IES-6000

Support Notes

Oct 2006

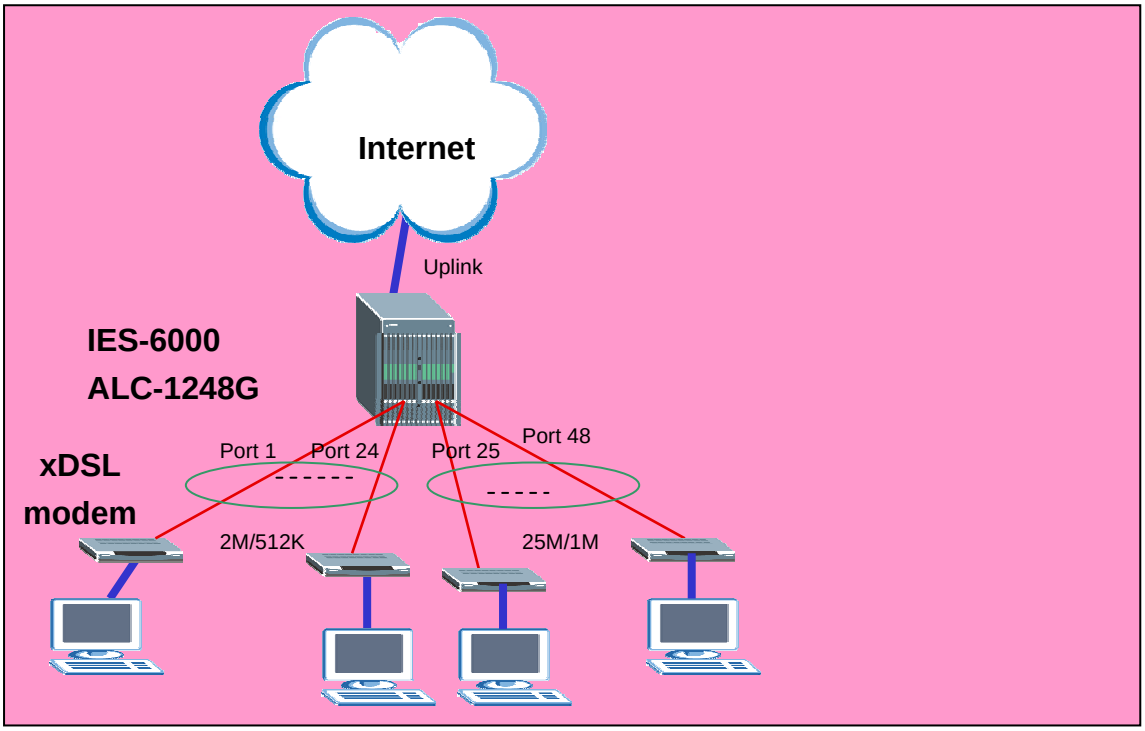
ZyXEL
Unleash Networking Power

INDEX

Application Notes

Providing Different DSL Port Speeds to different subscribers

An ISP might need to set different line speed for each DSL port. Our IES-6000 provides an easy way to do it. It is possible to create profiles that will be setting different parameters for different users and their requirements.
In this application example, we will setup two profiles. One is for low speed requirement with upstream/downstream data rate of 2M/512Kbps and the other is for high speed requirement with upstream/downstream data rate of 25M/1Mbps. We suppose there are general subscribers with a low speed profile on ports 1 through 24 and some enterprise users with high speed profile on ports 25 through 48.



How to apply the profile to the ports

In this application, we need to configure IES-6000 and ADSL CPE. We use ZyXEL Prestige 660R-61 CPE here.

1. IES-6000 Settings

1.1 Profiles settings

Set up Low Speed Profile. Give this profile a name like Profile_LowSpeed and set 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.

CI command:

a) High Speed (1M/24M) profile setup:
MSC1024G> profile adsl set 1_24M 1024 24576 minrate 64 64 delay 20 20 usmgn 310 0 60 dsmgn 310 0 60 usra startup 90 30 dsra startup 90 30

b) Low Speed (512k/2M) profile setup:
MSC1024G> profile adsl set 512_2M 512 2048 minrate 64 64 delay 20 20 usmgn 310 0 60 dsmgn 310 0 60 usra fixed 90 30 dsra startup 90 30

Save the current configuration:
MSC1024G> config save

1.2 Profile Assignment

Assign Profile_LowSpeed to the port 1. Select the Profile_LowSpeed profile. After finishing configuration of port 1, copy the settings of the port 1 to the ports from 2 to 24..

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

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

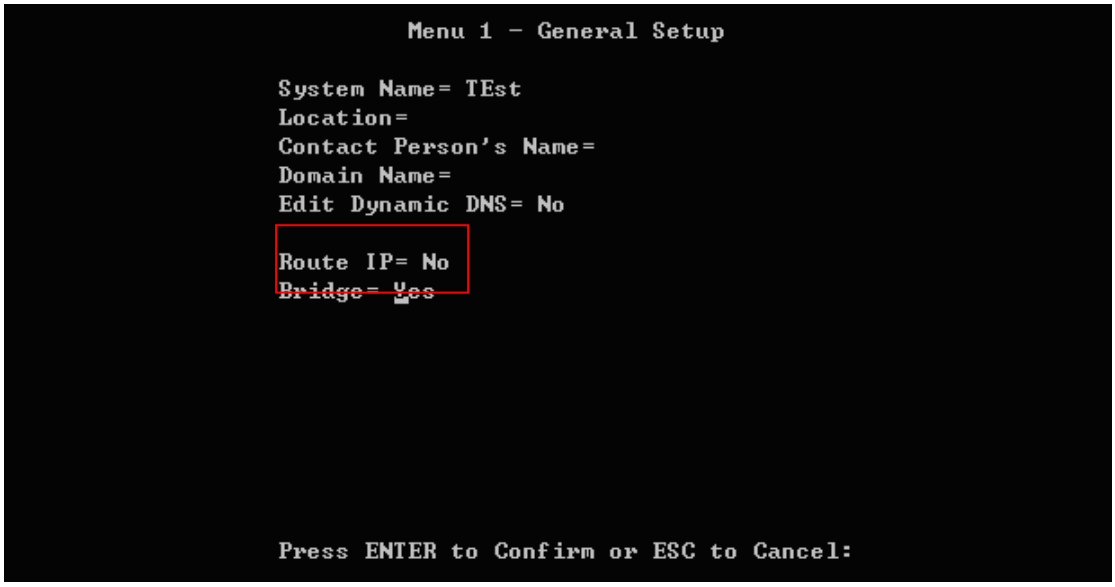
CI command:
MSC1024G> port adsl set 7-1~24 512_2M auto
MSC1024G> port adsl set 7-25~48 1_24M auto
MSC1024G> port enable 7-1~48
MSC1024G> port pvc set 7-1~48-0/33 DEFVAL llc 1 0
MSC1024G> config save

2. Prestige 660R-61 Settings

We set Prestige 660R-61 in bridge mode. The default VPI/VCI of IES-6000 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.

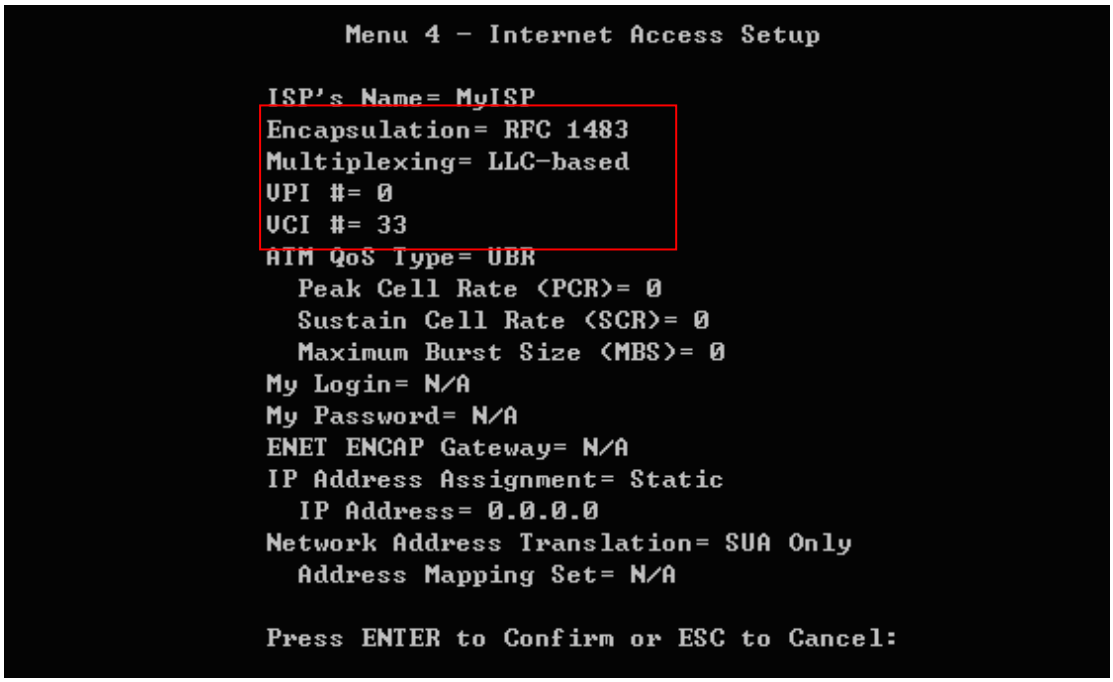
2.1 Menu1: General Setup

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 on IES-6000. LLC-based is the default mode of IES-6000. Additionally, we must check if the VPI/VCI is the same as IES-6000. As was mentioned above, the default VPI/VCI of IES-6000 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 in the menu 4. Setting “Edit ATM Options=Yes” will enter Menu 11.6.

```
                    Menu 11.1 - Remote Node Profile

 Rem Node Name= MyISP                 Route= None
 Active= Yes                          Bridge= Yes

 Encapsulation= RFC 1483              Edit IP/Bridge= No
 Multiplexing= LLC-based              Edit ATM Options= Yes
 Service Name= N/A                    Edit Advance Options= N/A
 Incoming:                            Telco Option:
   Rem Login= N/A                       Allocated Budget(min)= N/A
   Rem Password= N/A                    Period(hr)= N/A
 Outgoing:                              Schedule Sets= N/A
   My Login= N/A                        Nailed-Up Connection= N/A
   My Password= N/A                   Session Options:
   Authen= N/A                          Edit Filter Sets= No
                                        Idle Timeout(sec)= N/A


                Press ENTER to Confirm or ESC to Cancel:
```

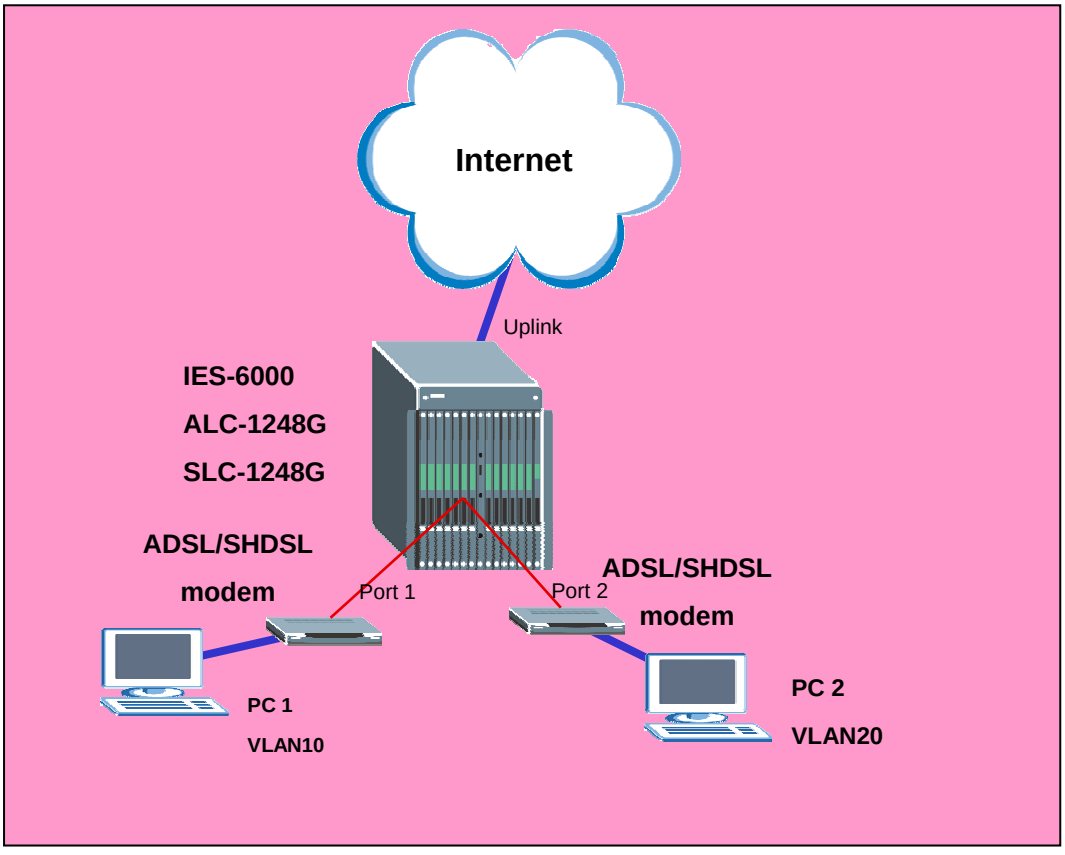
2.4 Menu11.6: Remote Node ATM Layer Options

Check whether the values above are the same as on IES-6000.

```
              Menu 11.6 - Remote Node ATM Layer Options
          VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

                VPI #= 0
                VCI #= 33
                ATM QoS Type= UBR
                Peak Cell Rate (PCR)= 0
                Sustain Cell Rate (SCR)= 0
                Maximum Burst Size (MBS)= 0




              Enter here to CONFIRM or ESC to CANCEL:
```

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 VLAN environment in this application. The following figure shows the VLAN example. Two PCs connect to the ports 1 and 2 of the line card and belong to different VLANs. One is VLAN 10 and the other is VLAN 20. Therefore, they can't communicate with each other. However, both PC 1 and PC 2 can connect to the Internet.



How to set up a VLAN environment

In this application, we need to configure IES-6000 and ADSL CPE (or SHDSL CPE). We use ZyXEL Prestige ADSL 660R-61 (or you may use P791 for SLC-1248G) CPE

here. Because the two ports belong to the different VLANs want to connect to the Internet via Uplink port of IES-6000, we need to set up an extra VLAN and let the two ports be members of this VLAN.

1. IES-6000 Settings

1.1 VLAN settings

Add VLAN10. Assign Port 1, ENET5 and ENET6 to be members of VLAN10:

CI command:

MSC1024G> vlan set 10 enet5 fix untag
MSC1024G> vlan set 10 enet6 fix untag
MSC1024G> vlan name 10 VLAN10
MSC1024G> port pvc vlan 7-1-0/33 10 join untag

Add VLAN20. Assign Port 2, ENET5 and ENET6 to be members of VLAN20:

CI command:

MSC1024G> vlan set 20 enet5 fix untag
MSC1024G> vlan set 20 enet6 fix untag
MSC1024G> vlan name 20 VLAN20
MSC1024G> port pvc vlan 7-2-0/33 20 join untag

Add VLAN200. Assign slot 7, Port 1, Port2, ENET5 and ENET6 to be members of VLAN200:

CI command:
MSC1024G> vlan set 200 enet5 fix untag
MSC1024G> vlan set 200 enet6 fix untag
MSC1024G> vlan name 200 VLAN200
MSC1024G> port pvc vlan 7-1-0/33 200 join untag
MSC1024G> port pvc vlan 7-2-0/33 200 join untag

1.2 PVID settings

After setting up all the three VLANs, we need to set the PVID.

We assign VLAN 200(PVID) to ENET5, ENET6. Also, we assign VLAN 10 and VLAN 20 to port1 and port2 respectively:

CI command:

MSC1024G> switch port pvid enet5 200
MSC1024G> switch port pvid enet6 200
MSC1024G> port pvc set 7-1-0/33 DEFVAL llc 10 0
MSC1024G> port pvc set 7-2-0/33 DEFVAL llc 20 0

1.3 Port Isolation

If we just want to isolate the ports of IES-6000 and don't want to set any VLAN, there is another easy way to do this. Setup **Port isolation as described below.**

CI command:

MSC1024G> switch isolation enable

2. Prestige 660R-61(P791) Settings

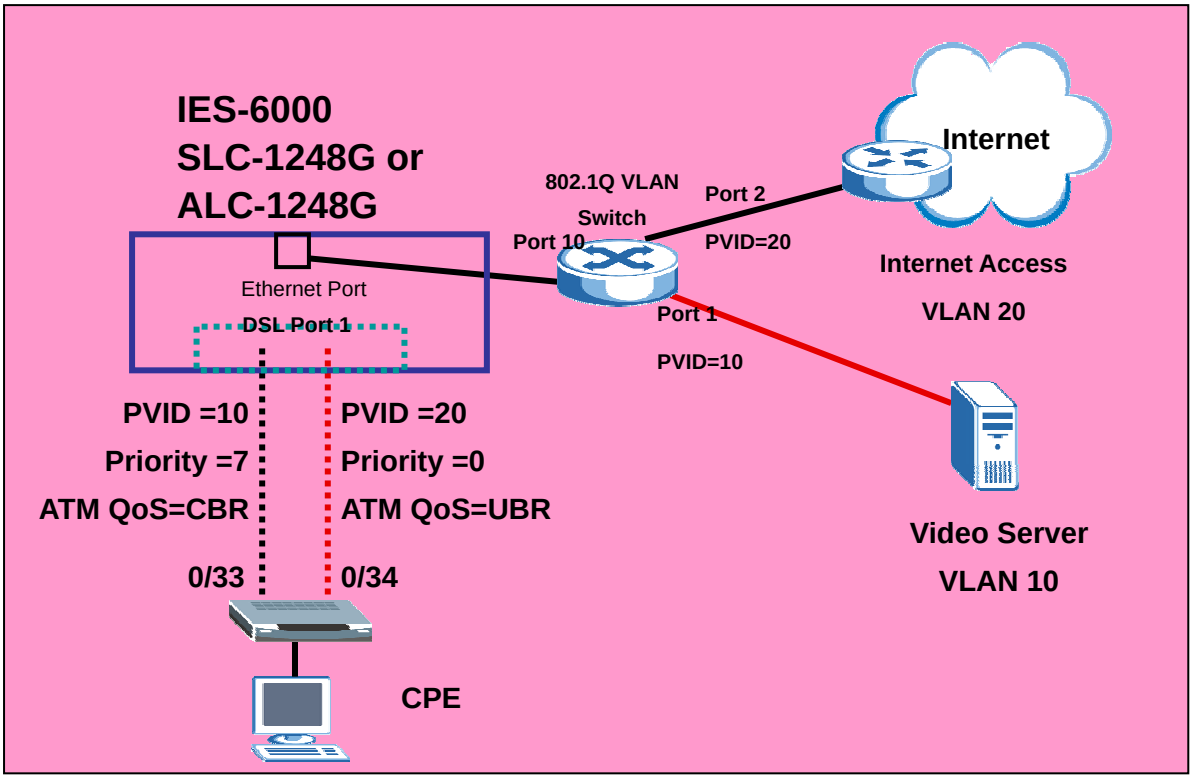
Please refer to the procedures in the previous application.

Triple play Application

The IES-6000 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 the ATM Quality of Service (QoS). The ATM QoS allows you to regulate the average rate and fluctuations of data transmission. This helps to eliminate congestion in order to allow transmission of real time data (such as audio and video).

In this application, we demonstrate how to set up multiple PVCs environment. In 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-6000, we can assign the two services with different VLANs and assign the PVCs with

different VLAN priority and ATM QoS. That will make the video traffic get higher priority than the 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-6000, VLAN-aware switch and ADSL (SHDSL) CPE. We use ZyXEL ES-2024 and Prestige 660R-61(You may use P791 for SLC-1248G) as VLAN-aware switch and xDSL CPE respectively.

1. IES-6000 Settings

1.1 VC profile setup

Add Defval_CBR VC profile for Profile Setup. Set up Encap, Class, PCR and CDVT as shown. Encap should be LLC, the same as IES-6000. Class should be CBR as it has higher priority in ATM QoS.

CI command:

MSC1024G> profile atm set Def_CBR cbr 300000 *

1.2 Multiple PVCs setup

We want VPI/VCI with 0/33 to get the higher priority. We should modify this VPI/VCI with Defval_CBR profile which we created before.

CI command:

MSC1024G> port pvc set 7-1-0/33 Def_CBR llc 10 7

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

CI command:

MSC1024G> port pvc set 7-1-0/34 DEFVAL llc 20 0

1.3 VLAN setup

We can setup VLAN by following the procedure described in VLAN application. Add VLAN10. Assign Port 1, ENET5 to be members of VLAN10 as show. We need to check the Tx Tagging on ENET5.

MSC1024G> vlan set 10 enet5 fix tag
MSC1024G> vlan name 10 VLAN10
MSC1024G> port pvc vlan 7-1-0/33 10 join untag

Add VLAN20. Assign Port 1, ENET5 to be members of VLAN20 as show. We need to check the **Tx Tagging** on ENET5.

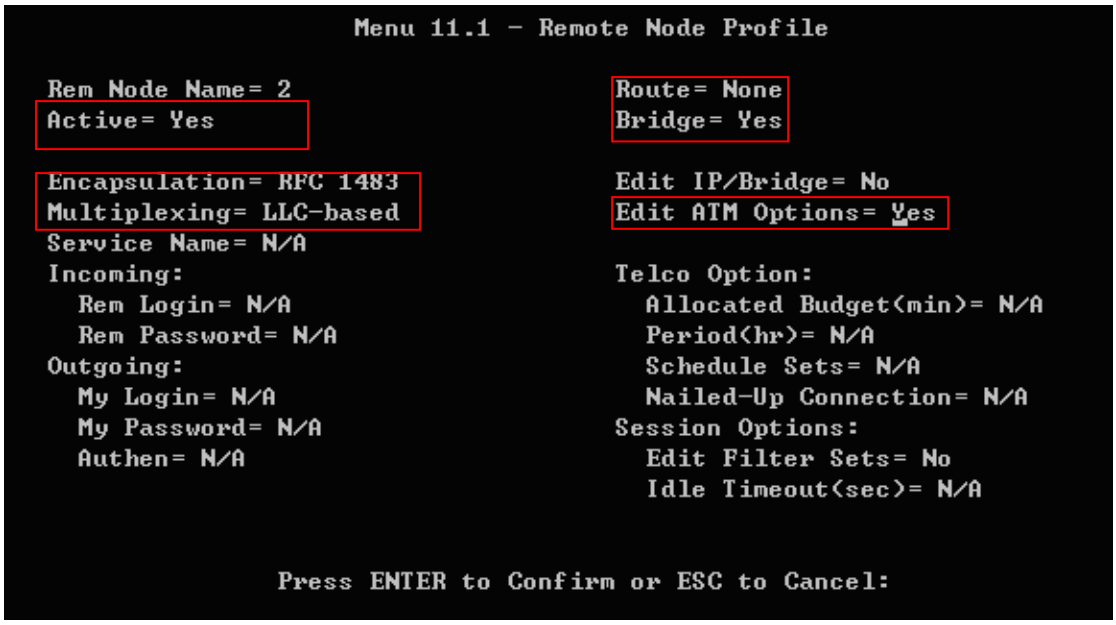
MSC1024G> vlan set 20 enet5 fix tag
MSC1024G> vlan name 20 VLAN20
MSC1024G> port pvc vlan 7-1-0/34 20 join untag

2. Prestige 660R-61(P791) 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 setup the second channel.

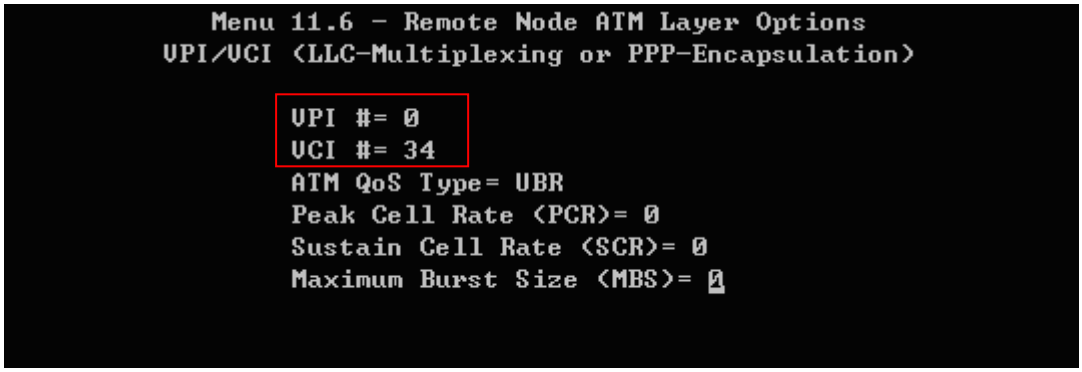
2.1 Menu11.1: Remote Node Profile

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

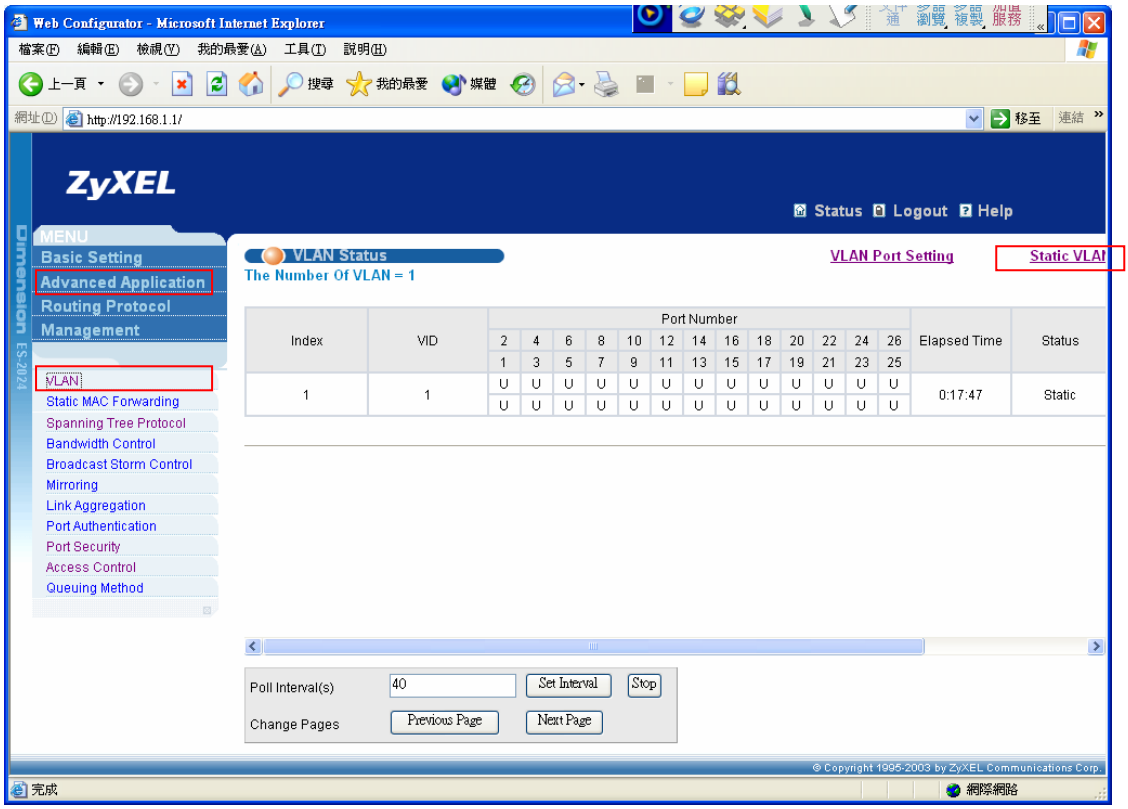
We should set up another VPI/VCI with 0/34, the same as in the IES-6000.



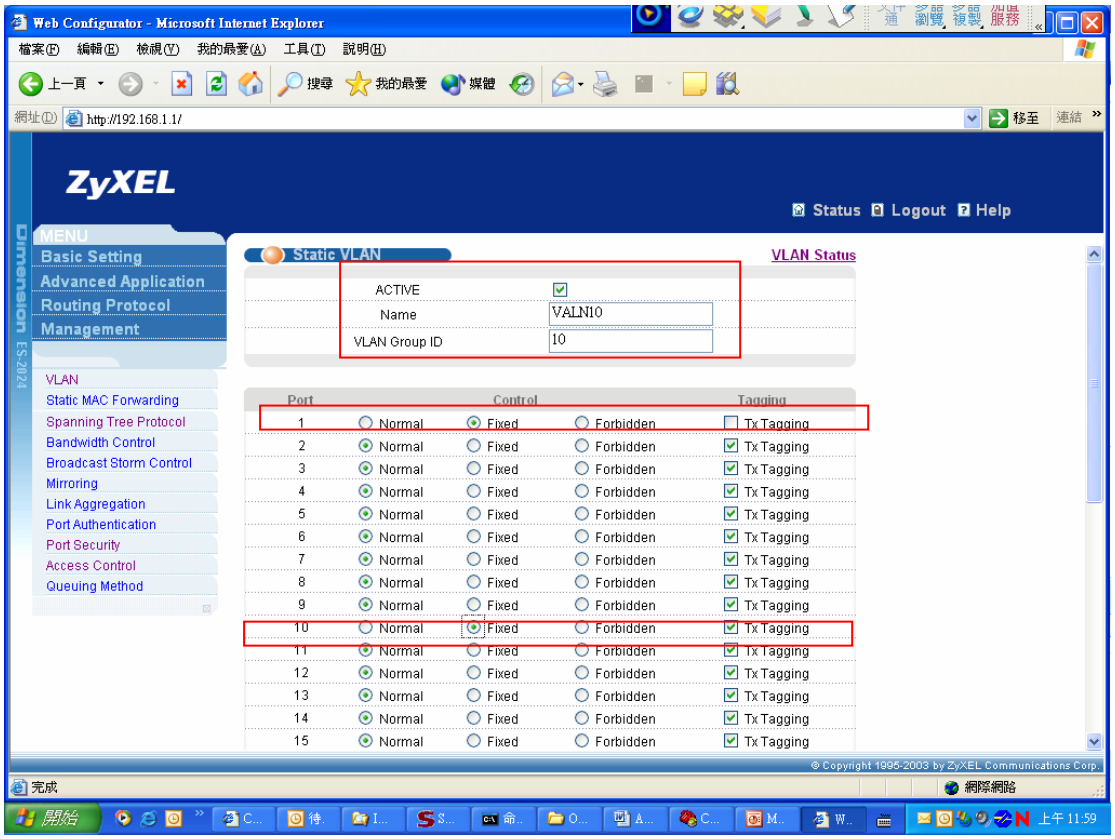
3. ES-2024 settings

3.1 VLAN

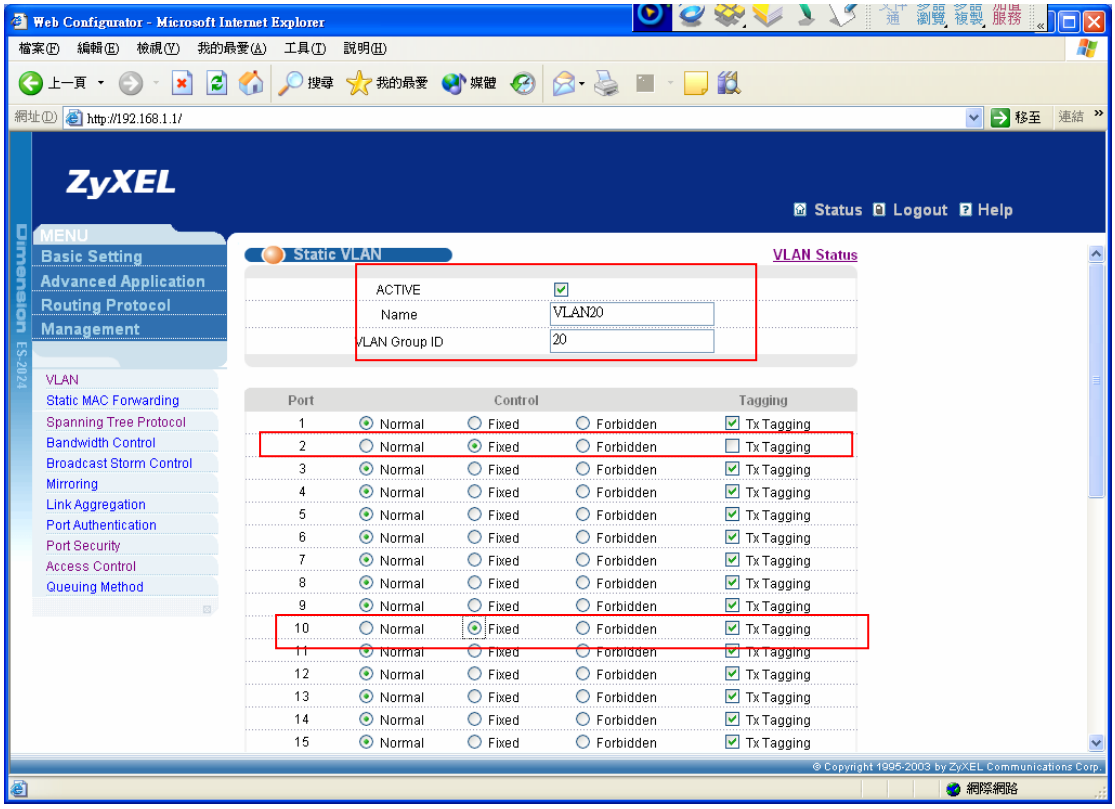
Click **Advanced Application** and **VLAN** in navigation panel to display the configuration screen shown below. Click **Static VLAN** to open the VLAN setup screen.



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

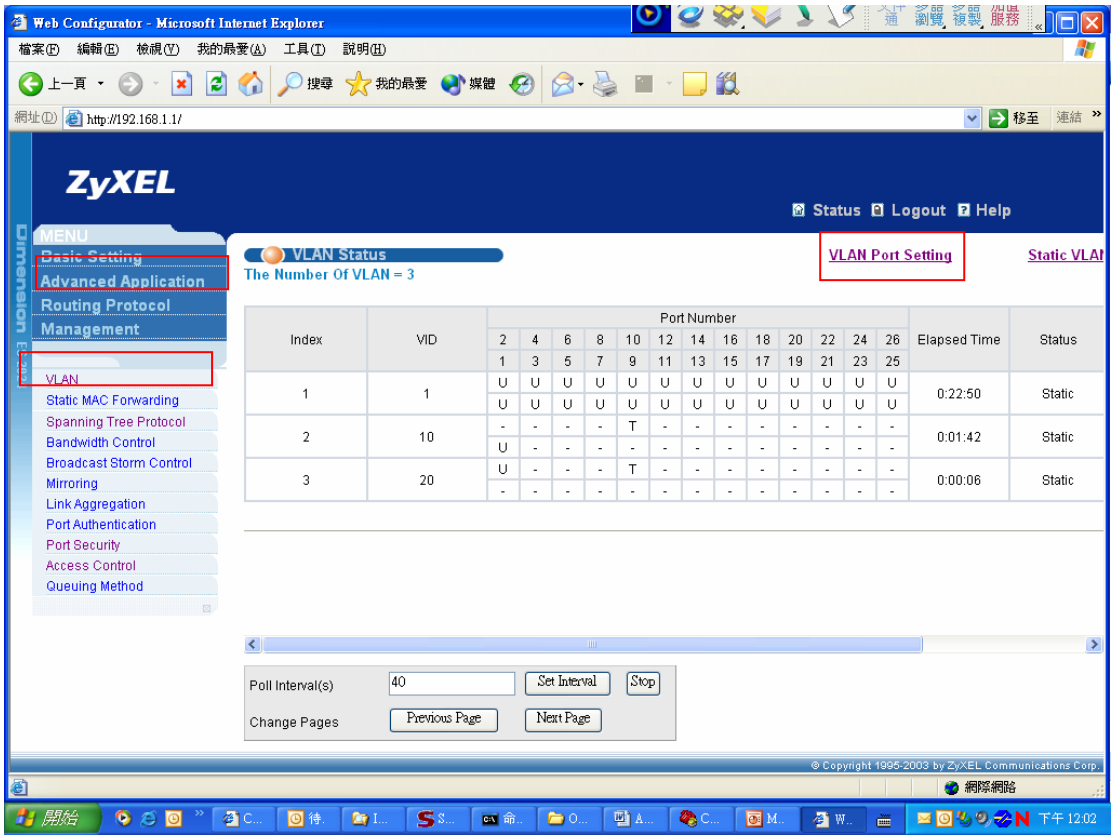


Add VLAN20. Assign Port 2, Port 10 to be members of VLAN20 as shown below. We need to check the **Tx Tagging** on Port 10.

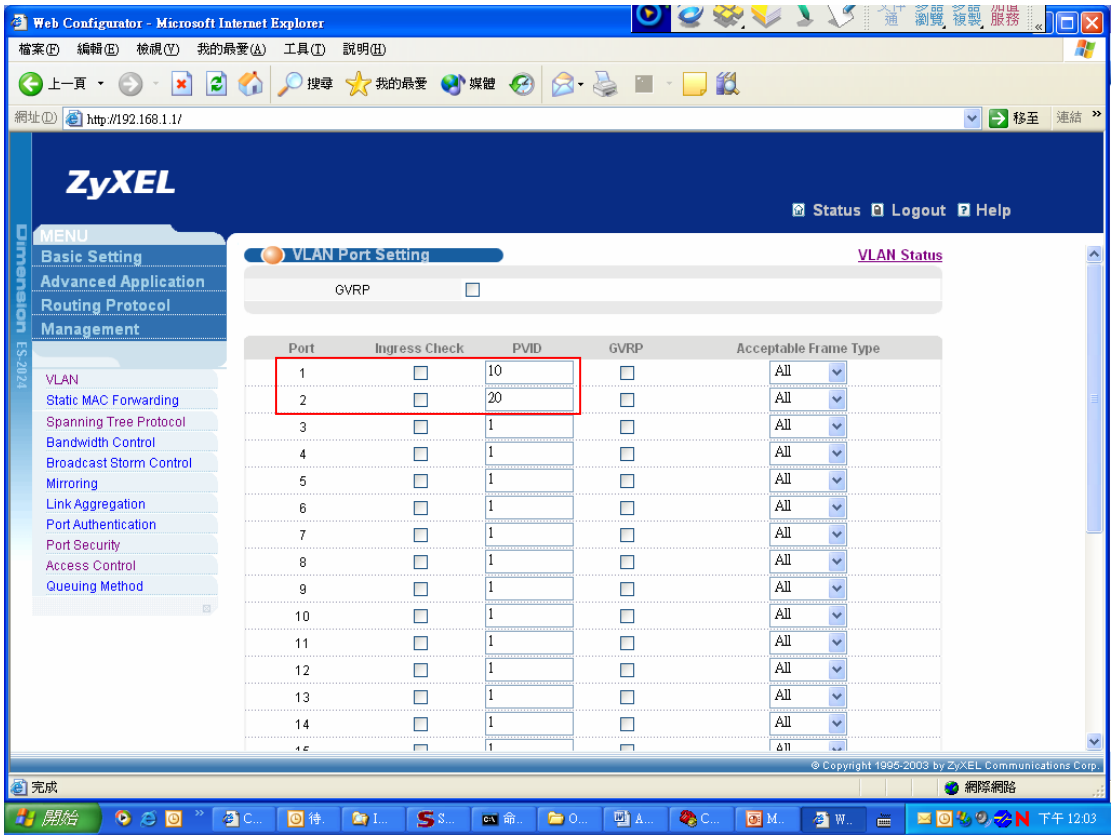


3.2 PVID setup

Click **Advanced Application** and **VLAN** in the navigation panel to display the configuration screen shown below. Click **VLAN Port Setting** to open the PVID setup screen.



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



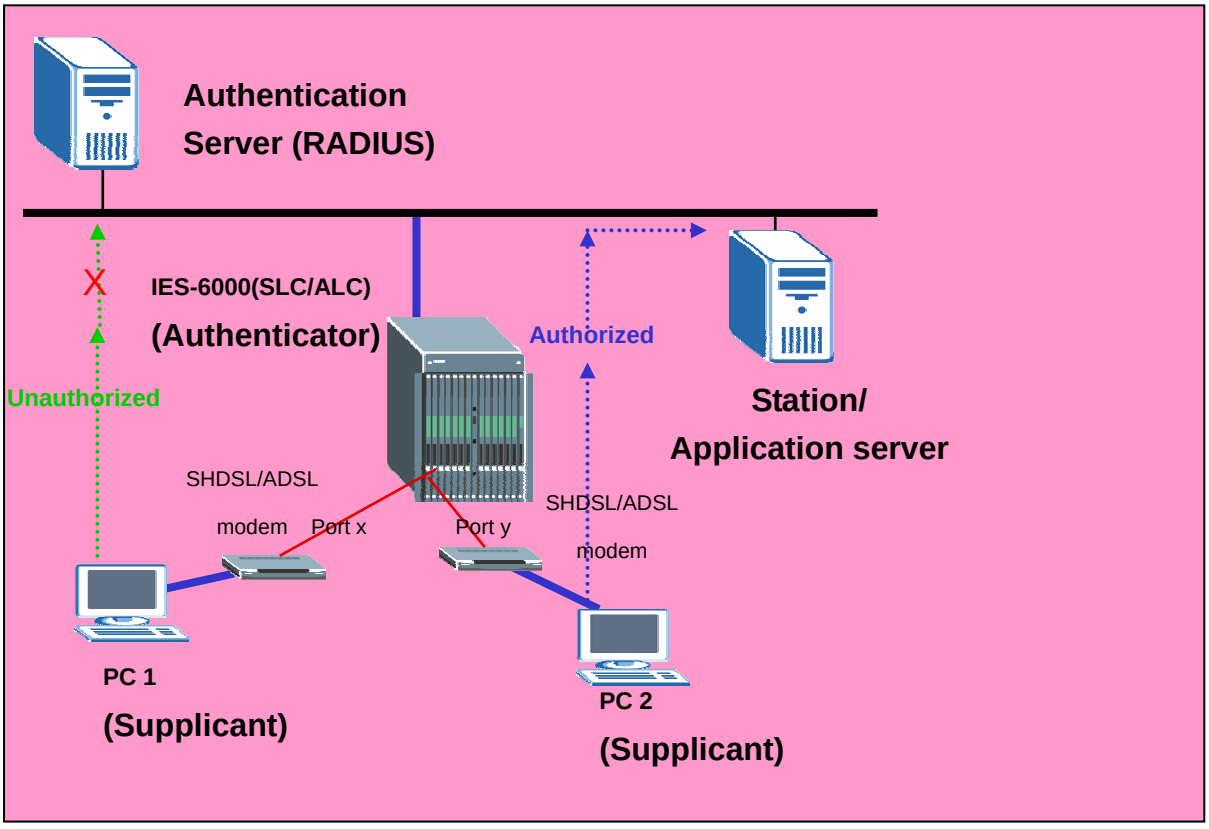
In this application, you will see that the video traffic will go via 0/33 and data traffic

will go via 0/34. The 0/33 get the higher priority so 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 the unauthorized ports (clients) from gaining access to the network. It is an extended authentication protocol that allows the 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 the 802.1x environment in this application. The following figure shows the 802.1x application example. PC1 (supplicant) and PC2 (supplicant) want to access the application server. If PC1 is not unauthorized, the traffic from PC1 to the application server will be blocked. If PC2 is an authorized client, then it can access to the application server. On the figure below you can see that IES-6000 acts as an authenticator.



How to configure the 802.1x environment

We should configure Authenticator, RADIUS and Supplicant, the three components of the 802.1x environment. The Microsoft 802.1x client and ZyXEL Vantage 50 will be used as supplication and the RADIUS server respectively. The following sections will describe the detailed procedure of setting up the environment.

1. IES-6000 (Authenticator) settings:

1.1 RADIUS settings:

Enable the 802.1x Authentication and the RADIUS server IP address, UDP port and shared Secret, which is the same as in the Radius server. Then click Apply to make the settings take effect.

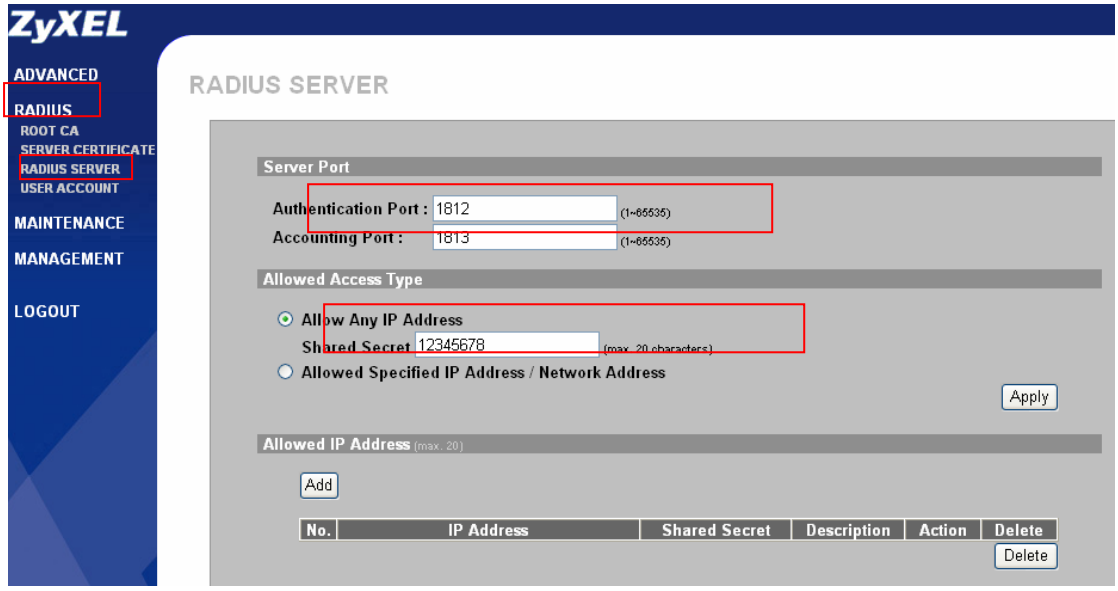
MSC1024G> acl dot1x enable
MSC1024G> acl dot1x radius ip 192.168.1.3
MSC1024G> acl dot1x radius port 1812
MSC1024G> acl dot1x radius secret 12345678
MSC1024G> config save

2. Vantage 50 (RADIUS) settings:

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

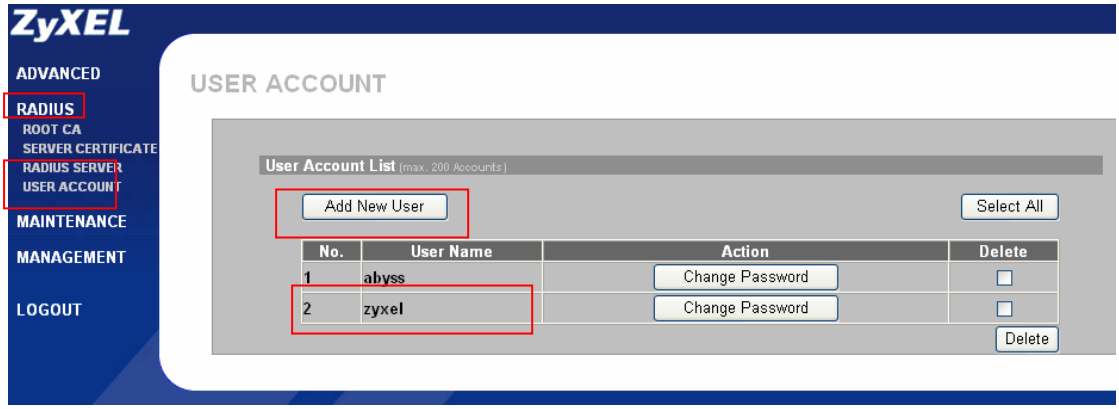
2.1 RADIUS server setup

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



2.2 Create User Account

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

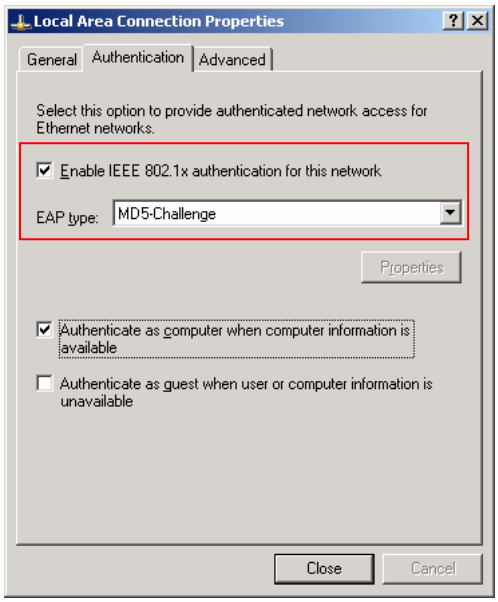


3. Windows XP (Supplicant) settings

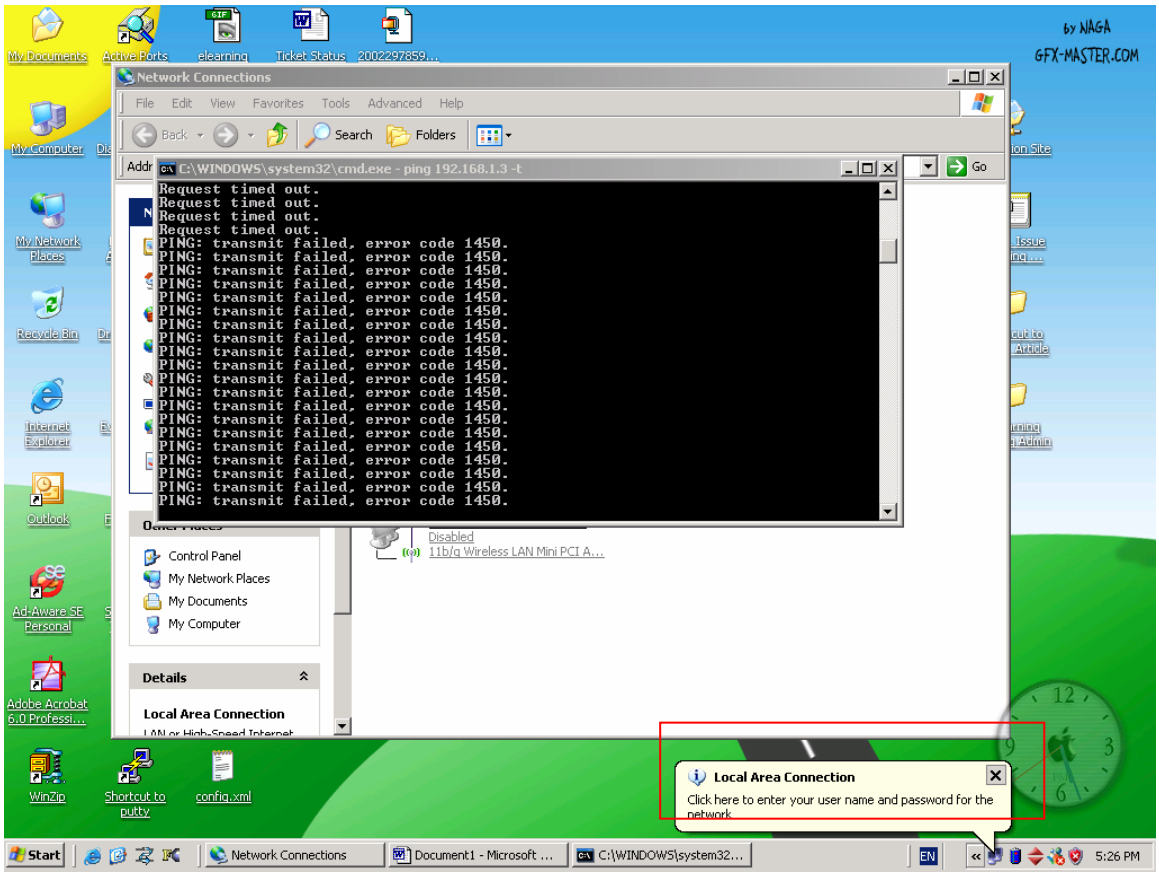
There are many supplicants we can choose: e.g. MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client. We take Microsoft 802.1x client as an example here.

3.1 802.1x/MD5-challenge setup

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

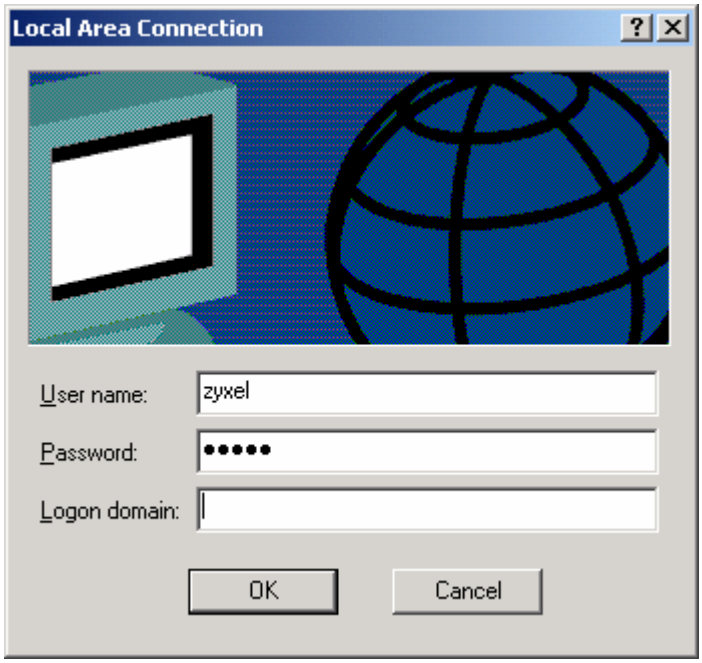


When the 802.1x starts, it will prompt you to enter the user name and the password. Please see the following figure.



After clicking the icon, a dialog for entering the user name and password will appear. Click

ok after entering the correct user name and the password that are in the database of the authentication server. The setting of the client side is finished.



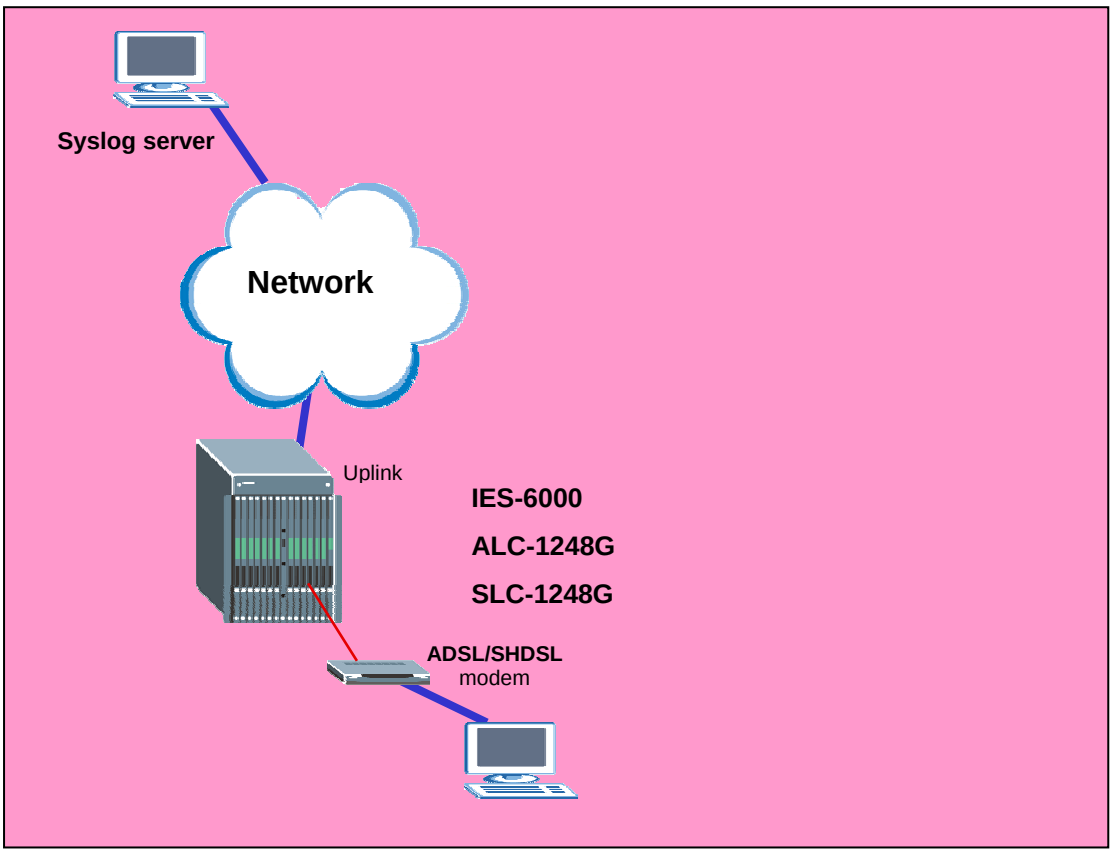
After the above procedure, we can allow the authenticated port to the access the server. If the DSL port is not authenticated, the PCs behind the port can't access the network.

4. Prestige 660R-61 Settings

Please refer to the procedures in the previous application.

Setting up the Syslog Server

ZyXEL products are able to send system log to a Syslog daemon such as Unix Syslogd and Kiwi's Syslog Daemon (http://www.kiwisyslog.com/). When DSL or Ethernet ports are linked up/down, IES-6000 sends a record to Syslog server. The Syslog server can be placed on the network, which IES-6000 can access.

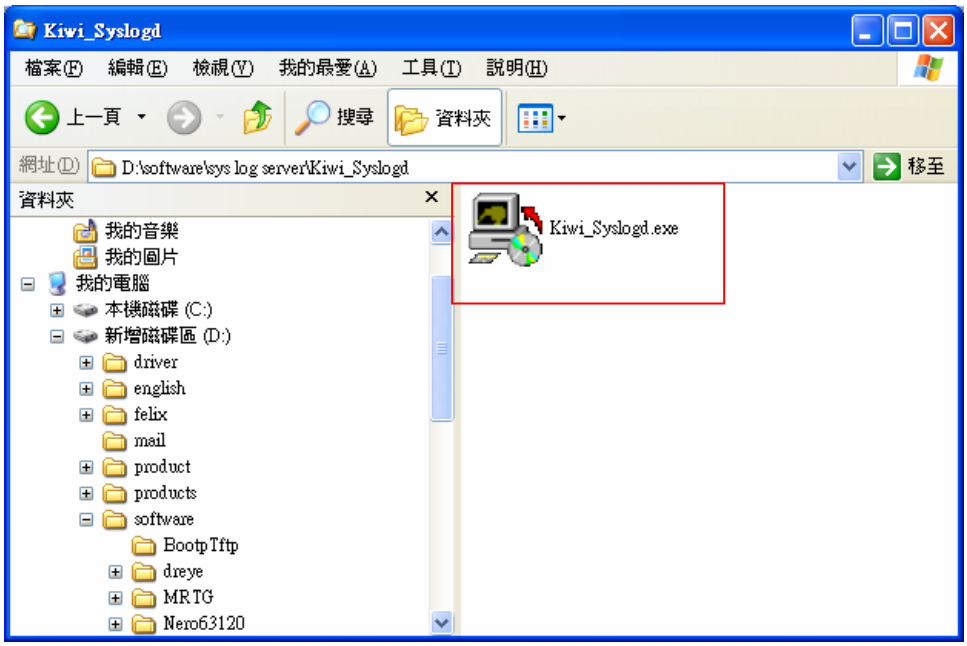


How to set up a Syslog server

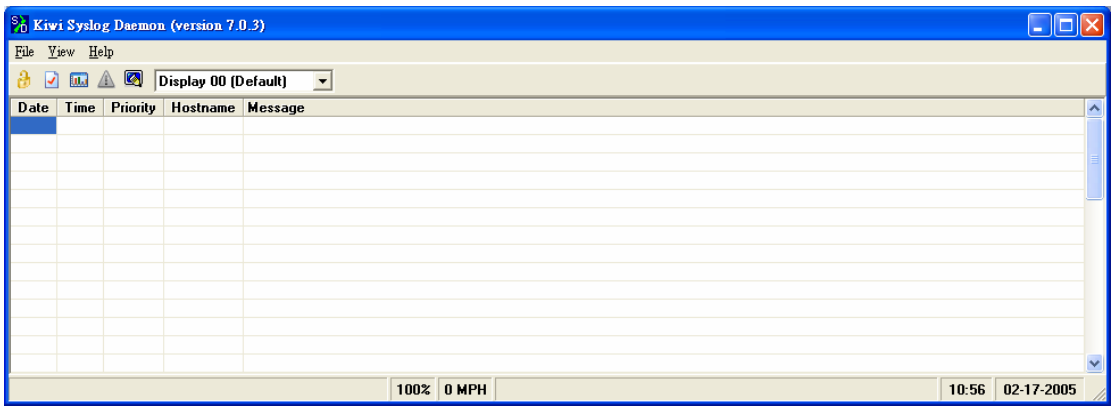
We should configure IES-6000 and Syslog server in this application. Here, we use the Kiwi's Syslog Daemon as an example. Following sections will describe the detailed procedures to set up the environment.

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. You will see following dialog. The Server's IP is 192.168.1.77.



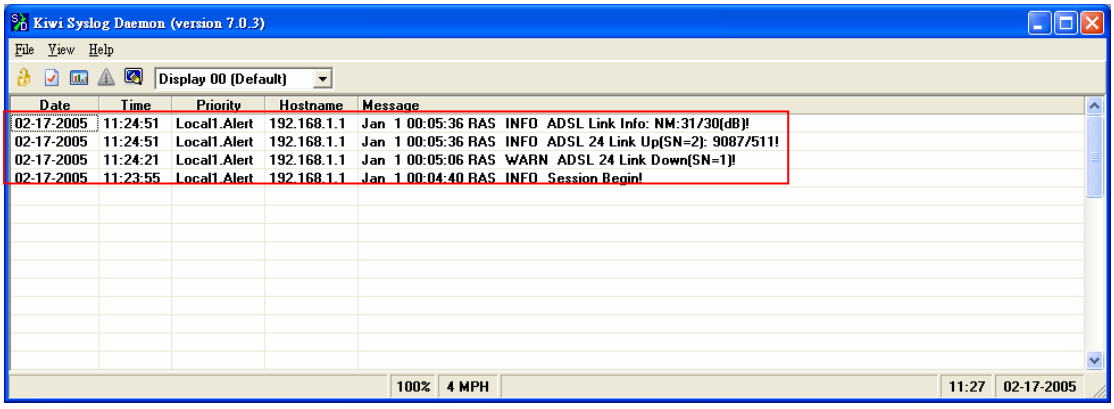
2. IES-6000 settings

Enable the Syslog server on IES-6000. Assign the UNIX Syslog Server IP, 192.168.1.77 in this case. Choose a log facility from 'Local 1' to 'Local 7'. Then save the configuration.

CI command:

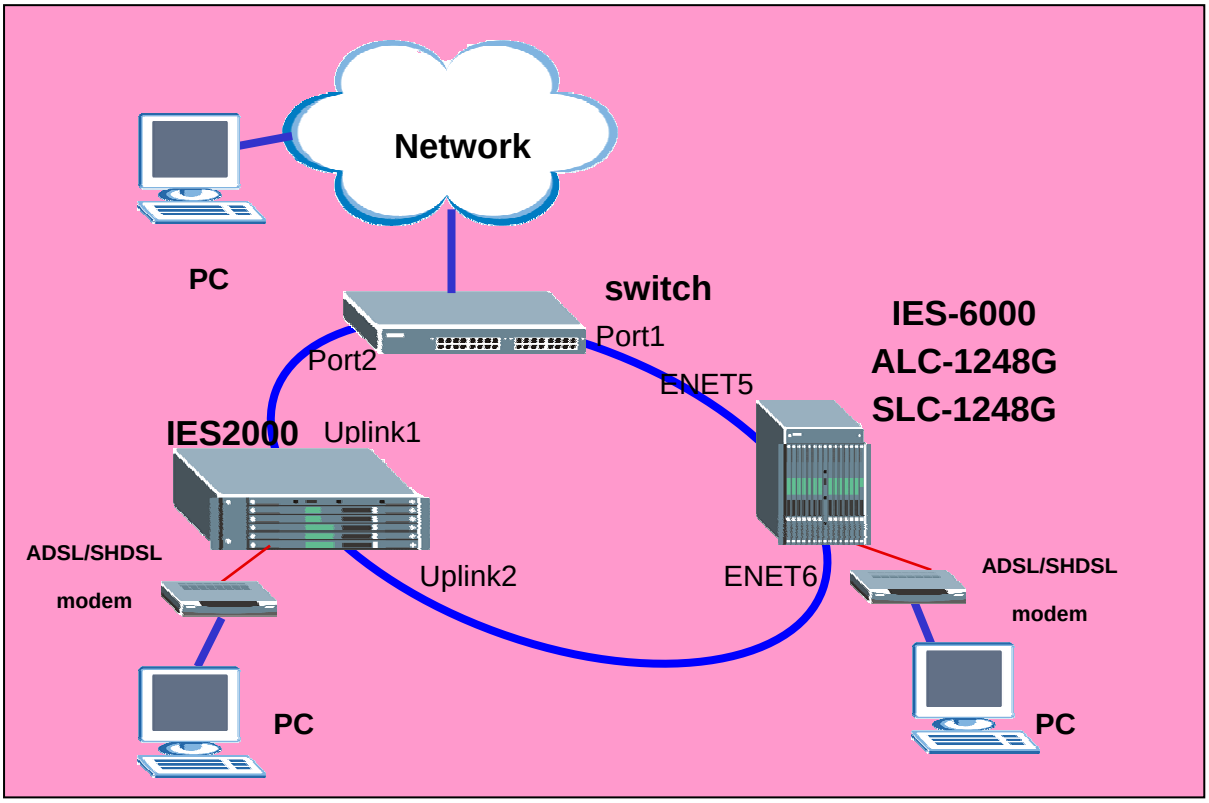
MSC1024G> sys syslog enable
MSC1024G> sys syslog server local1 192.168.1.77
MSC1024G> config save

When the DSL ports are linked up/down, IES-6000 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 devices is broken. So, in the ring topology, the network will work well if one link is broken. In the Ring Topology, you must enable RSTP/STP to prevent the loop issue.



How to Setup a Ring Environment

We will setup the Ring environment with one IES-6000, one IES-2000 and one ES-4024. A PC behind IES can connect the PC in the network even when one of the links is broken. Following sections will describe the detailed procedures to set up the environment.

1. IES-6000 settings

1.1 Enable Spanning Tree protocol on Ethernet ports

Configure Spanning Tree Protocol settings.

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

CI command:

MSC1024G> switch mstp enable

MSC1024G> switch port mstp enable enet5 0

MSC1024G> switch port mstp enable enet6 0

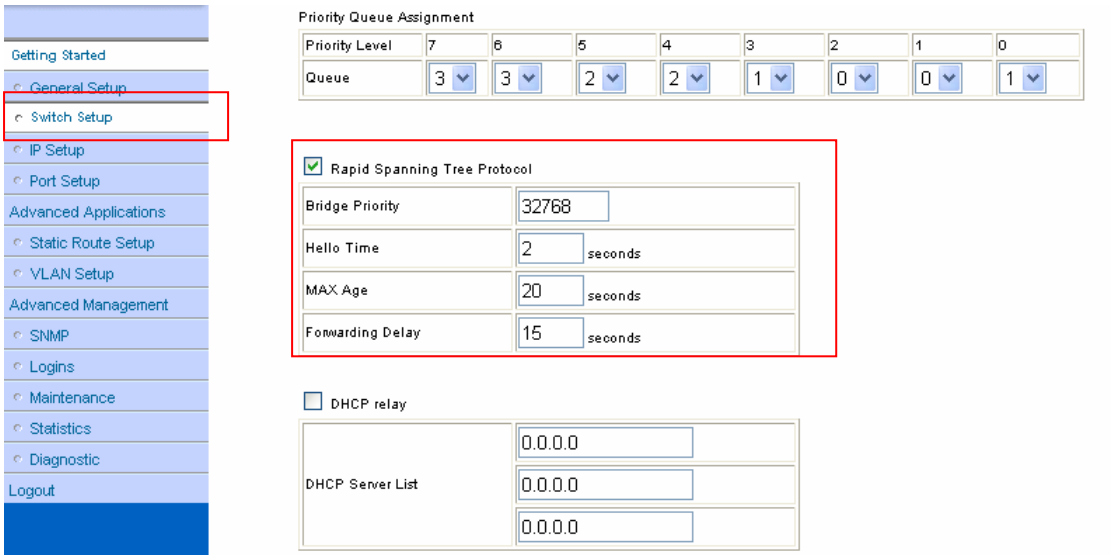
MSC1024G> switch mstp version rstp

2. Setup IES-2000

2.1 Enable Spanning Tree protocol

Click **Switch Setup** in the navigation panel to display the configuration screen shown below.

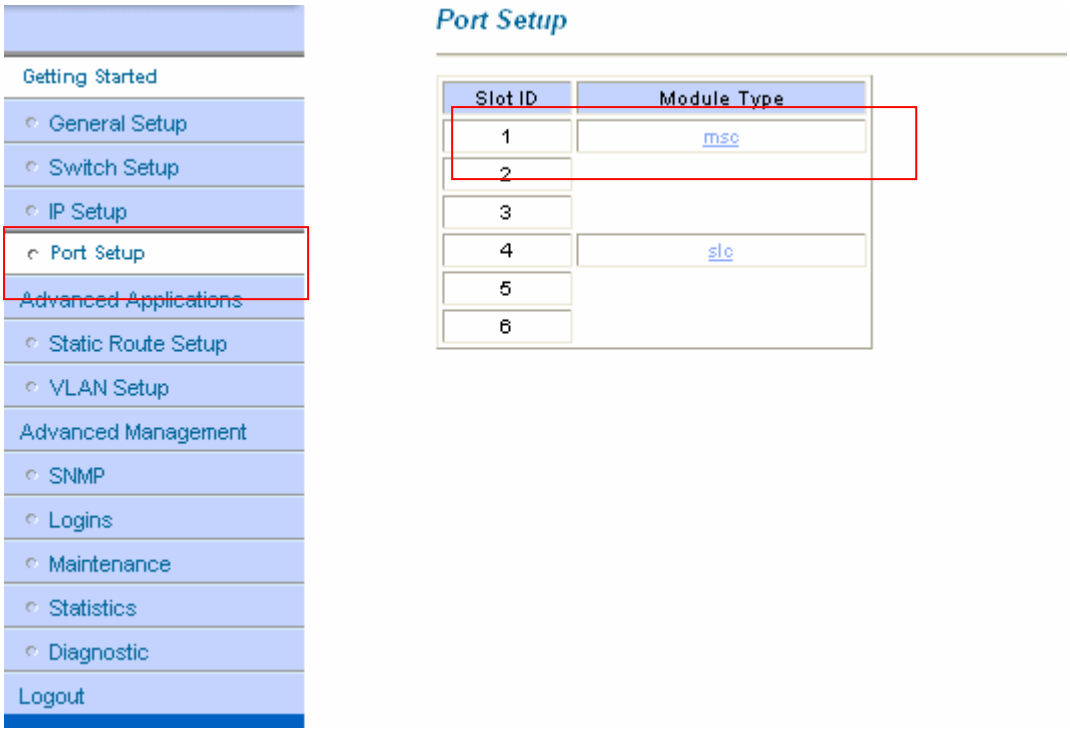
Then check **Spanning Tree Protocol** to enable it.



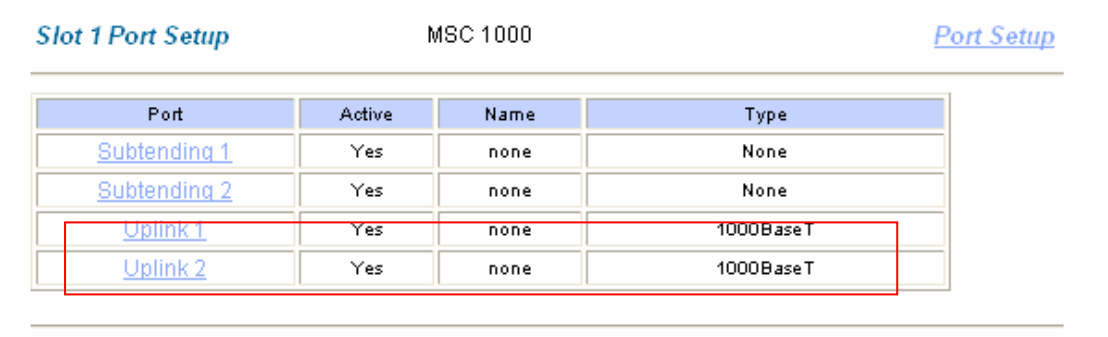
2.2 Enable Spanning Tree protocol on Ethernet ports

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

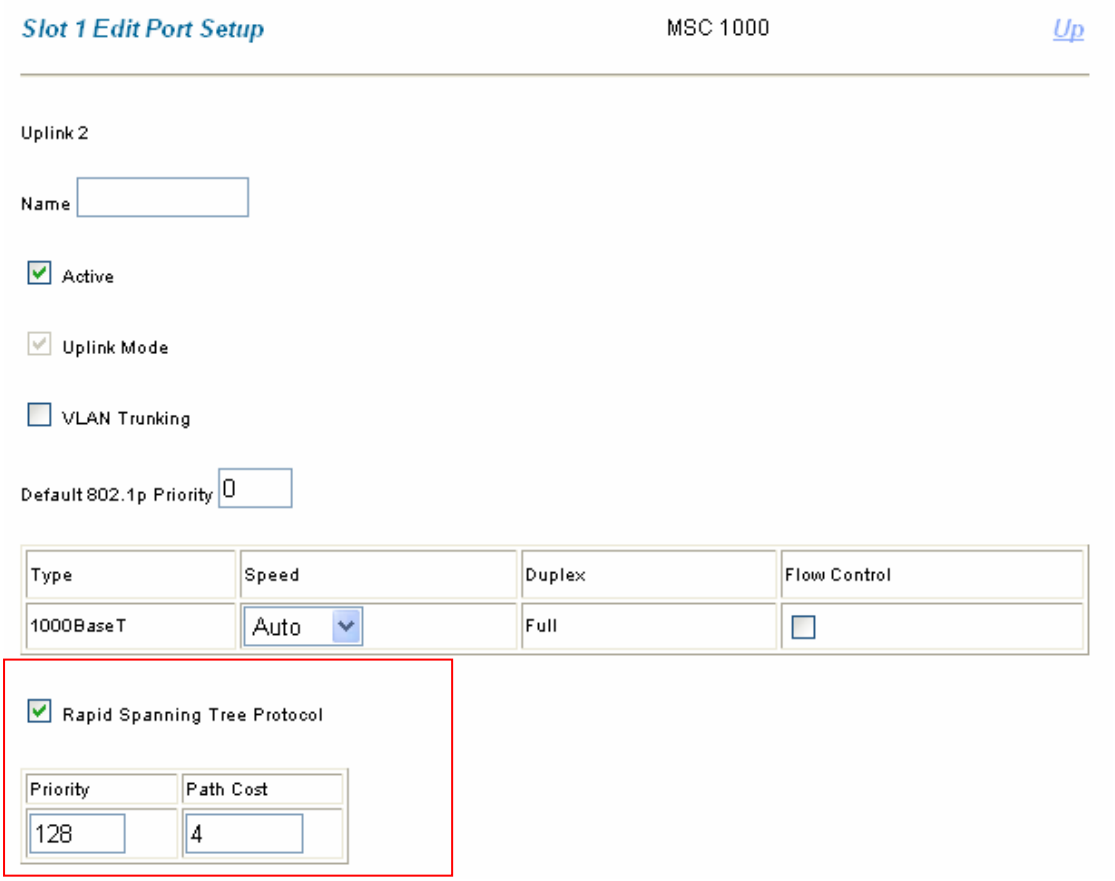
Click **msc** to display the MSC card Port setup.



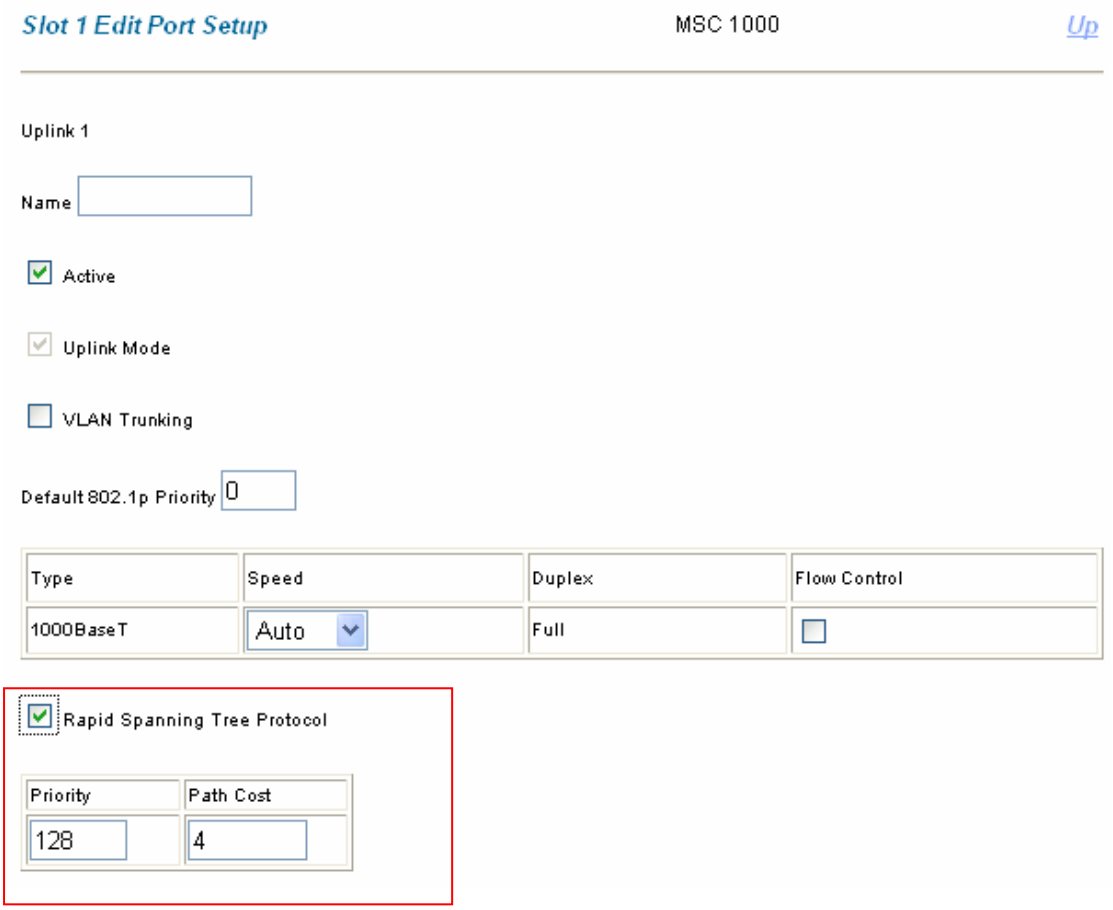
Click **Uplink2** to set up this port.



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



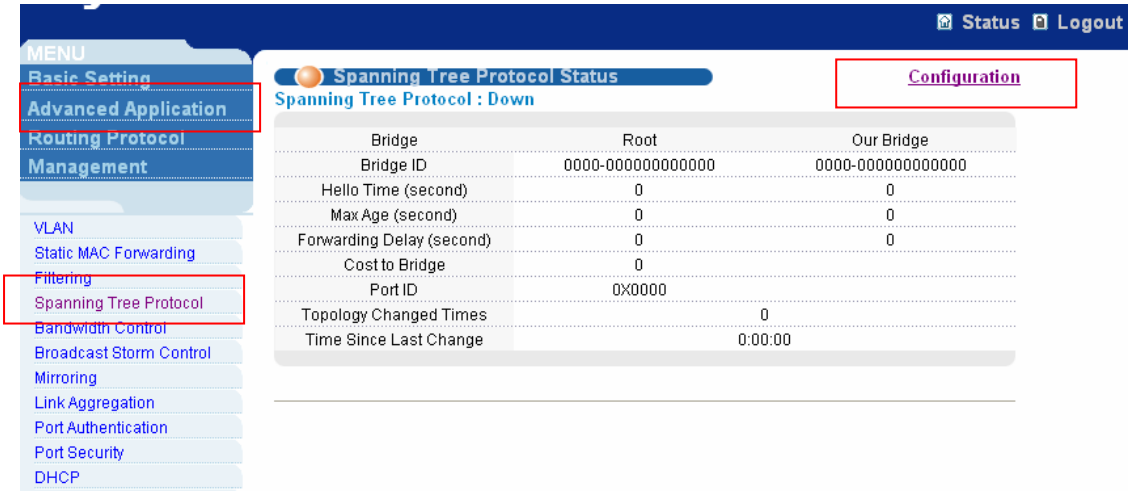
Apply the same steps to Uplink1. Please see the following figure.



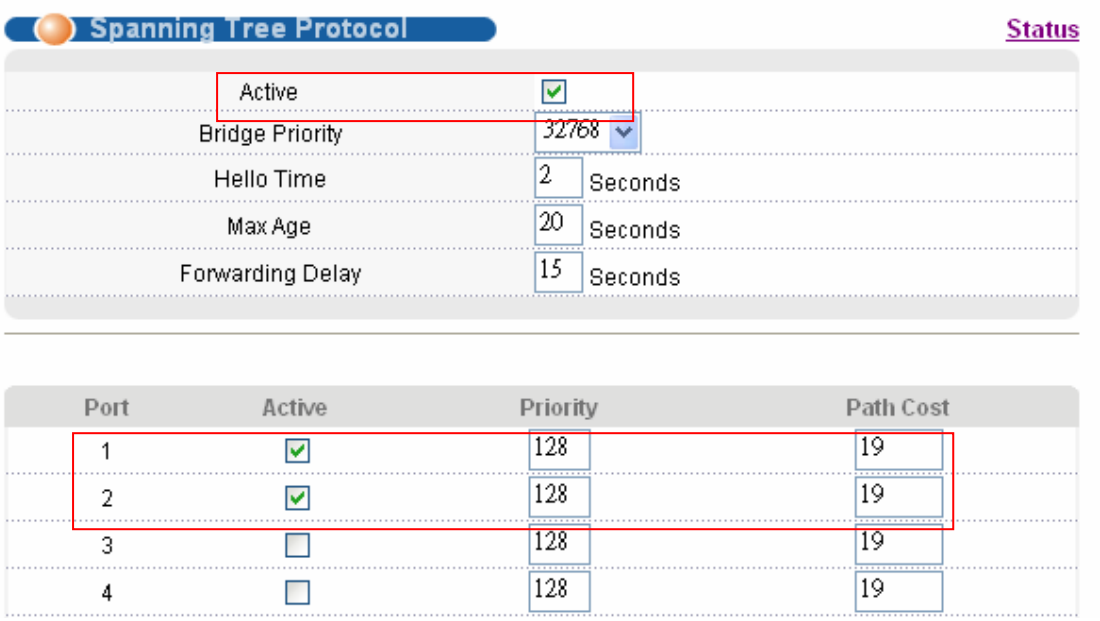
3. Setup ES-4024

3.1 Enable Spanning Tree protocol on the Ethernet ports

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

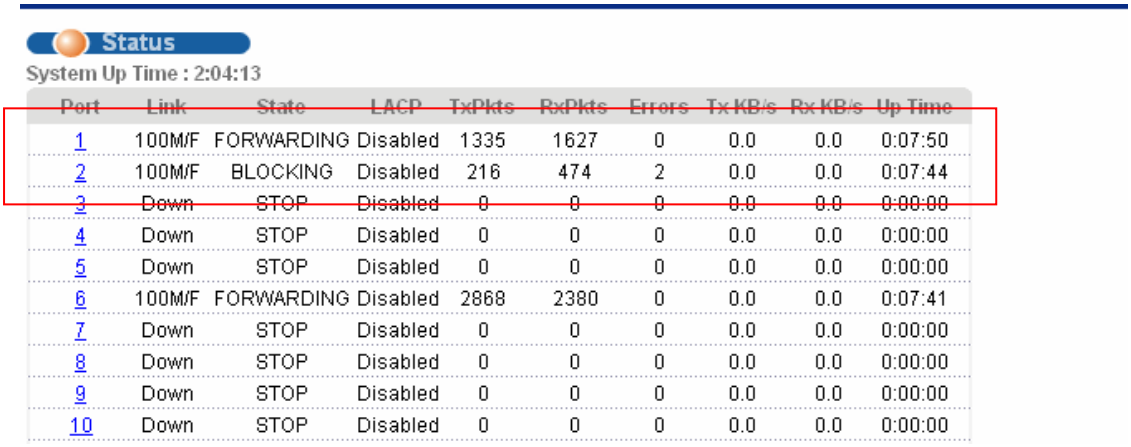


Click **Active** to enable Spanning Tree Protocol. Then enable it on **Port 1** and **Port 2**.



4. Results

We can see the link between port 2 of ES-4024 and Uplink1 of IES-2000 will be blocked as shown after we connect.



After we remove the cable between port 1 of IES-6000 and port 1 of ES-4024, the connection still exists. We can remove any one of the cables as it will not affect the connection. As you can see, the blocking port will become the forwarding port.

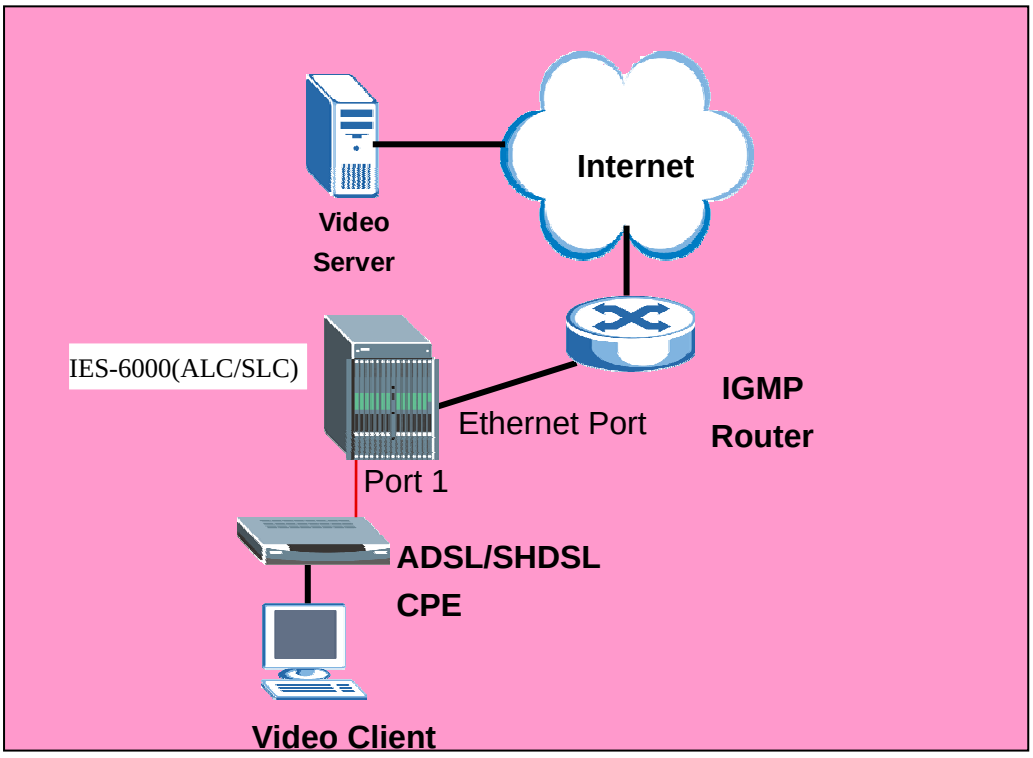
Status

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, the multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to the ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce the multicast traffic passing through the IP-DSLAM. IGMP filtering is for allowing a port to join some specific IGMP groups. This can be applied by the Video service providers. They can only open some specific channels (groups) to specific ports.



How to set up IGMP snooping/IGMP filtering

Here, we only configure IES-6000 to support the IGMP snooping and the 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 wants to subscribe two channels, 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 the movies.

1. IES-6000 settings

1.1 Enable IGMP Snooping

Enable IGMP Snooping to switch on the IGMP Snooping function.

CI command:

MSC1024G> multicast igmp enable snooping

1.2 Set up IGMP Filtering

If we don't set up IGMP filtering, the subscriber will receive all the movies. We set up an IGMP filter Profile and apply it to specific port to limit the channels the subscriber can see.

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

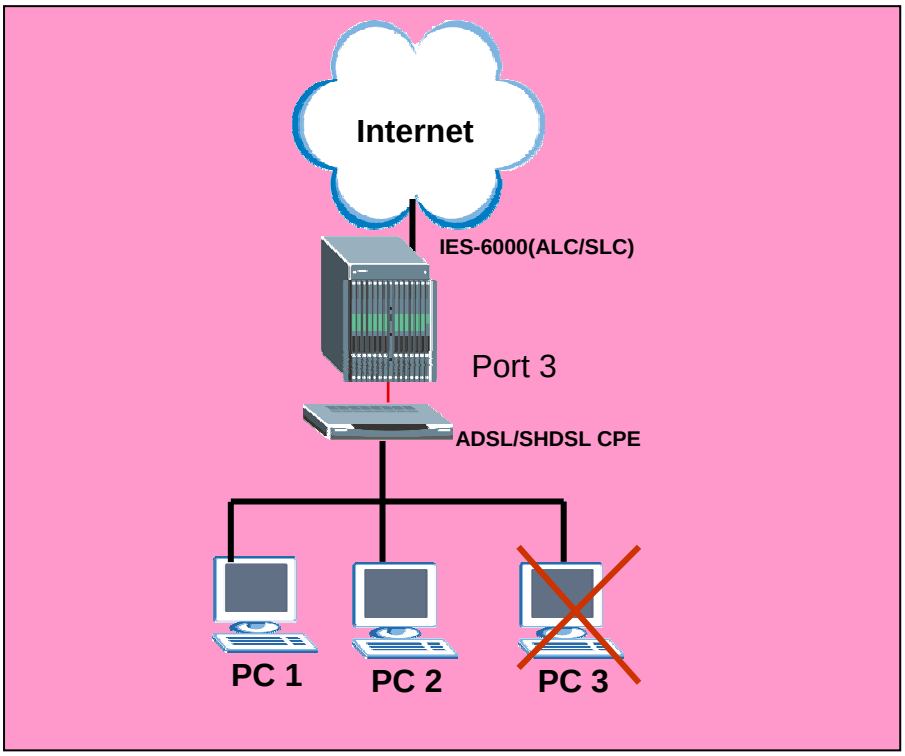
We create the IGMP Filter profile and apply the profile to port 1. Then, we select the **Subscriber1** in the **IGMP Filter Profile**. Then we will save the configuration for the settings to take effect.

CI command:

MSC1024G> profile igmpfilter set Subscriber1 1 224.10.10.8 224.10.10.9
MSC1024G> multicast igmpfilter set 7-1 Subscriber1
MSC1024G> config save

Limit the users behind the certain DSL port

ISP may want to limit the number of PCs behind certain DSL port accessing 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 allowing PCs with certain MAC address, and certain number of PCs behind port 3 to access the Internet.

1. IES-6000 settings

1.1 Set up the MAC filter

Enable the MAC filter for port 3, and enter the MAC address you want to allow to access the Internet. Save the configuration for it to take effect.

Only the MAC addresses listed here can access the Internet from behind certain ports.

CI command:

MSC1024G> acl macfilter enable 7-3

MSC1024G> acl macfilter set 7-3 00:a0:c5:12:34:56
MSC1024G> acl macfilter set 7-3 00:a0:c5:77:88:99
MSC1024G> config save

1.2 Set up Port Security

Input the MAC address number you want to limit to access to the Internet. Note that the MAC filter and Port security can't be used at the same time.

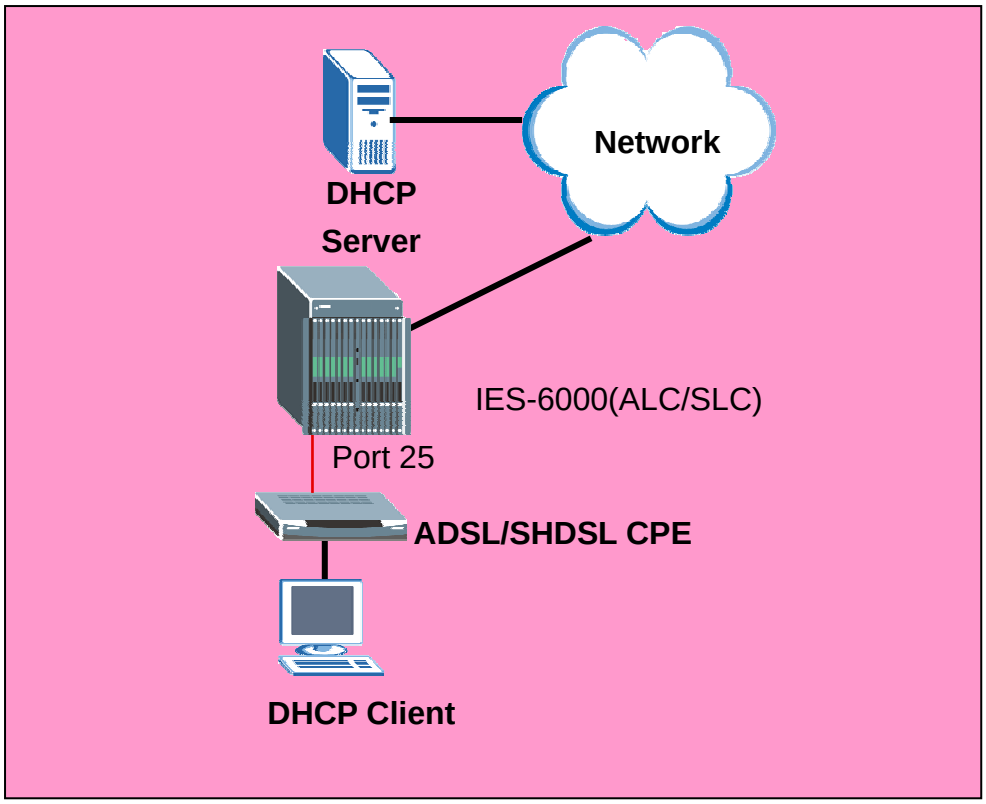
Here we allow only 1 user to access the Internet on slot 7 port 3.

CI command:

MSC1024G> acl maccount enable 7-3
MSC1024G> acl maccount set 7-3 1
MSC1024G> config save

DHCP Relay Option 82 Application

ISP may want to limit the number of IP addresses or deliver some specific IP addresses according to certain DSL port, VLAN ID and option 82 strings. They can easily 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 allowing a PC get DHCP IP address from 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 "6000". 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 "6000".

1. IES-6000 settings

Enable the DHCP relay and Option 82 functions including the IP address of DHCP server. The IP address is 192.168.1.99 in our case. Also, enter "6000" as the Option 82 string.

CI command:

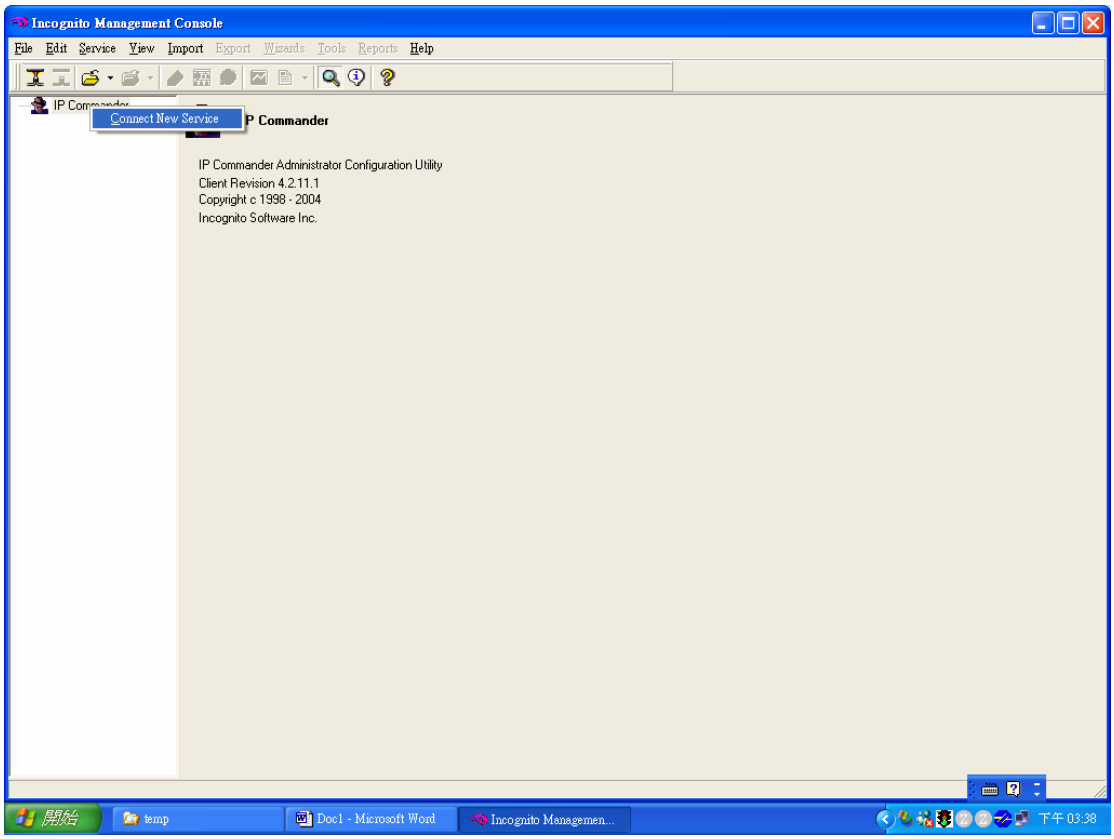
MSC1024G> acl dh set 1
MSC1024G> acl dhcprelay82 enable 1 1
MSC1024G> acl dhcprelay82 server set 1 192.168.1.99
MSC1024G> acl dhcprelay82 info 1 6000

2. CPE settings

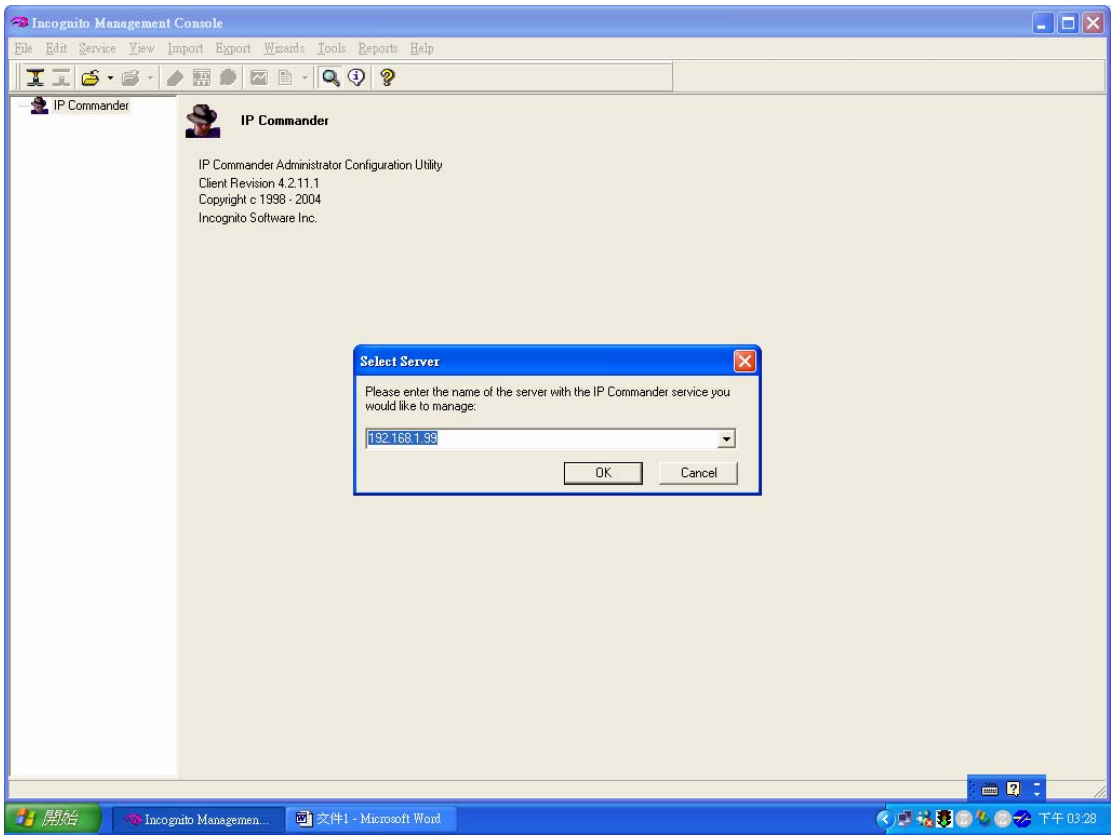
Connect CPE to the 25th DSL port. Please see the former applications for detailed settings.

3. IP Commander settings

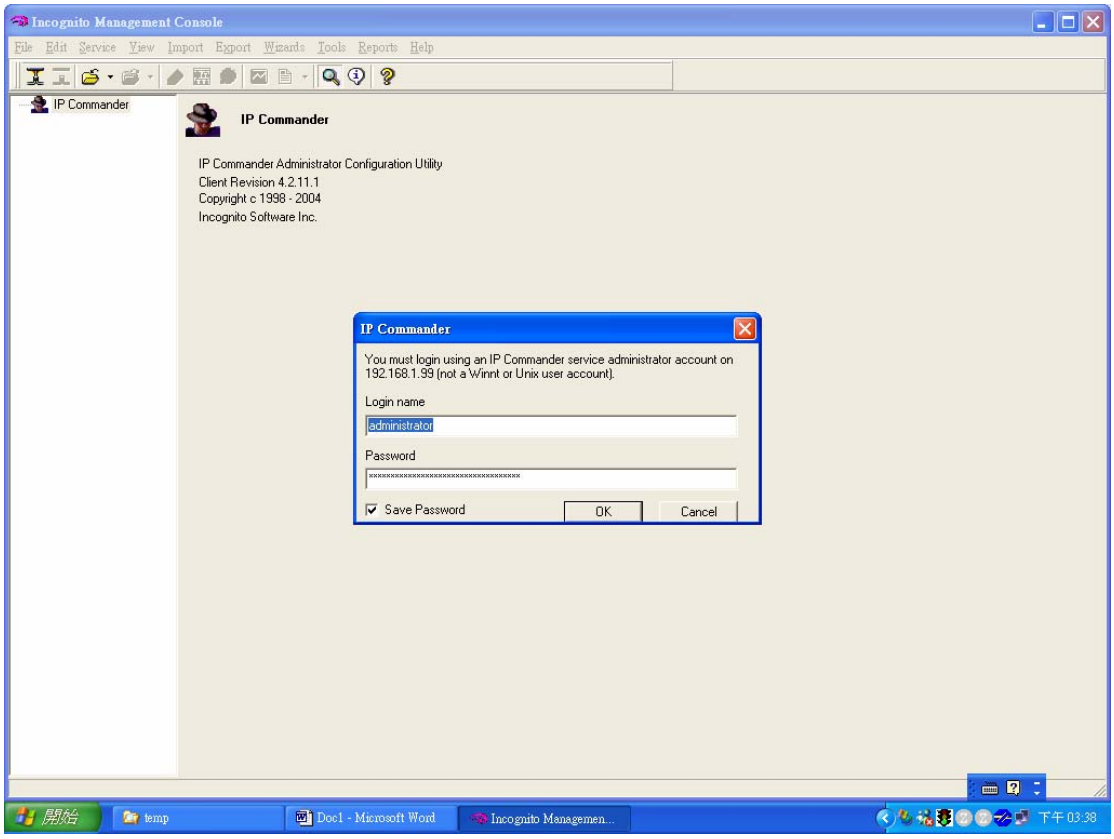
Open IP Commander. Right click “IP commander and then click “**connect new server**”.



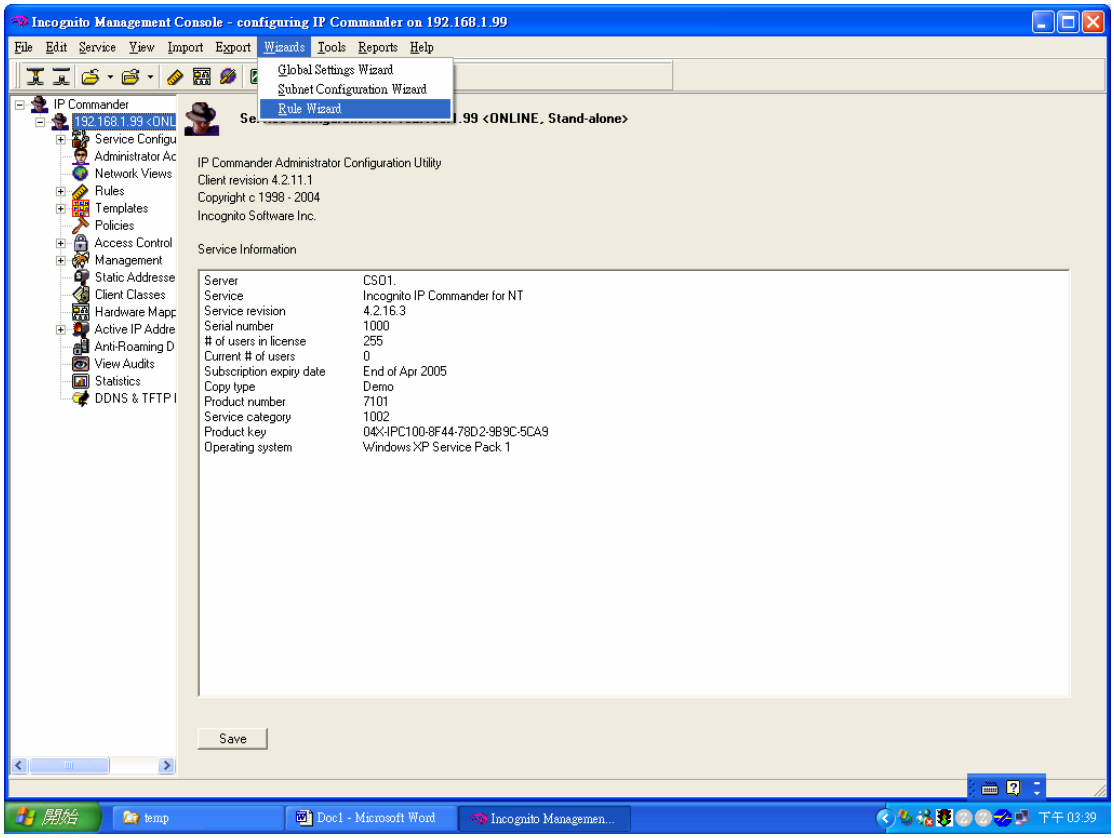
Input the DHCP IP address or domain name and click “ok”. Our IP is 192.168.1.99.



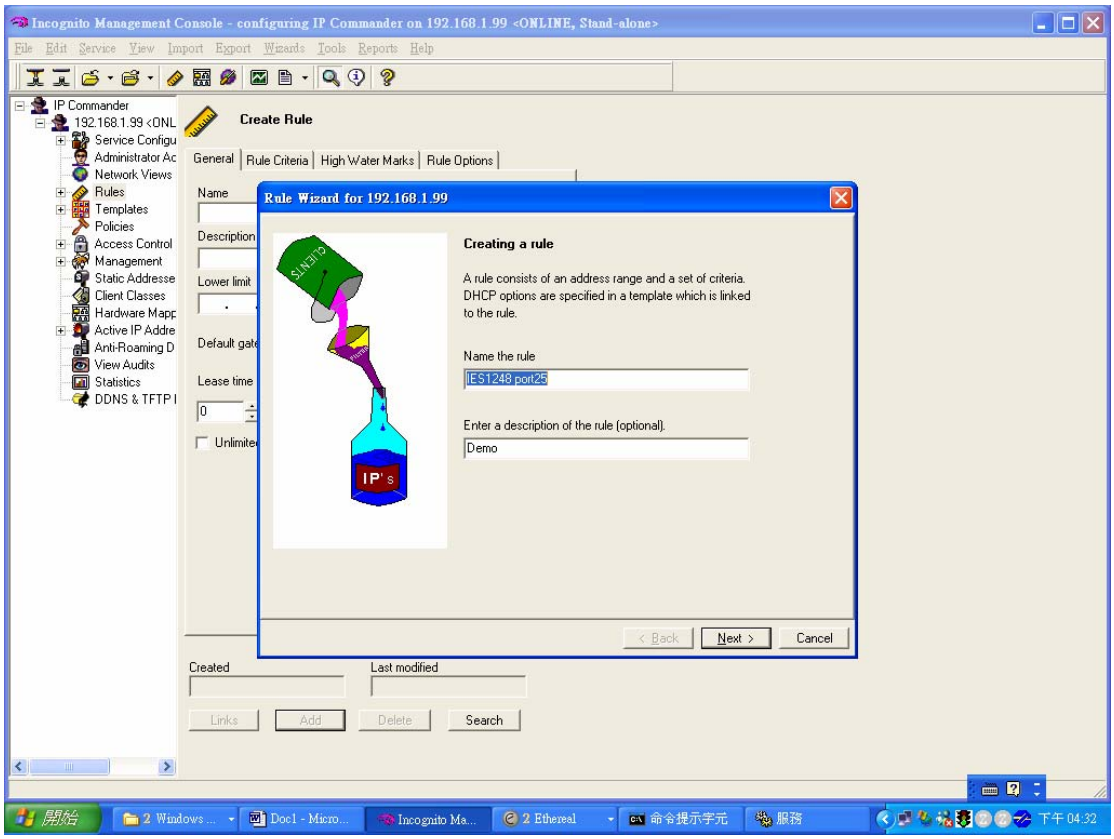
Input the user name and the password. The default user name is “administrator” and the password is “incognito”.



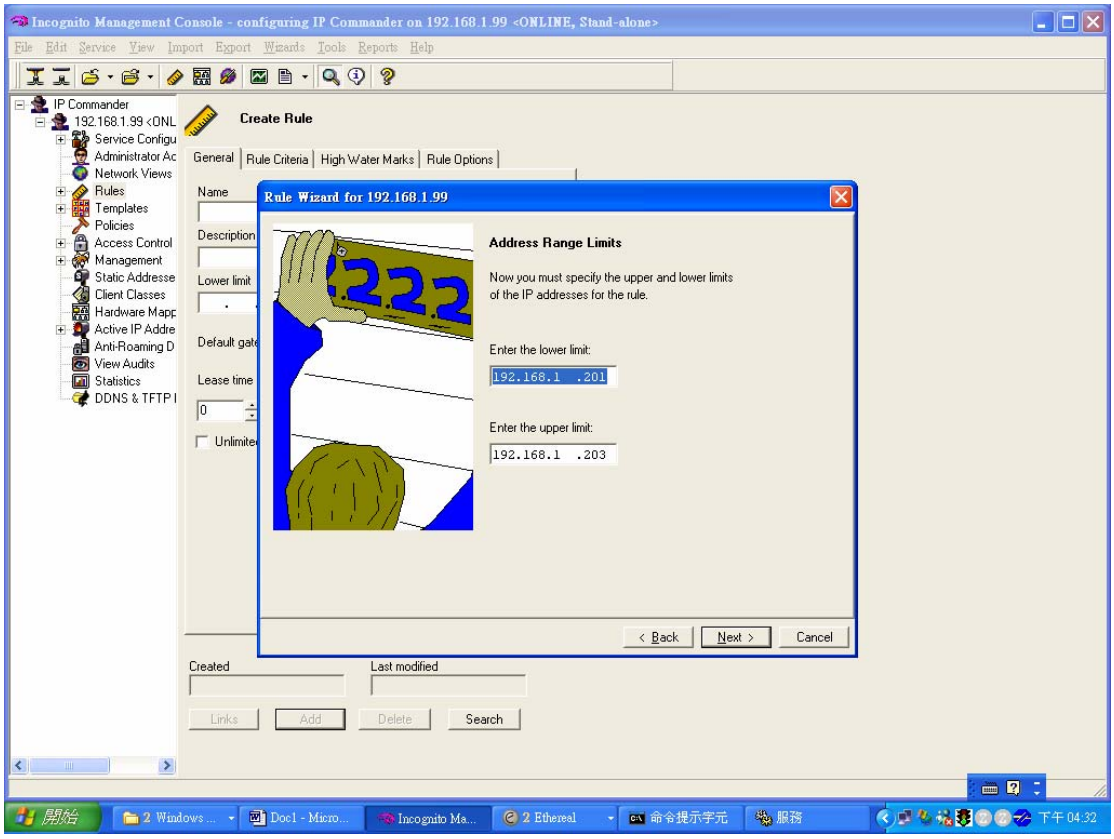
It will bring up the following screen, please make sure that your DHCP is in "**online**" status. Then click "**wizard**" in the top tool bars and select "**rule wizard**".



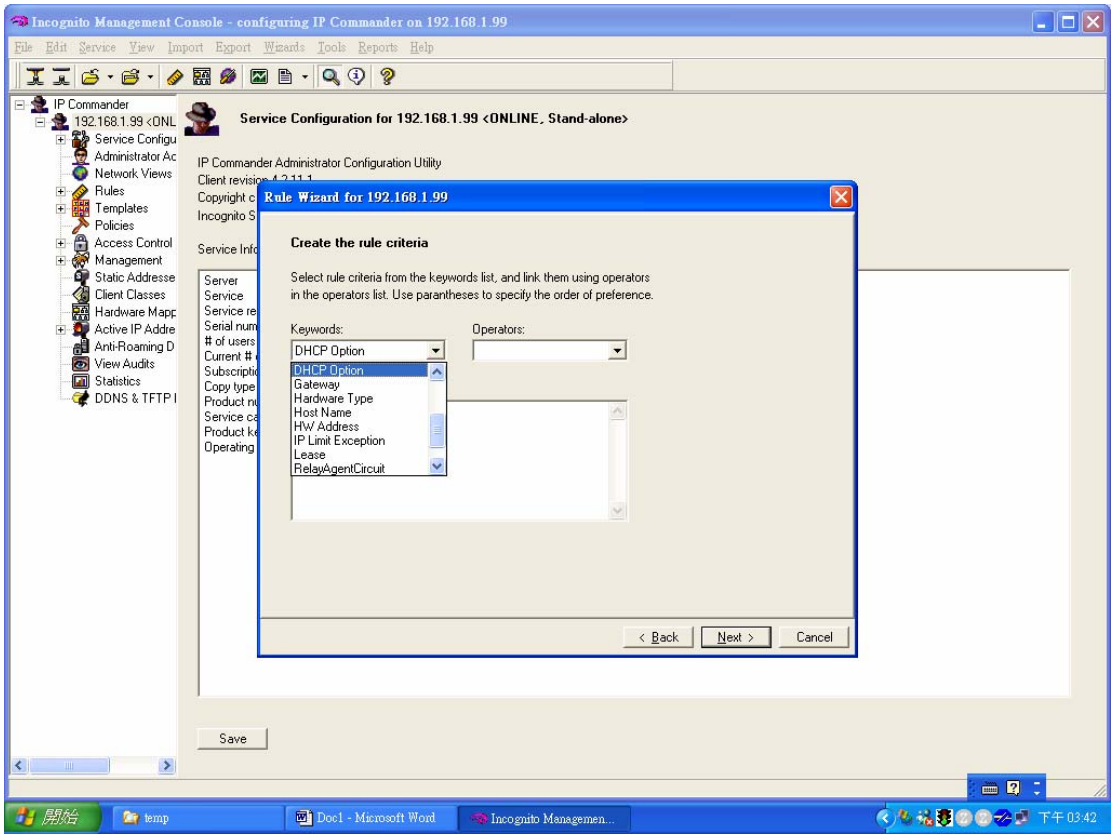
Give a name and description to the new rule.



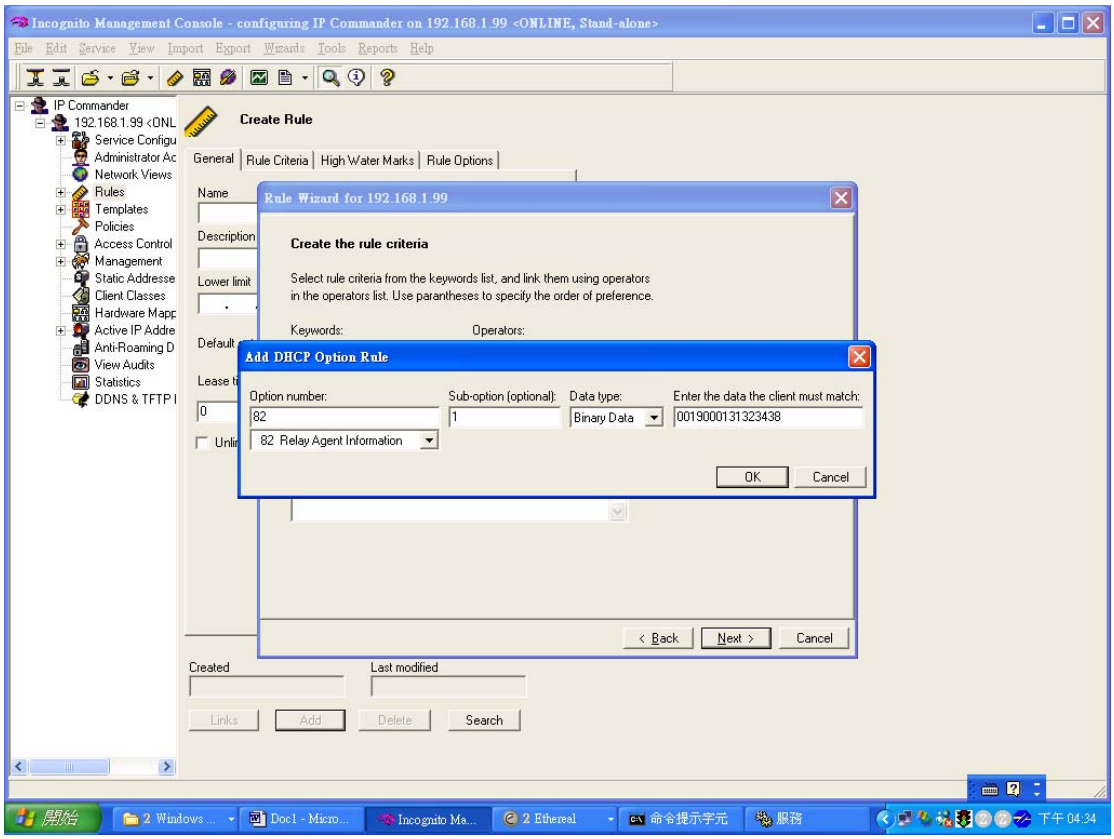
Assign a range of IP addresses or just one IP address to this rule. In our case, we set the IP pool ranging from 192.168.1.201 to 192.168.1.203.



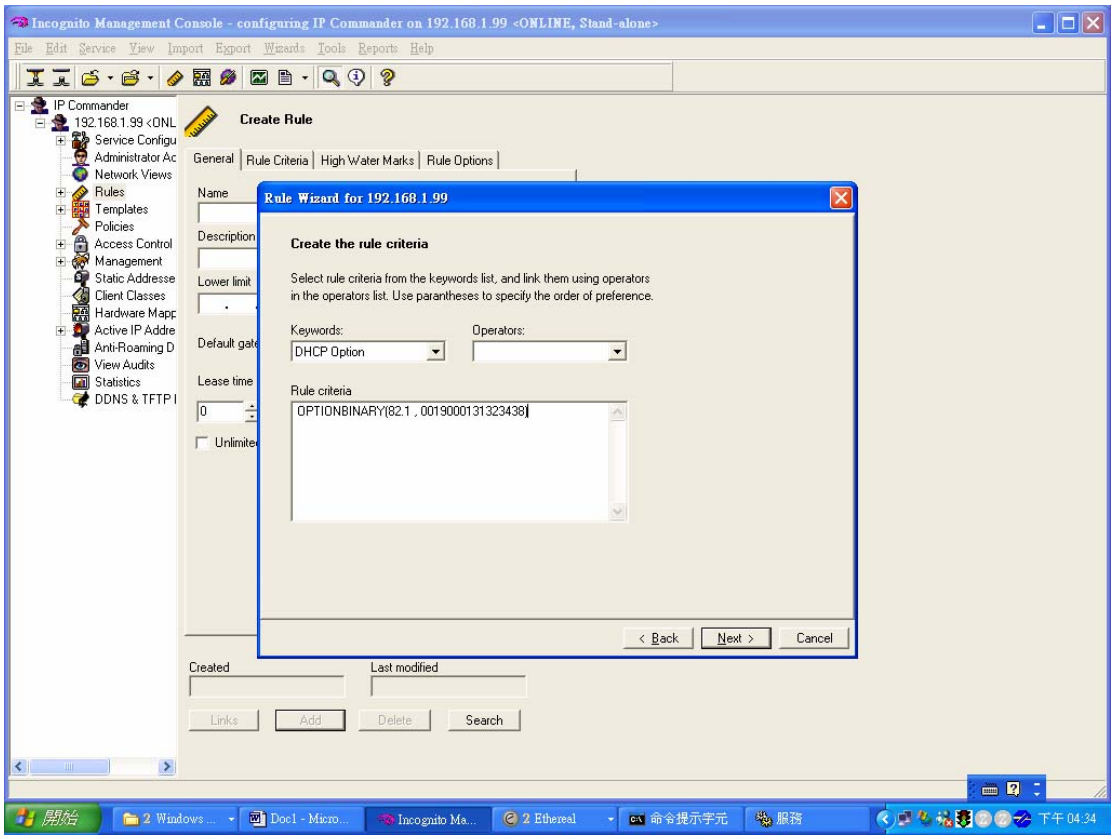
After choosing the IP pool, we select “DHCP Option” in Keywords combo box.



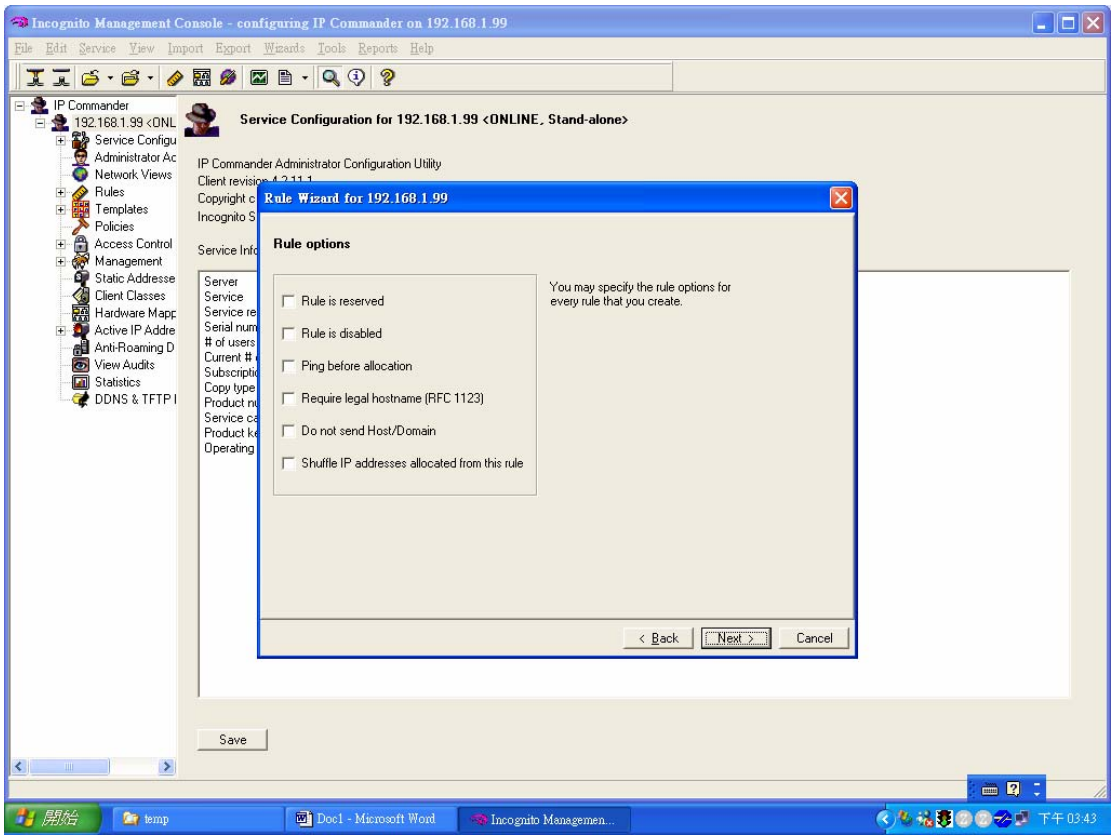
After selecting the “DHCP Option”, the “Add DHCP Option Rule” dialog will pop up. Select “option 82 Relay Agent Information”, sub-option 1, binary data. For port 25, VLAN 1, “6000”, type in “0019000136303030” as the key value and click OK. Please note that the first 2 bytes define port number, the second 2 bytes are VLAN ID and the other bytes are the Option 82 string.



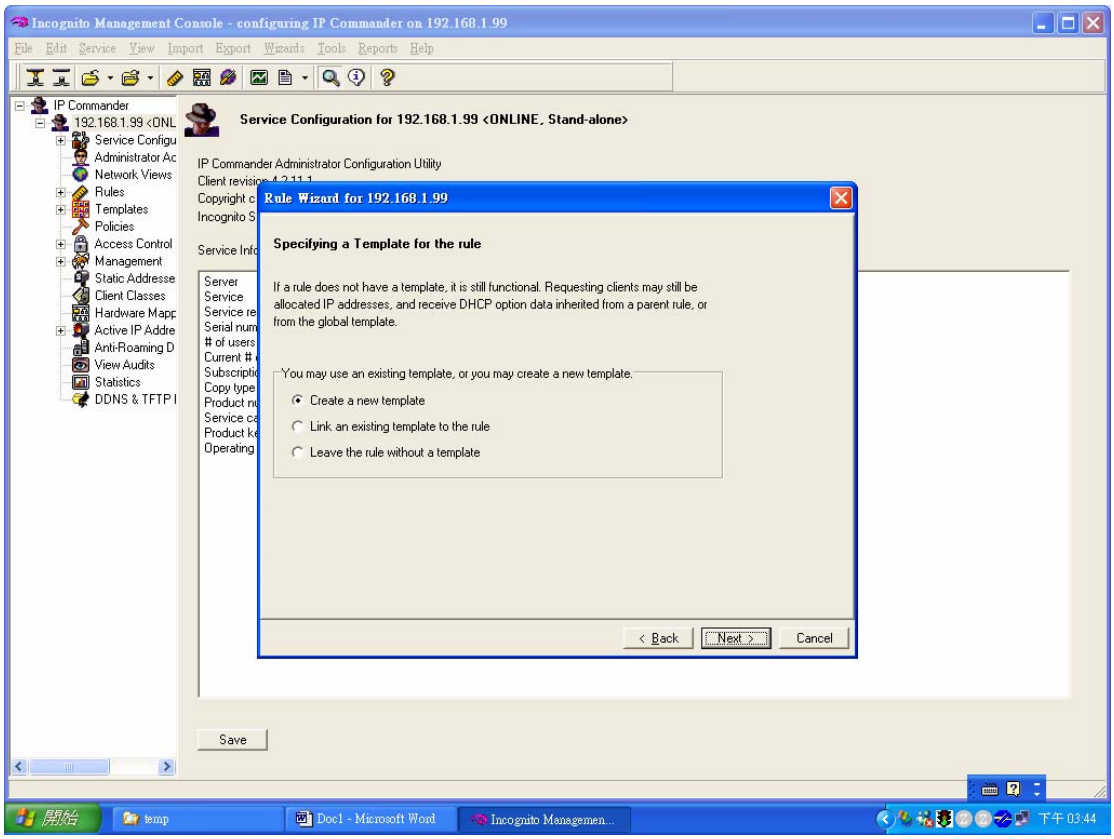
After you finish the above step, you will see the following figure.



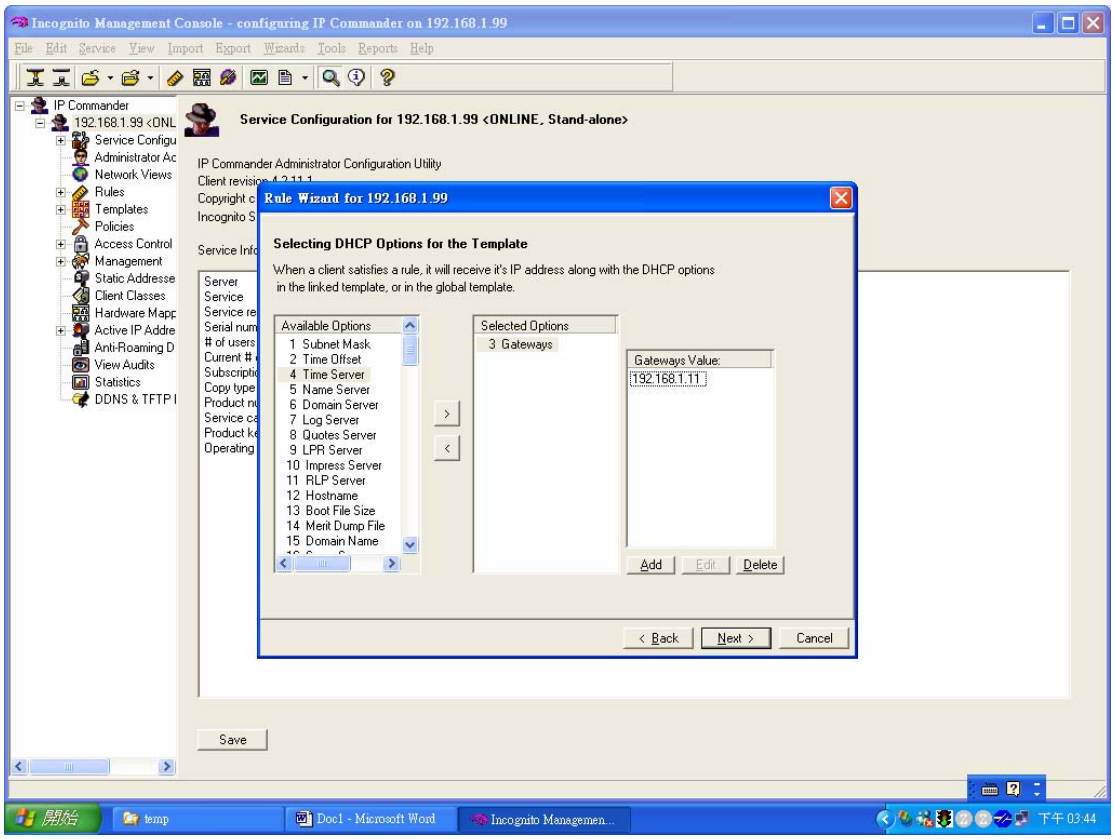
Move to the following screen and just press the **Next** button again.



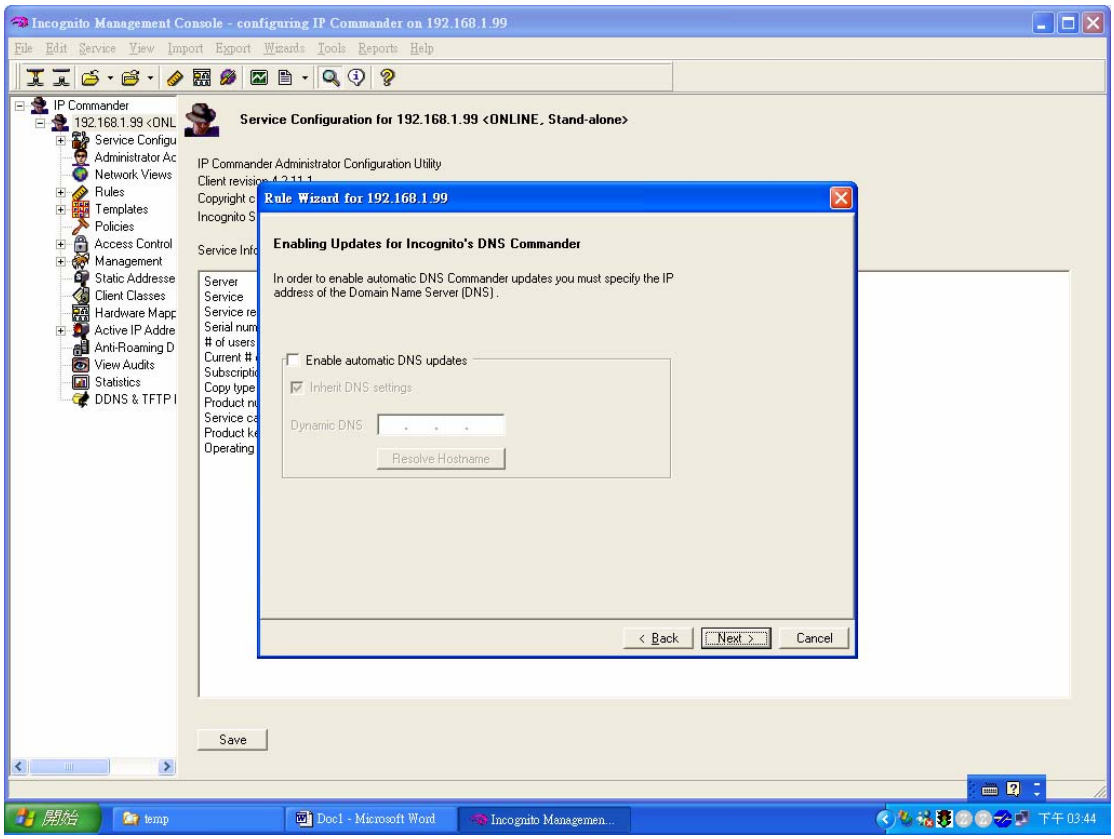
Then you can add a DHCP template (option) such as gateway, DNS server and so on.



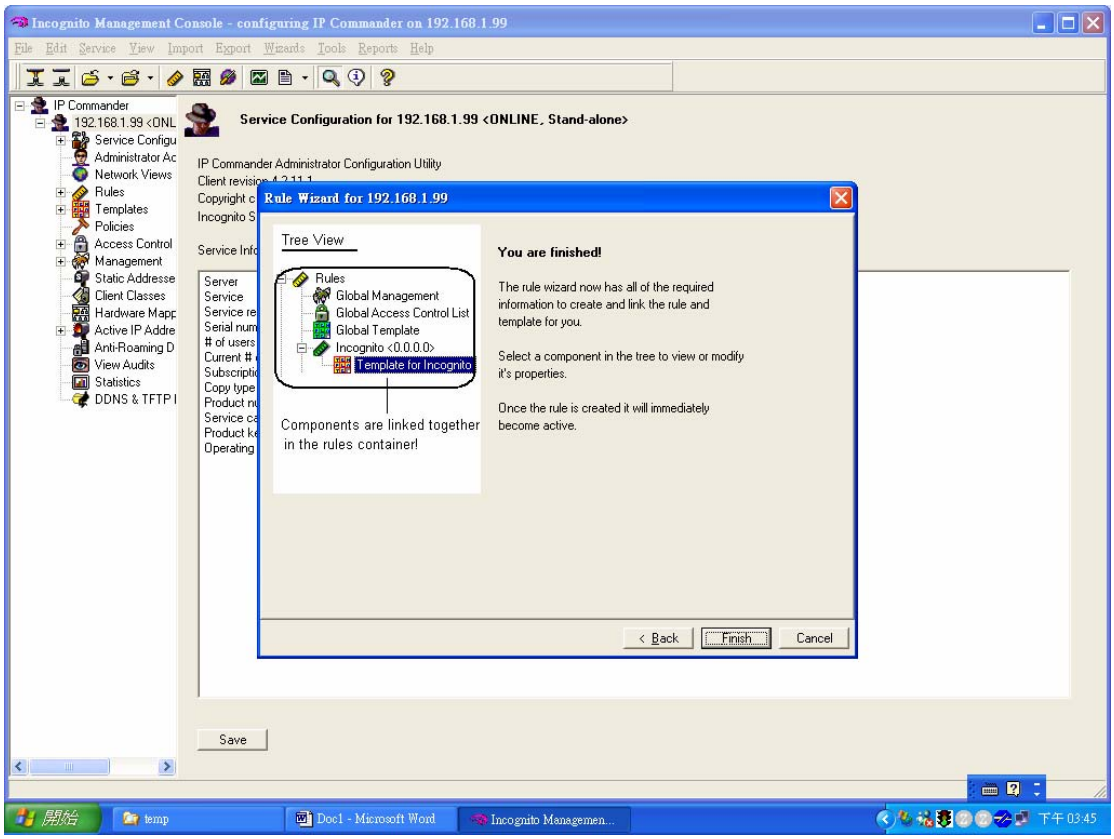
Here we use “192.168.1.1” as the gateway IP address of the DHCP client PC.



You can apply the DDNS service to the DHCP server, but you don't have to.



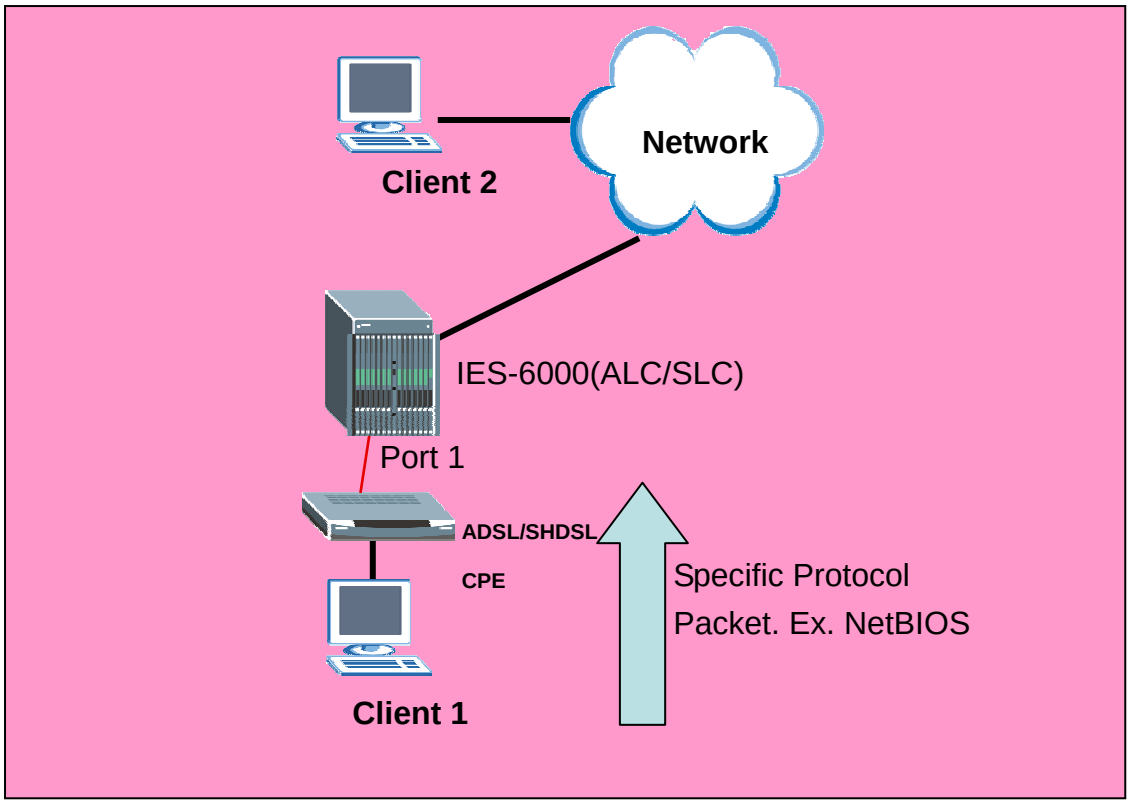
The rule creation has been finished.



After finishing all the 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-6000 provides “Packet Filter” function to filter some specific packets, like IP, ARP, DHCP, EAPoL, PPPoE, NETBIOS and IGMP.



How to Filter Some Specific Packets

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

1. IES-6000 ALC-1248G/SLC 1248G settings

Type the following packet filter command with specific slot-port:

MSC1024G> acl pktfilter set 7-1 netbios

Display the port filter status on slot 7.

CI command:

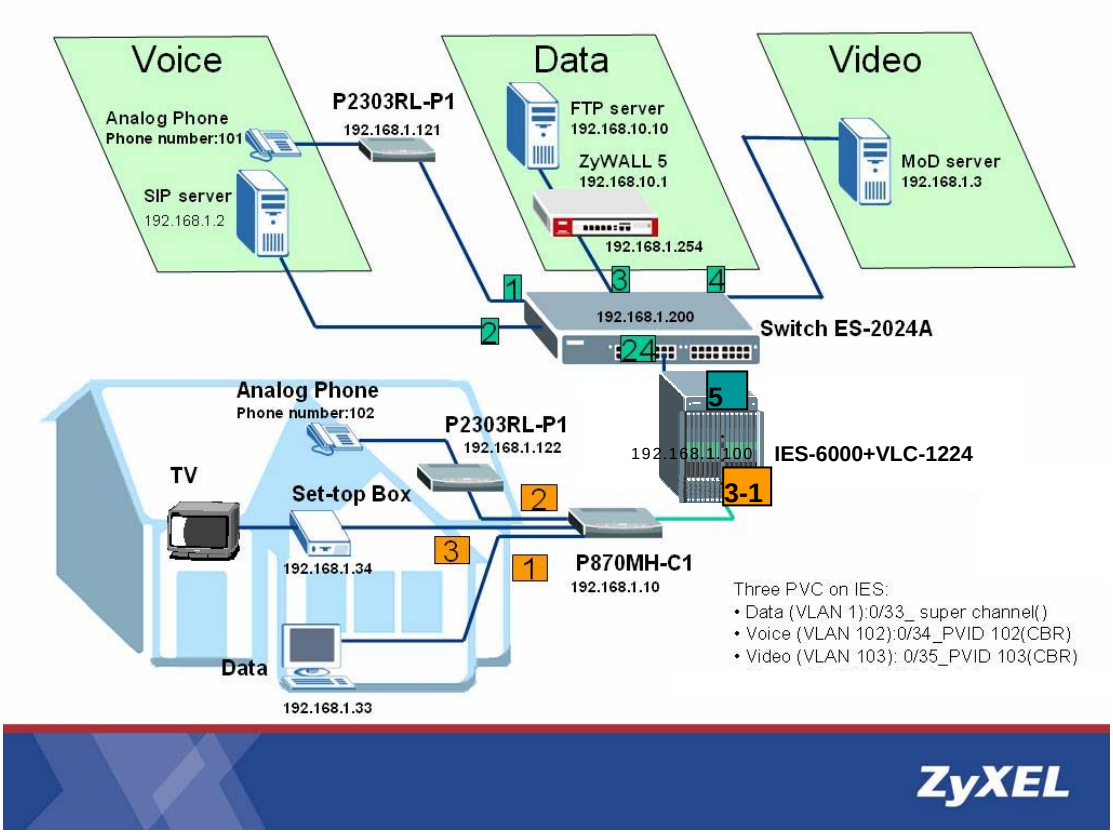
MSC1024G> acl pktfilter show 7
port filter
----- ----------
7- 1 netbios
7- 2 accept-all
7- 3 accept-all
7- 4 accept-all

7- 5 accept-all
7- 6 accept-all
7- 7 accept-all
7- 8 accept-all
7- 9 accept-all
7-10 accept-all
7-11 accept-all
7-12 accept-all
7-13 accept-all
7-14 accept-all
7-15 accept-all
7-16 accept-all
7-17 accept-all
7-18 accept-all
7-19 accept-all
7-20 accept-all
7-21 accept-all
7-22 accept-all
7-23 accept-all
7-24 accept-all
7-25 accept-all
7-26 accept-all
7-27 accept-all
7-28 accept-all
7-29 accept-all
7-30 accept-all
7-31 accept-all
7-32 accept-all
7-33 accept-all
7-34 accept-all
7-35 accept-all
7-36 accept-all
7-37 accept-all
7-38 accept-all
7-39 accept-all
7-40 accept-all
7-41 accept-all
7-42 accept-all

7-43 accept-all
7-44 accept-all
7-45 accept-all
7-46 accept-all
7-47 accept-all
7-48 accept-all
MSC1024G>

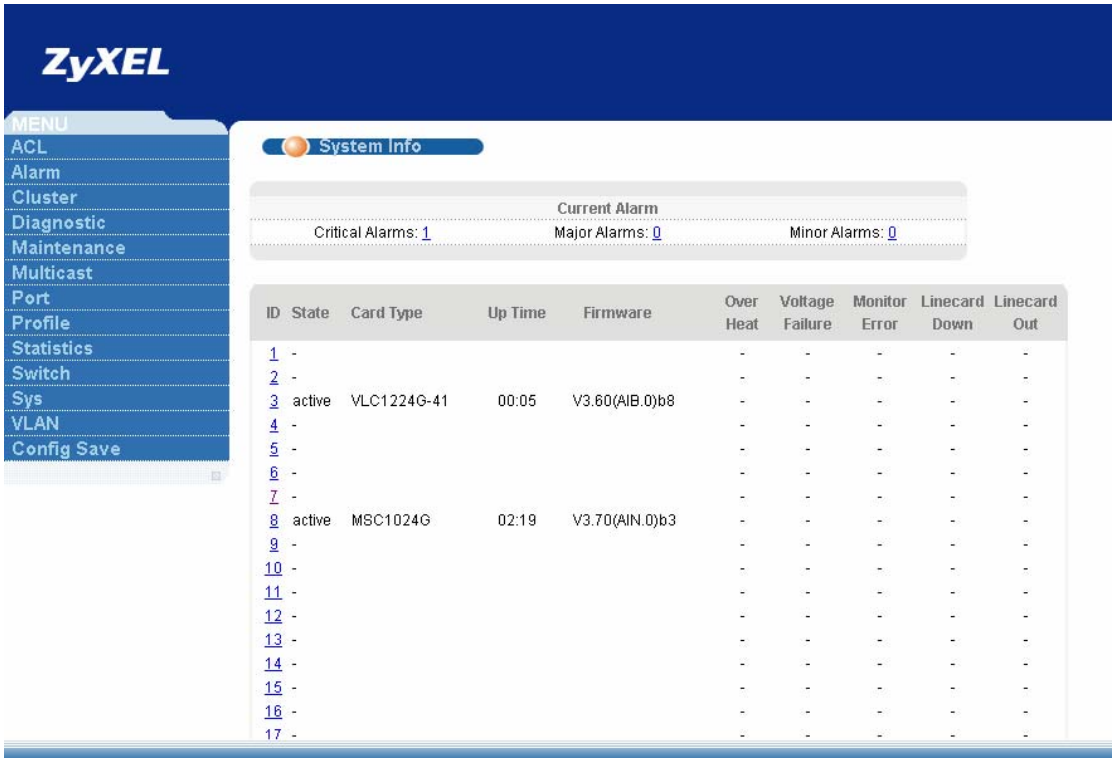
VDSL Application- Triple Play

For the Triple-play scenario, 3 PVCs for multiple services (Data, Voice and Video) on the VDSL port of IES-6000 VDSL line card are to be configured. The IEEE VLAN & 802.1p mechanism is used to guarantee the Voice stream and Video stream will be running smoothly without interruption. The instructions to configure the IES-1248-71 device are following.



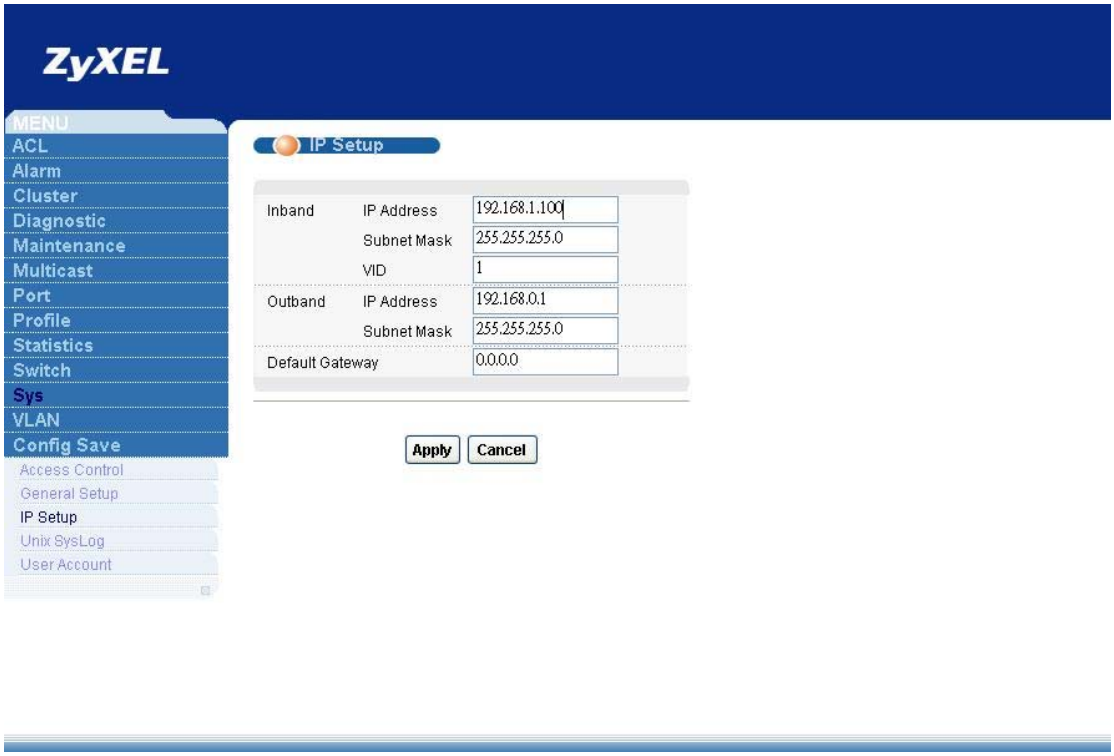
IES-6000 Settings

1. Connect to the IES-6000 using Web GUI. The default Inband IP address of IES-6000 is **192.168.1.1**. Enter the default id '**admin**' and password **'1234'** to access the device.



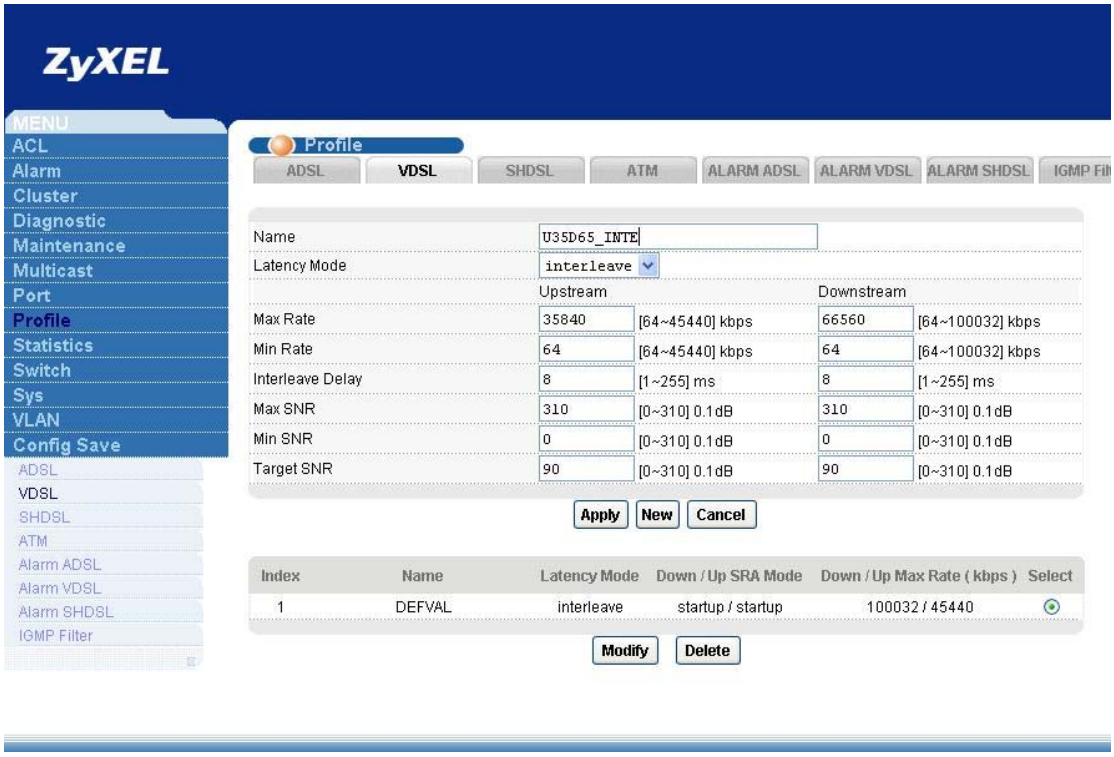
2. Set the IES-6000's IP address to '**192.168.1.100**'.

Click the **Sys > IP Setup**. Type in the IP address **'192.168.1.100'** and the subnet mask **'255.255.255.0'.**



3. Create the VDSL profile

Type in the **Name** and select the **Latency Mode**. Then set the **Max Rate of Downstream/Upstream** (here is an example **'U35D65_INTE'** for 65Mbps/35Mbps line) and the other related parameters.

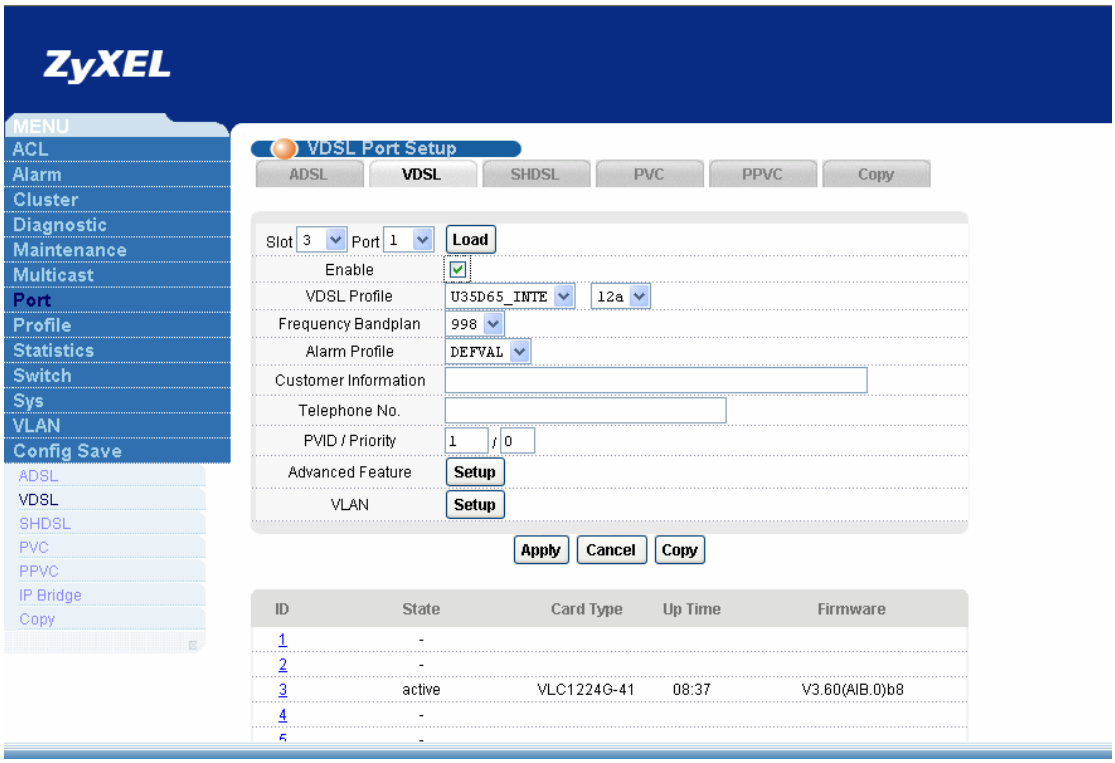


4. Apply the VDSL profile to the VDSL ports

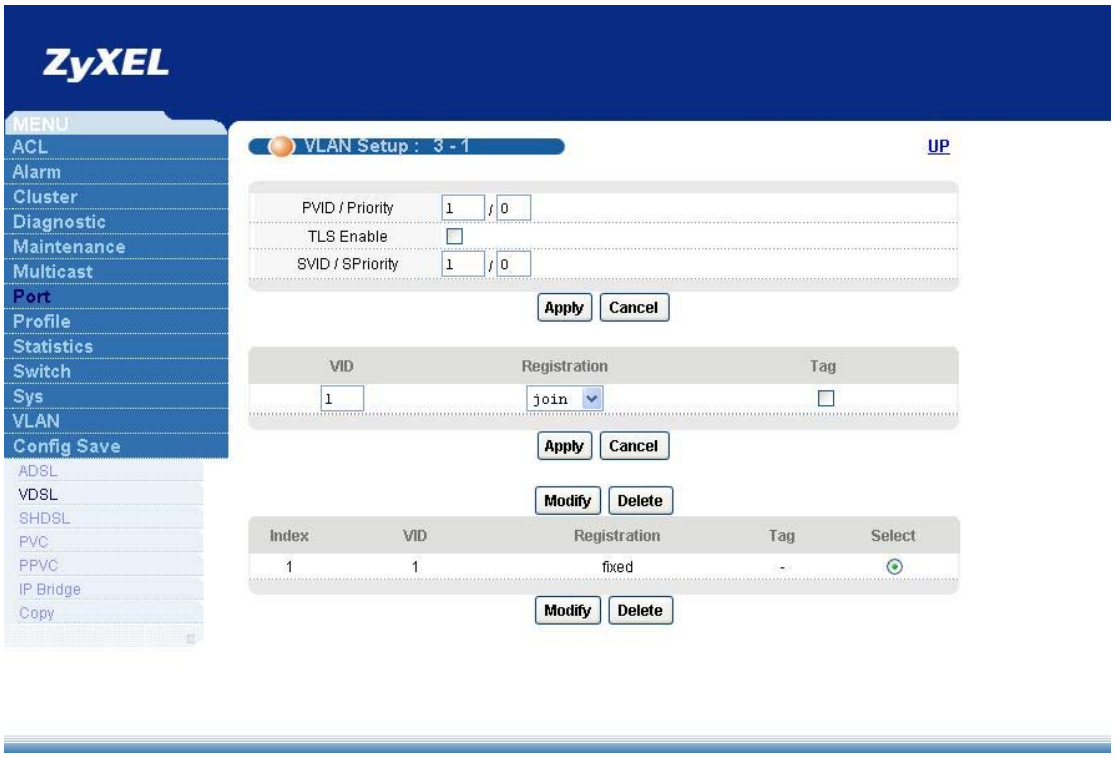
Then select to which VDSL ports you want to apply the VDSL profile you just created to.

Click **Port > VDSL**

Choose **Slot 3** and **Port 1**. Check '**Enable'**. Choose **'U35D65_INTE'** in the **VDSL Profile** option. Click **Apply** for the settings to take effect.

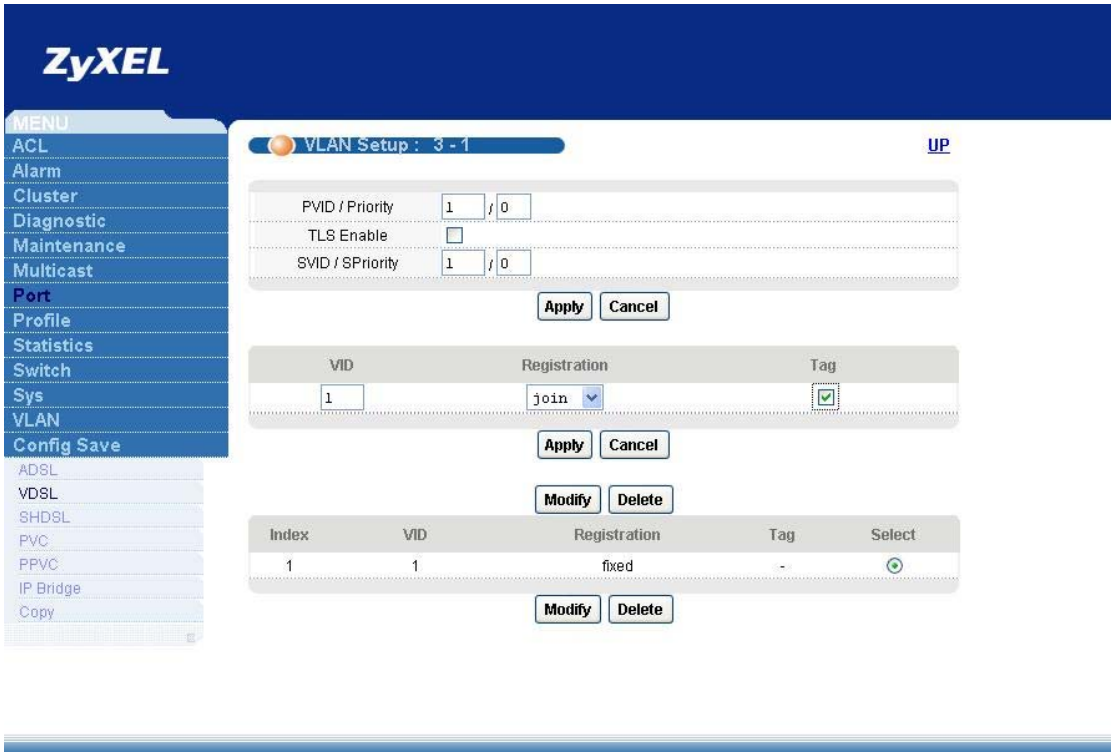


5. Go to **Setup** in the **VLAN** option to create 3 VLANs: VLAN 1 (for DATA), VLAN 102 (for VOICE) and VLAN 103 (for VIDEO) for the VDSL port.



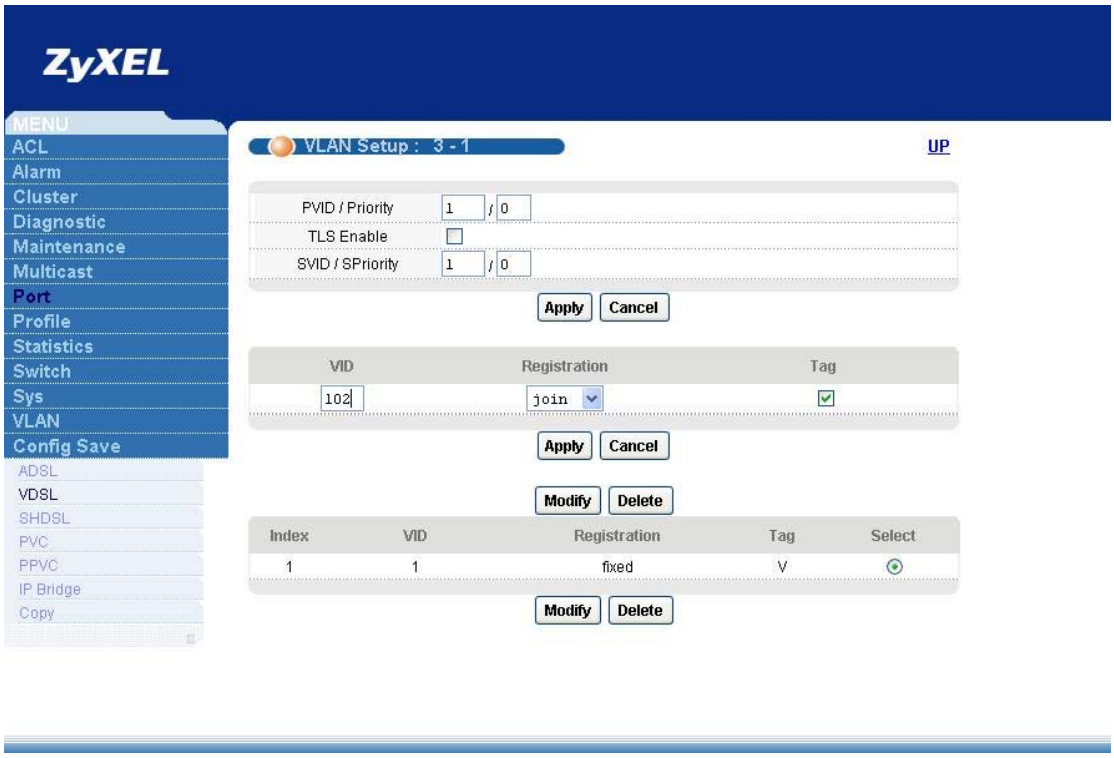
a. Create VLAN 1

VLAN 1 is created by default. Click **Modify** and check the **Tag** box. Click **Apply** to finish the VLAN 1 configuration.



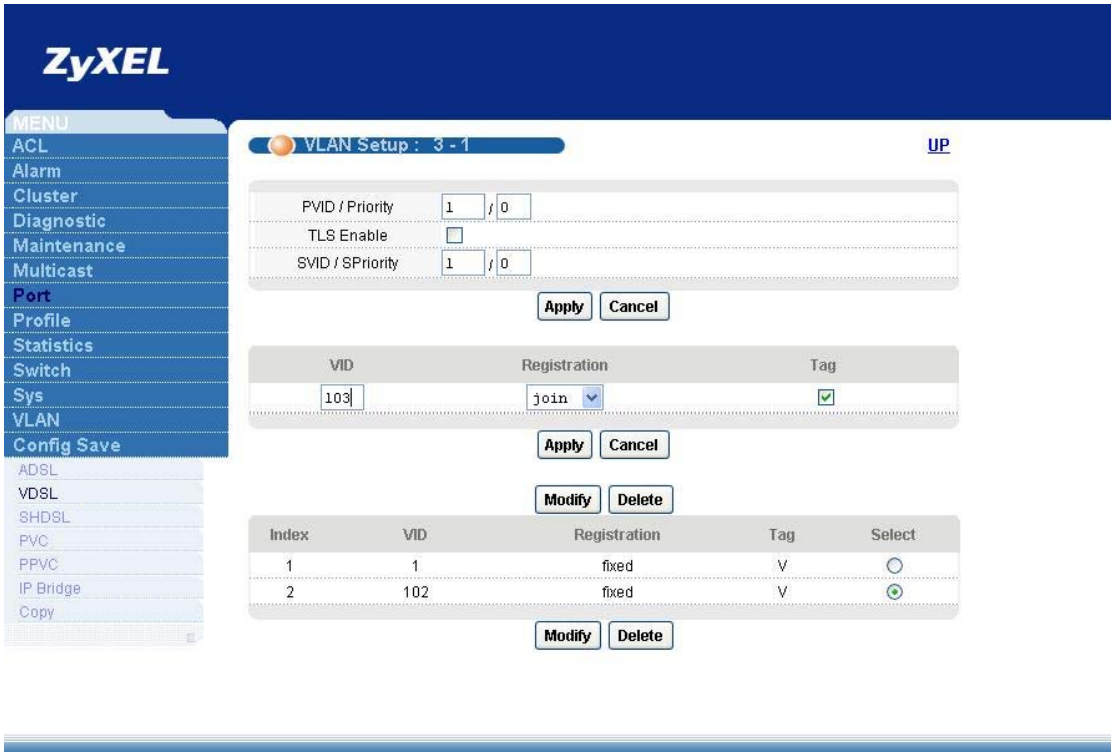
b. Create VLAN 102

Fill in **VID** with **'102'** and check the **Tag** box. Click **Apply** to finish the VLAN 102 configuration.



c. Create VLAN 103

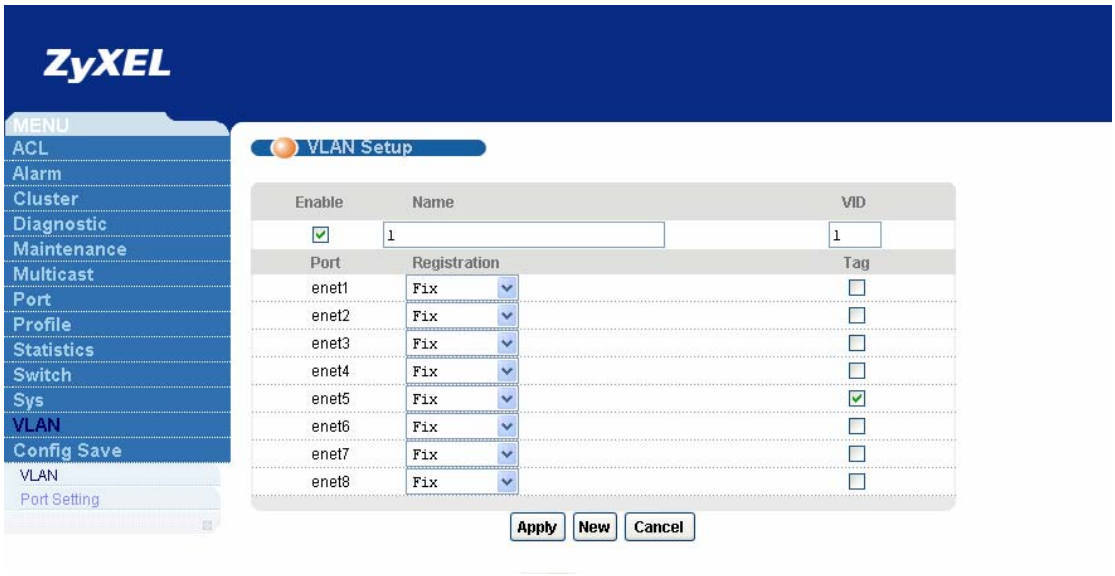
Fill in **VID** with **'103'** and check the **Tag** box. Click **Apply** to finish the VLAN 103 configuration.



6. Configure VLANs on ENET5

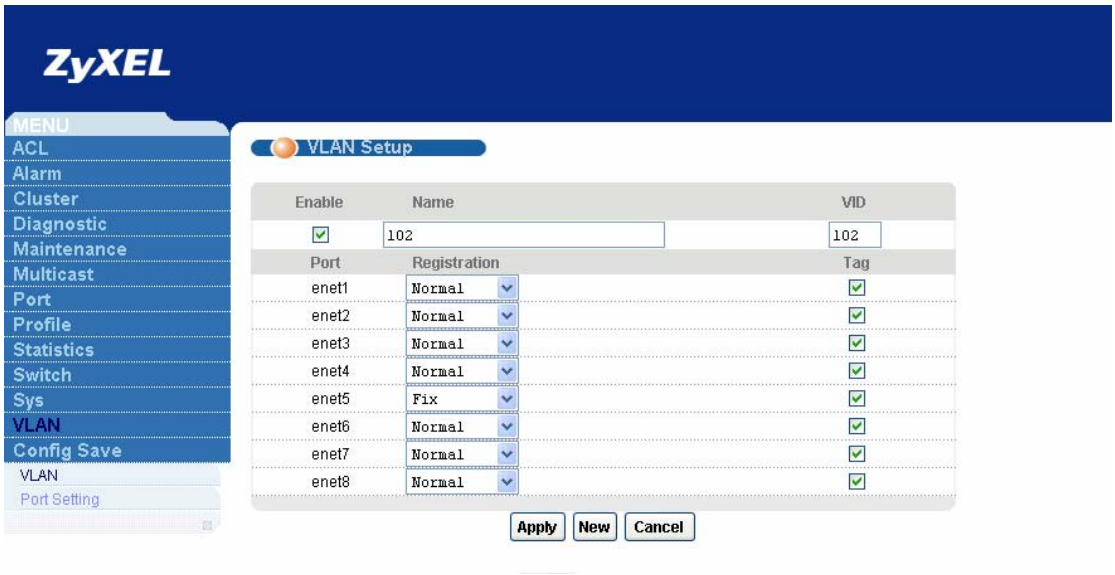
a. Configure VLAN 1

Select **Index 1** and click **Modify**. Check the **Tag** box on **enet5**. Click **Apply** for the settings to take effect.



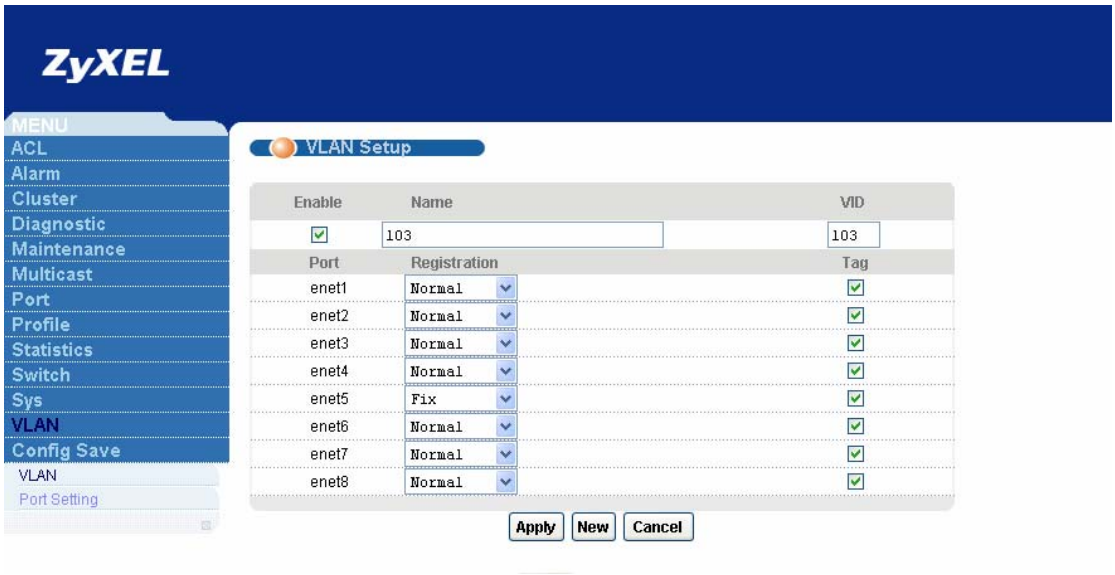
b. Configure VLAN 102

Select **Index 2** and click **Modify**. Choose the **Registration** as **'Fix'** and check the **Tag** box on **enet5**. Click **Apply for the settings** to take effect.



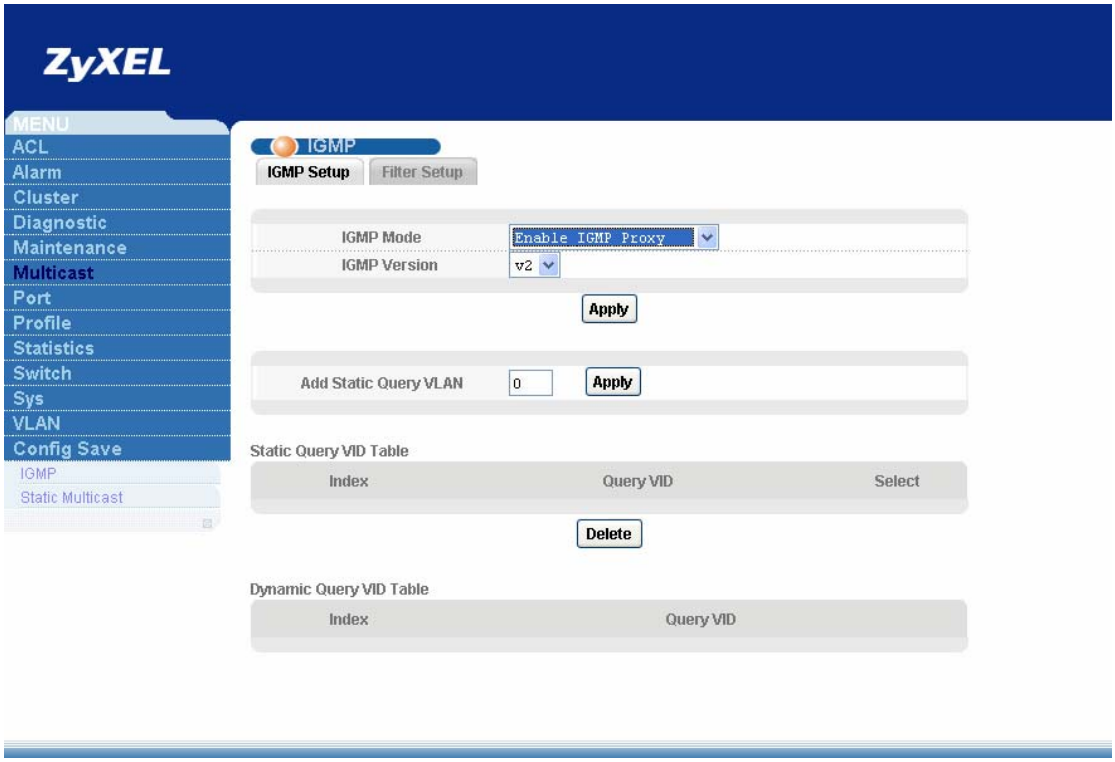
c. Configure VLAN 103

Select **Index 3** and click **Modify**. Choose the **Registration** as **'Fix'** and check the **Tag** box on **enet5**. Click **Apply** for the settings to take effect.

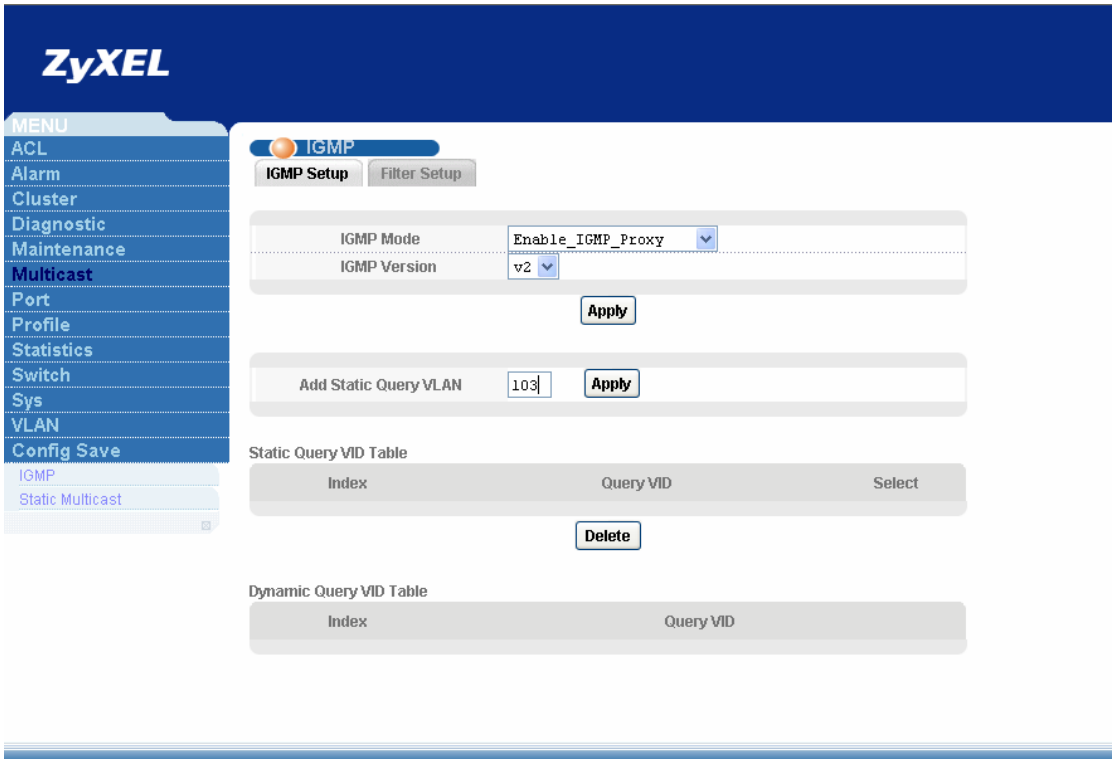


7. Enable **IGMP Proxy** on IES-6000

Click **Multicast > IGMP**. Choose the **IGMP Mode** as **Enable_IGMP_Proxy** and click **Apply** to finish the setup.

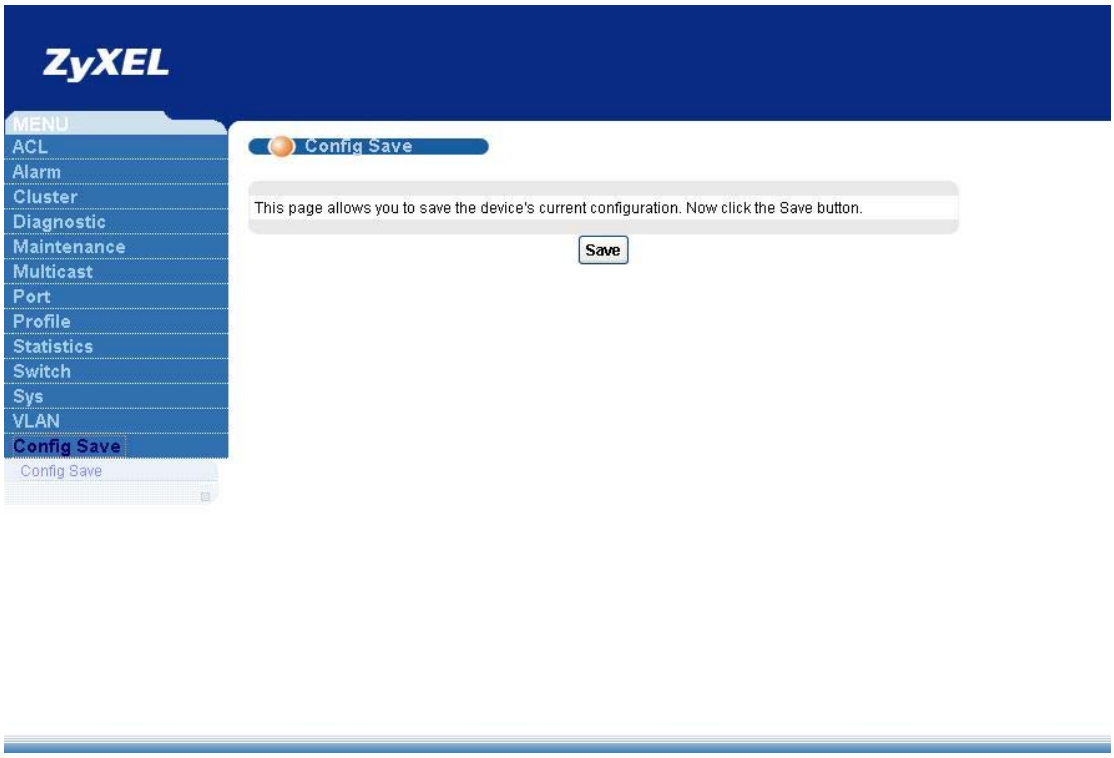


Fill in **Add Static Query VLAN** with '**103**' and then click **Apply** for the settings to take effect.



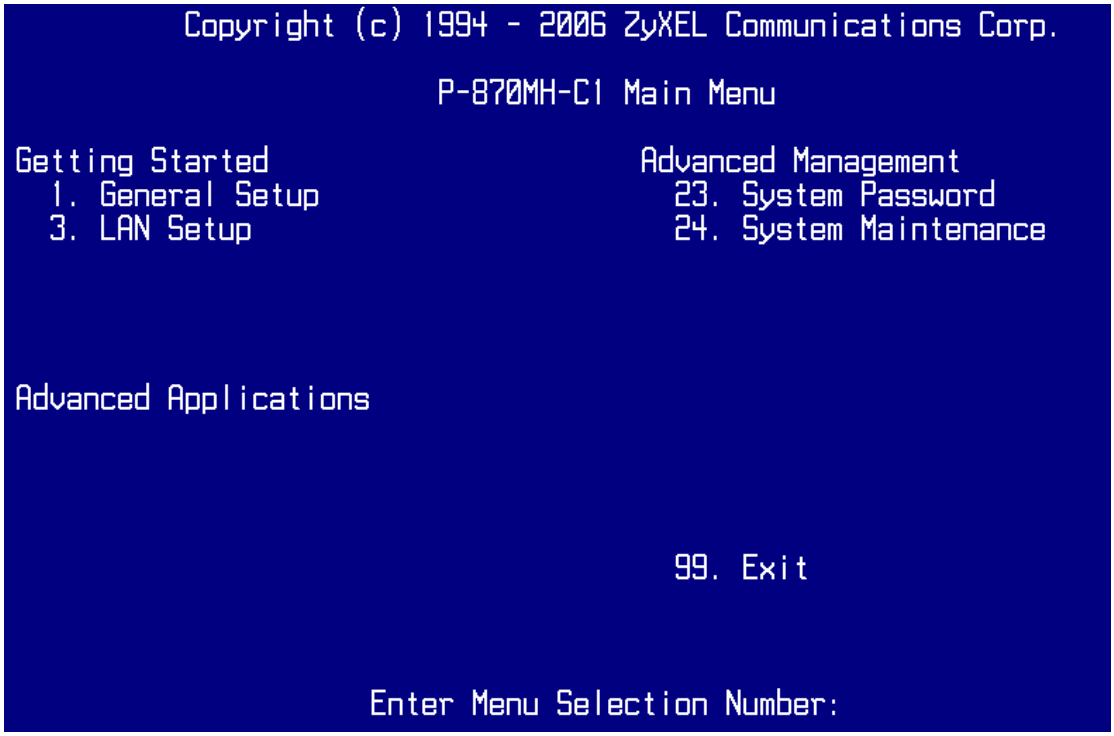
8. Save configurations

Click **Config Save > Config Save** and click the **Save** button to save the configuration.



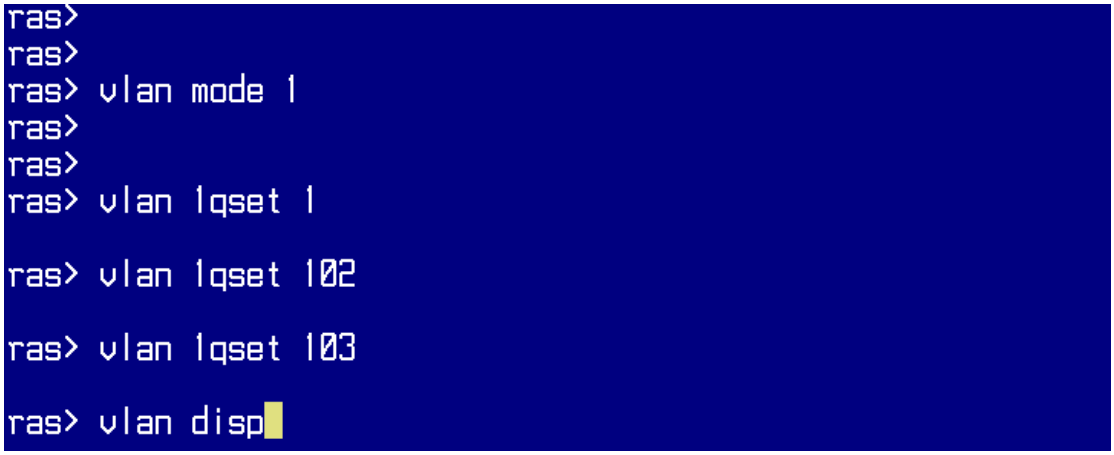
P870MH-C1 Installation

1. Connect to the device by Telnet. Access the SMT menu 24.8 and switch into CI command mode.



2. Change mode to 802.1q by entering the ‘vlan mode 1’ command. Also create 3 VLANs on P870MH-C1, VLAN 1/102/103.

After you have created 3 VLANS, check where the VLAN are located by the ‘VLAN disp’ CI command.



3. Display the configured VLANs, check the relationship between "ITEM" and the VID which we just have configured. Bind VLAN1 with port 1, VLAN 102 with port 2, Vlan 103 with port 3 without transmitting any Tagged frame. Also, add the VLAN tag (1, 102 & 103) onto the outgoing VDSL port.

```
ras>
ras> vlan lqconfig 1 U 1

ras> vlan lqconfig 1 T 5

ras> vlan lqconfig 6 U 2

ras> vlan lqconfig 6 T 5

ras> vlan lqconfig 7 U 3

ras> vlan lqconfig 7 T 5
```

4. Port 1(VLAN 1) is for Data access, Port 2(VLAN 102) is for VoIP and Port 3(VLAN 103) is for IPTV service. On Port 2 & Port 3, we can assign a higher priority (qos=High) when a traffic congestion occurs. For Port 1's traffic, we can assign the priority as 'Low' since the Internet traffic on this port is not time sensitive.

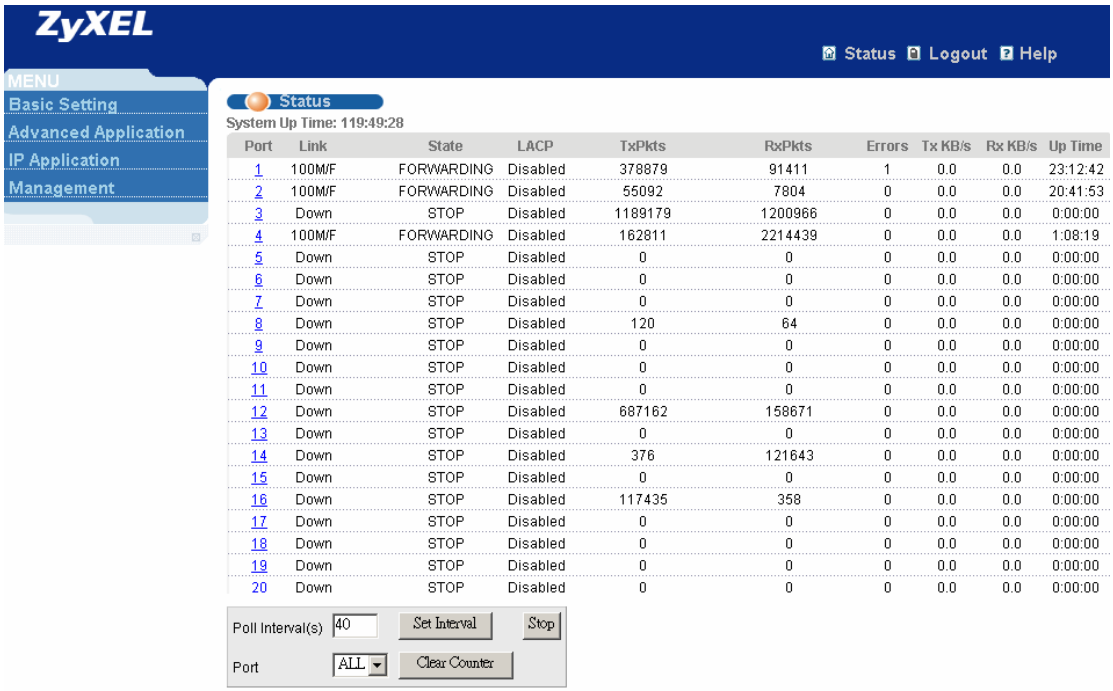
```
ras> vlan qos 1 0
ras> vlan qos 2 1
ras> vlan qos 3 1
ras>
ras> vlan save
ras>
```

5. Check whether all the settings are correct.

```
======================   802.1Q Setting   ======================
(T):TAGGING; (F):FORBIDDEN; (U):UNTAGGED;

Port ID       :    0     1     2     3     4     5
Priority      :    L     L     H     H     L     L
                 WLAN  LAN1  LAN2  LAN3  LAN4  VDSL
ITEM  VID     :
 0      0
 1      1            U                       T
 2      0
 3      0
 4      0
 5      0
 6    102                  U                 T
 7    103                        U           T

================================================================

Broadcast Storm is DISABLE
Action for UnKnown Multicast frames is FLOODING
================================================================
ras>
```

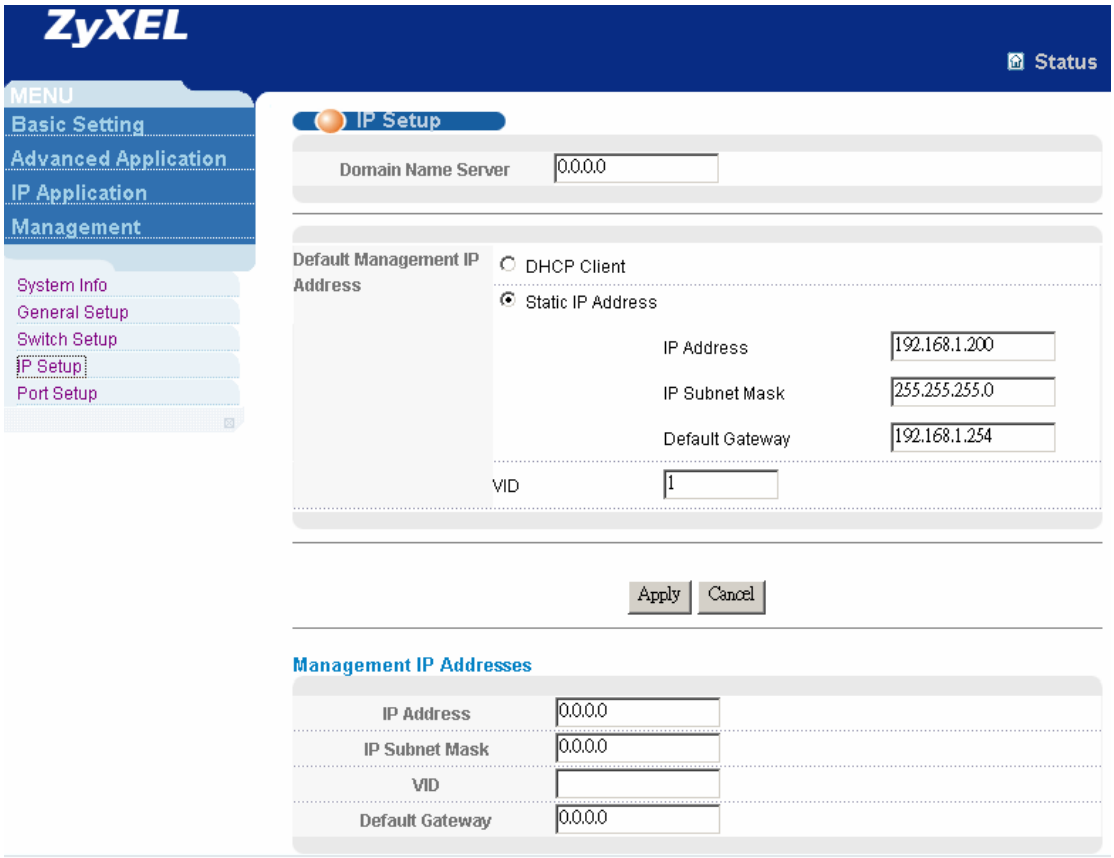
ES2024A Settings

5. Connect to IES-1248 by Web GUI. The default IP address of ES-2024A is **192.168.1.1**. Enter the default password **‘1234’** to get into the device.



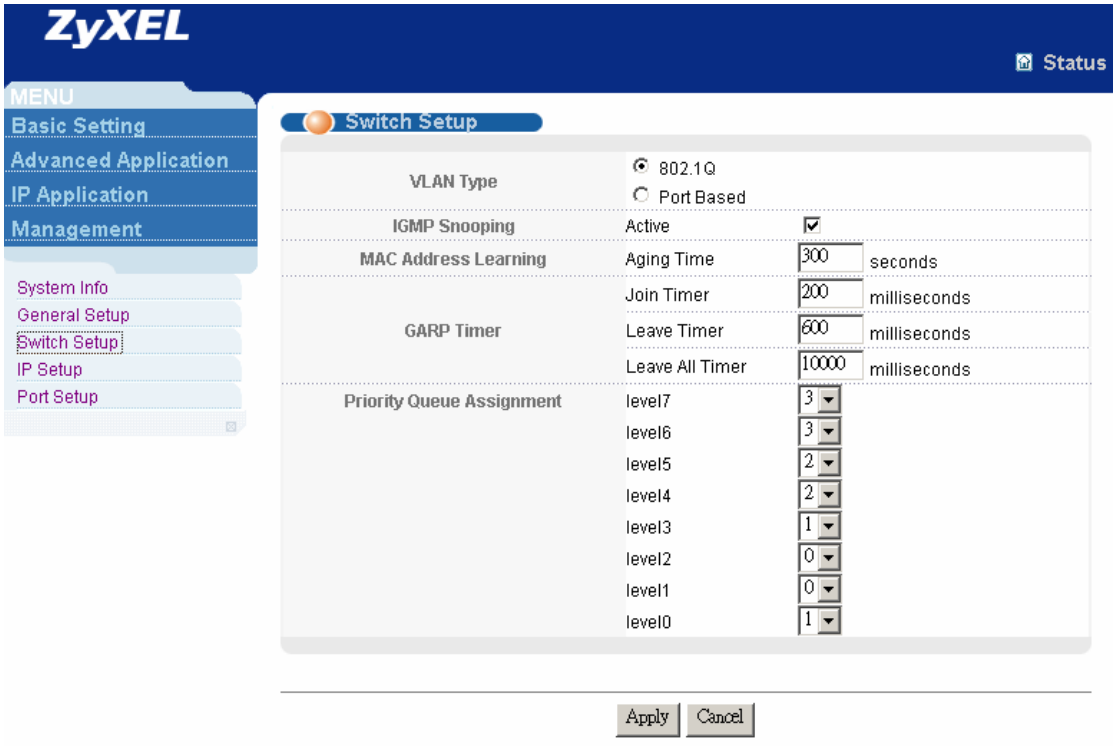
6. Set the IES-1248's IP address to '**192.168.1.200**'.

Open **Basic Setting> IP setup**. Type in the IP address **'192.168.1.100'** and its subnet mask **'255.255.255.0'.**



7. Enable the IGMP Snooping service in order to allow the Multicast traffic pass through the ES-2024A.

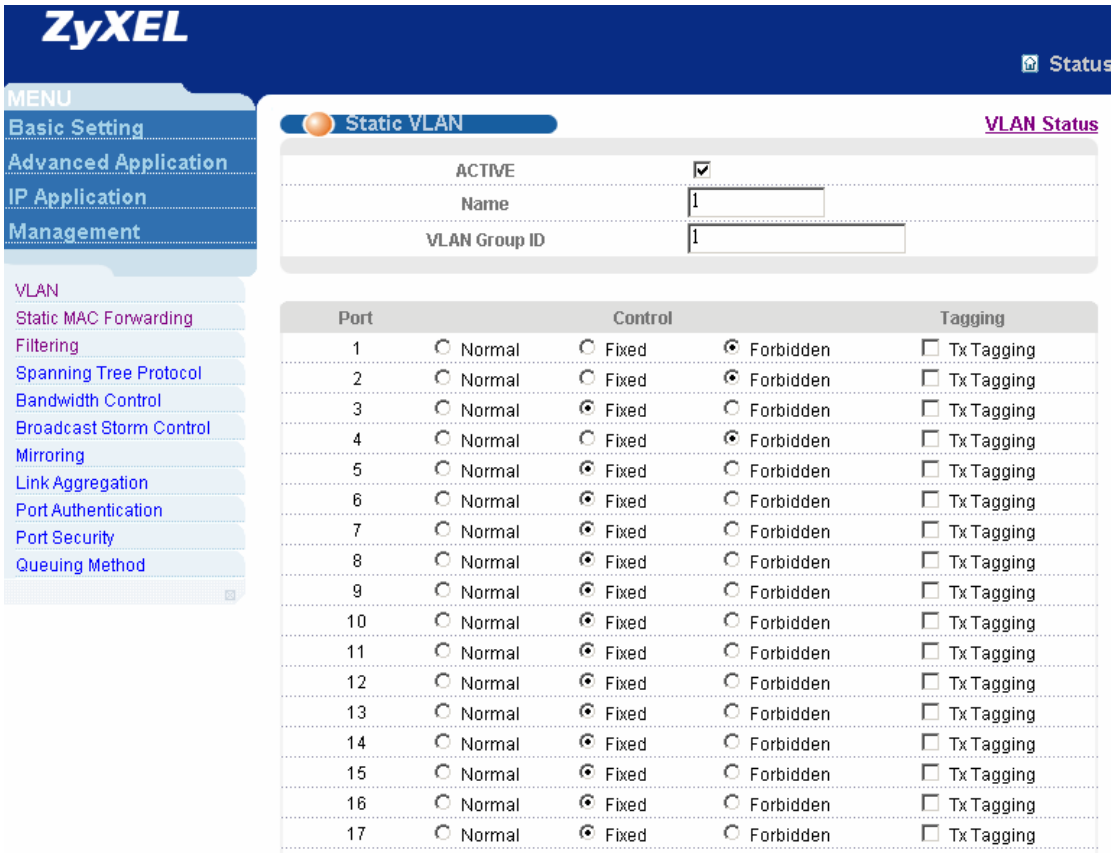
Click Basic Setting> Switch Setup. Then click on the **Active checking Box** of **IGMP Snooping.**



8. Create 3 VLANs, VLAN 1 for Data access (FTP server) connected to Ethernet port 3, VLAN 102 for Voice (SIP server & ATA) connected to the Ethernet port 1 & 2 and finally VLAN 103 for the Video server connected to the Ethernet Port 4. The Uplink port is 24.

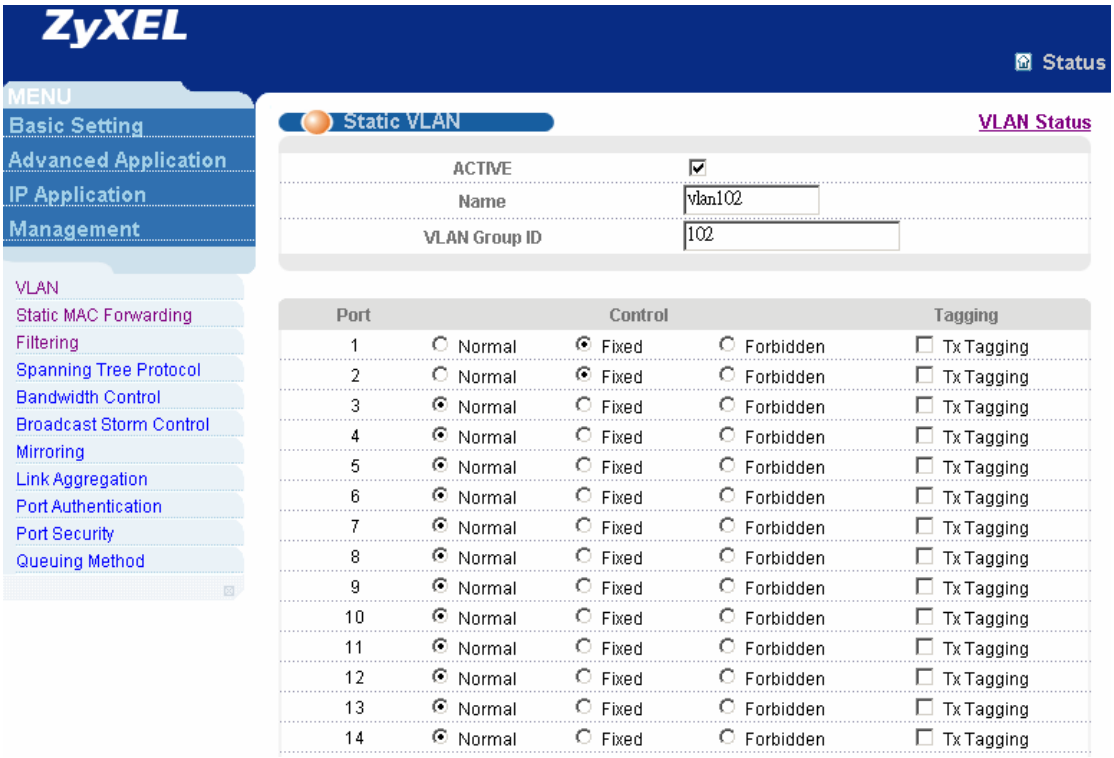
d. Create VLAN 1

Click **Advanced Application> VLAN> Static VLAN Setting** and then click on **VID 1**. Check the **Active Box** then **check** the Tx Tagging Box on **Port 24** (for the other ports have this option unchecked) and switch **Ports 1, 2 and 4** to the status '**Forbidden'**. Click **Add** to finish the VLAN 1 configuration.



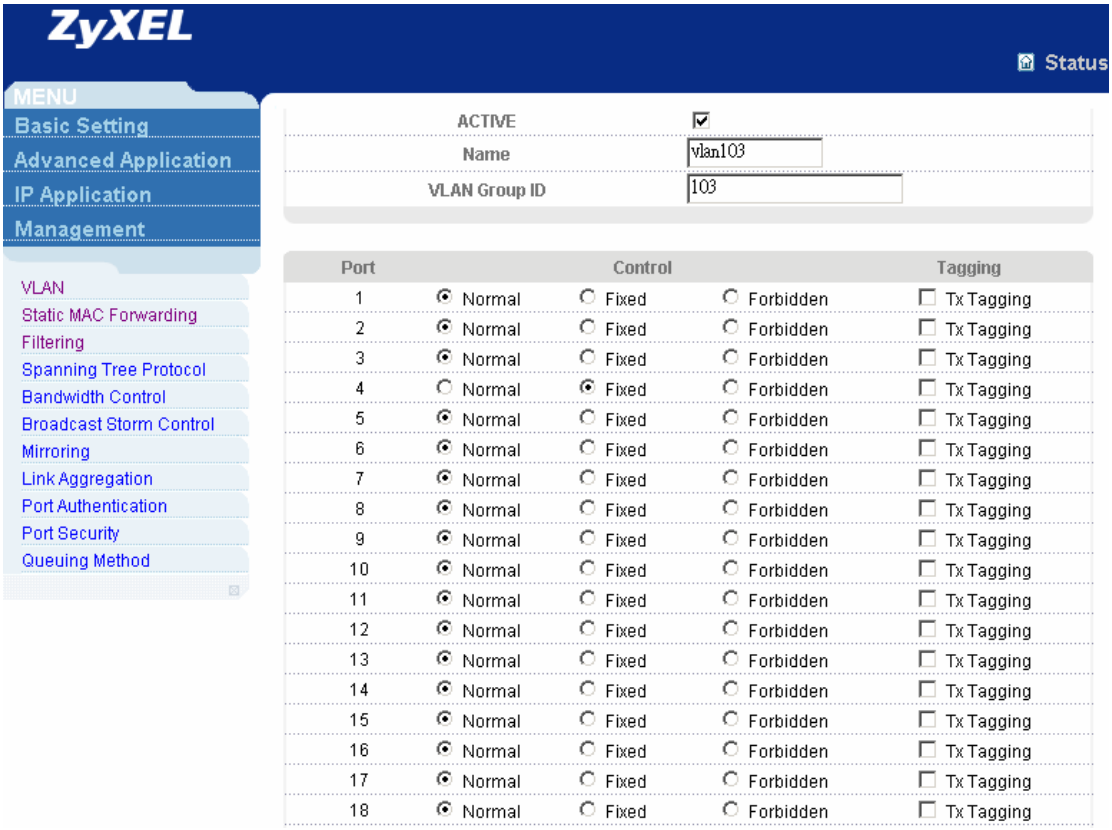
e. Create VLAN 102

Click **Advanced Application> VLAN> Static VLAN Setting** then check the **Active Box**, enter a name for VLAN as well as VLAN ID102. Then **check** the Tx Tagging Box on **Port 24** (for the other ports, make this option unchecked) and switch **Ports 1, 2 and 24** to status '**Fixed'**. Click **Add** to finish the VLAN 102 configuration.



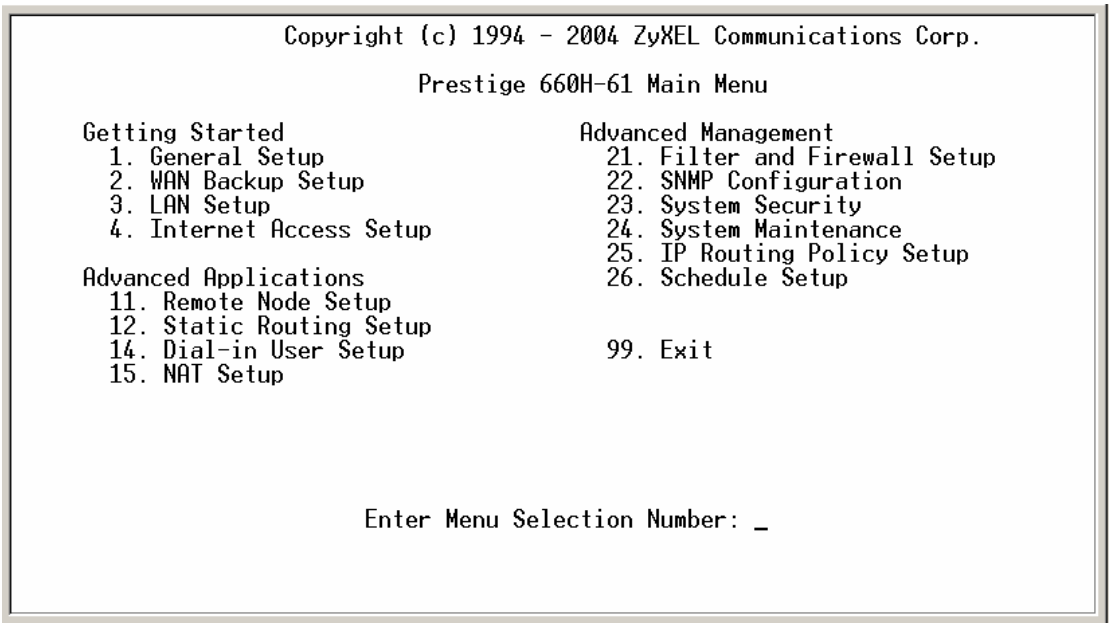
f. Create VLAN 103

Click **Advanced Application> VLAN> Static VLAN Setting** then check the **Active Box**, enter a name for VLAN as well as VLAN ID 103. Then **check** the Tx Tagging Box on **Port 24** (for the other ports make this option unchecked) and switch **Ports 4 and 24** to status '**Fixed'**. Click **Add** to finish the VLAN 103 configuration.



P660H settings

9. Connect to the P660HW-61 using Telnet. The default IP address of P660H-61 is 192.168.1.1. Enter the default password '1234' to access the device.



10. Disable the VC hunt mechanism and Reboot the device.

Go to SMT menu 24 and 8 and switch to the Command Interface Mode. Type **'wan atm vc active no'** and then **'wan atm vc save'** to save the settings. Reboot the device for the changes to take effect.

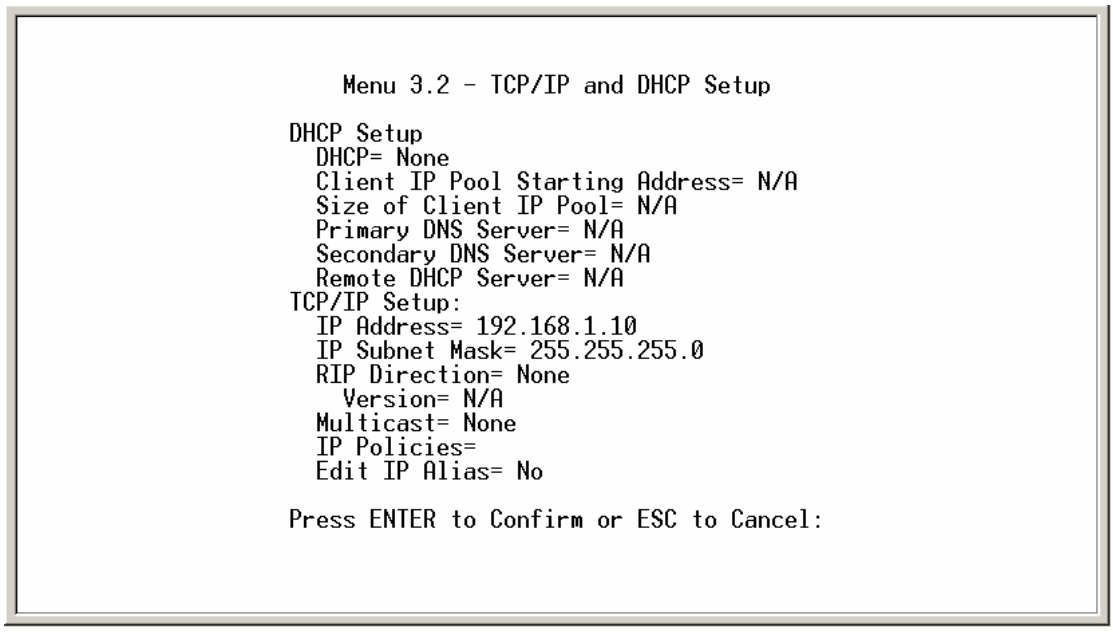
```
                        Menu 24 - System Maintenance

                      1.  System Status
                      2.  System Information and Console Port Speed
                      3.  Log and Trace
                      4.  Diagnostic
                      5.  Backup Configuration
                      6.  Restore Configuration
                      7.  Upload Firmware
                      8.  Command Interpreter Mode
                      9.  Call Control
                      10. Time and Date Setting
                      11. Remote Management



                        Enter Menu Selection Number: 8

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
111> wan atm vc active no
111> wan atm vc save_
```

3. There will have three bridge PVCs on the P660H-61. Configure the system to support the Bridge mode.

Access the SMT menu 1, type in the System Name and e**nable** the **Bridge=Yes.**

```
                        Menu 1 - General Setup

                System Name= P660
                Location=
                Contact Person's Name=
                Domain Name=
                Edit Dynamic DNS= No

                Route IP= No
                Bridge= Yes




                Press ENTER to Confirm or ESC to Cancel:
```

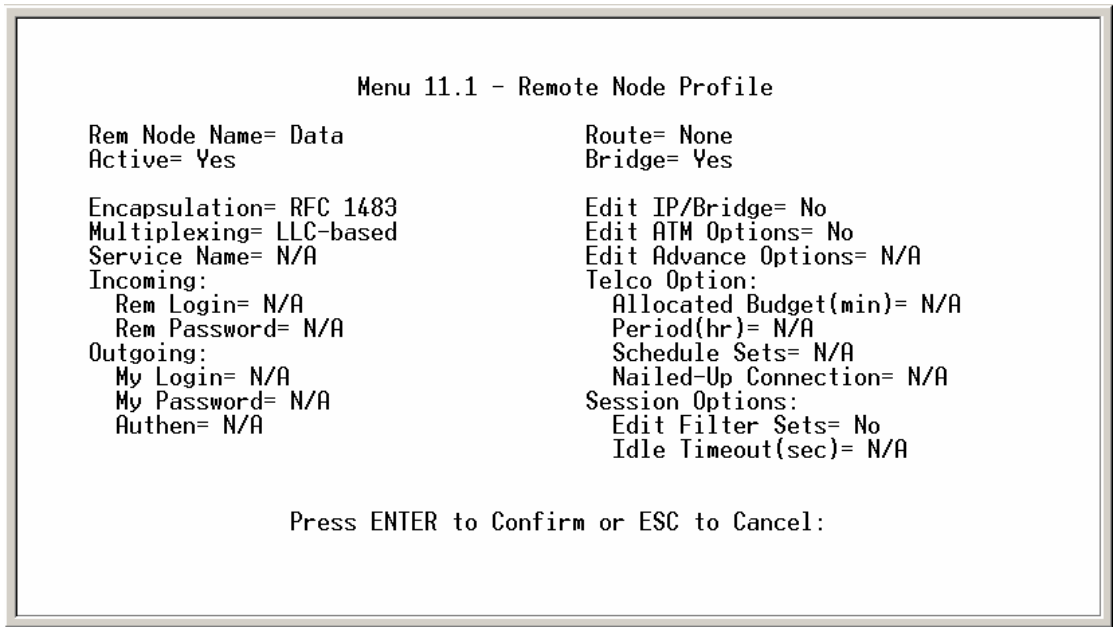
4. Change the P660H-61's IP address to **192.168.1.10** and **disable** the DHCP server function in SMT menu 3.2.



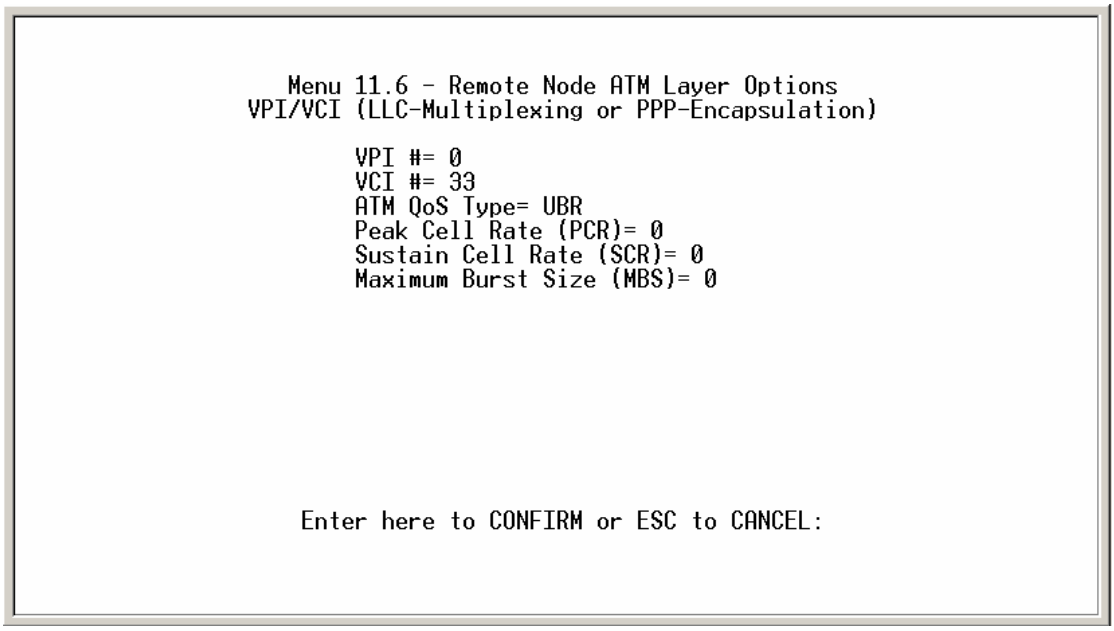
5. Create 3 PVCs in the P660H for the Triple-play application (Data, Voice and Video)

a. Create a PVC for the Data access (Internet access)

Get into the SMT menu 11.1 and switch the **Rem Node Name=Data, Active=Yes, Encapsulation= RFC 1483, Multiplexing= LLC-based** and **Route=None Bridge=Yes.**

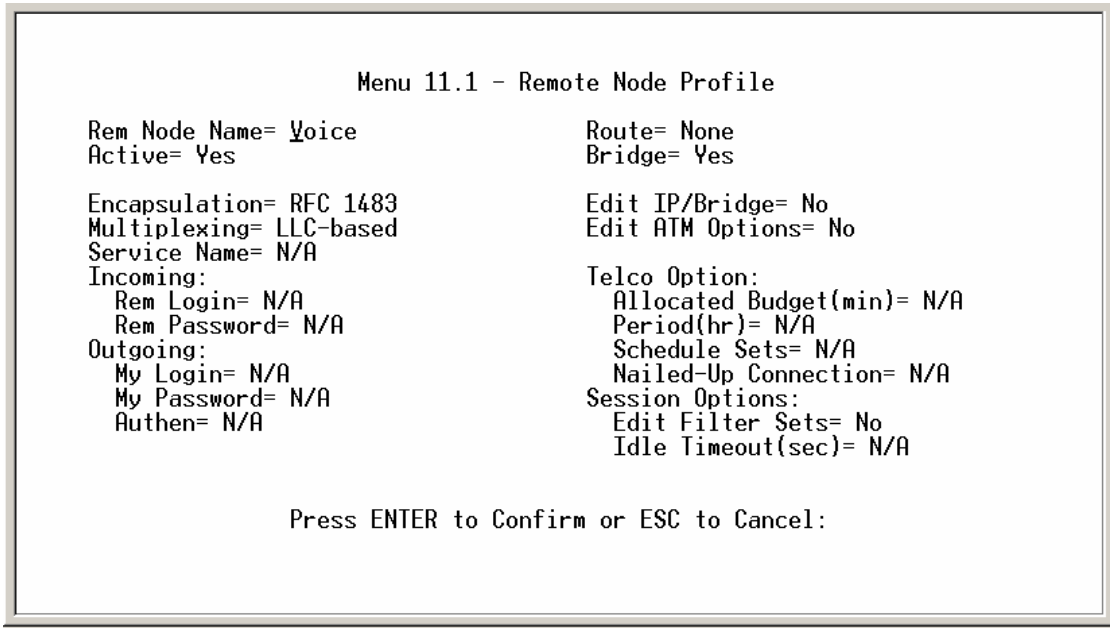


Select the **ATM options=Yes**, **VPI/VCI=0/33** then press ‘Enter’ to apply the changes.



b. Create a PVC for the Voice channel

Get into the SMT menu 11.2, select the **Rem Node Name=Voice , Active=Yes, Encapsulation= RFC 1483, Multiplexing= LLC-based and Route=None Bridge=Yes.**



Select the **ATM options=Yes**, **VPI/VCI=0/34** then press 'Enter' to apply the changes.

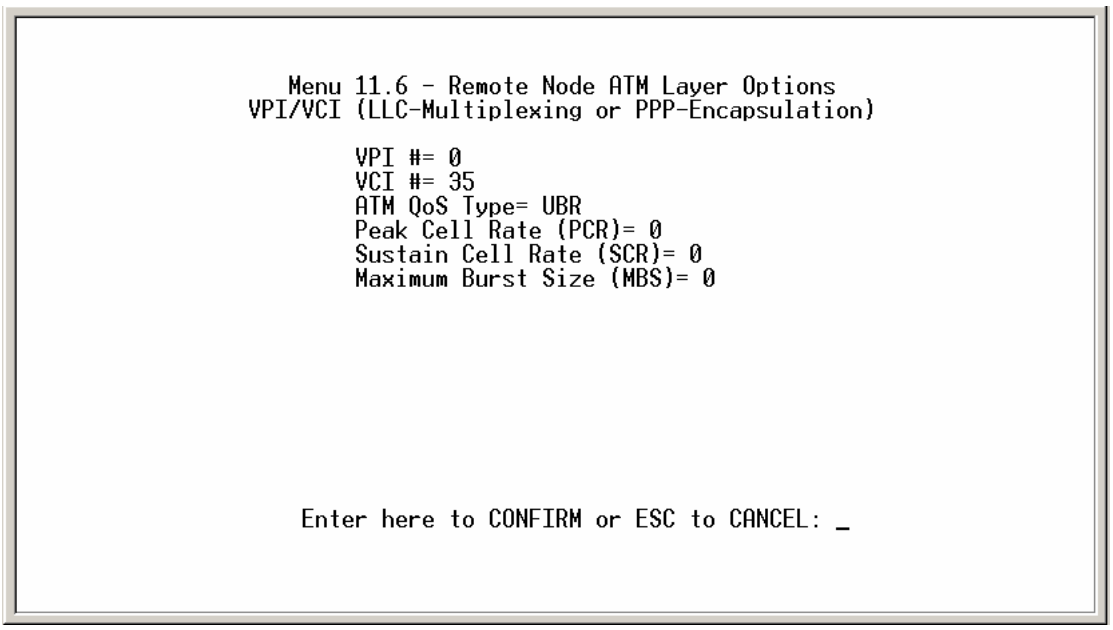
```
                Menu 11.6 - Remote Node ATM Layer Options
          VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

                VPI #= 0
                VCI #= 34
                ATM QoS Type= UBR
                Peak Cell Rate (PCR)= 0
                Sustain Cell Rate (SCR)= 0
                Maximum Burst Size (MBS)= 0




                   Enter here to CONFIRM or ESC to CANCEL: _
```

c. Create a PVC for the Video channel

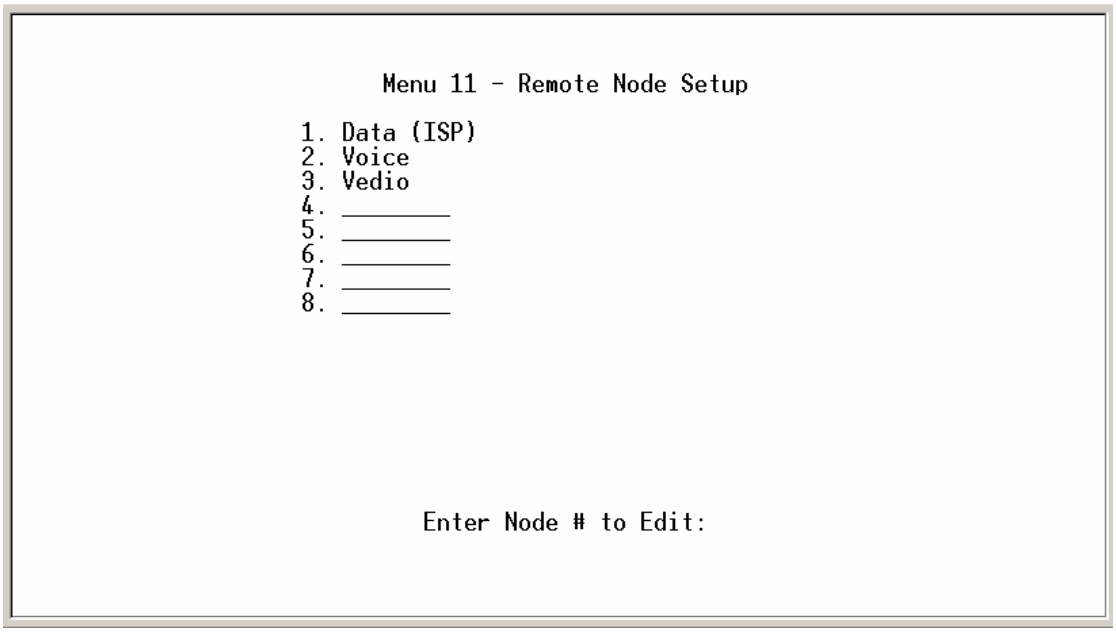
Access the SMT menu 11.3 and select the **Rem Node Name=Video, Active=Yes, Encapsulation= RFC 1483, Multiplexing= LLC-based and Route=None Bridge=Yes.**

```
                        Menu 11.1 - Remote Node Profile

Rem Node Name= Vedio                    Route= None
Active= Yes                             Bridge= Yes

Encapsulation= RFC 1483                 Edit IP/Bridge= No
Multiplexing= LLC-based                 Edit ATM Options= No
Service Name= N/A
Incoming:                               Telco Option:
  Rem Login= N/A                          Allocated Budget(min)= N/A
  Rem Password= N/A                       Period(hr)= N/A
Outgoing:                                 Schedule Sets= N/A
  My Login= N/A                           Nailed-Up Connection= N/A
  My Password= N/A                      Session Options:
  Authen= N/A                             Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A


                    Press ENTER to Confirm or ESC to Cancel:
```

Select the **ATM options=Yes**, **VPI/VCI=0/35** then press ‘Enter’ to apply the changes.



3 PVCs will be created as on the following figure:



6. Map 3 PVC to specific Ethernet port of the P660H-61.

Access SMT menu 24.8

Type ‘sys triple port set 1 1’ to map the Ethernet port 1 to PVC 1(Data)

Type ‘sys triple port set 2 2’ to map the Ethernet port 2 to PVC 2(Voice)

Type ‘sys triple port set 3 3’ to map the Ethernet port 3 to PVC 3(Video)

```
                        Enter Menu Selection Number: 8


Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
P660>
P660>
P660> sys triple port set 1 1
Port Base Policy Configuration have been configured as follow. If you need
save and apply, Please execute CI cmds: sys tripleplay portbase save
EPort  --  PVC
  1    --   1
  2    --   2
  3    --   3
  4    --   disable
P660> sys triple port set 2 2
Port Base Policy Configuration have been configured as follow. If you need
save and apply, Please execute CI cmds: sys tripleplay portbase save
EPort  --  PVC
  1    --   1
  2    --   2
  3    --   3
  4    --   disable
P660> sys triple port set 3 3_
```

7. Check whether the ADSL physical layer is UP in the SMT menu 24.1. and if the PVC counter is running.

```
                    Menu 24.1 - System Maintenance - Status          19:34:09
                                                              Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up Time
 1-1483  Up          376905      737167           0       0       0    17:51:41
 2-1483  Up            1846        2512           0       0       0    17:51:41
 3-1483  Up            3865      559943           0       0       0    17:51:41
 4       N/A              0           0           0       0       0     0:00:00
 5       N/A              0           0           0       0       0     0:00:00
 6       N/A              0           0           0       0       0     0:00:00
 7       N/A              0           0           0       0       0     0:00:00
 8       N/A              0           0           0       0       0     0:00:00

My WAN IP (from ISP): 192.168.1.10

    Ethernet:                                WAN:
      Status:                Tx Pkts: 1301745    Line Status: Up
      Collisions: 0          Rx Pkts: 386079     Upstream Speed:   511 kbps
    CPU Load =    2.82%                          Downstream Speed:  6141 kbps
                                  Press Command:
                     COMMANDS: 1-Reset Counters  ESC-Exit
```