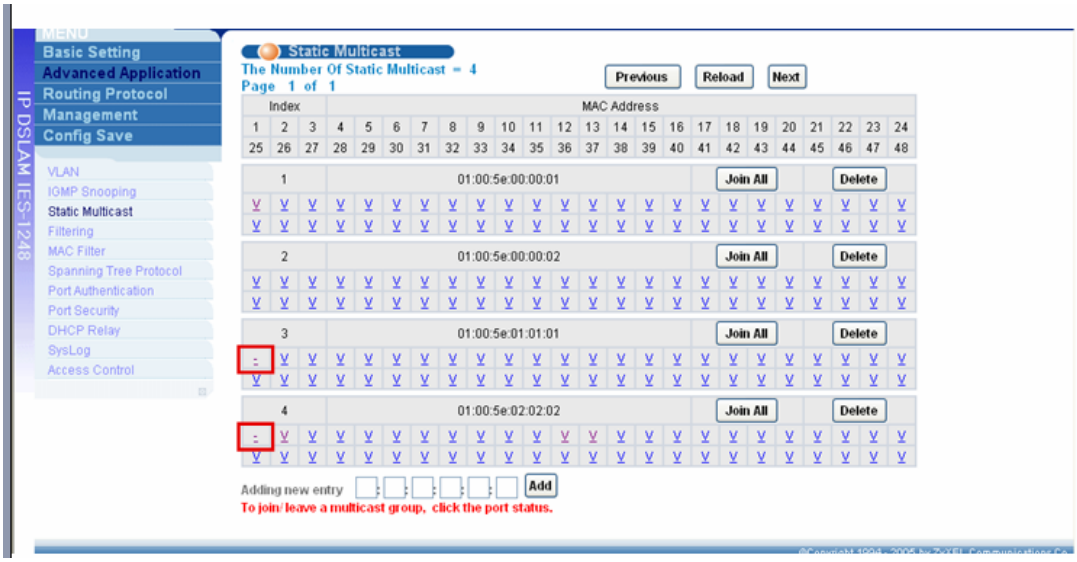
3. Please do the same step to add “01:00:5e:00:00:02” static multicast entry.



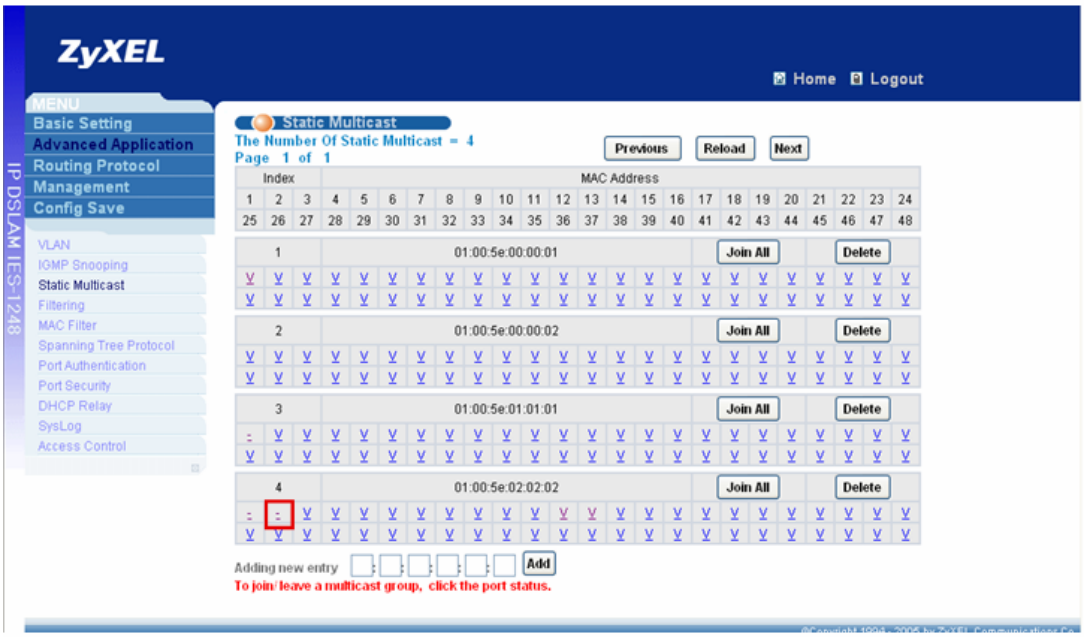
4. Please add channel 1 multicast MAC address “01:00:5e:01:01:01” and channel 2 multicast MAC address “01:00:5e:02:02:02” as above.



5. Because port 1 is not member of both 2 channels, so it should be set as non-member of these 2 channels. Please single-click “port 1” to change its status of group address “01:00:5e:01:01:01” and “01:00:5e:02:02:02” as non-member.



6. For port 2, set it as non-member of channel 2 “01:00:5e:02:02:02”



7. For port 3, no need to change anything because its status as member of these channels by default. Don’t forget to click “Config Save” to save your configuration into flash.

CLI Command related:

switch	**Smcast**			**Use the static multicast filter**
		show		**Display all MAC addresses joined to ADSL ports**
		set	**<adsl port> <multicast MAC> <join|leave>**	**Use join|leave to add/remove multicast**

				MAC address on specified ADSL ports, a range of ADSL ports or all ports,
		delete	**<multicast MAC>**	**Remove a static multicast filter entry by deleting the associated MAC address.**

How to achieve the same goal by CLI command?

>switch smcast set 1,2,3 01005e000001 join

>switch smcast set 1,2,3 01005e000002 join

>switch smcast set 1 01005e010101 leave

>switch smcast set 2,3 01005e010101 join

>switch smcast set 1,2 01005e020202 leave

>switch smcast set 3 01005e020202 join

>switch smcast show

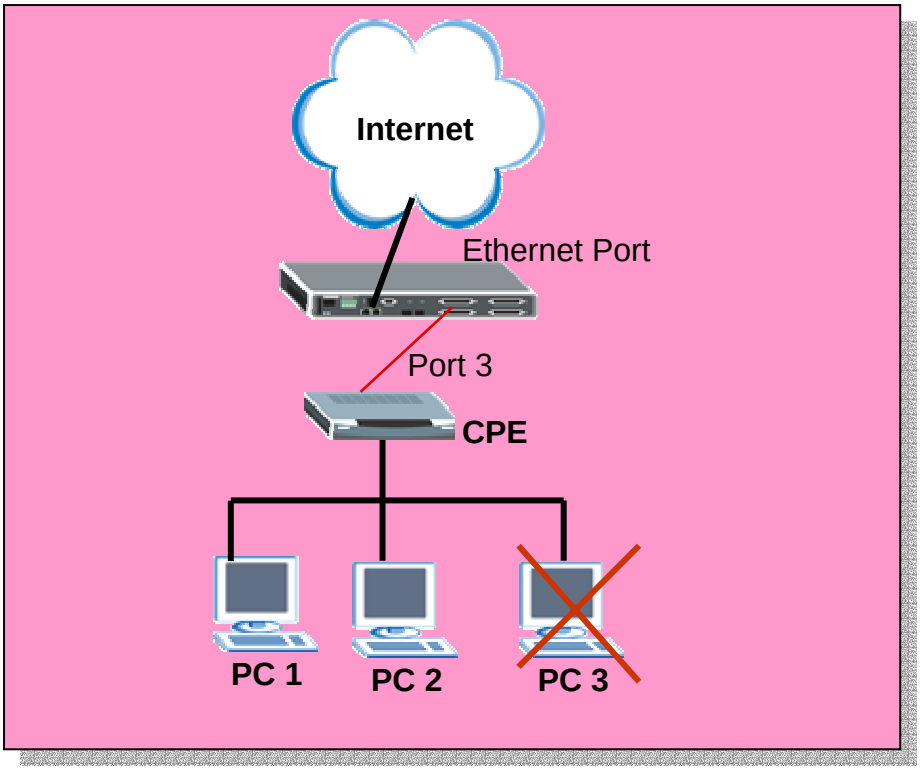
```
Static Mcast Groups                                          J:join L:leave

index MAC address       12345678901234567890123456789012345678901234567890123456789012345678
-------------------------------------------------------------------------------------------
    1 01:00:5e:00:00:01 JJJLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
    2 01:00:5e:00:00:02 JJJLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
    3 01:00:5e:01:01:01 LJJLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
    4 01:00:5e:02:02:02 LLJLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
```

PS: Default statuses of other ADSL ports without configuration are **DIFFERENT** between WEB GUI (default status is Join) and CLI Command (Default status is Leave), so please choose the better way to do static multicast filter configuration to get most convenience.

Limit the users behind the certain DSL port

ISP may want to limit the number of PC behind certain DSL port to access the Internet or allow PCs with specific MAC address to access the Internet. They can easily to achieve this with Port Security and MAC filter features.



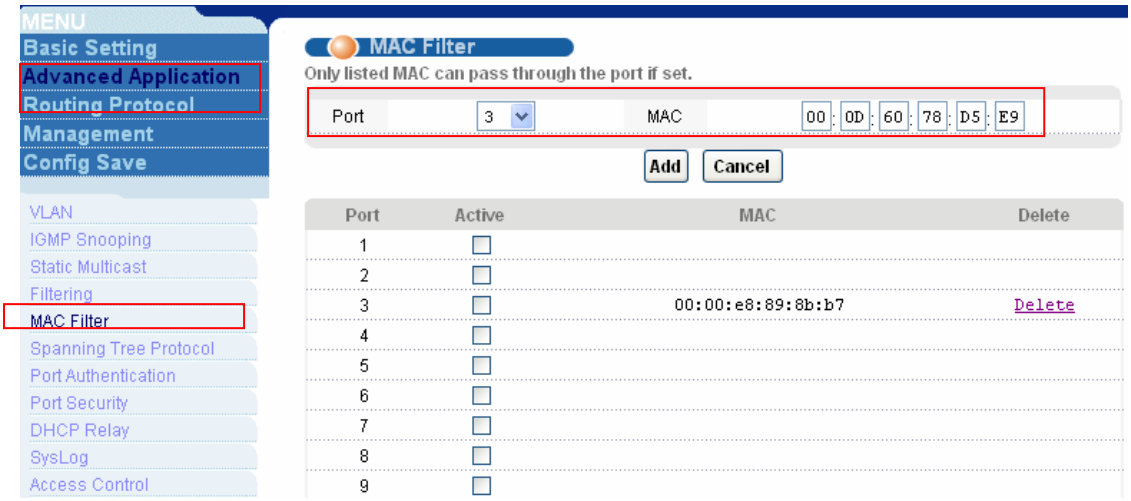
How to set up MAC Filter/Port Security

Here, we will set up an environment to allow PCs with certain MAC address and the number of PCs behind port 3 to access the Internet.

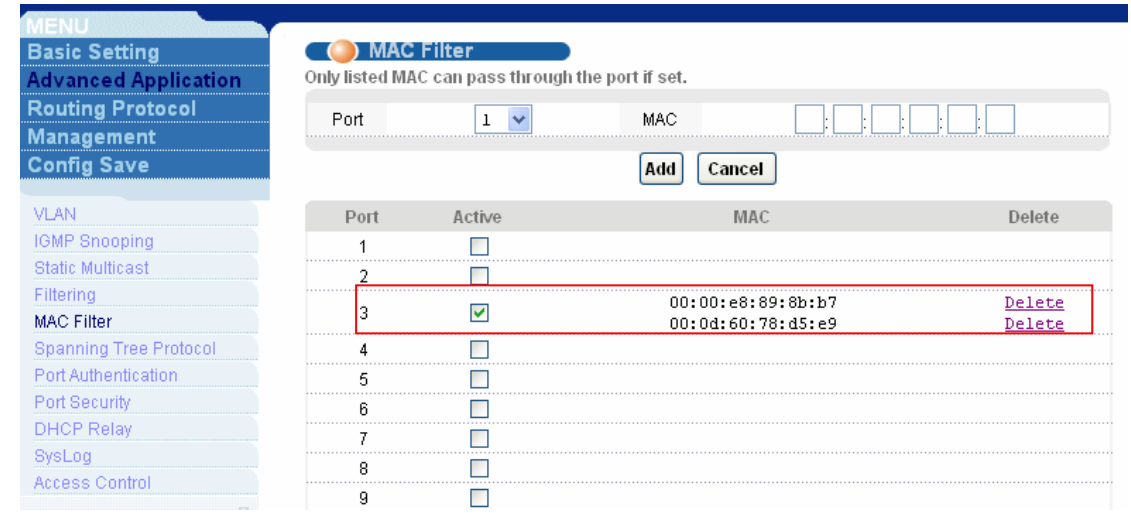
1. IES-1248 settings

1.1 Set up MAC filter

Click **Advanced Application**, **MAC Filter** in the navigation panel to display configuration screen as shown. You will see the **MAC Filter** setup page. Select the Port 3 and input the MAC address you allow to access the Internet. And don't forget the press **Apply** button to let it takes effect.

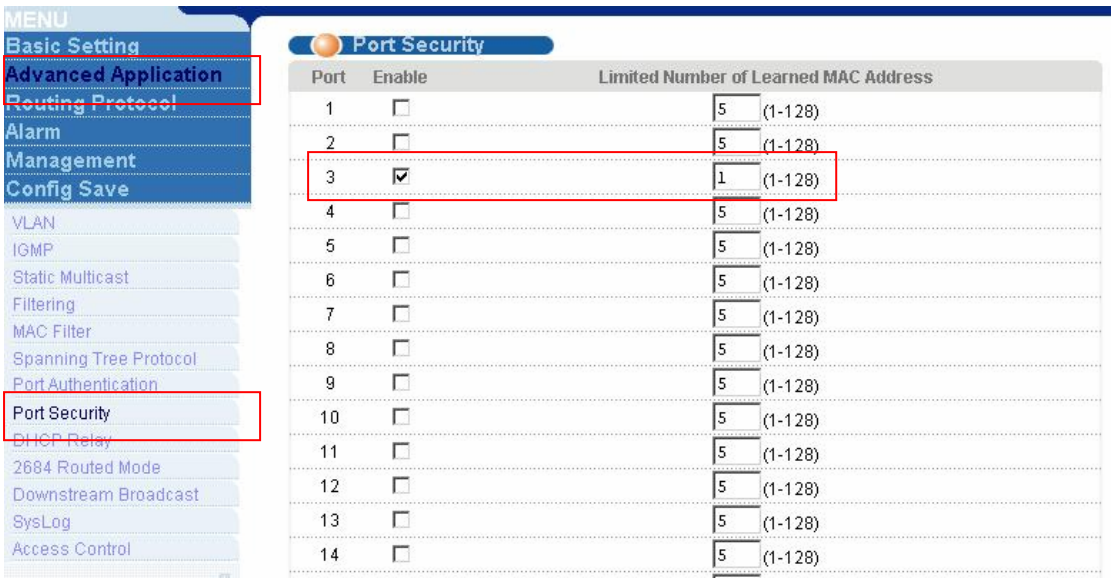


You will see the MAC address in the MAC field. Then check the **Active** check box of Port 3 and press **Apply** button to enable this feature. Only the MAC addresses listed here can access the Internet behind certain ports.

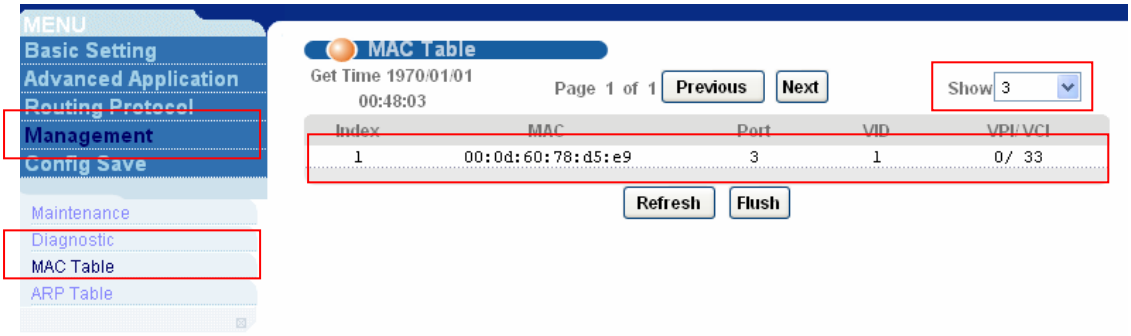


1.2 Set up Port Security

Click **Advanced Application**, **Port Security** in the navigation panel to display configuration screen as shown. You will see the **Port Security** setup page. Check the **Enable** check box of Port 3 and input the MAC address number you want to limit to access the Internet. And don't forget the press **Apply** button to let it takes effect. Note that the MAC filter and Port security can't be used at the same time.

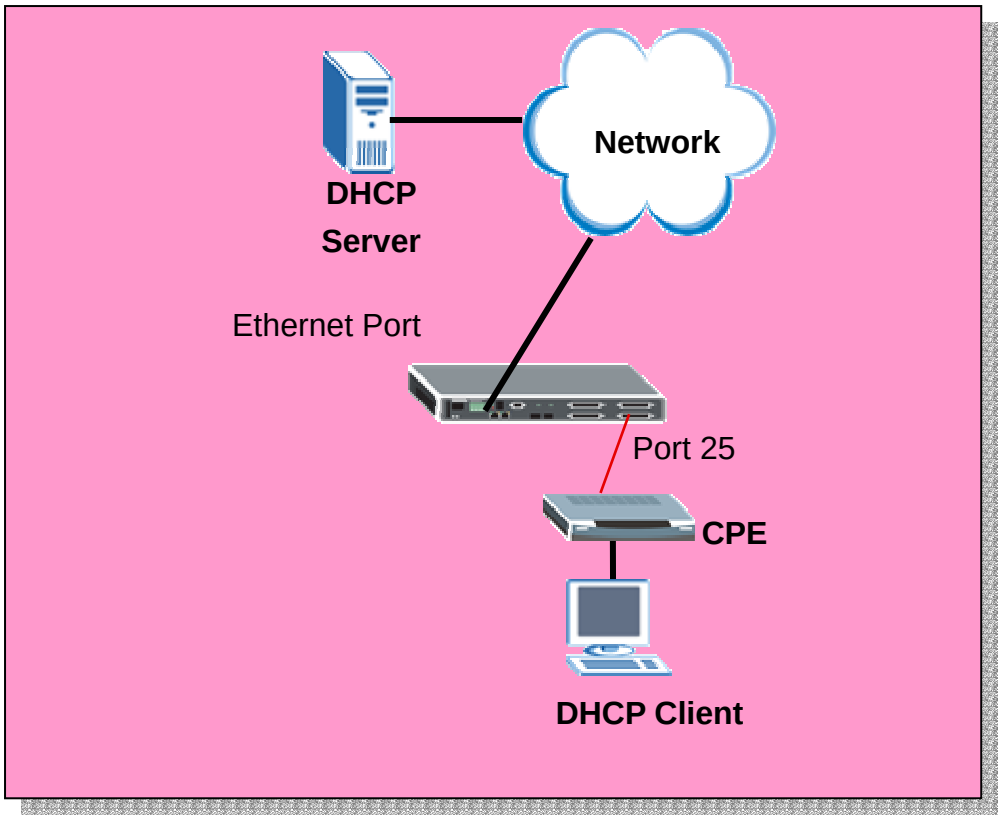


Click **Management**, **MAC Table** in the navigation panel to display configuration screen as shown. And select port 3. You will see the MAC table will be shown as you configured in previous steps.



DHCP Relay Option 82 Application

ISP may want to limit the number of IP address or deliver some specific IP addresses according to certain DSL 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.

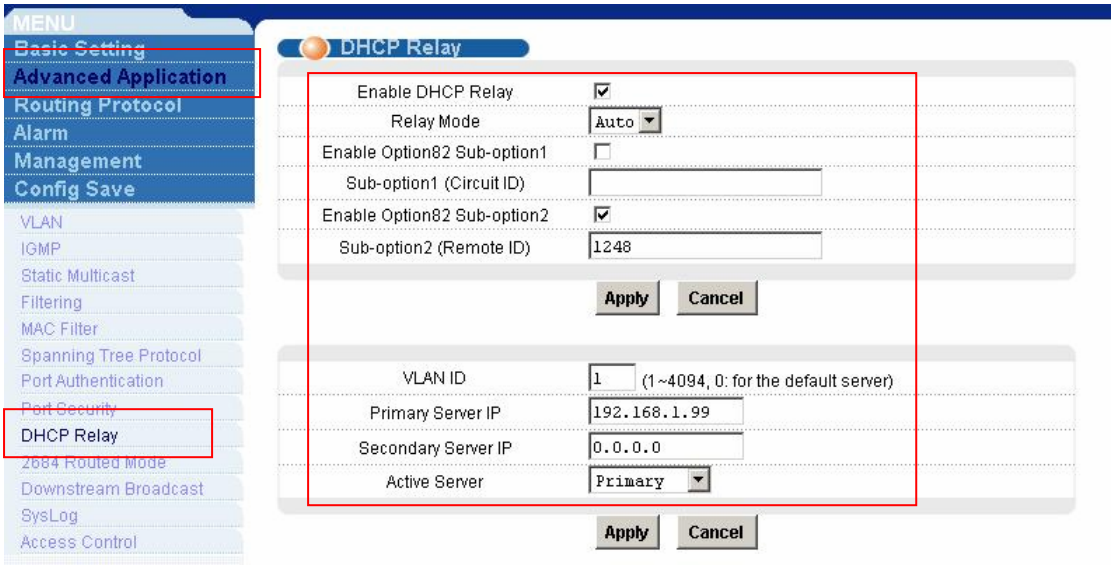


How to set up DHCP Relay Option 82 Environment

Here, we will set up an environment to allow a PC get DHCP IP address in specific IP pool according to its DSL port, VLAN ID and the option 82 string. In this case, the PC is behind 25th DSL port and the option 82 string is a string "1248". 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, DSL port=25 and the option 82 string is "1248".

1. IES-1248 settings

Click **Advanced Application**, **DHCP Relay** in the navigation panel to display configuration screen as shown. You will see the **DHCP Relay** setup page. Enable the DHCP relay and Option 82 function. Fill the IP address of DHCP server in this page. The IP address is 192.168.1.99 in our case. Also, enter "1248" as the Option 82 string.

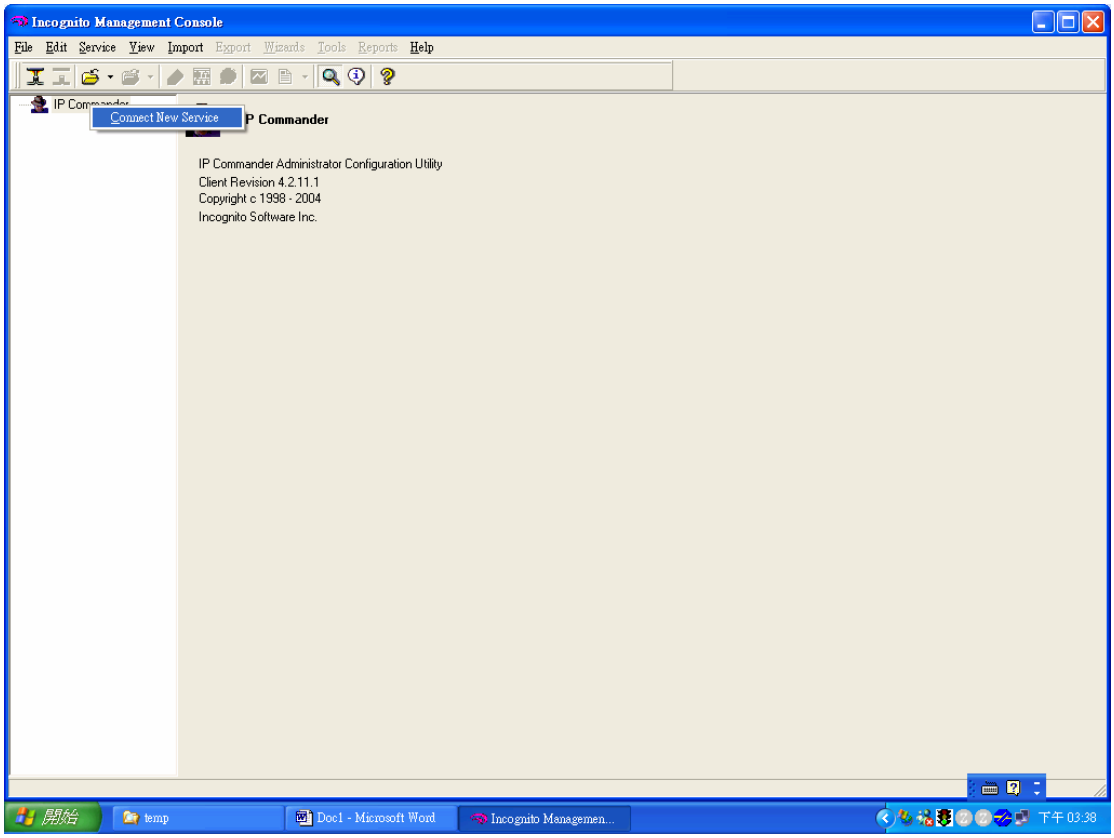


2. CPE settings

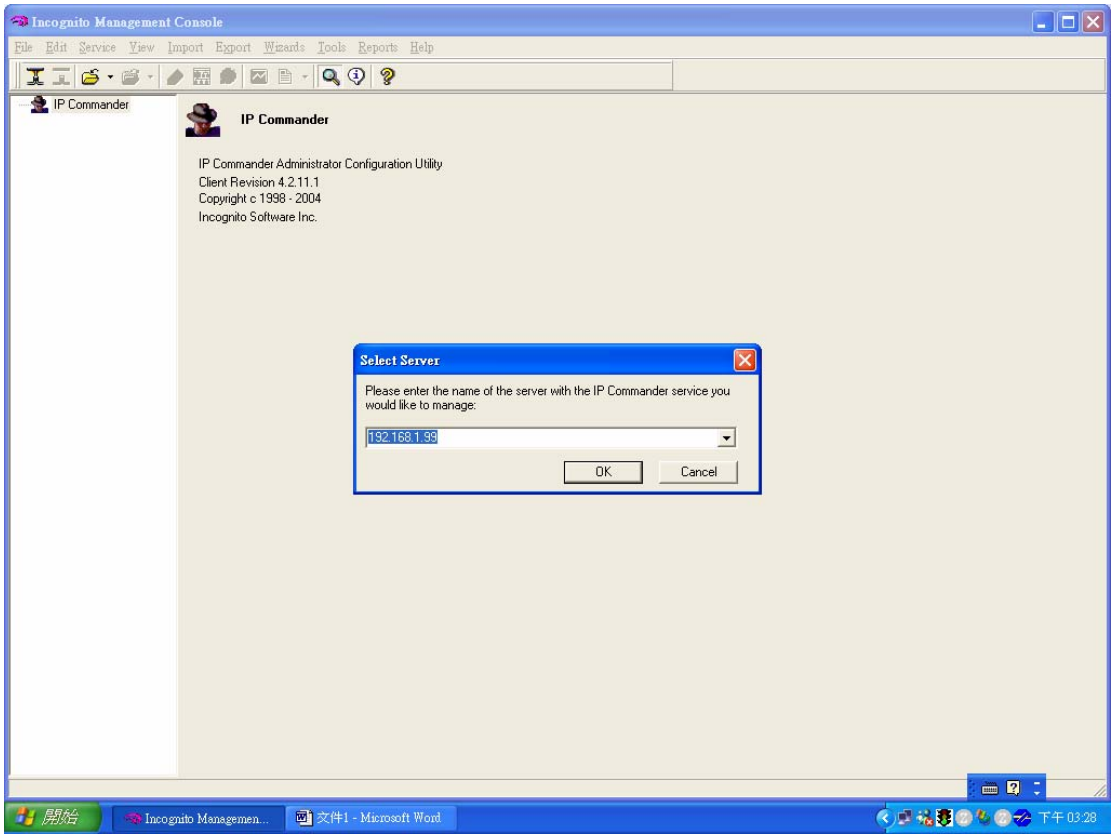
Connect CPE to the 25th DSL port. Please see former applications for Detailed settings.

3. IP Commander settings

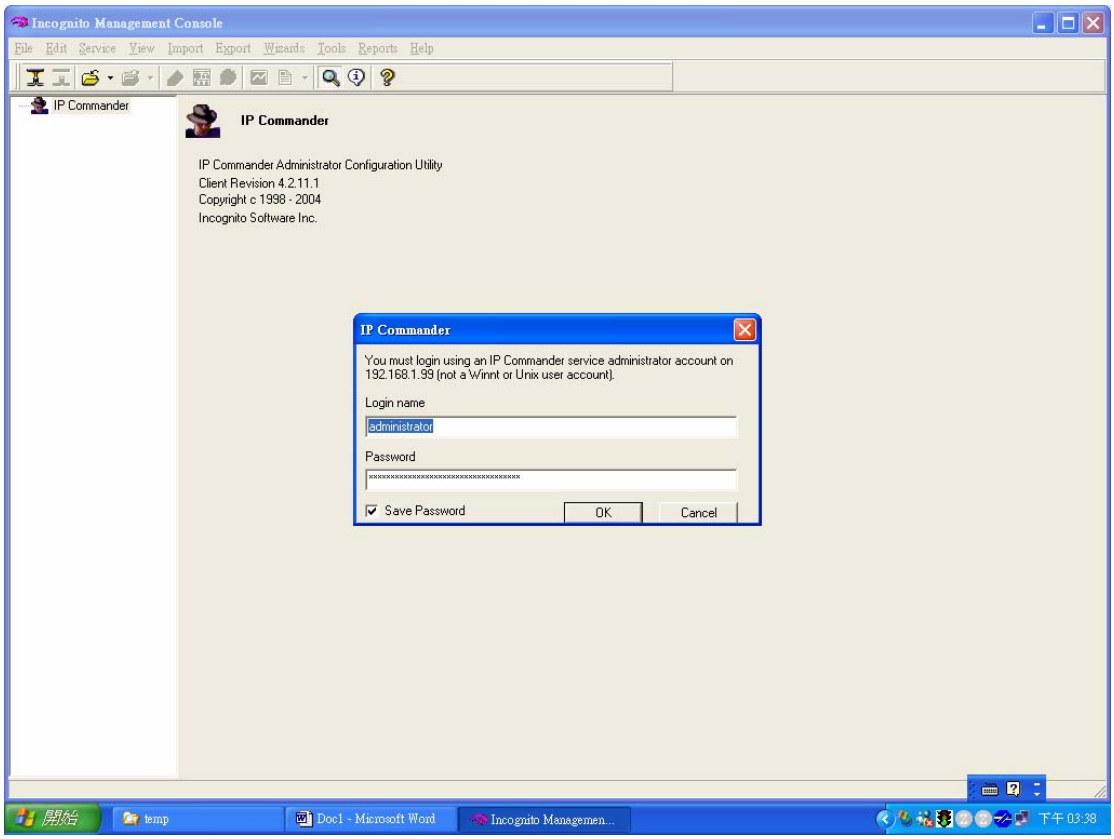
Open IP Commander. Right click “IP commander and then click “**connect new server**”.



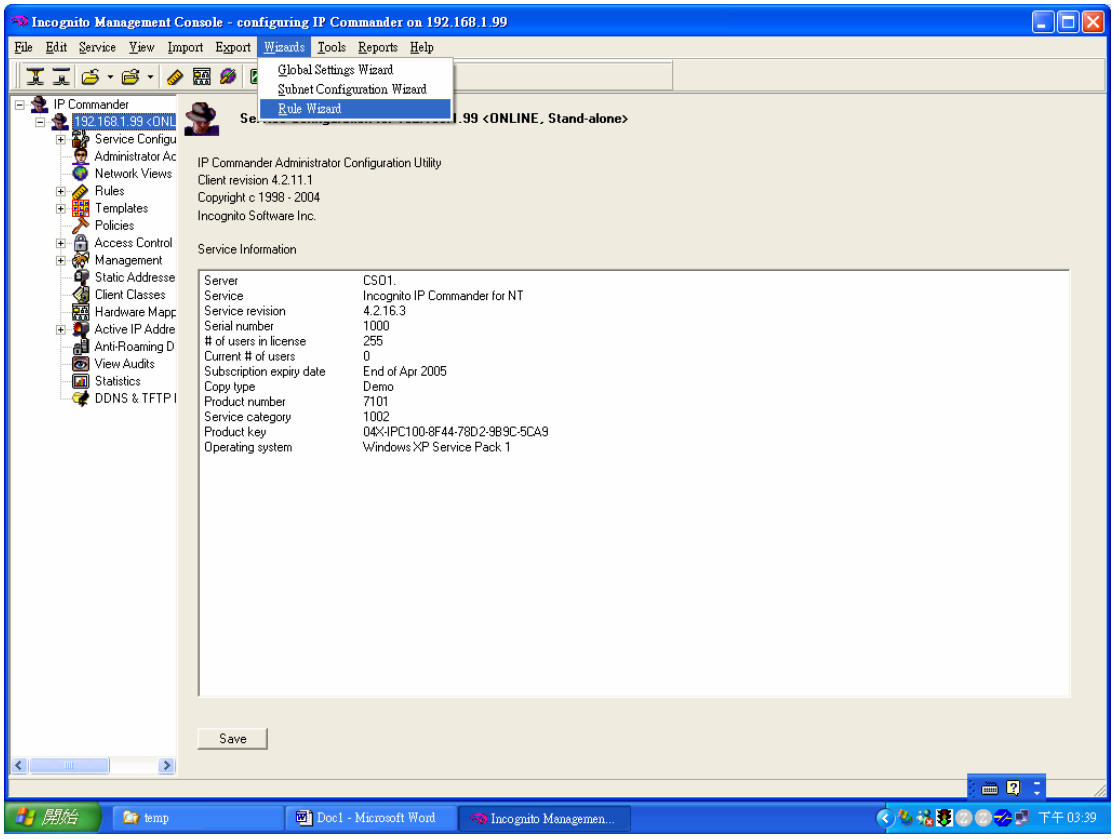
Input the DHCP IP address or domain name and click “ok”. Our IP is 192.168.1.99.



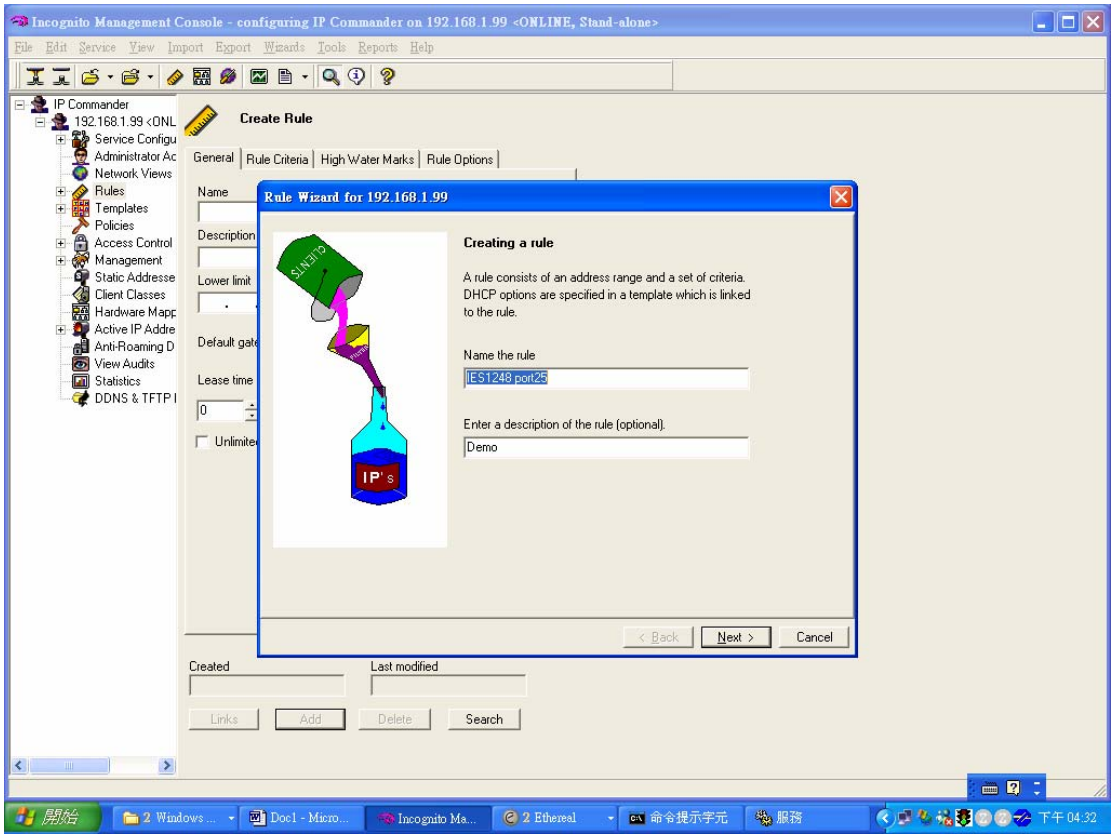
Input user name and password. The default user name is “administrator” and password is “incognito”.



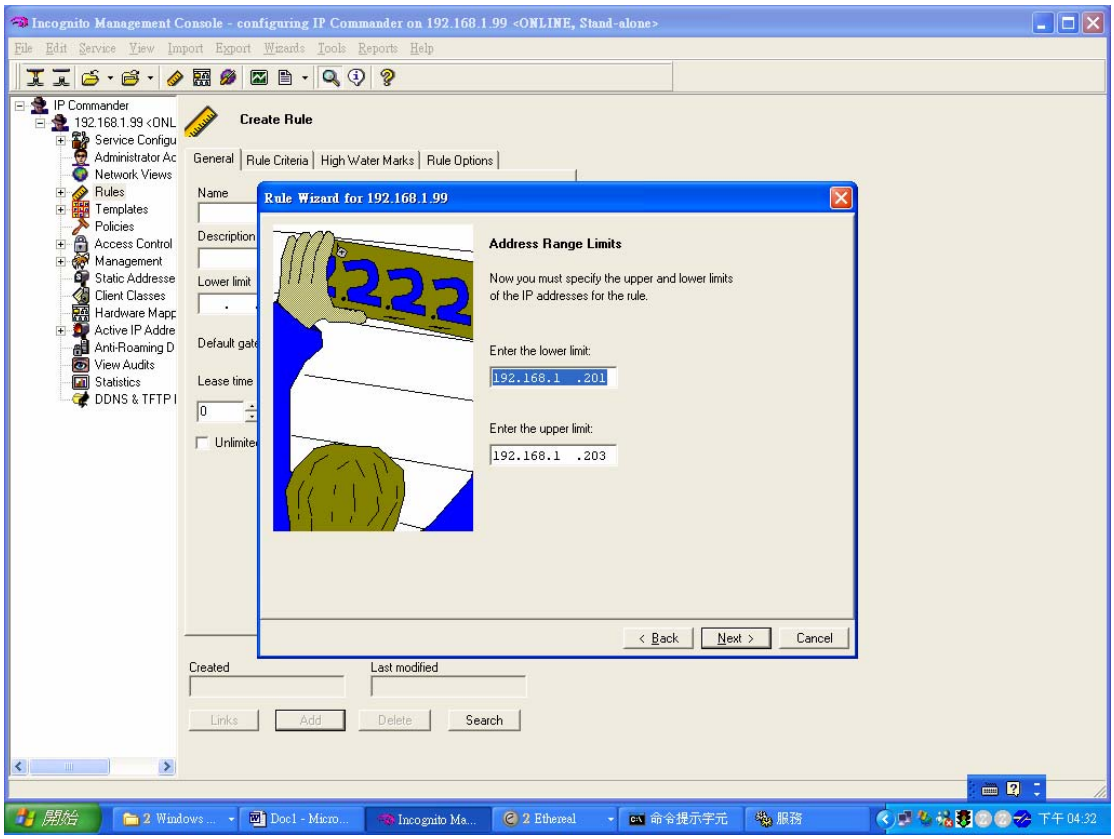
It will bring up the following screen, please make sure that your DHCP is in "**online**" status. Then click "**wizard**" in the top tool bars and select "**rule wizard**".



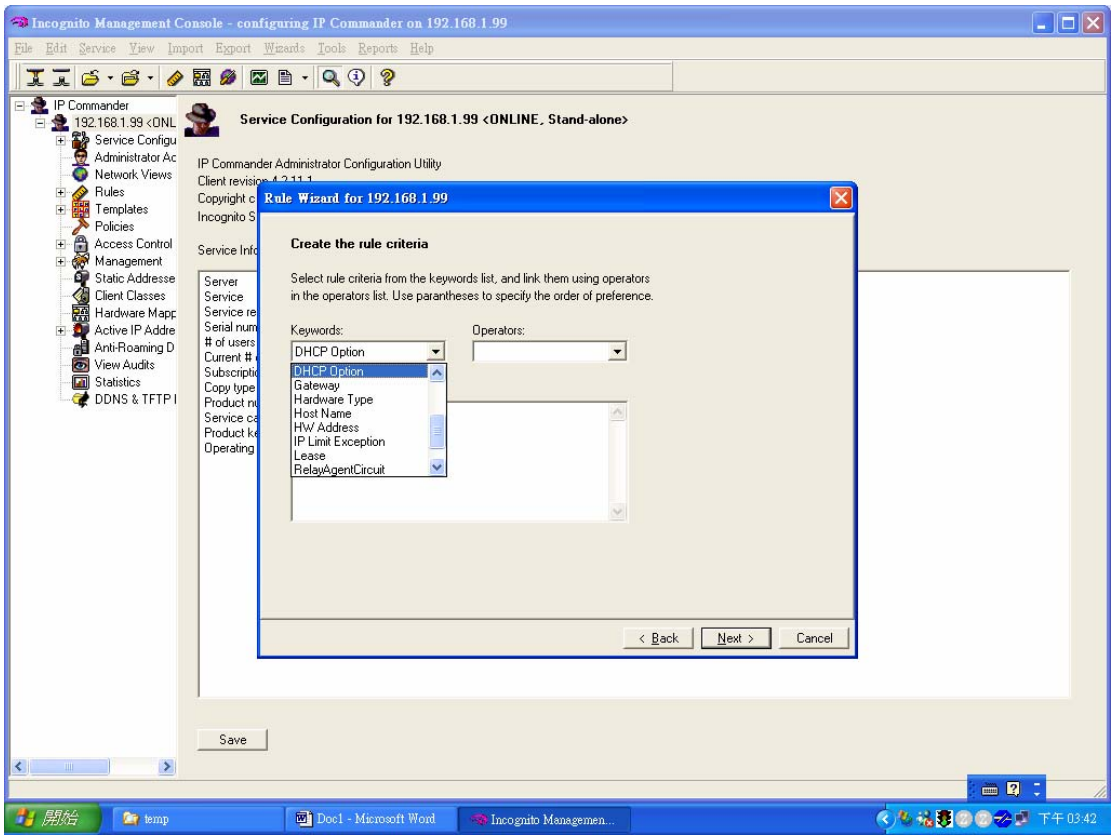
Give a name and description to the new rule.



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.

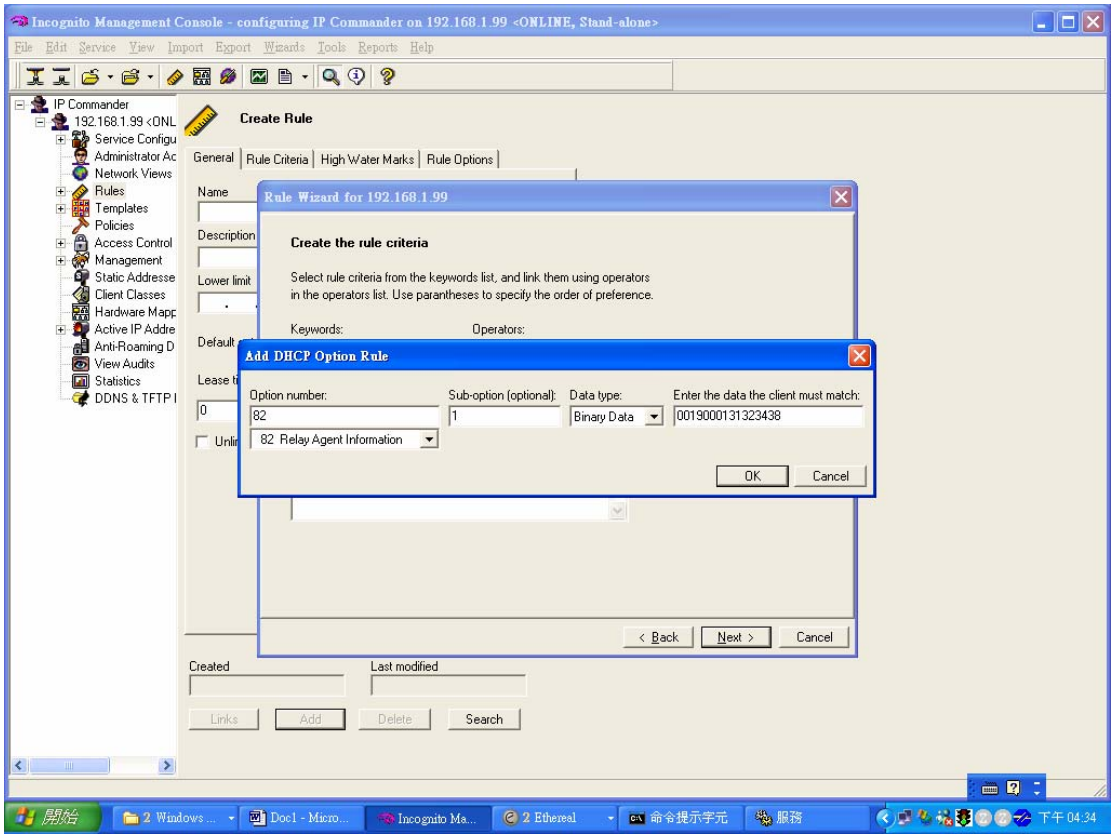


After input IP pool, we select “DHCP Option” in Keywords combobox.

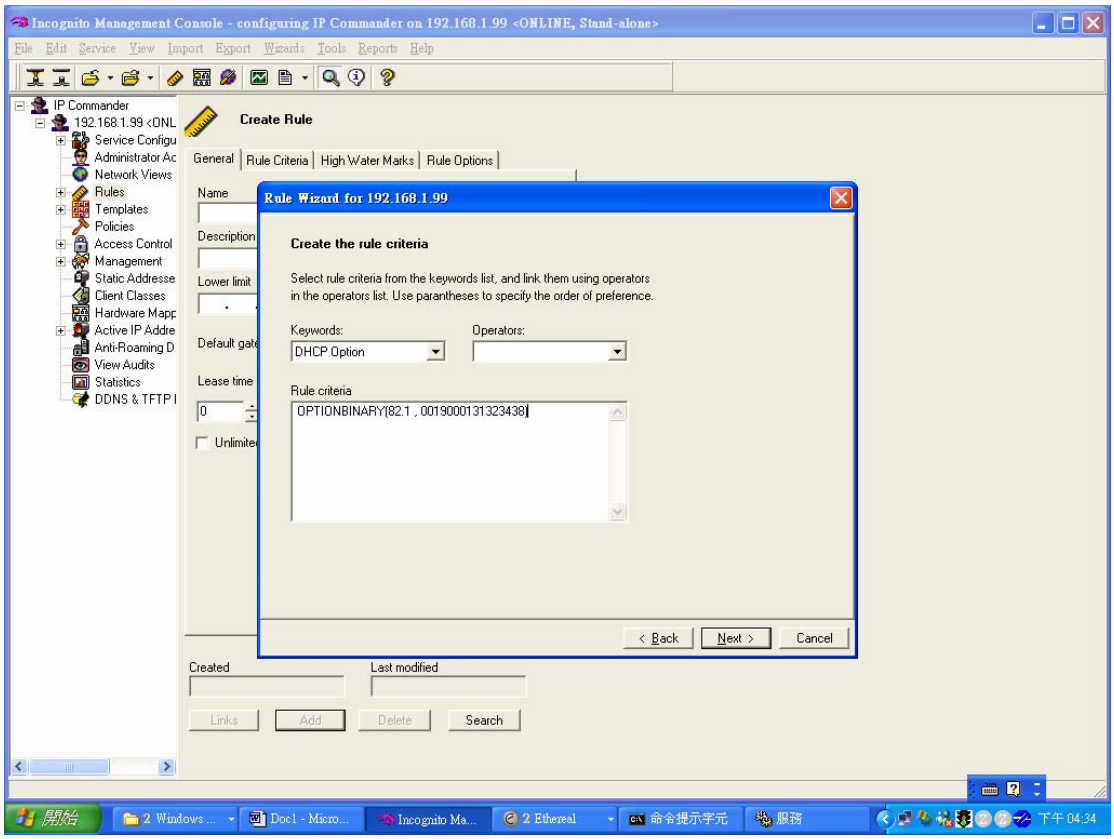


After select the “DHCP Option”, it will pop up “Add DHCP Option Rule” dialog.

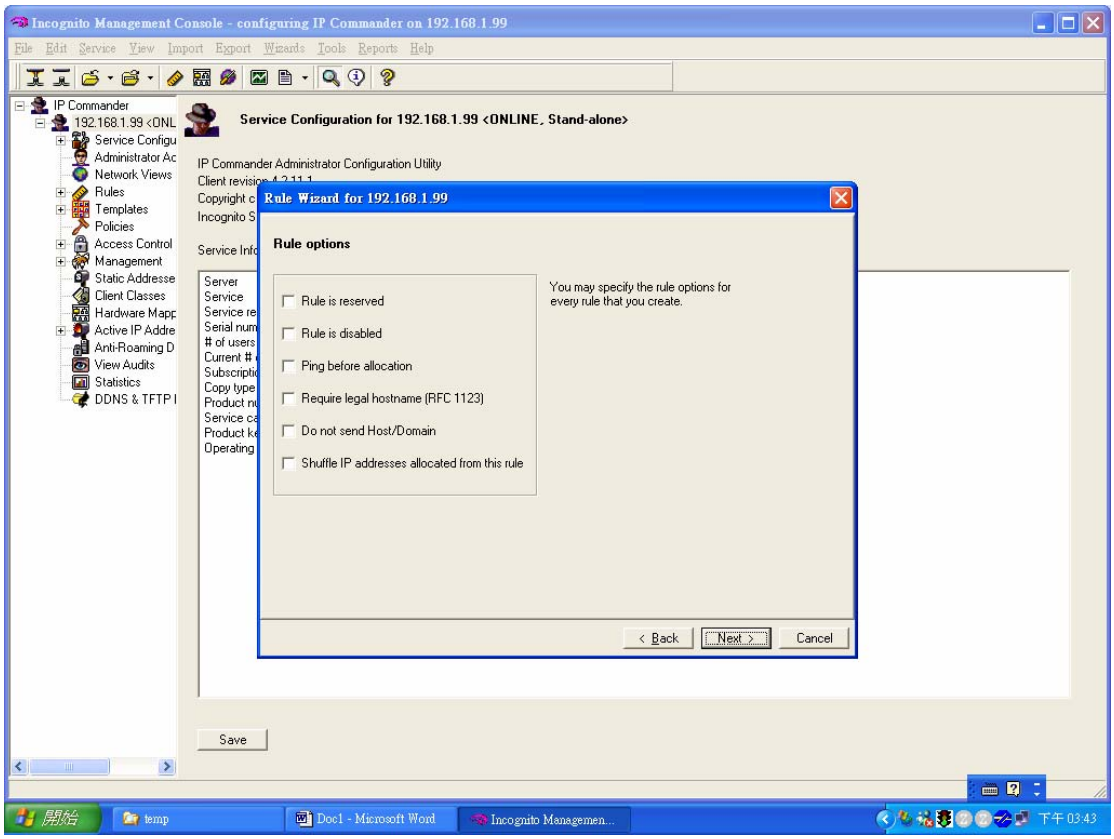
Select “option 82 Relay Agent Information”, sub-option 1, binary data. For port 25, VLAN 1, “1248”, please key in “0019000131323438” as the key value and click OK. Please note that the first 2 bytes define port number, the second 2 bytes is VLAN ID and the other bytes are the Option 82 string.



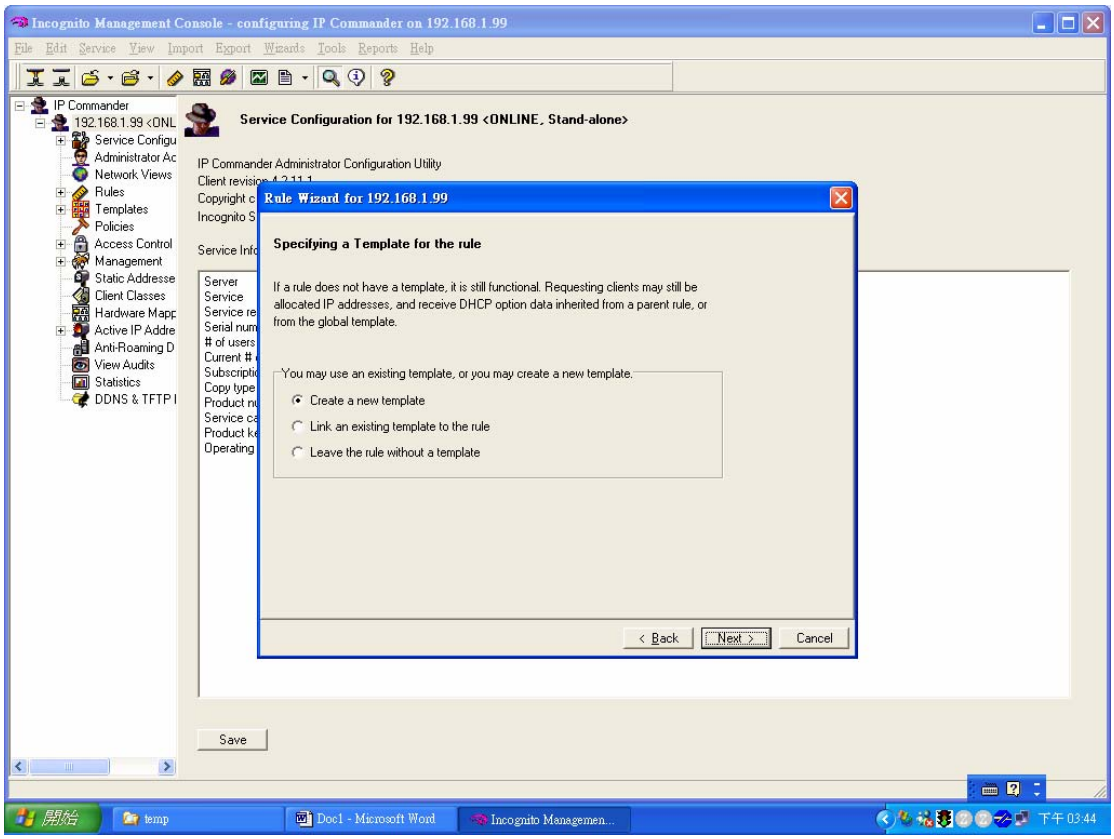
After you finish above step, you will see the following figure.



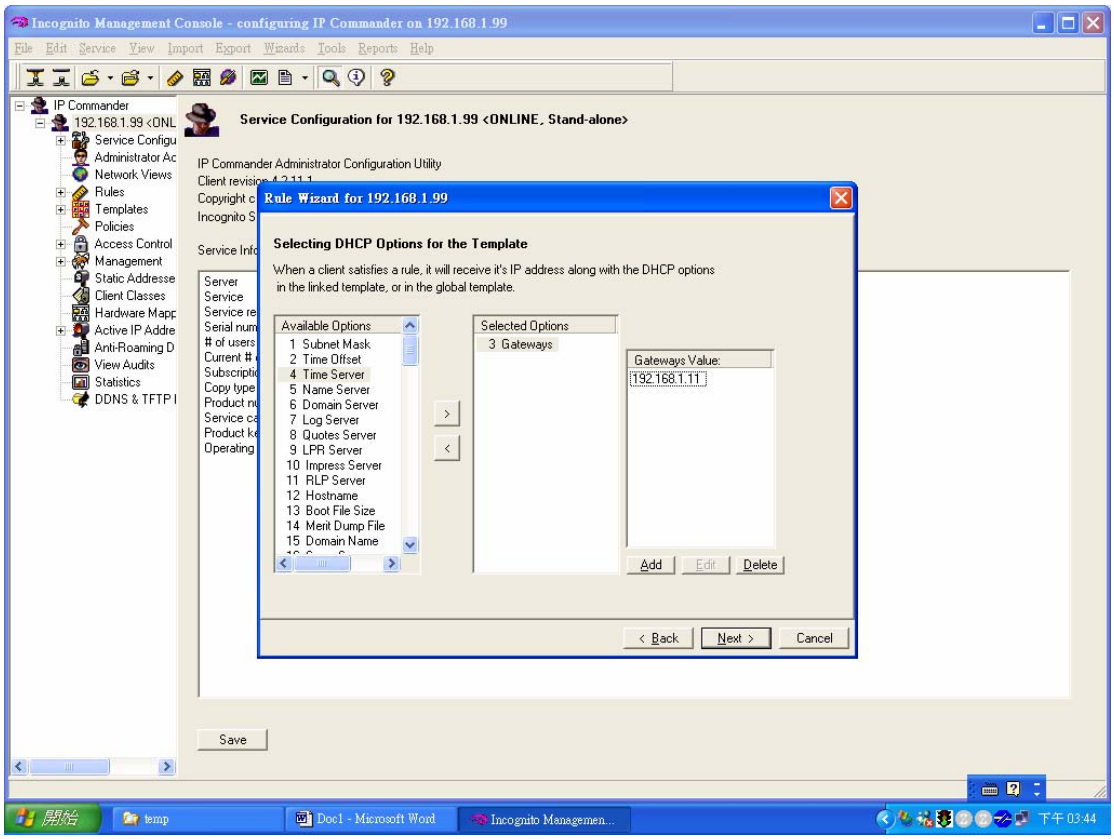
Then pop up the following screen and you can just press **Next** button.



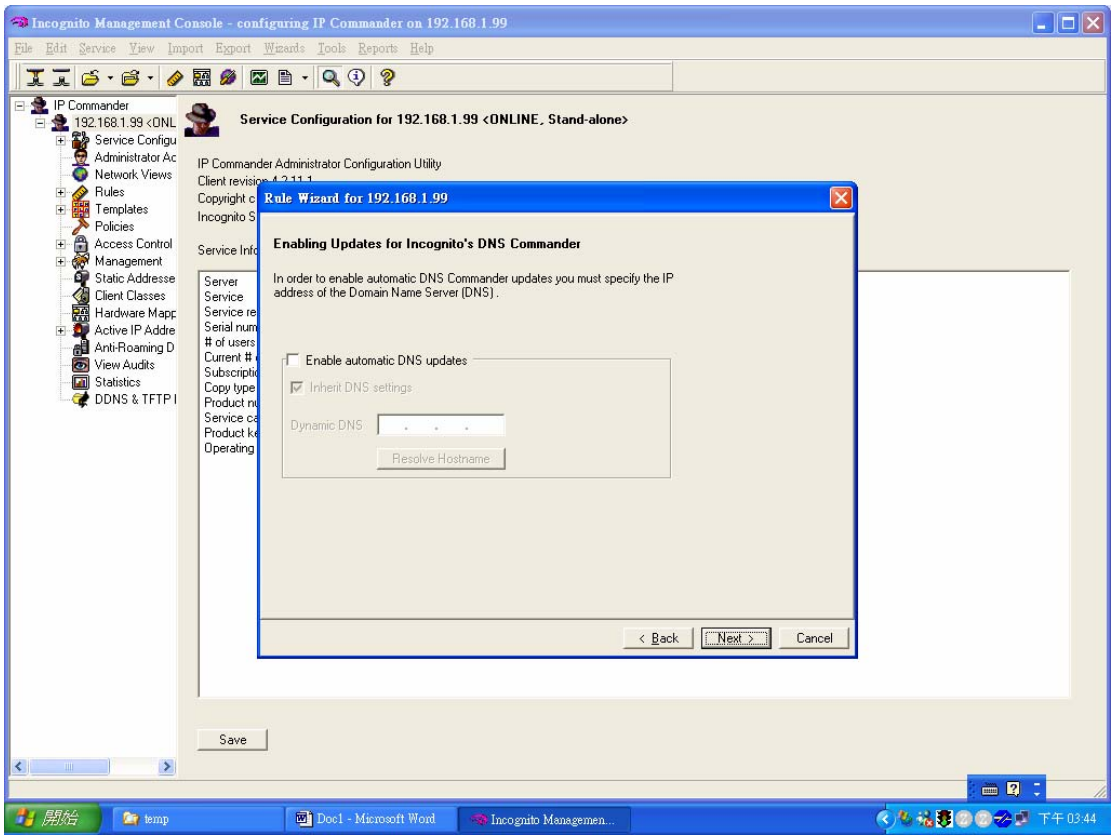
Then you can add DHCP template (option) such as gateway, DNS server and so on.



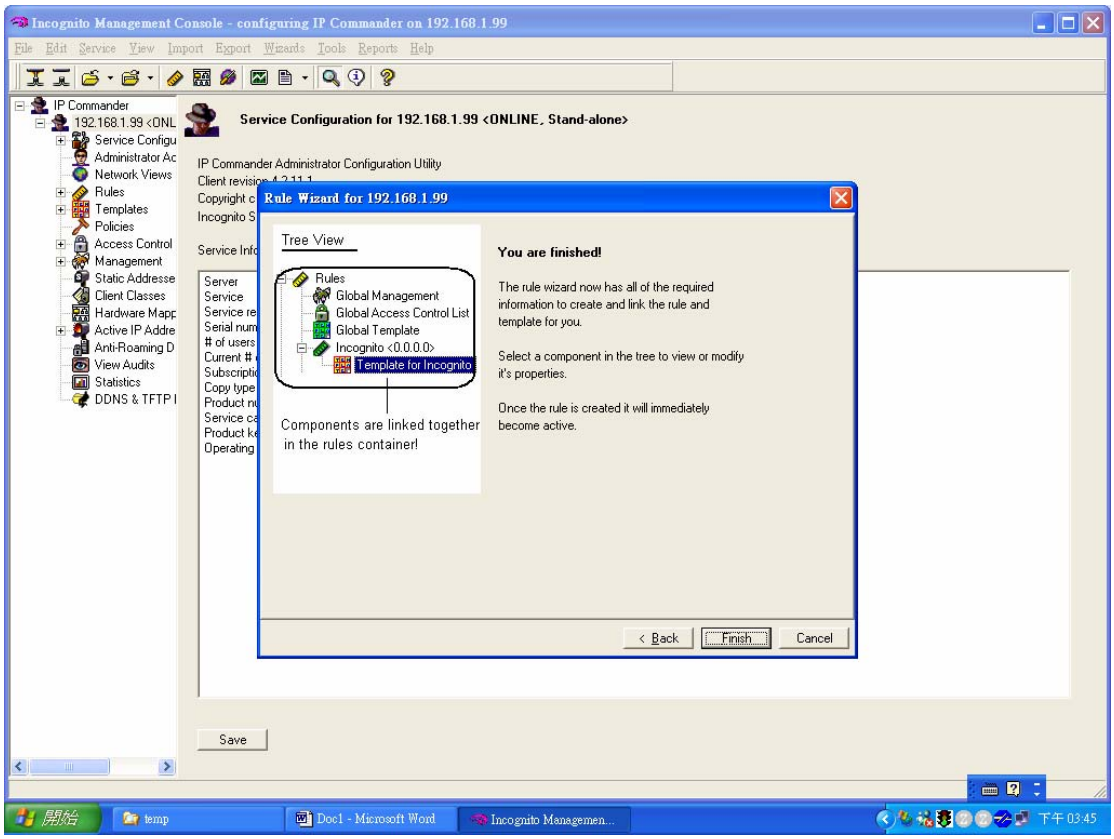
Here we use “192.168.1.1” as gateway IP address of DHCP client PC.



You can apply DDNS service to DHCP server or not.



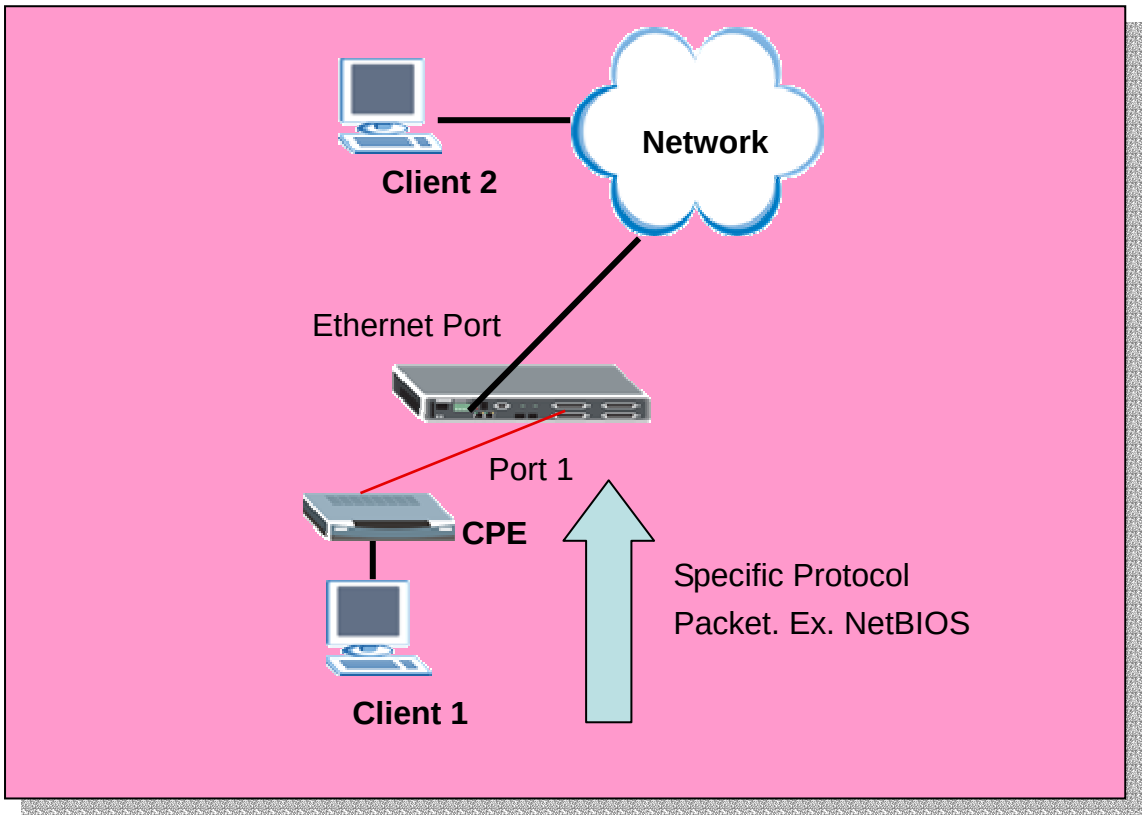
The rule creation has been finished.



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

Filter Some Certain Packet

ISP may want to filter some kinds of packets. IES-1248 provides “Packet Filter” function to filter some specific packets, like IP, ARP, DHCP, EAPoL, PPPoE, NETBIOS and IGMP.

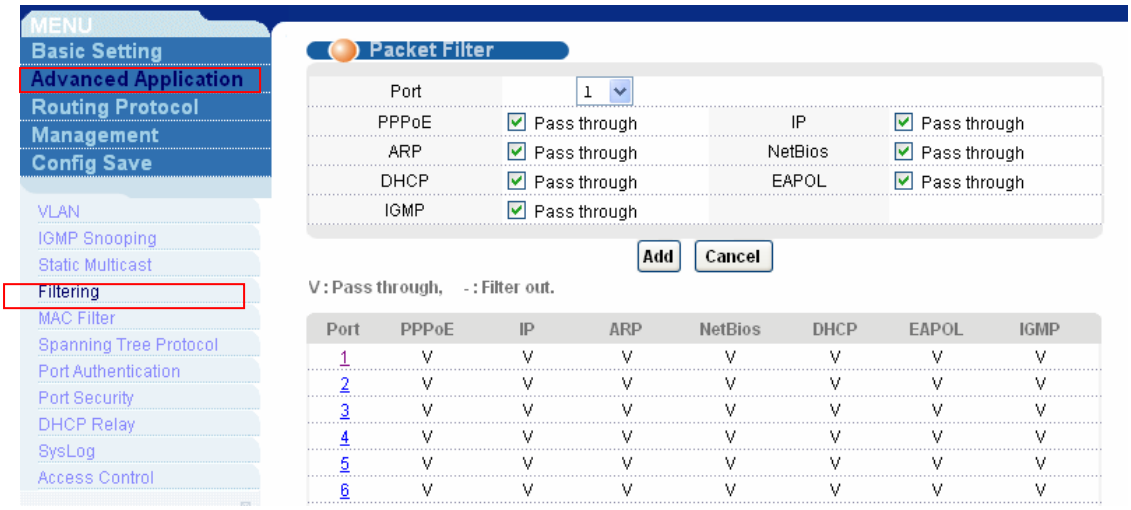


How to Filter Some Specific Packet

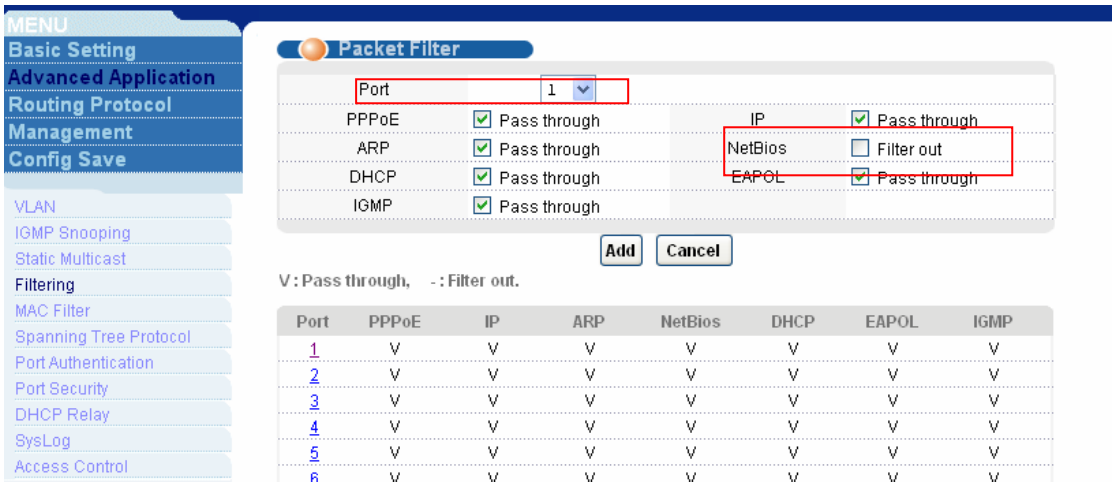
Here, we will set up an environment to block NETBIOS protocol packets.

1. IES-1248 settings

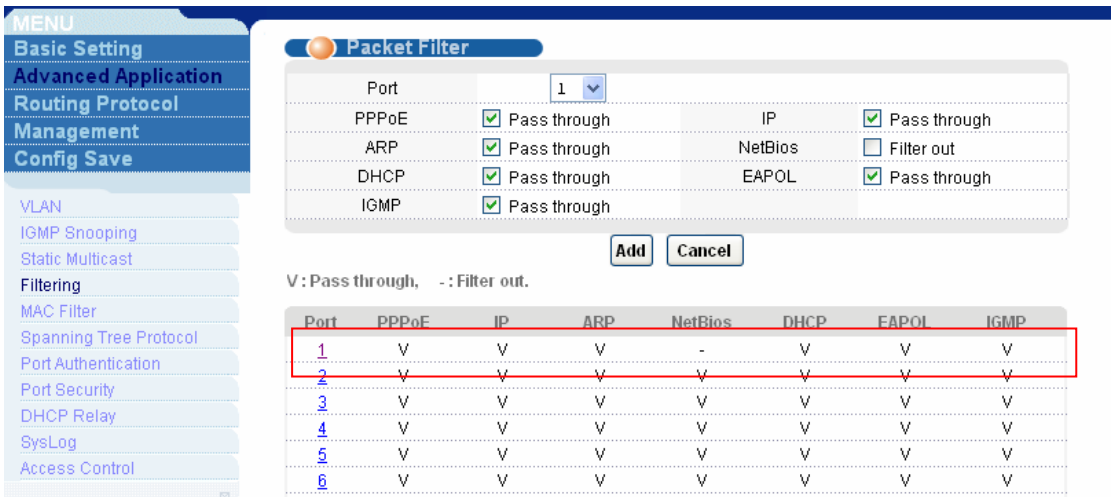
Click **Advanced Application**, **Filter** in the navigation panel to display configuration screen as shown. You will see the **Packet Filter** setup page.



Please select port 1 and clear the **NetBios** check box. Meanwhile, you will see **Filter Out** in **NetBios** check box. Press **Add** button make the change take effect.

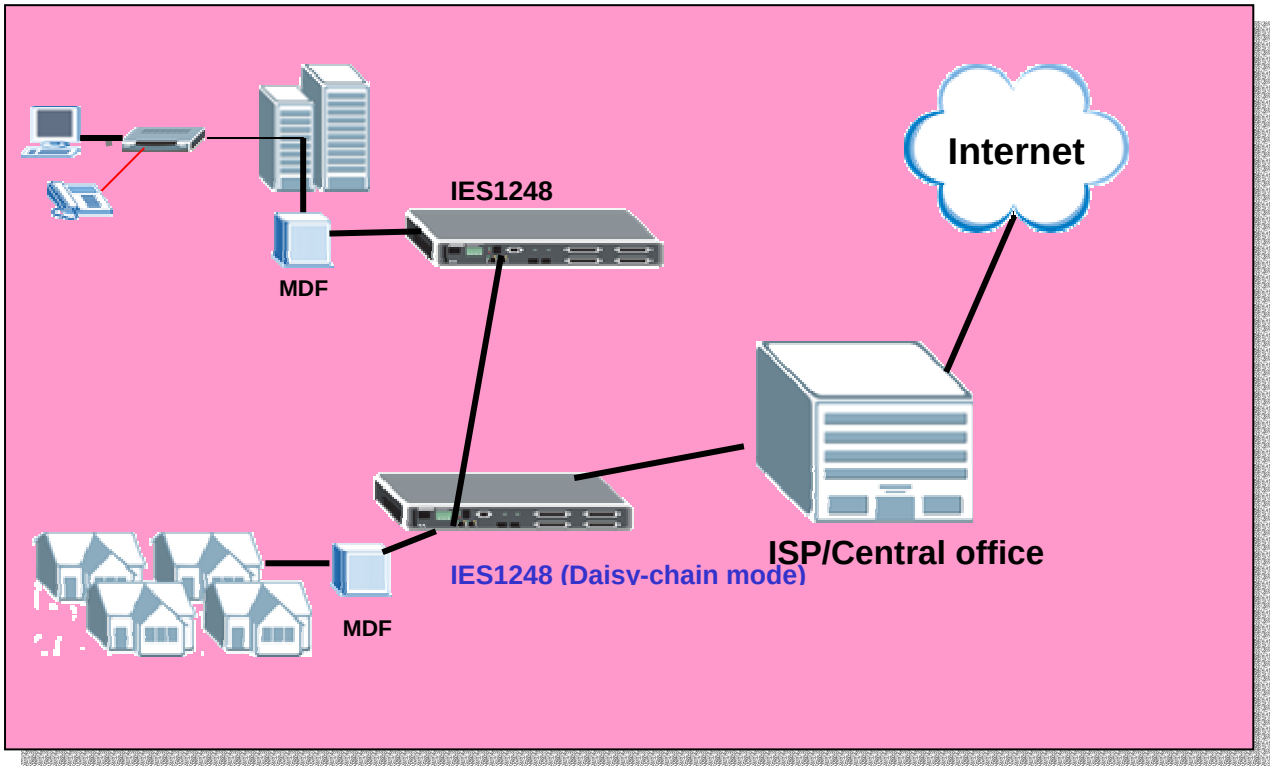


So you will see the port 1 will block the NetBios protocol packets.



Cascade two IES1248 (Daisy chain mode)

You know, the IES1248 is a remote mini-DSLAM. When the subscriber number is increased, ISPs may cascade or daisy-chain the more then one IES1248 to extend the port number. They can daisy-chain up to three IES1248.

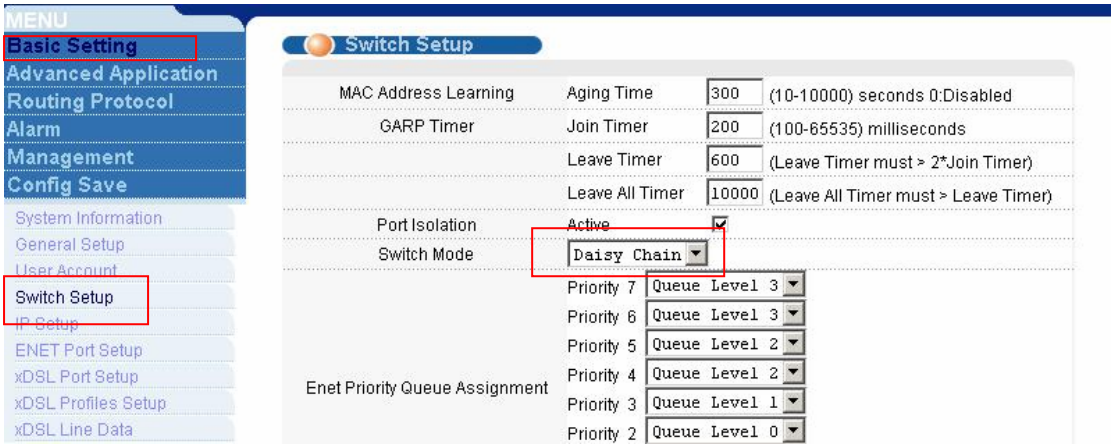


How to setup Daisy-chain mode

In this case, we daisy-chain two IES1248. Please see the figure above. We only set the one connected to the ISP as Daisy-Chain mode. In Daisy-Chain mode, connect the Ethernet Port 1 to the Ethernet backbone and connect the Ethernet Port 2 to another IES1248. Note that we don't suggest using loop network topology while using daisy-chain mode.

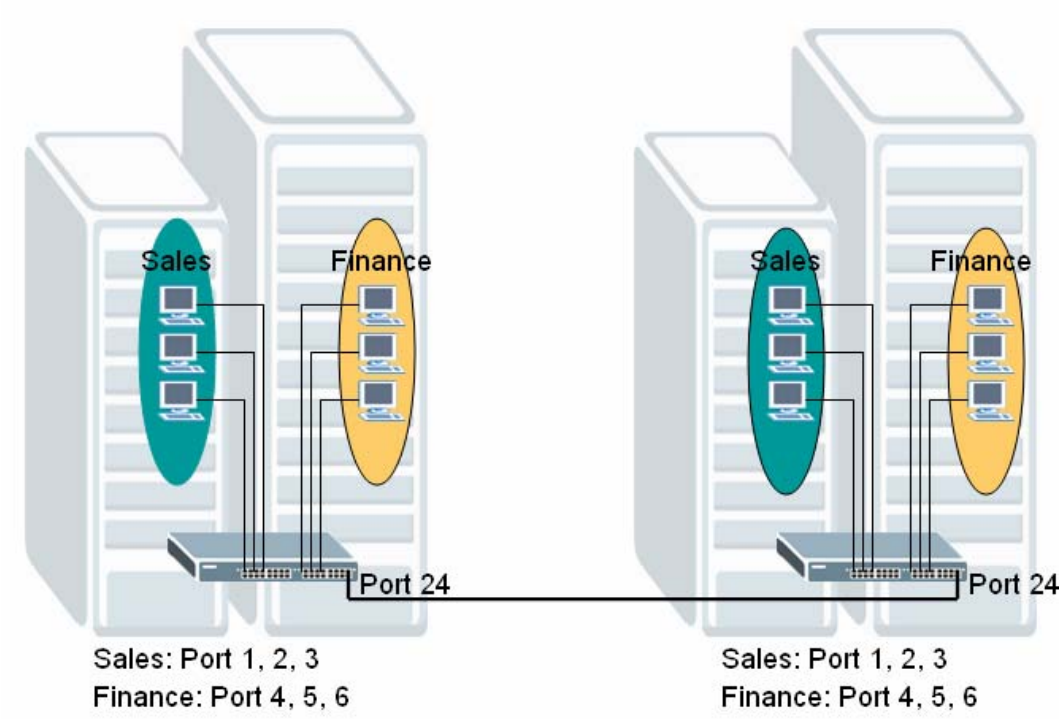
1. IES-1248 settings

Click **Basic Setting**, **Switch setup** in the navigation panel to display configuration screen as shown. You will see the **Switch setup** page. In **Switch Mode** combobox, select the **Daisy chain**. Don't forget press **Apply** button to let the setting take effect.



VLAN Application

Application Scenario A:



Scenario Description

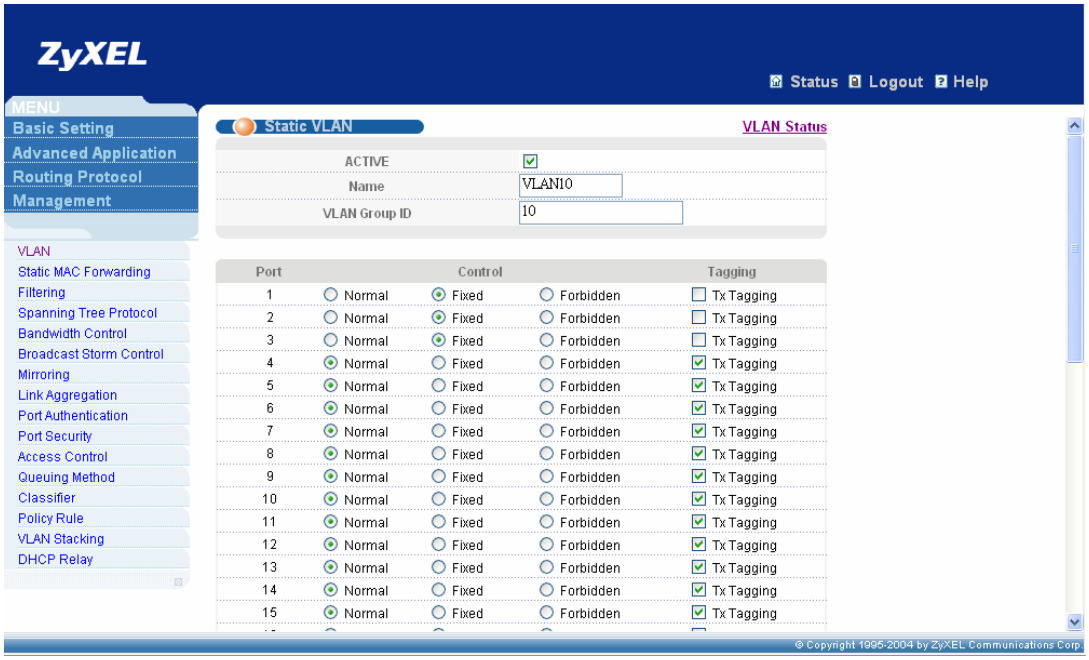
In this scenario, each building has 2 departments, and users belong to the same

department could communicate with each other, but communication between different departments is forbidden for security and confidential reason.

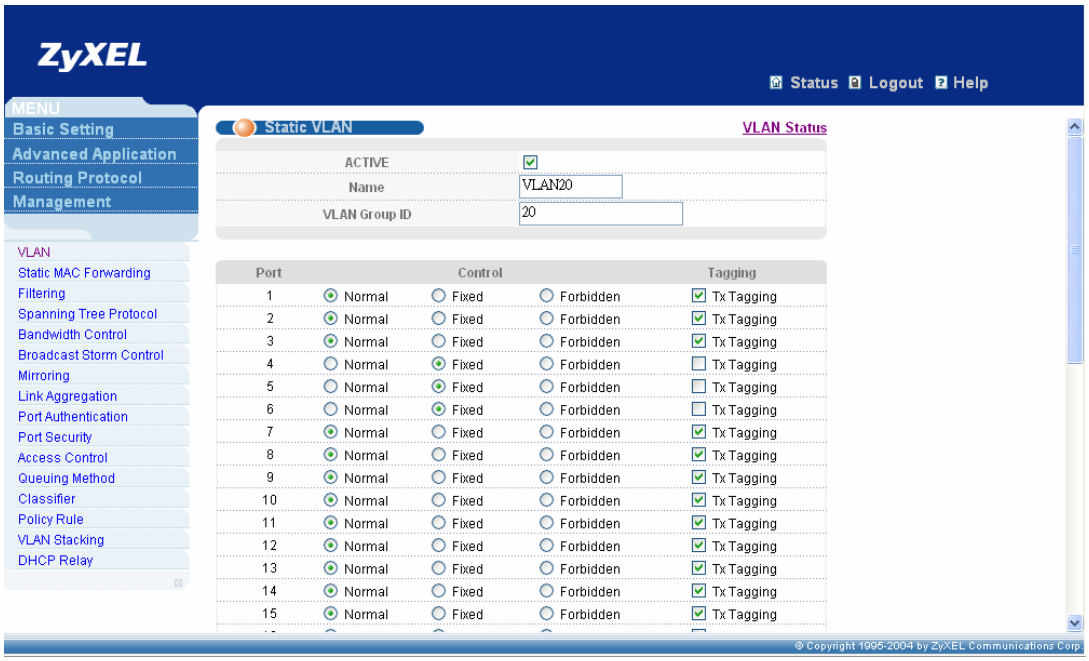
PCs from Sales department (VLAN 10) connected to Port 1, 2, 3 of both switches while Finance department (VLAN 20) using Port 4, 5, 6 connected to switches. Because this is a symmetric switch setting, so configuration of both switches are same.

How to configure VLAN:

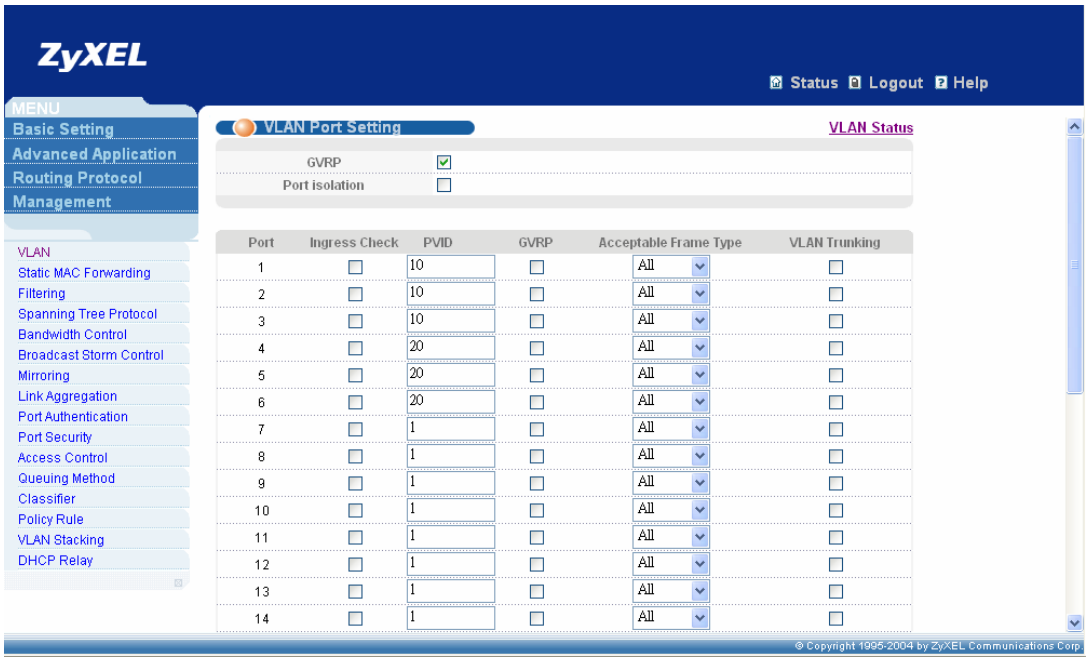
1. Please enter VLAN setting under Advanced Application menu and click “static VLAN” to bring up the following screen, adding **VLAN 10: port 1, fixed, untag; port 2, fixed, untag; port 3, fixed, untag; port 24, fixed, Tx tagging.**



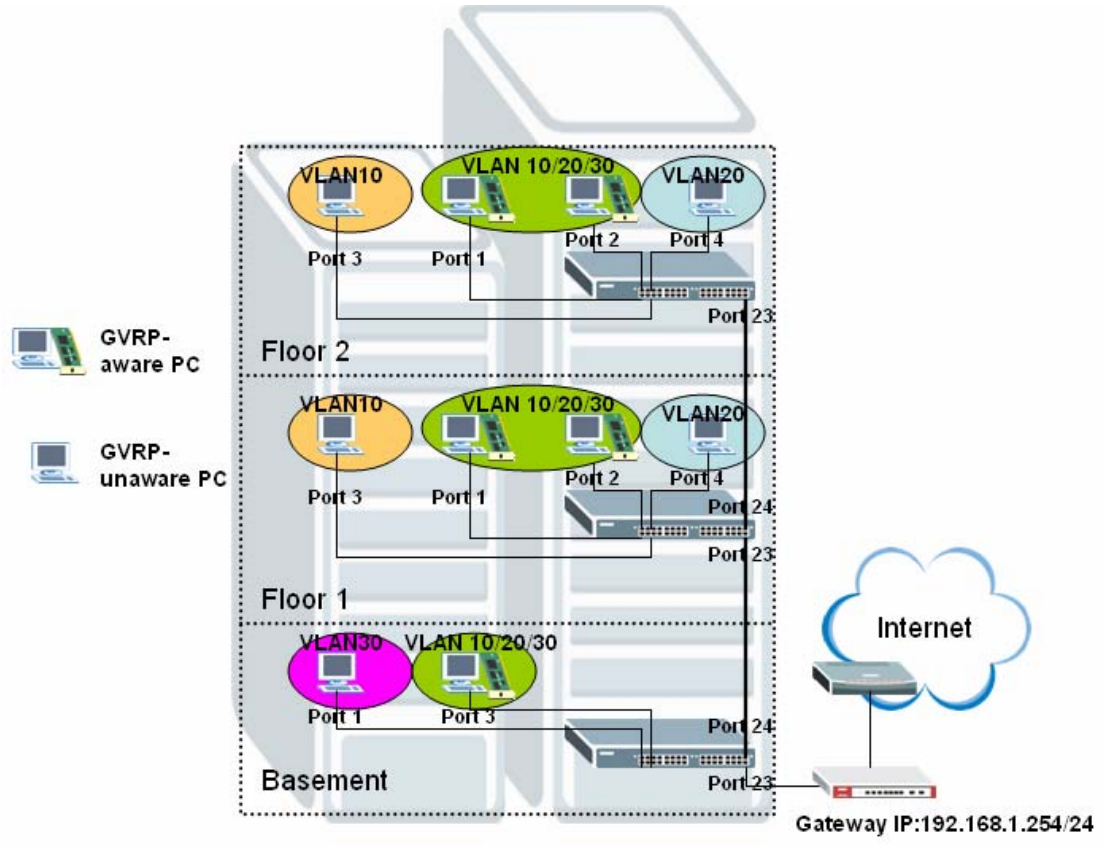
2. Follow the above step to add **VLAN 20: port 4, fixed, untag; port 5, fixed, untag; port 6 fixed, untag. port 24, fixed, Tx tagging.**



3. Please click VLAN port setting to bring up the following screen, setup **PVID 10 for port 1, port 2, port 3; PVID 20 for port 4,port 5, port 6.**



Application Scenario B:



Scenario Description:

In this scenario, PCs belong to different divisions within a single corporation can not communicate with each other, and we left some ports of switches are for GVRP-aware PC and others are for VLAN-unaware PC. So network administrator can manage and configure VLAN smartly based on different devices and requirements.

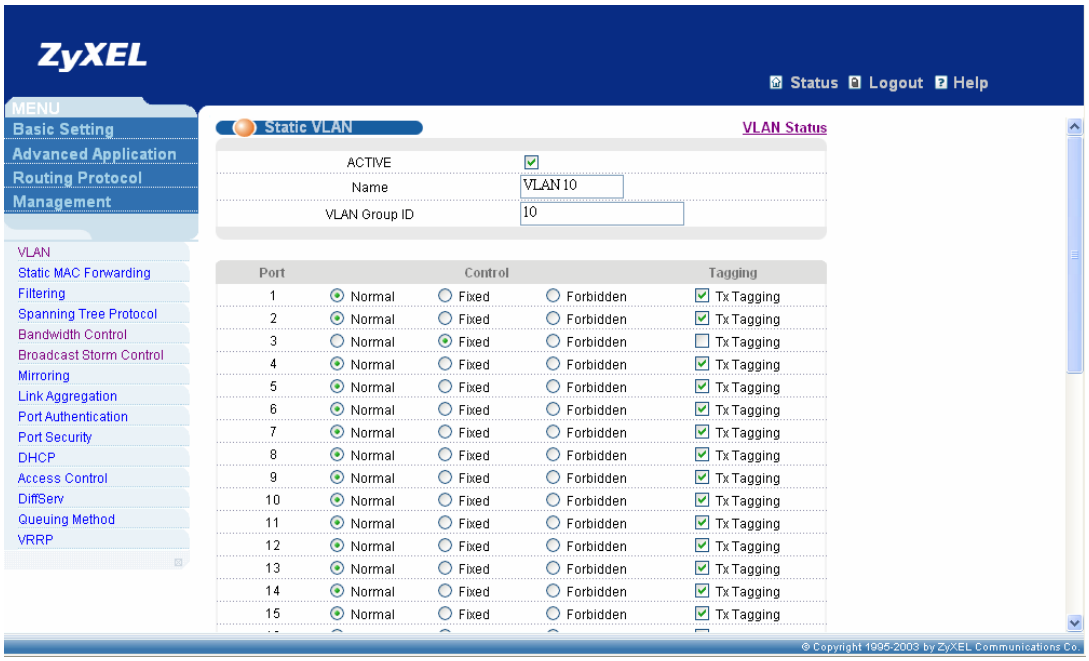
For switches on floor 1&2, PC connected to port 3 joins VLAN 10 statically, PC connected to port 4 joins VLAN 20 statically, and PCs connected to port 1&2 can join VLAN 10/20/30 which determined by its configuration on GVRP-aware NIC dynamically. For switch on basement, PC connected to port 1 joins VLAN 30 while PC connected to port 3 can join VLAN10/20/30 dynamically.

Please Note: all clients connected to switches in this scenario should be located in the same subnet (in this example, the subnet is 192.168.1.0/24)

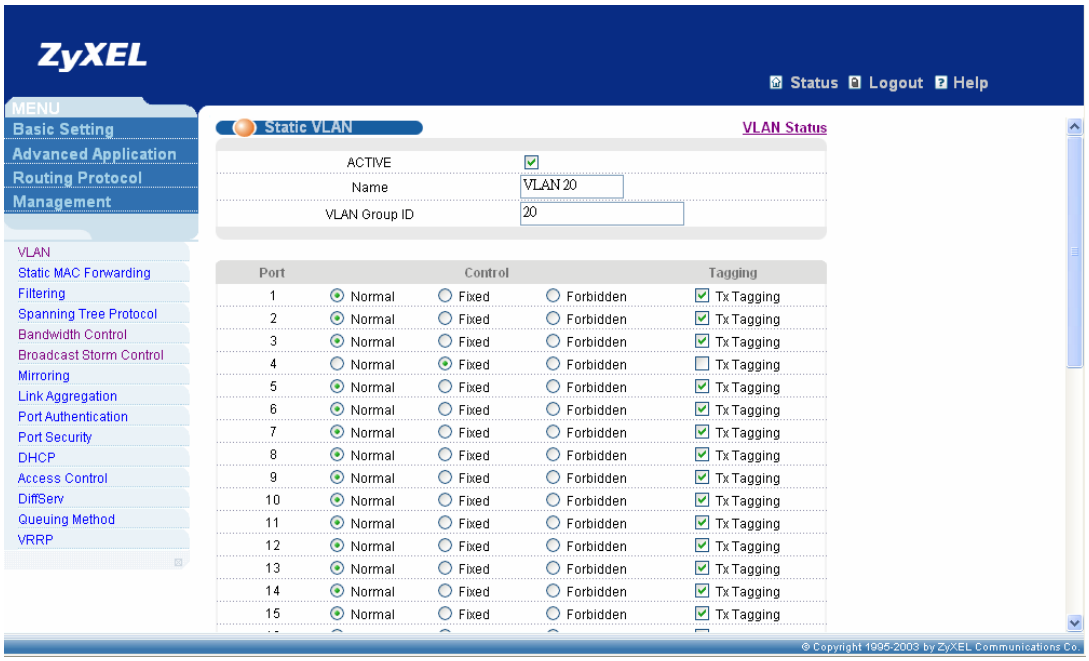
How to configure this scenario:

1. For Switch A on Floor 2:

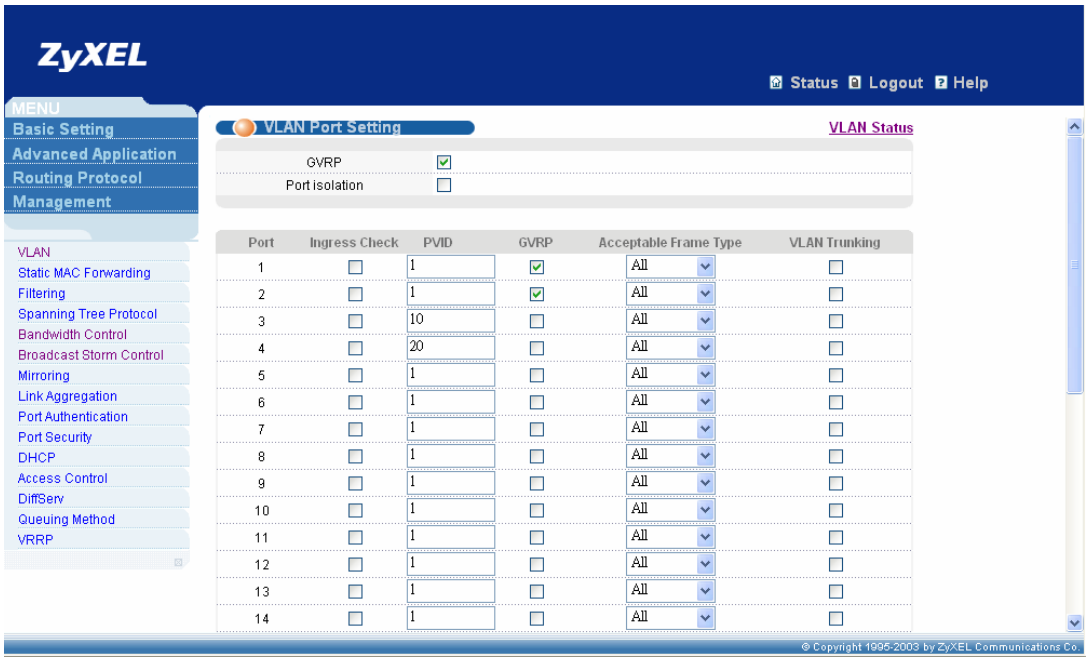
Please enter VLAN setting under Advanced Application menu and click “static VLAN” to bring up the following screen, adding **VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging”.**



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

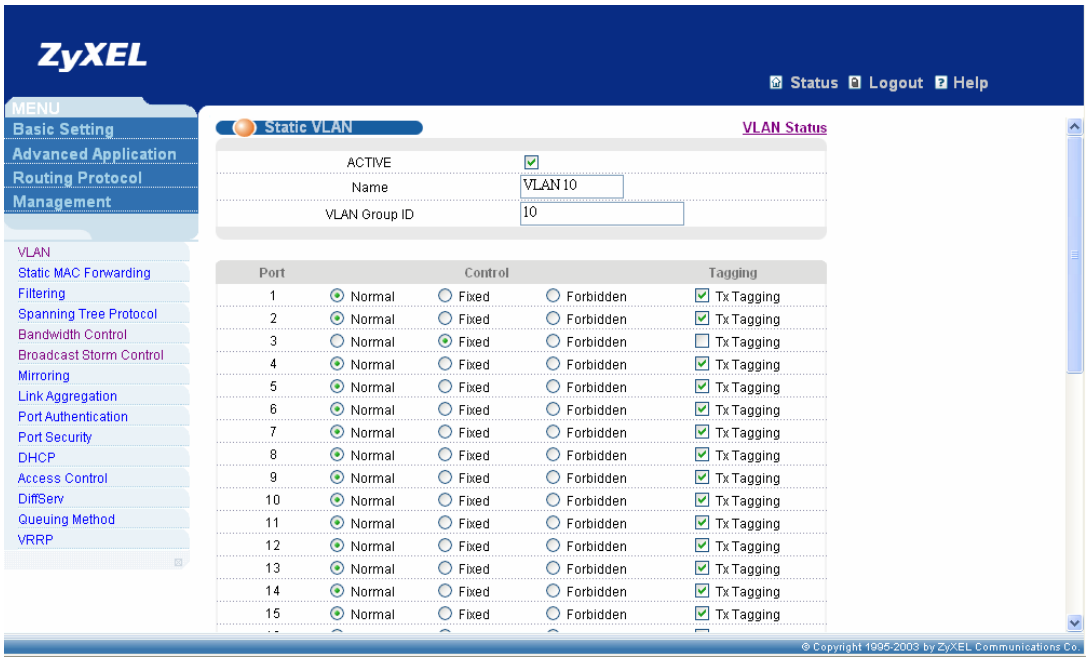


Please click VLAN port setting to bring up the following screen, setup **PVID 10 for port 3, PVID 20 for port 4**, and enable GVRP on the top of the screen and **port 1, port 2, port 23.**

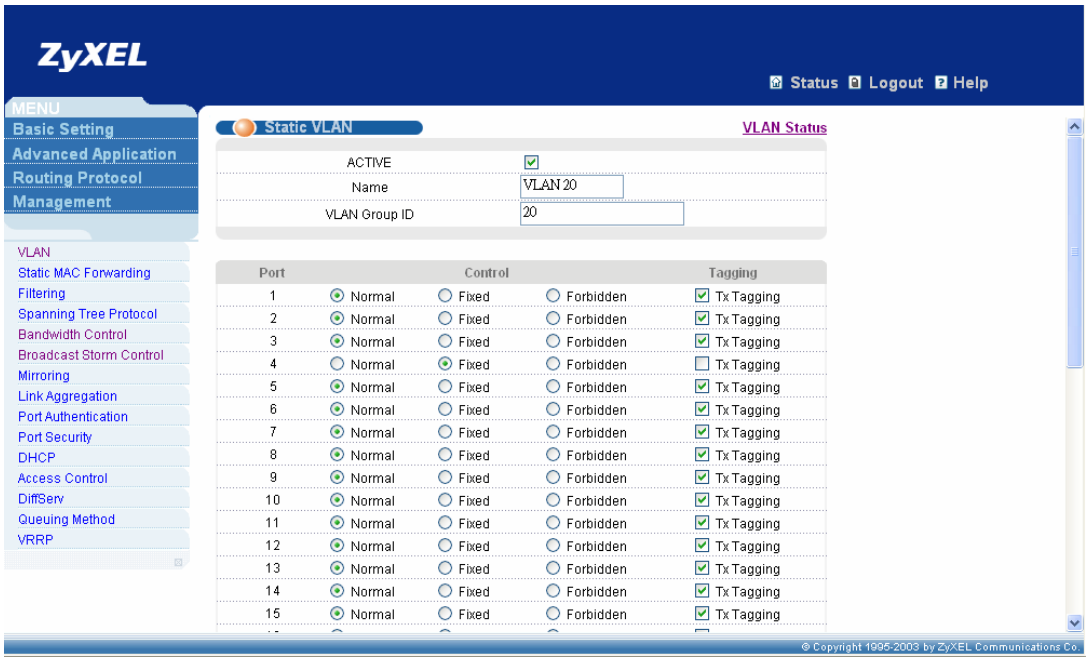


2. For Switch B on Floor 1:

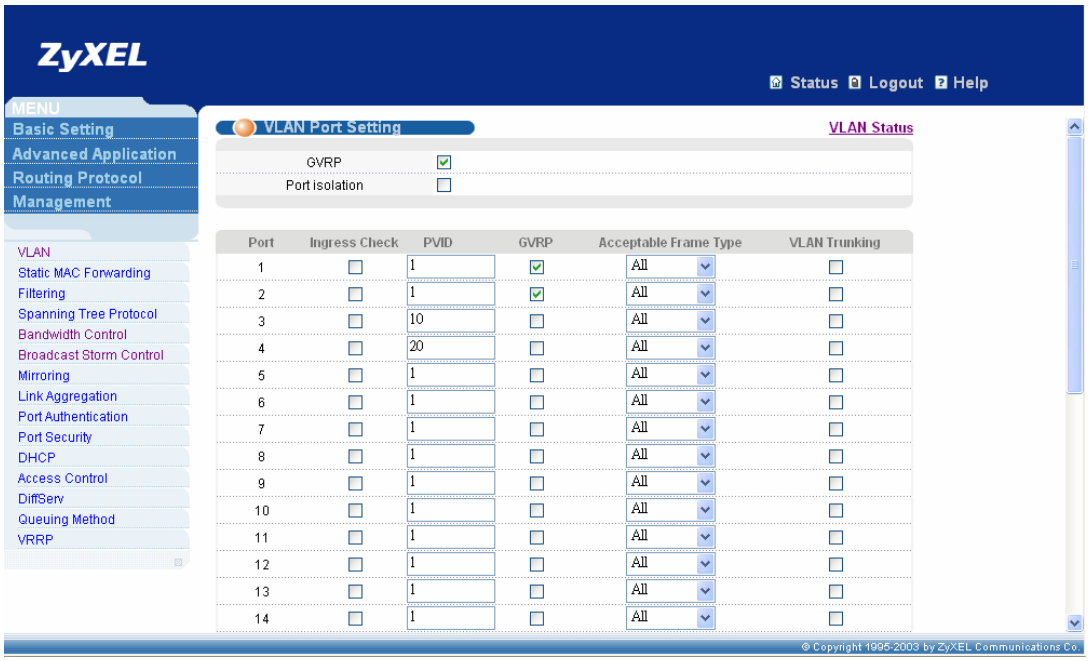
Please follow the same steps to adding **VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging; port 24, fixed, Tx tagging".**



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

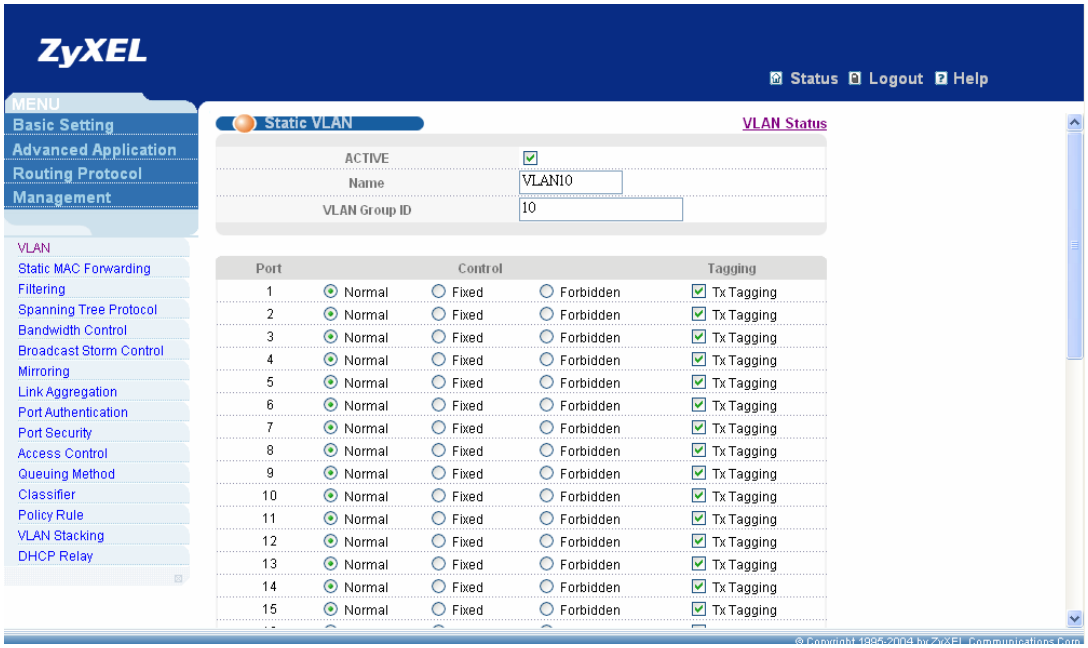


Please click VLAN port setting to bring up the following screen, setup **PVID 10 for port 3, PVID 20 for port 4,** and **enable GVRP on the top of the screen and port 1, port 2, port 23, port 24.**

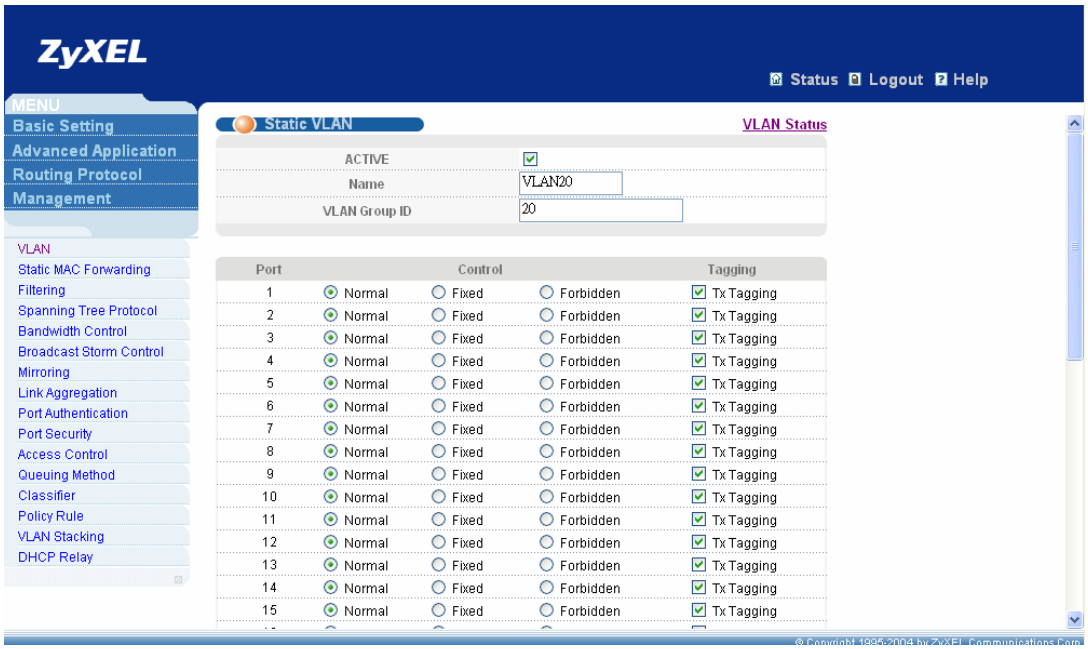


3. For Switch C on Basement:

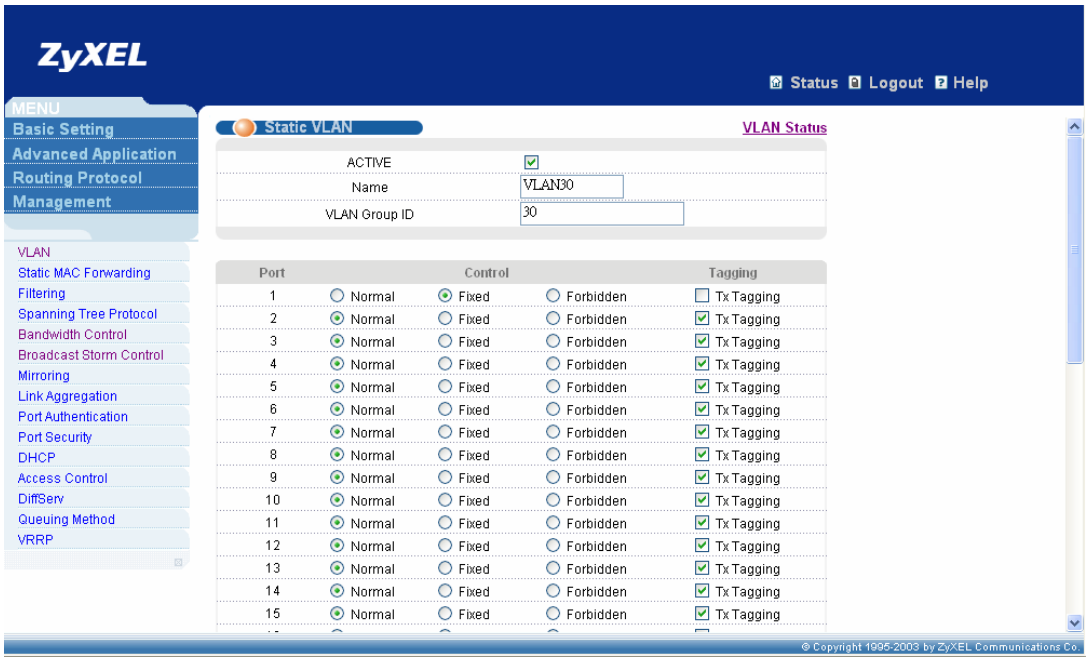
Please set static **VLAN 10: port 23, fixed, untag.**



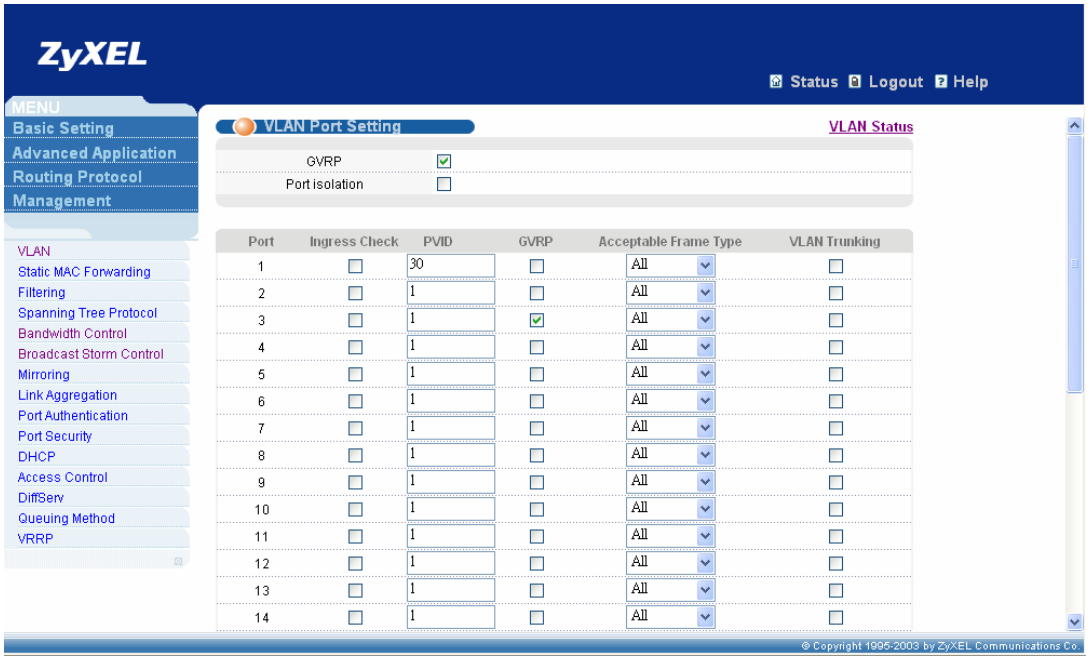
Please set static **VLAN 20: port 23, fixed, untag**.



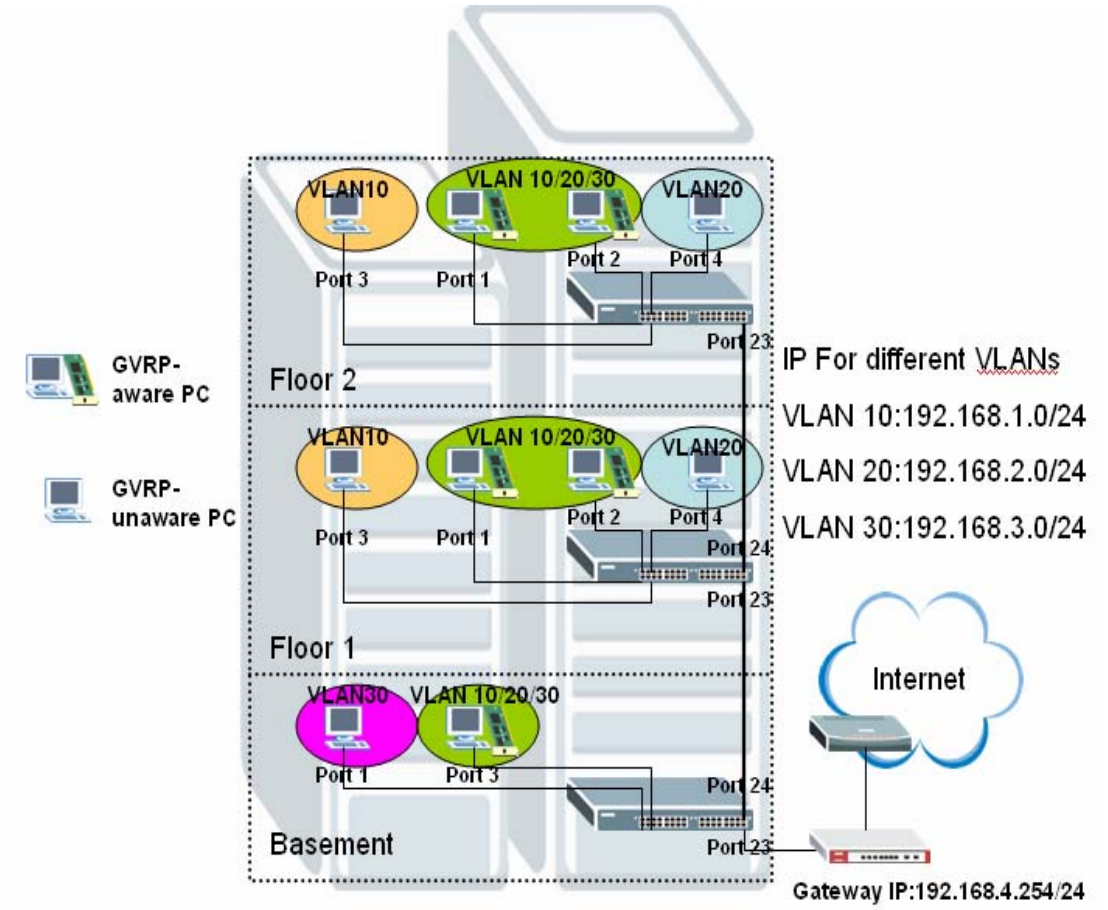
Please add **VLAN 30: port 1, fixed, untag; port23, fixed, untag; port 24, fixed, Tx tagging.**



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



Application Scenario C:



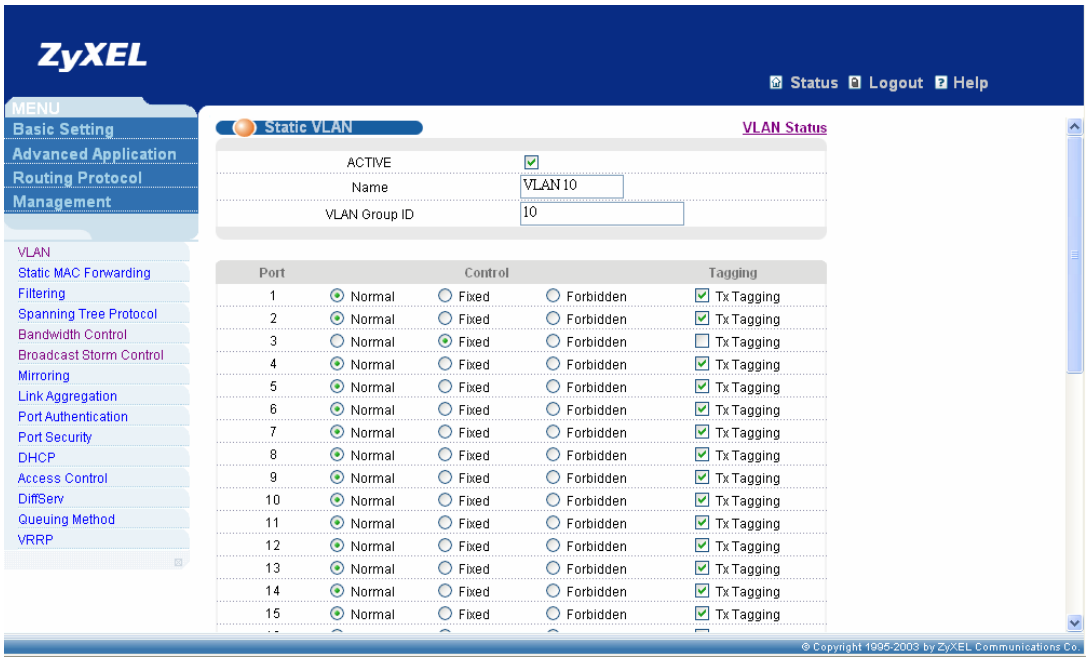
Scenario Description:

Scenario C is for all clients can surf Internet or public resource when dividing multiple subnets for the same structure from scenario B. In this scenario, there are 3 subnets match to 3 VLANs to let network administrator manage VLAN more expediently: subnet 192.168.1.0/24 for VLAN 10; subnet 192.168.2.0/24 for VLAN 20; subnet 192.168.3.0/24 for VLAN 30. In order to control traffic routing between different subnets, we put a layer 3 switch (ES4024/ES4024A/GS4024) on basement. The configuration of switch A and switch B are the same as scenario B, only switch C need more configurations in this network environment.

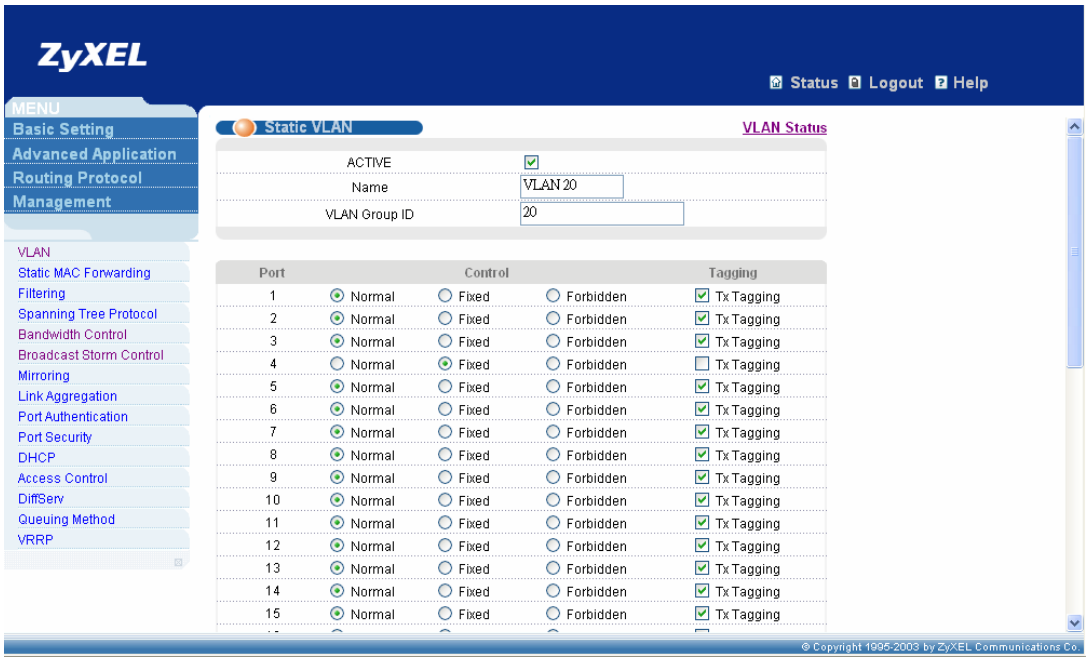
How to configure this scenario:

1. For Switch A on Floor 2:

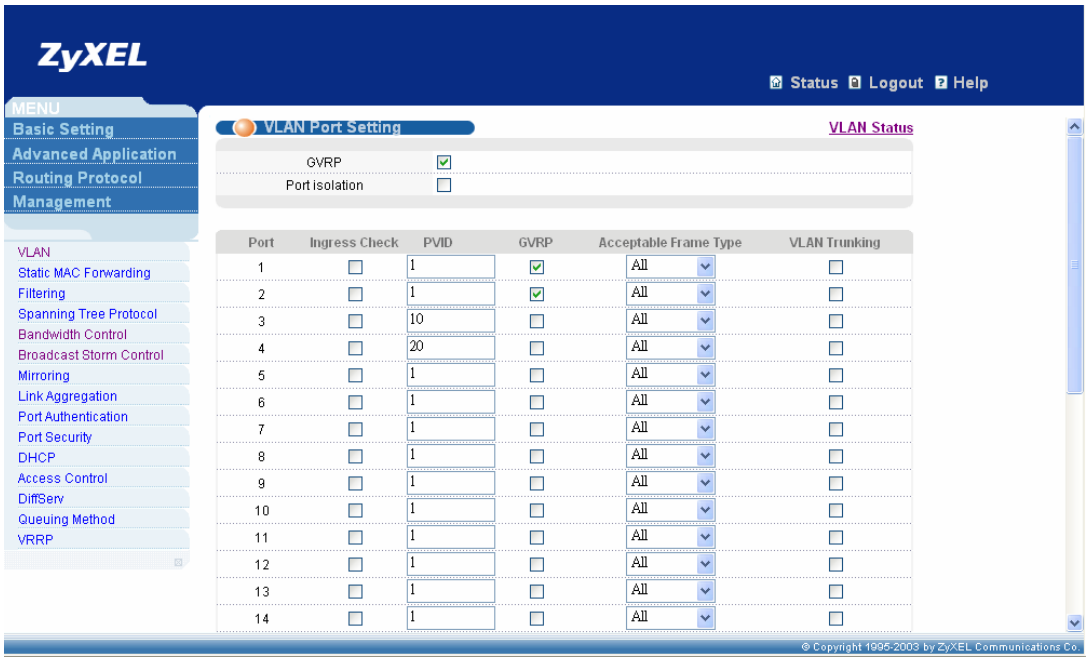
Please enter VLAN setting under Advanced Application menu and click “static VLAN” to bring up the following screen, adding **VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging”.**



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

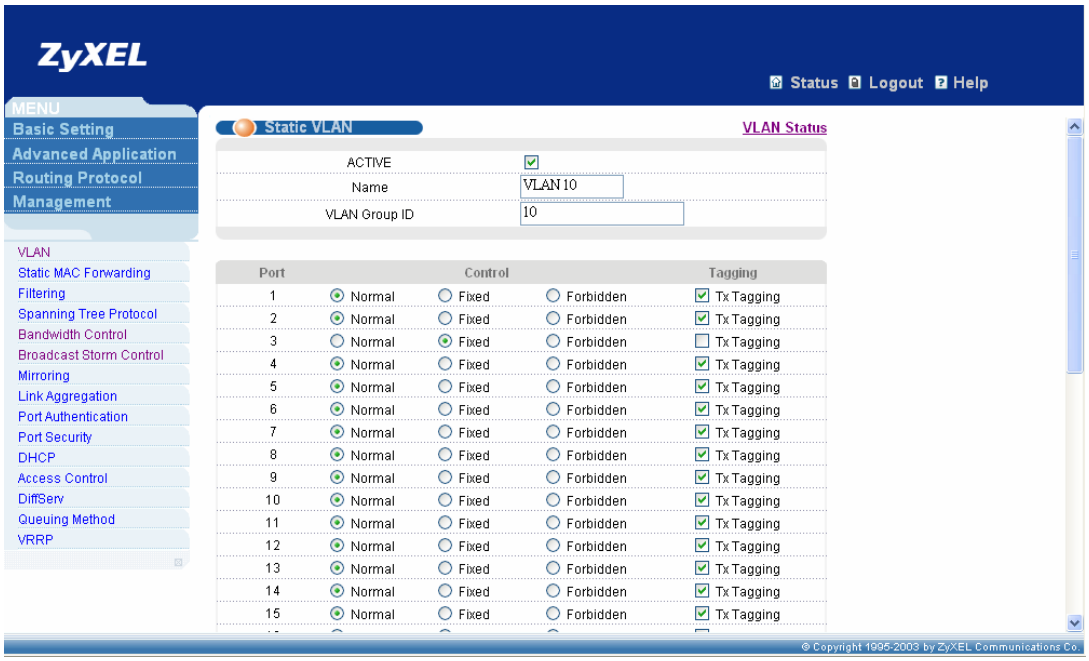


Please click VLAN port setting to bring up the following screen, setup **PVID 10 for port 3, PVID 20 for port 4**, and enable GVRP on the top of the screen and **port 1, port 2, port 23.**

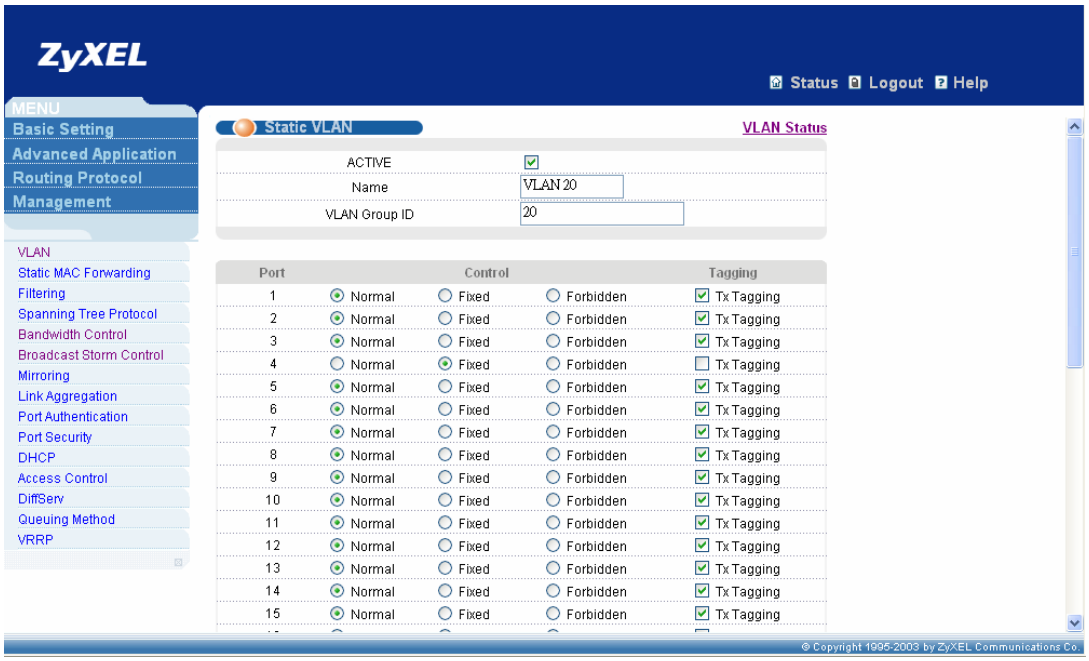


2. For Switch B on Floor 1:

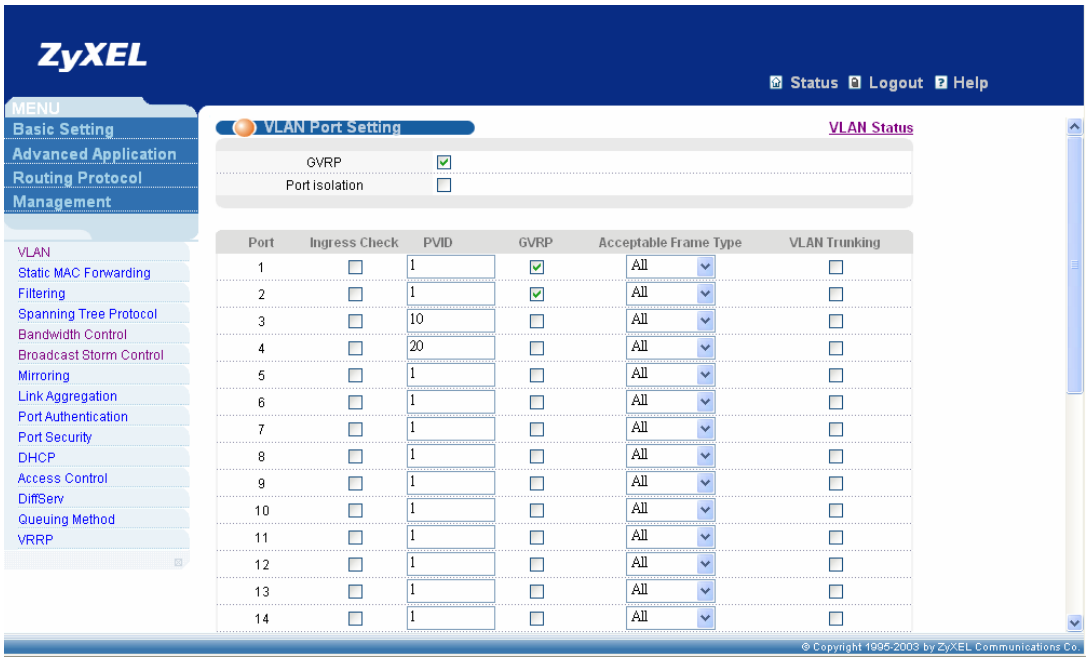
Please follow the same steps to adding **VLAN 10: port 3, fixed, untag; port 23, fixed, Tx tagging; port 24, fixed, Tx tagging".**



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

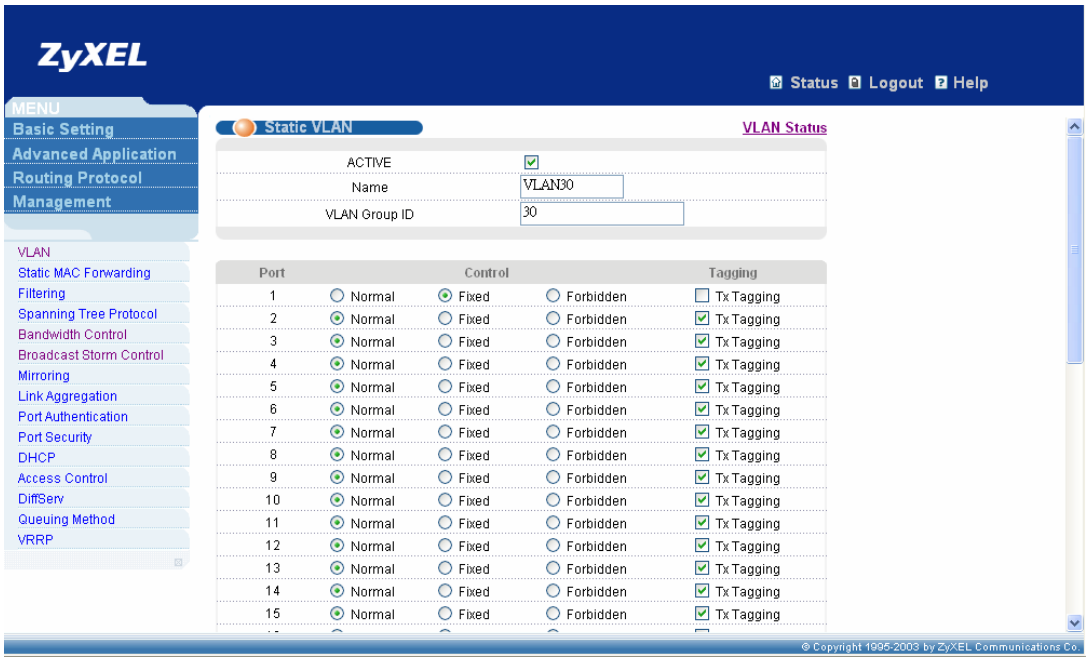


Please click VLAN port setting to bring up the following screen, **setup PVID 10 for port 3, PVID 20 for port 4,** and **enable GVRP on the top of the screen and port 1, port2, port 23, port 24.**

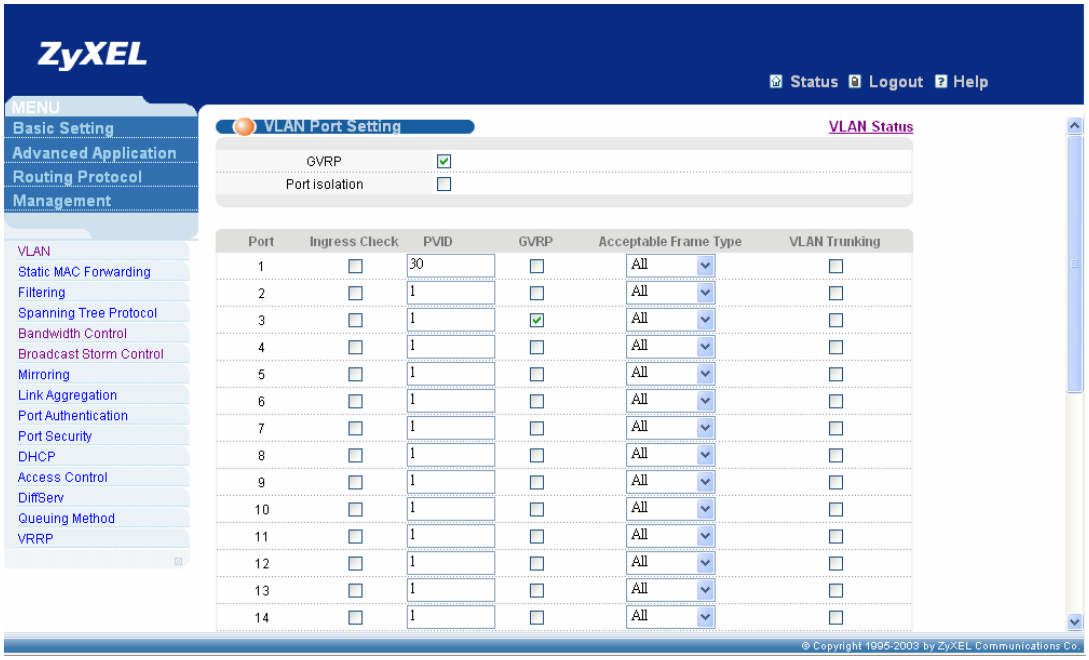


2. For Switch C (layer 3 switch) on Basement:

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

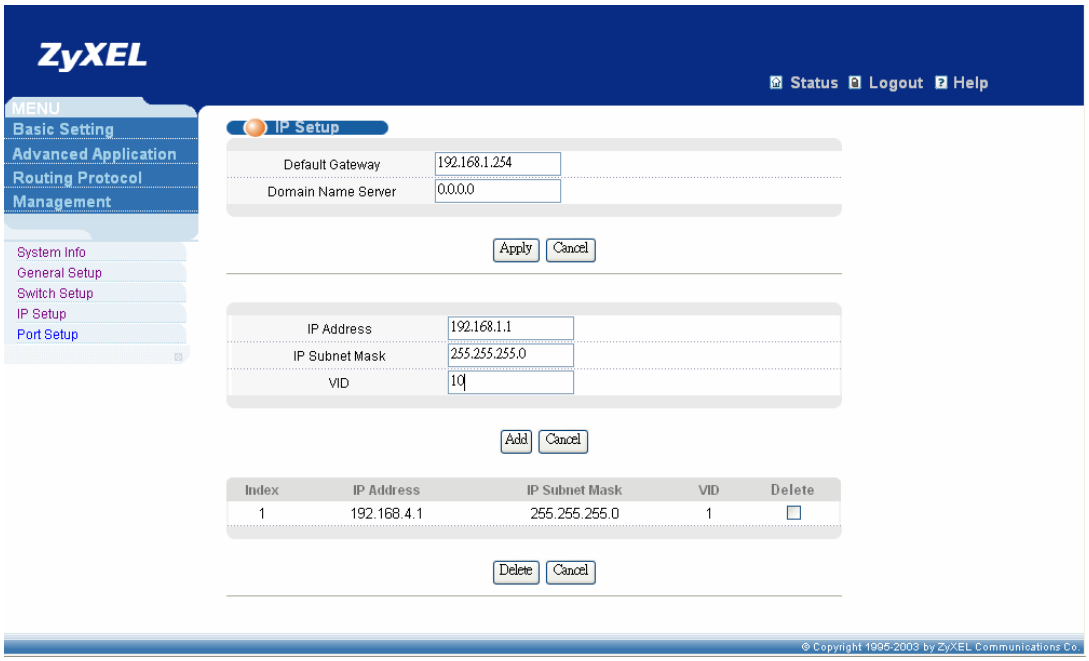


Please **setup PVID 30 for port 1** and **enable GVRP on port 3 and port 24.**

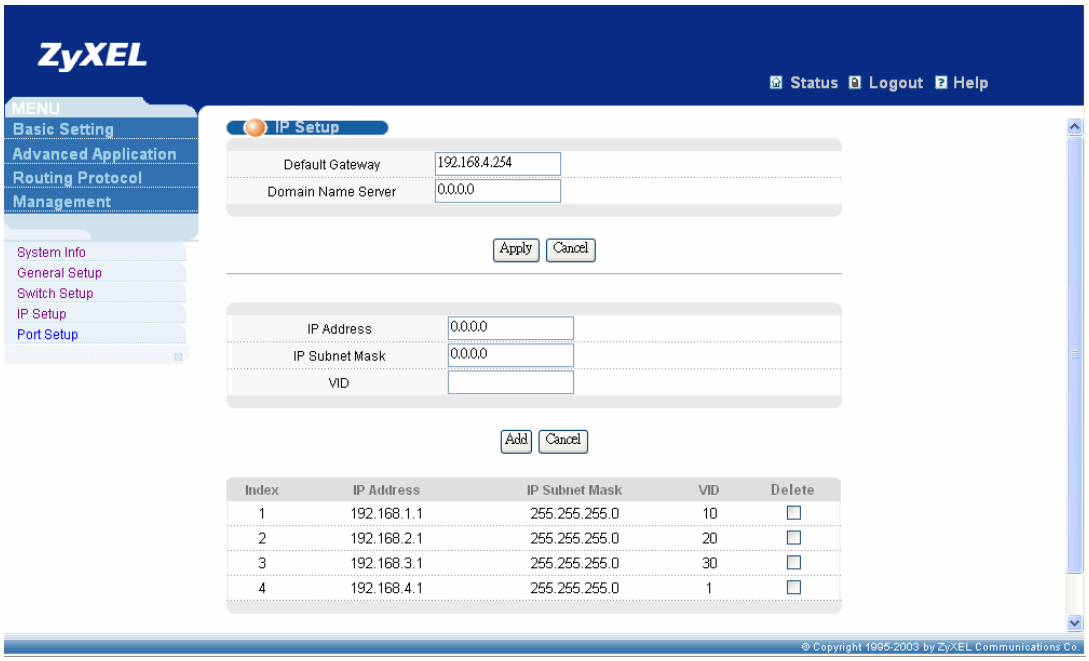


Please click “IP setup”, then setup 4 domains on ES4024/GS4024:

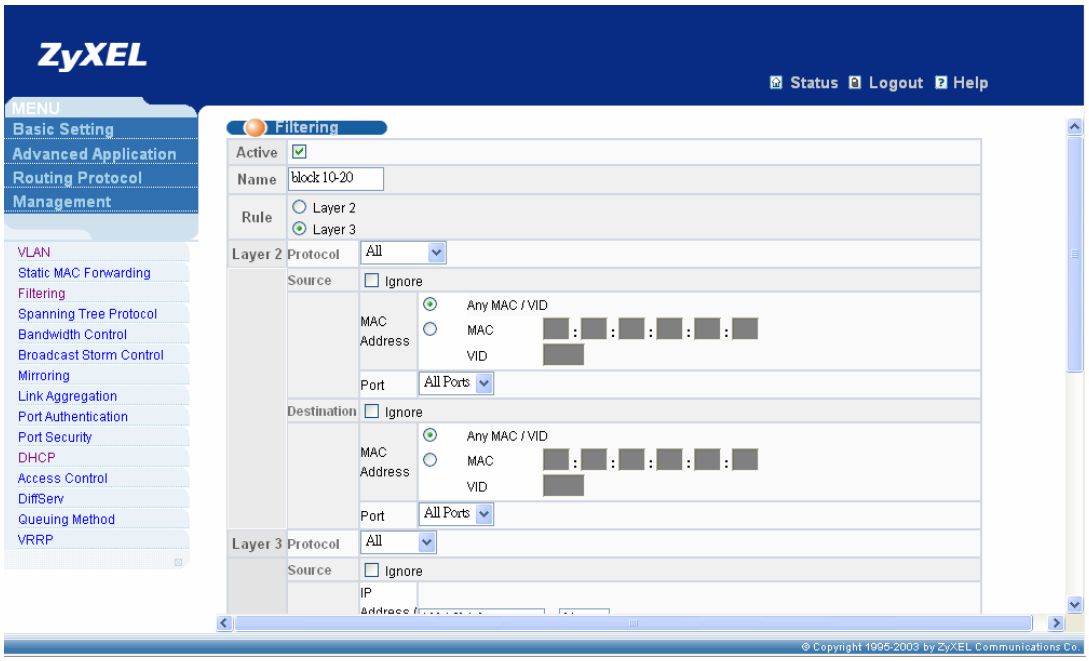
Index	IP address	IP Subnet mask	VLAN ID
1	192.168.1.0	255.255.255.0	10
2	192.168.2.0	255.255.255.0	20
3	192.168.3.0	255.255.255.0	30
4	192.168.4.0	255.255.255.0	1

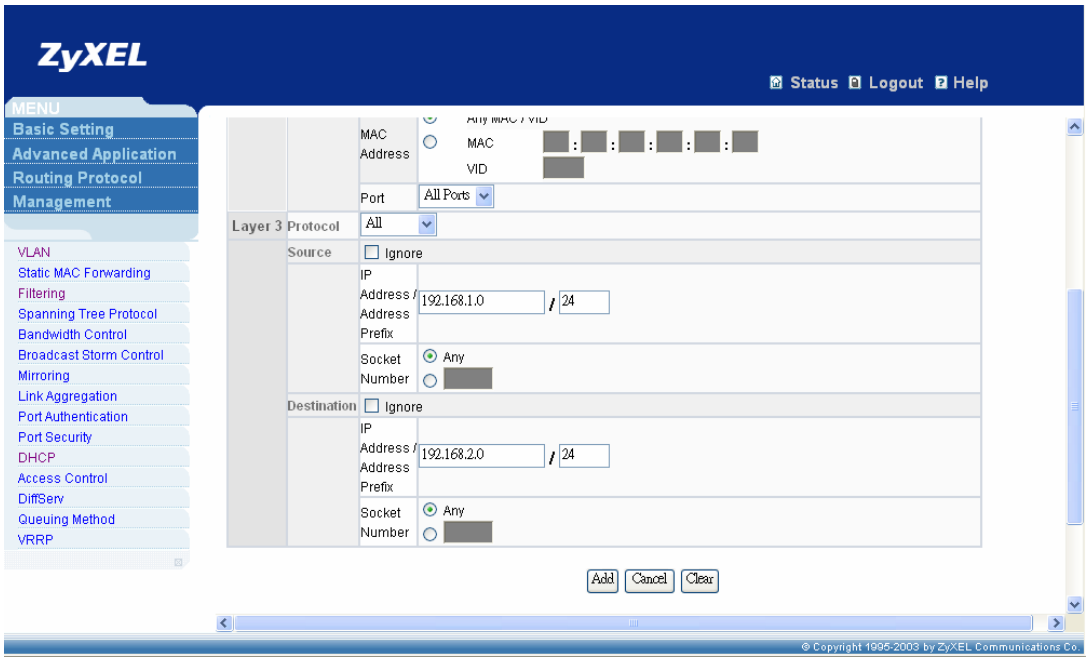


After finish domain setting, please change the default gateway and domain name server setting and click “Apply”.

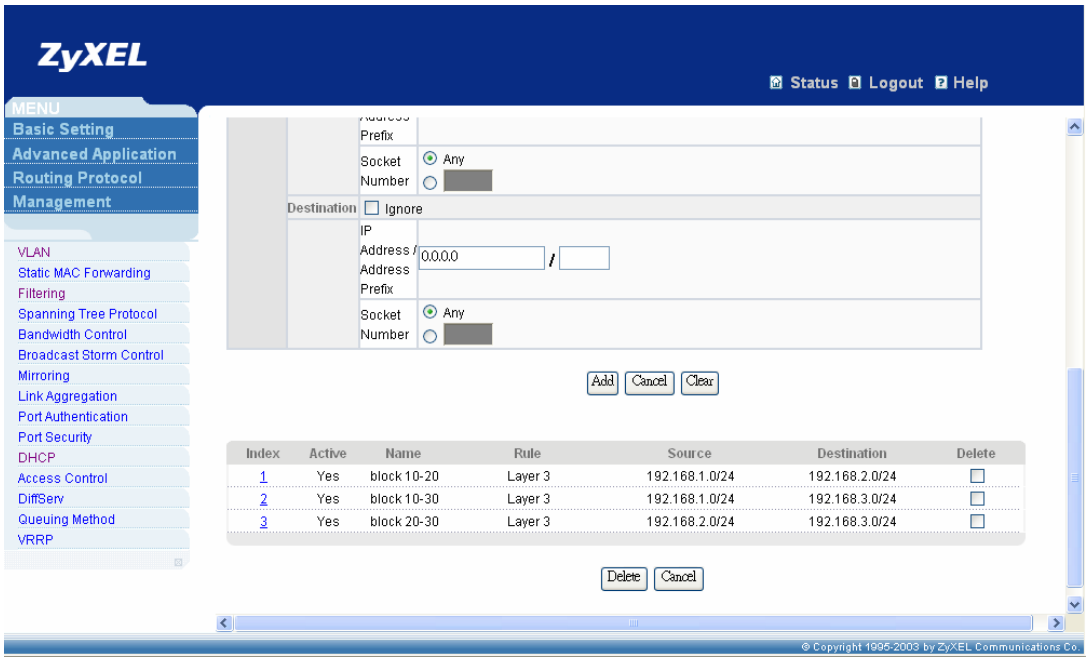


Please click “Filtering” under “Advanced Application” menu list to bring up the following screen and add 3 filter rules to block traffic from different subnets.





You will see the following screen after finish filtering setting.



Advise:

1. Please also configure routing protocol to make layer 3 Switch and gateway exchange their routing information in this scenario.
2. You can also enable DHCP feature based on VID on layer 3 Switch (ES4024/GS4024), which will help you to dynamically assign IP to different VLANs more expediently.

FAQ

What is the maximum line rate of IES1248 ?

It can support ADSL2+, so line rate can reach to 1.2Mbps in upstream direction and 25 Mbps in downstream in a short distance.

How many management instances can access IES-1248 at the same time?

Only one console, one WEB GUI and four telnet accounts can access IES at the same time.

What is the difference between IES1248-71 and IES1248-73 ?

- IES1248-71 : ADSL Annex A for POTS.
- IES1248-73 : ADSL Annex B for ISDN.

What is the power requirement of IES- 1248?

- Power Input is –48VDC(-36~-72VDC).
- Maximum power consumption is 90W.

What kind of the DSL standard does IES1248 compliant ?

- ADSL : G.992.1, G.992.2, T1.413 issue 2, G.lite
- ADSL 2 : G.992.3, G.992.4
- ADSL 2+ : G.992.5.

What is the ADSL chipset of IES1248?

Centillium Maximus

What is the Network Processor of IES1248 ?

Wintegra's WinPath787D4

How many Flash memory and SDRAM that IES 1248 supports?

- Flash memory : 4Mbytes
- SDRAM : 64Mbytes

What kind of the features that IES 1248 supports ?

- RFC 2684 Bridge Mode (Replace RFC 1483)
- IEEE 802.1Q
- VLAN acceptable frame type filter
- IGMPv2 Snooping
- ATM QoS (UBR, CBR, VBR) per PVC
- DHCP Relay Agent Information Option 82.
- MAC Filter
- MAC Count Filter (Limit the numbers of MAC address)
- Packet Type Filter
- IEEE 802.1x Port-based Network Access Control
- ADSL Port Isolation
- Multiple PVCs
- Support VC profile

What is the default console rate of IES1248 ?

9600, 8bit data, no parity, stop bit=1, no flow control.

How many static VLAN entries can IES1248 support ?

IES1248 supports up to 1024 VLAN entries..

How many VLANs can each ADSL port of IES1248 join ?

Each ADSL port can join at most 16 VLANs.

How many VLANs can each ADSL port of IES1248 join ?

Each ADSL port can join at most 16 VLANs.

What kinds of profiles can IES1248 supprot?

- Number of VLAN: 1024
- ADSL profile: 96
- ATM profile: 48
- IGMP filter profile: 128
- ADSL ALARM profile: 8
- Dot1X profile: 64
- DHCP relay server: 32

- IP ROUTE: 128
- Static multicast address: 32
- Igmp groups: 512 groups
- MAC learning: 14k (128 per ADSL port, 4k per ENET port)
- RPVC gateway IP address: 96

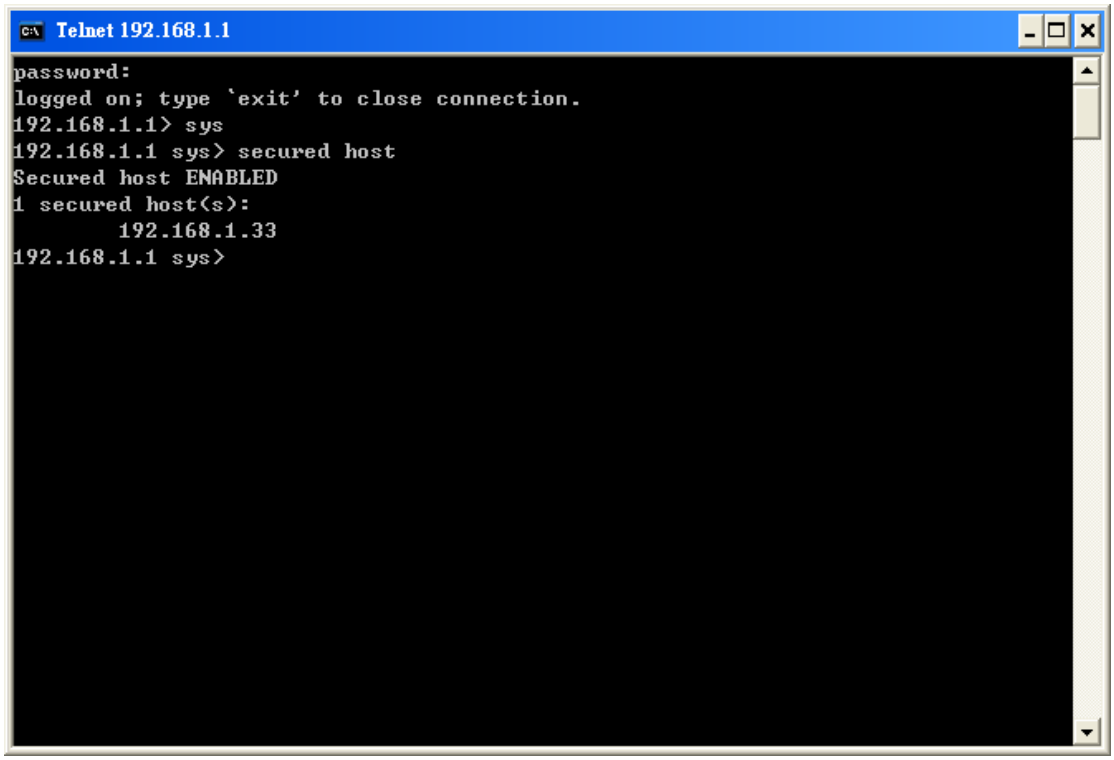
Trouble Shooting

If my computer can't access the DSLAM by WEB/Telnet/Ping from Ethernet port, only console screen can access successfully, what can I do?

1. Make sure that the Ethernet port has the appropriate speed mode setting.
2. Please check the Ethernet cable and connections between Ethernet port and PC, make sure the Ethernet LED is on when cable connection is already.
3. Make sure that both inband and outband IP of IES and Your PC are properly configured.
4. Please check Security host IP and service port setting from console port. Only the PC configured with IP of secured host has the authority to access the IPDSLAM. Please enter console screen via HyperTerminal by mini RJ-11 cable.

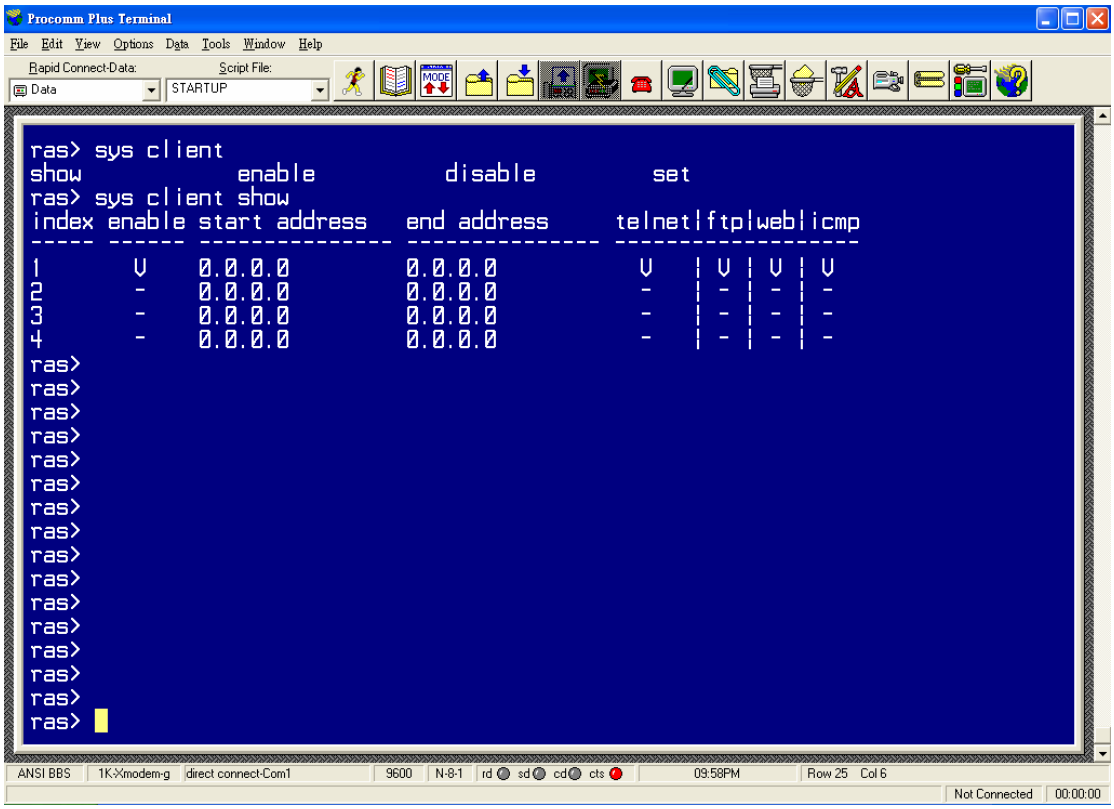
a) IES-1000

Please enter "sys" under "sys" submenu. Then key in "secured host" to check Security Host state.

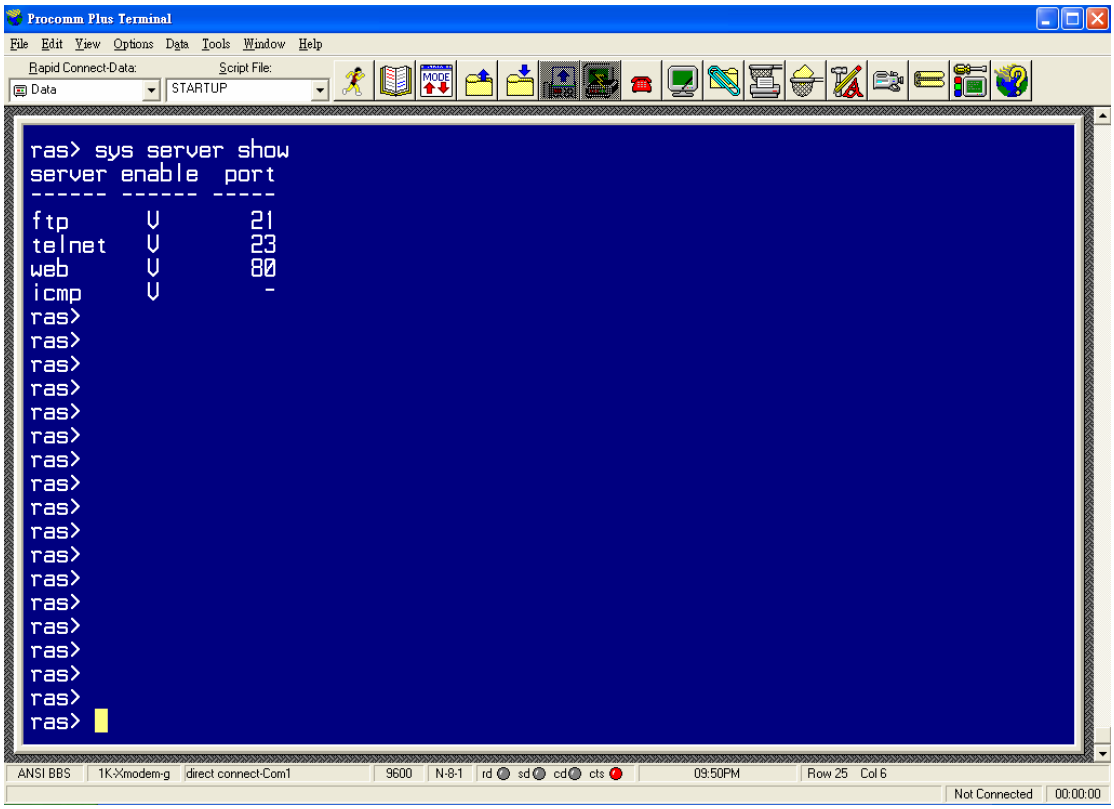


b) IES2000/3000 & IES 1248

Please key in "sys client show" to check security host IP to see your PC is included in the list or not.



Please key in “sys server show” to check server port, make sure that your application follow the server port in the list shown.



5. Please check VLAN configuration, make sure that traffic from outside is tagged or

will be added with CPU VLAN ID when access the IES.
6. please check your topology if you are not connect PC or device to IES directly.

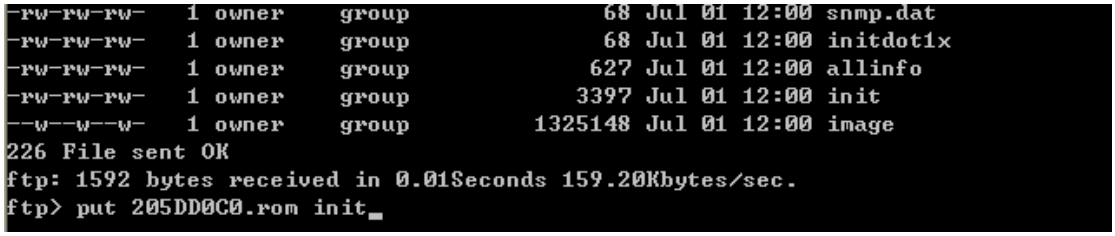
If DHCP Relay Option 82 can't work, for example, PC can not get desired IP address from DHCP server, what can I do?

1. Please check your VLAN configuration on IES, make sure that IES can reach DHCP server.
2. Please check your DHCP option 82 description configuration, make sure that description information is match to your DHCP server setting; otherwise DHCP server won't assign any IP from its IP pool to an invalid DHCP request.
3. Please make sure that your DHCP server support DHCP option 82, and check your configuration on DHCP server are all correct.
4. Please check your DHCP client, make sure that it is working on "obtain an IP address automatically" normally.

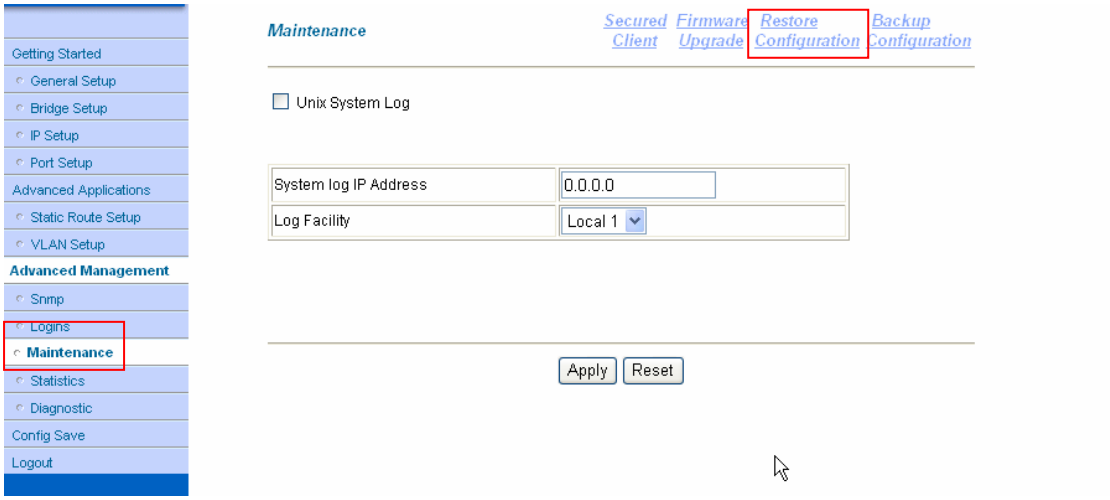
How to reset this device as factory default?

a) IES1000

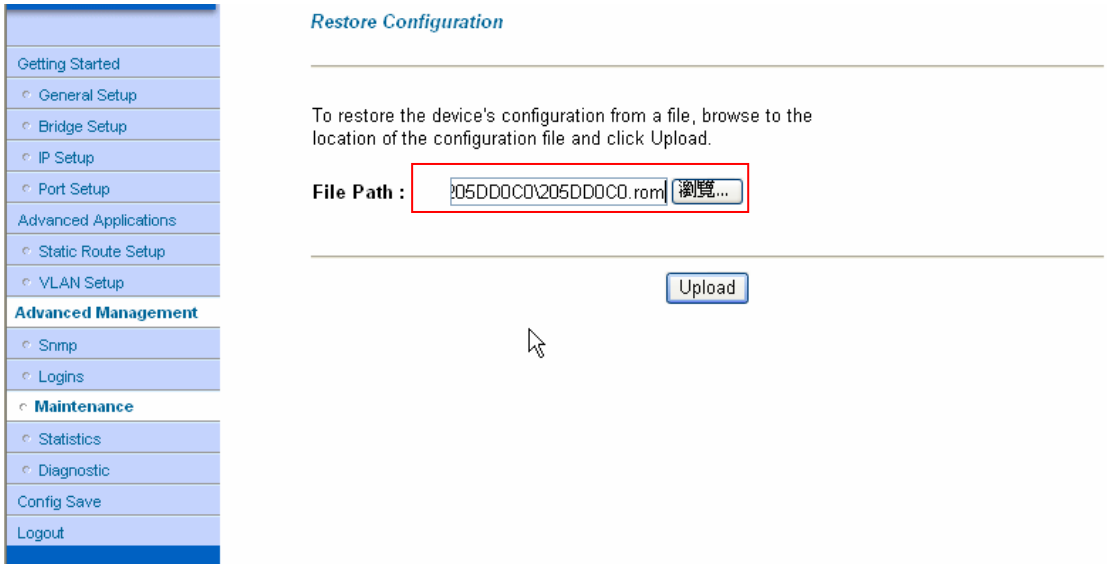
Upload the default file to IES1000 by ftp, web. Or upload the bin file by BOOTP/TFTP.
ftp:
Please ftp into the DSLAM. Replace the "init" with the default rom file by put command.



WEB:
Please open Maintenance page. Click "Restore Configuration" link.



Press Browse button to select the default rom file. Then press “Upload” button.



b) IES2000/3000

Upload default rom file to IES2000/3000 by ftp, web or console

Console:

When the system reboots, press any key within 3 seconds to enter debug mode.

```
Bootbase Version: V1.02(MSC1000) | 09/26/2002 13:15:56
RAM: Size = 32768 Kbytes
FLASH: Intel 32M

ZyNOS Version: V3.50(DS.6) | 04/21/2004 12:35:23
"Press any key to enter debug mode within 3 seconds."
.....
Enter Debug Mode

MSC 1000>
```

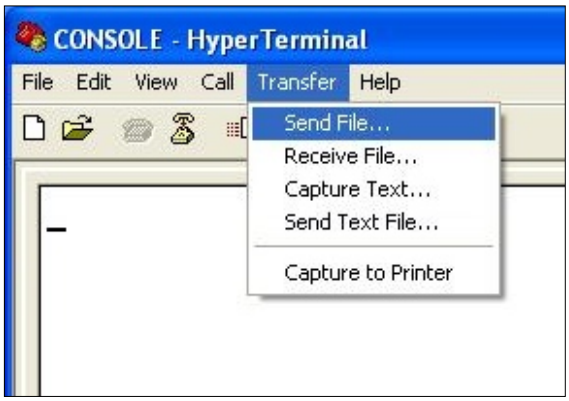
Suggest changing it to 115,200 temporarily to speed up speed by "atba5" command.

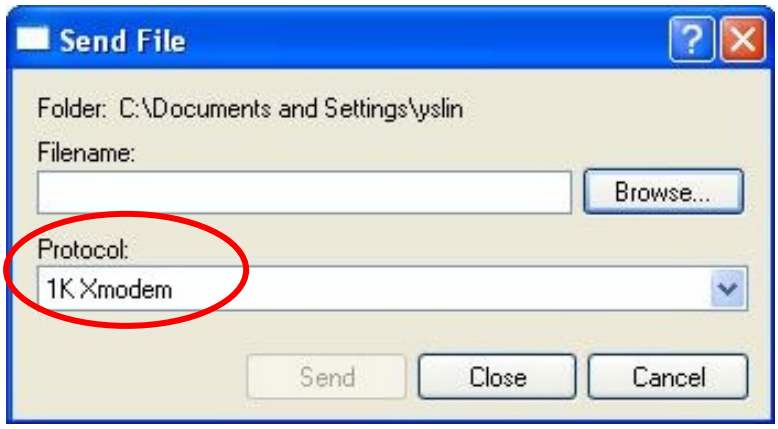
```
MSC 1000> atba5
Now, console speed will be changed to 115200 bps
```

Take "atlc" command to restore the default configuration file.

```
MSC 1000> atlc
Starting XMODEM upload (CRC mode)....
CCCC    ← Send file to MSC via 1K-Xmodem when see this message.
```

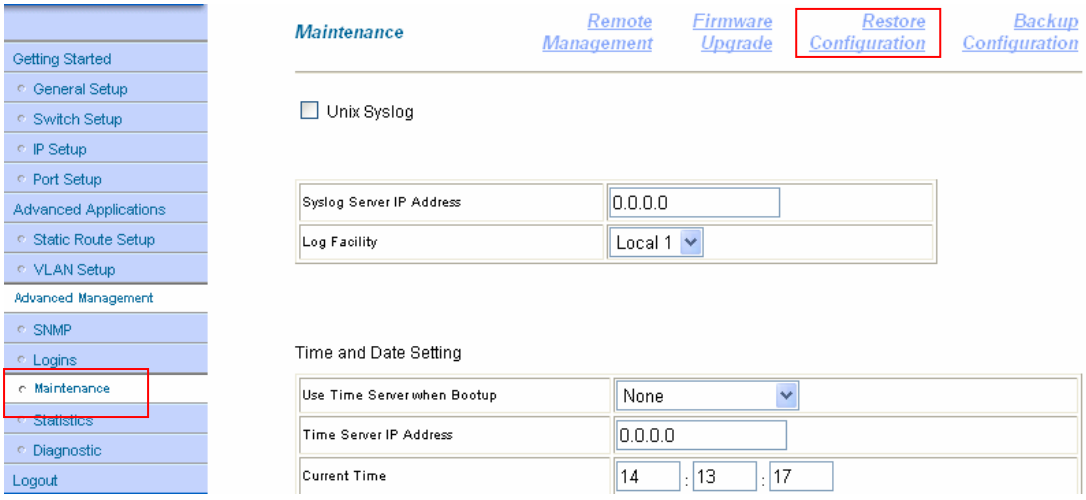
When you see "cccc…", please send the default rom file to MSC via 1k-Xmodem or Xmodem. See following two figures.



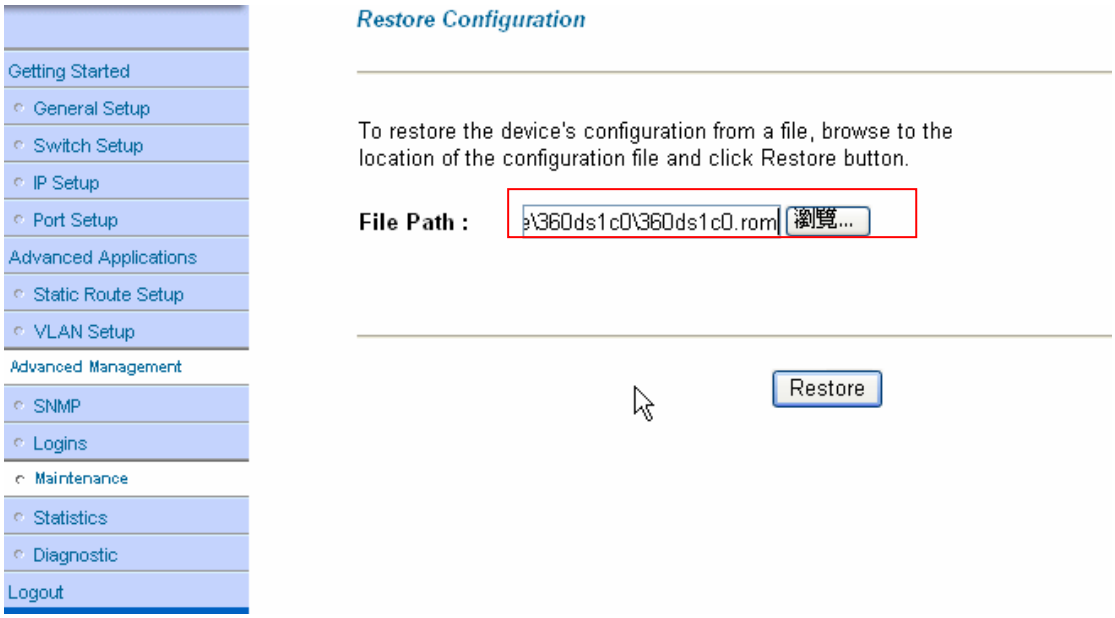


WEB:

Please open Maintenance page. Click “Restore Configuration” link.

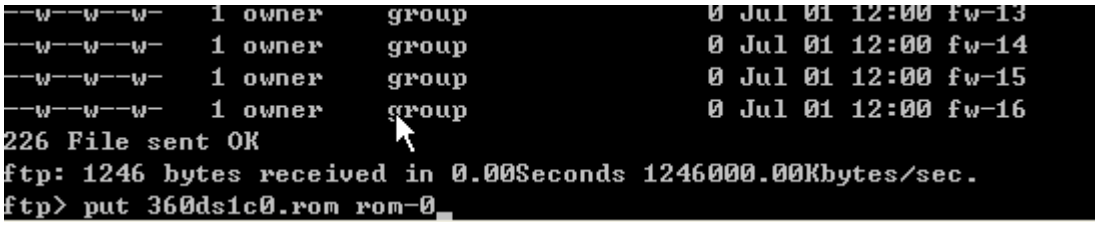


Press Browse button to select the default rom file. Then press the “Restore” button.



ftp:

Please ftp into the DSLAM. Replace the rom-0 with the default rom file by put command.

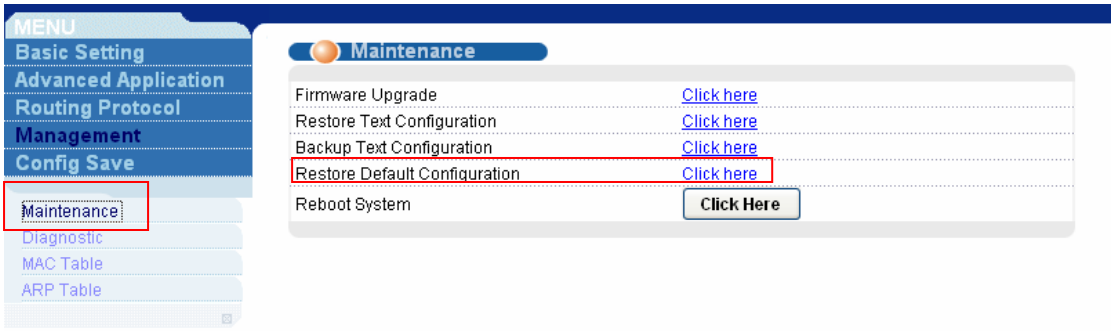


c) IES1248

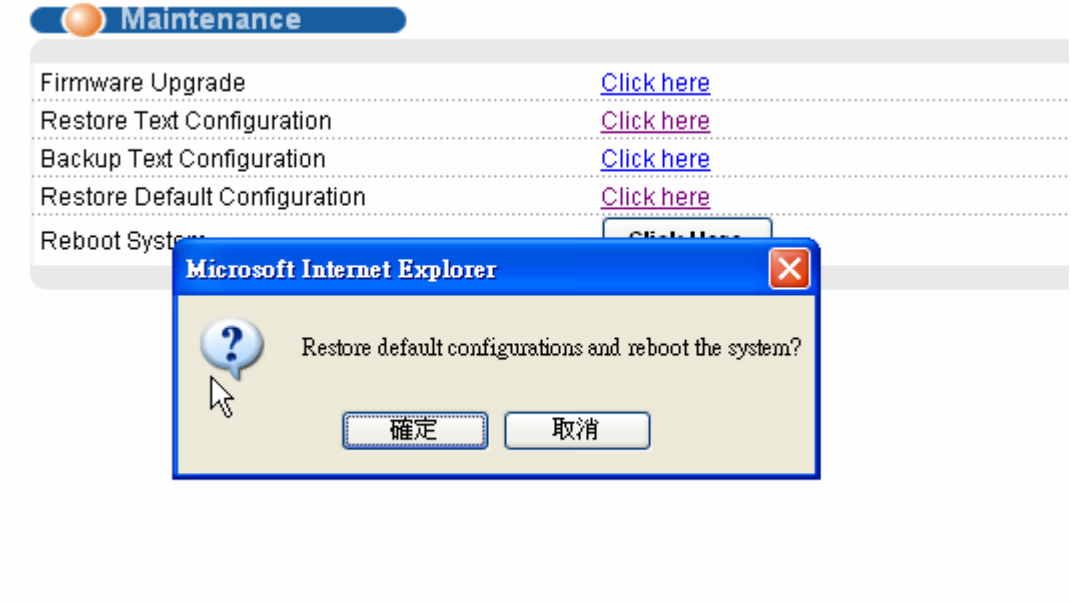
You can set the factory default by CLI command or WEB

WEB:

Please open Maintenance Page. Click the “Restore Default Configuration” link.



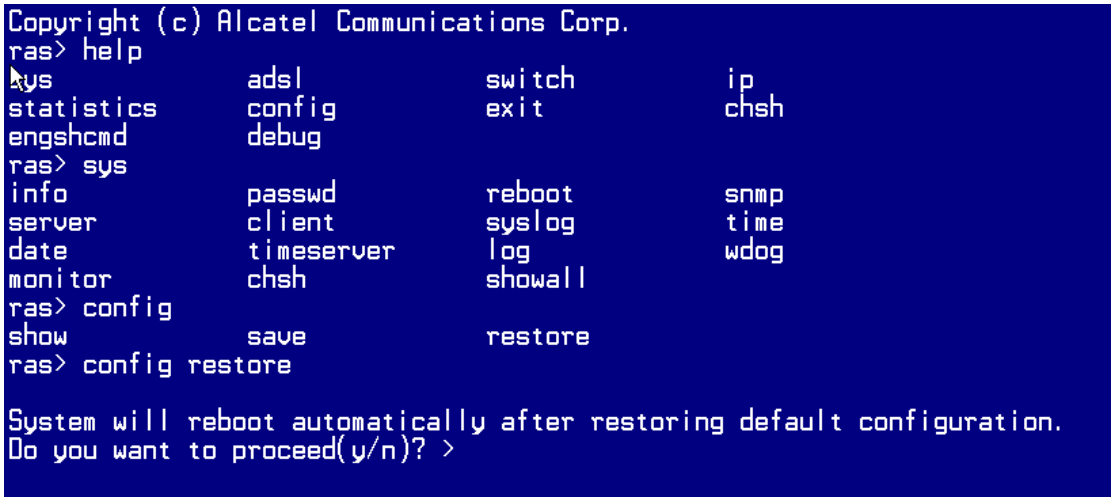
It will pop up a dialog to ask for your confirmation. Please click “Ok” button.



Console/telnet:

You can enter the CLI command mode by console or telnet. Type “config restore” to restore the default settings. Then it will ask for your confirmation. Type “Y” to start

restoring.



xDSL link fail?

1. Check if the DSL port is enabled.
2. Check if the cable is plugged well.
3. For ADSL, check the ADSL modem and line card are in the same mode (Annex A or Annex B).
4. For G.SHDSL, check the modem and line card use the same PSD(Annex A or Annex B).
5. For G.SHDSL, check if the modem is in remote mode.
6. Check if the distance is too long. Actually, we don't suggest the distance between CO and CPE is more than 4Km. Of course, it depends on your real line quality. To verify this, you can replace the original cable with a shorter one.
7. Set the smaller value in MIN rate to check if the MIN rate is too high.
8. Change the Cable.
9. Change the CPE.
10. Change the DSL port.
11. Change the line card.

If above procedures can't resolve the link fail issue, please call RMA.

Which new version I should upgrade?

Please link to http://www.zyxel.com/support/fwlib.php web site. Select the Product Category and Model Name of your device to search the latest firmware. Or you can select the Keyword to search that.

I forgot the Password, how do I recover it?

a.) IES-1000

Please use the BOOTP/TFTP and bin file to recover the configuration to factory default. Please refer to IES-1000's user manual to see the recovery procedure within Chapter 36.2 'BOOTP/TFTP Firmware Recovery of the Network'. All of your former configurations will recover to factory default. The default password is 1234.

b.) IES-2000/3000/1248

The only solution is to reset the password to default '1234' by resetting the whole IES-2000/3000/1248 configurations. To reset the settings you need to upload our default configuration file (*.rom). Please read through the following steps to do it.

1. Connect your IES-2000/3000/1248 console port to PC's serial port.
2. Start a Terminal program with 9600bps, N/8/1 settings.
3. Power on the router you should see the power up message on the Terminal screen.
4. Enter 'Debug Mode' during the device power on.
5. Type 'atsh' to check the current firmware version.
6. Download the above firmware *.zip from our FTP site or ask it from the local distributor if it is not on our Web/FTP.
7. Extract the *.rom file in the zip to your hard disk.
8. Type 'atlc' command in debug mode to start to upload the *.rom file.
9. To send file, please select the file transfer function in terminal program to start it.
10. Use X-Modem as protocol to send file.
11. Enter 'atgo' to start up the IES-2000/3000/1248.

I can not access the DSLAM via console port. What should I do?

1. Double check if the baud rate is correct, by default, the baud rate on ZyXEL IP DSLAM is 9600 N/8/1.
2. Check if the Console cable is RS-232 standard using DB9 connectors, but not

null-modem cable.
3. Check if the Console is damaged; if possible, try to change another one to give a try.
4. Try to use the other Terminal software tool to see if it's a Terminal software issue.

There is no traffic could be transmitted through the DSLAM, what should I do?

1. Check if the ADSL physical link is UP.
2. Check if the port on DSLAM have been enabled.
3. Check the VPI/VCI and Encapsulation are correct.
4. Use OAM loopback test to check the ATM layer is ok.
5. Check the Filter table's settings(MAC filter/Packet filter)
6. Customer's IP address settings are correct.
7. Check if the Port Isolation mechanism has been enabled on the DSALM.
8. Check if there is any limitation on port MAC counter of the DSLAM.
9. Check the VLAN setting including PVID, VLAN group and Egress settings.

Alarm Led is always on, what should I do?

1. Please check the HW monitor to see what happened.
2. For IES-3000, you need dual power supply for the device.