P-870HW-51a v2

802.11bg Wireless VDSL 4 port gateway

Support Notes

Firmware Version 1.0
January 2009
Edition 1.0

ZyXEL
Unleash Networking Power

INDEX

General Application Notes

Why use P-870HW-51aV2?

- **High Speed Internet Access**

  The P-870HW-51aV2 is a VDSL gateway supporting the downstream transmission up to 100Mbps and upstream transmission up to 50 Mbps.

- **Quality of Service (QoS)**

  The P-870HW-51aV2 with Quality of Service features ensures that the Triple Play Service keeps the high quality delivery in VDSL high speed Internet access.

- **PPP over Ethernet**

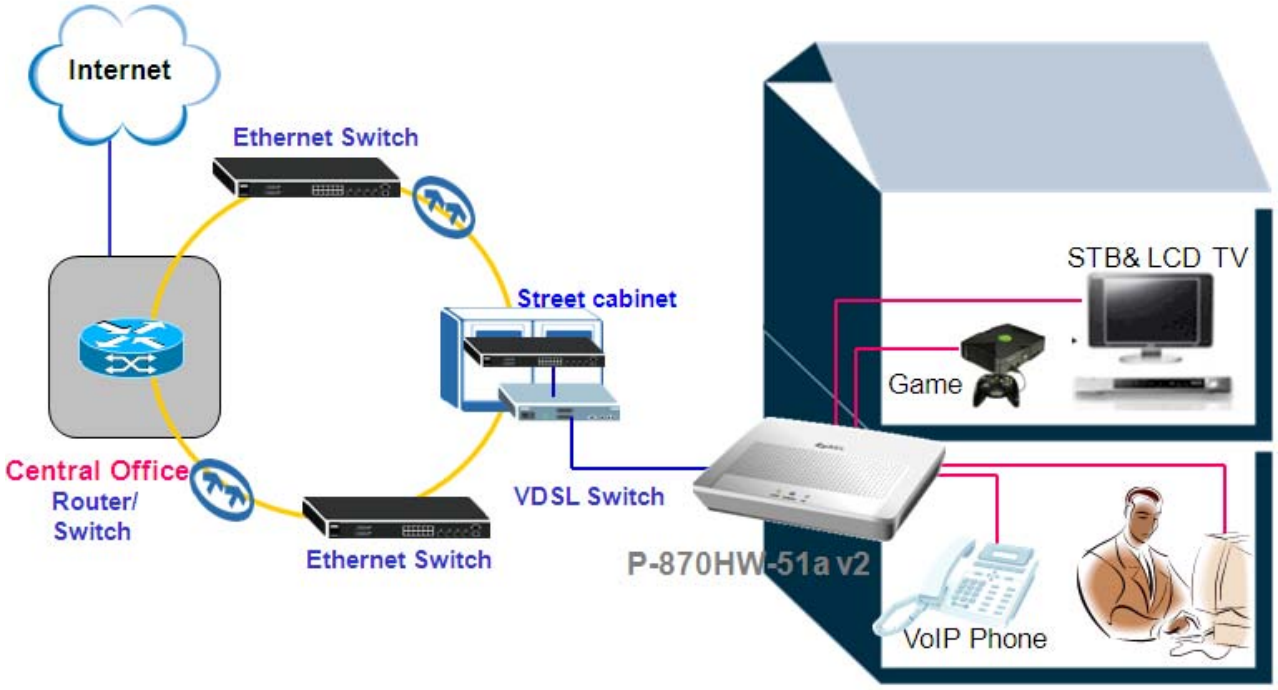
  Since the PPPoE will benefit both Telco and ISP, the P-870H/HW-51 V2 shall implement this feature and be tested well with the PPPoE servers.

- **Multi-NAT**

  The NAT provides system administrators an easy solution to create a private IP network for the security and IP management. Powered by NAT technology, the P-870HW-51aV2 supports the complete NAT mapping and most popular Internet multimedia applications, such as NetMeeting, MSN Messenger, Skype, ICQ, IPTV, QuickTime, Real Player (RSP/RTSP), VoIP SIP ALG, etc.

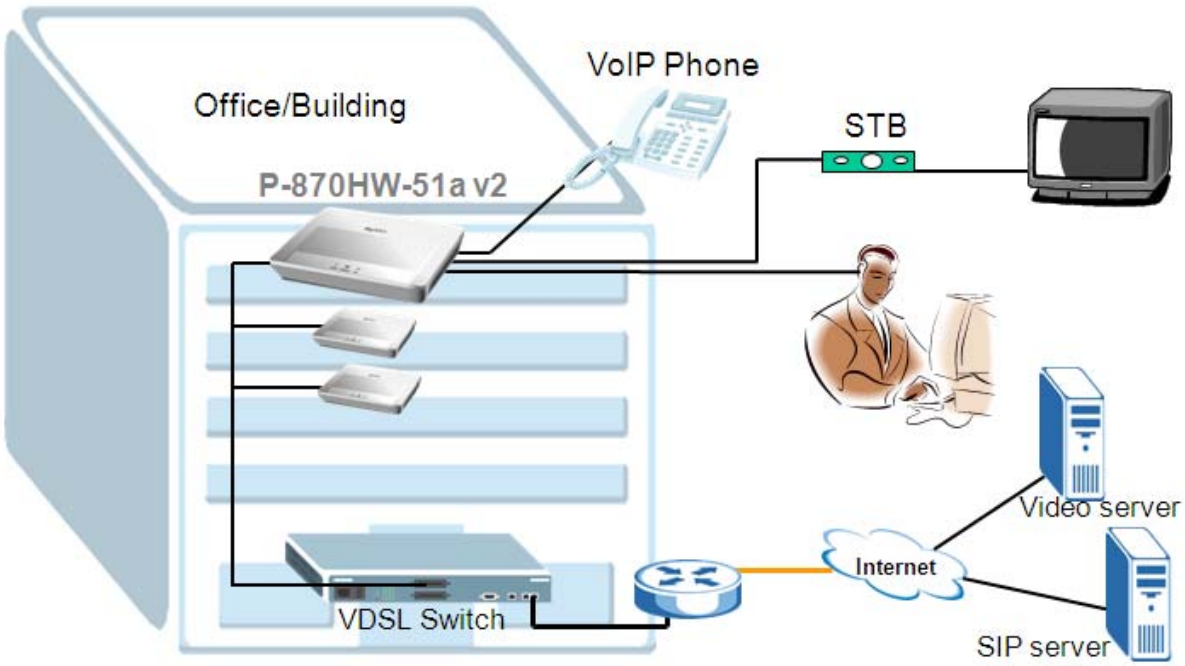
Application Scenario

FTTx - FTTC Solution



A typical scenario is used with P-870HW-51aV2 in a FTTC (Fiber to the Curb) solution. The P-870HW-51aV2 serves as a home gateway, providing the high speed INTERNET service and High Quality IPTV service. The COE (VDSL switch) is located in a street cabinet, providing a high speed service within a 700 feet range, assuring the bandwidth reaching up to 100/50Mbps (Downstream/Upstream) at maximum.

FTTx – FTTB Solution



An often seen scenario is used with P-870HW-51aV2 in a FTTB (Fiber to the Building) solution. The P-870HW-51aV2 serves as a home gateway, providing the high speed INTERNET service, High Quality IPTV service and VoIP service. The COE (VDSL switch) is located inside the cabinet of building, providing a high speed service covering the whole apartment, assuring the bandwidth reaching up to 100/50Mbps (Downstream/Upstream) at maximum.

Prologue

- Before we begin.

The device is shipped with the following factory defaults:

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.1.33
3. Default username/password = 1234/1234

- Setting up the PC (Windows OS)

1. Ethernet Connection

- All PCs must have an Ethernet adapter card installed

2. TCP/IP Installation

You must first install the TCP/IP software on each PC before you can use it for the Internet access. If you have already installed the TCP/IP, go to the next section to configure it; otherwise, follow these steps to install:

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** windows, select **Protocol** and click **Add**.
- In the **Select Network Protocol** windows, select **Microsoft** from the manufacturers, then select **TCP/IP** from the **Network Protocols** and click **OK**.

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

- In the **Control Panel/Network** window, click the **TCP/IP** entry to select it and click **Properties** button.
- In the **TCP/IP** Properties window, select **obtain an IP address automatically**.

Note: Do not assign the arbitrary IP address and subnet mask to your PCs; otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.

- Click the **Gateway** tab. Highlight any installed gateways and click the **Remove** button until there are none listed.
- Click the **DNS Configuration** tab and select **Disable DNS**.
- Click **OK** to save and close the **TCP/IP** properties window.
- Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the PC. Make sure that your Device is powered on before answering “Yes” to the prompt. Repeat the aforementioned steps for each Windows PC on your network.

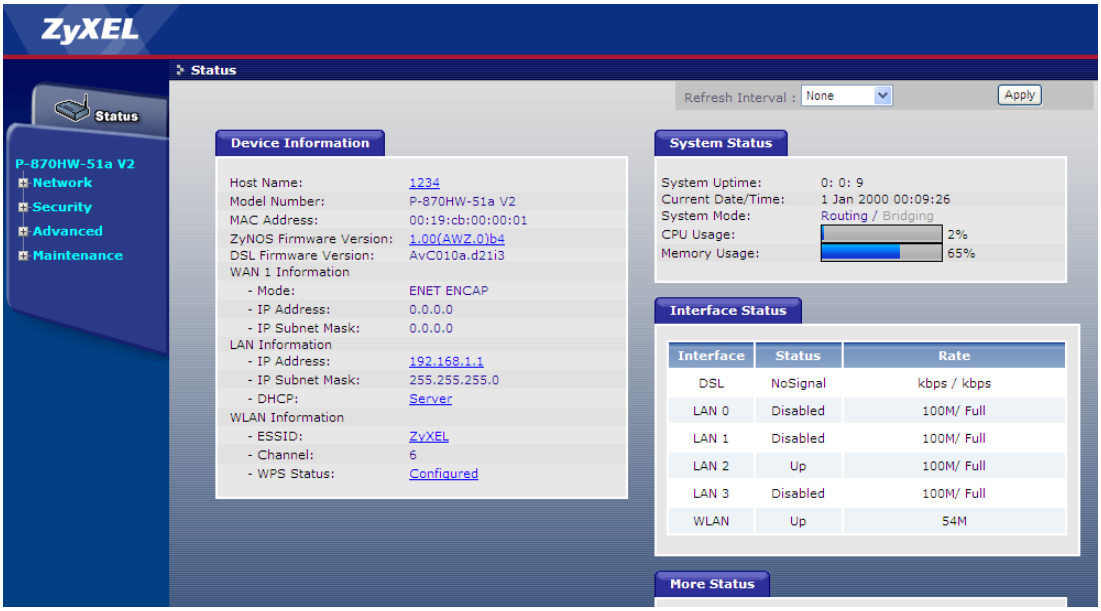
Access Application Notes

Web GUI

The following procedure is for the most typical usage of device using a Browser. The device supports the embedded Web server that allows you to use Web browser to configure it. Before configuring the router using Browser, please be sure there is no Telnet or Console login.

a. Login the P-870HW-51a v2 via Web GUI.

1. Set up your PC/NB IP address to be a DHCP client.
2. Connect to a LAN port of P-870HW-51a v2 via RJ45 Ethernet cable and open your IE browser.
3. The default IP of P-870HW-51a v2 is 192.168.1.1 username/password = 1234/1234.

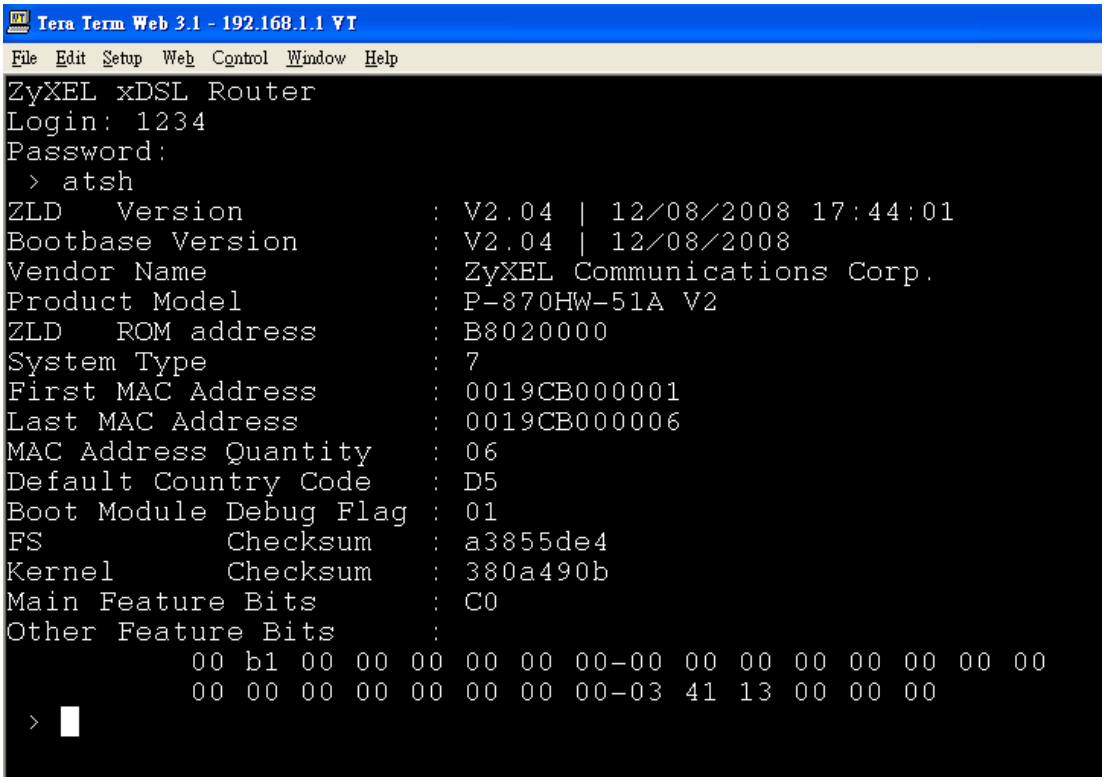


Telnet

Telnet is also a common way to configure the device, but we have to use CI commands which may not be quick-to-learn. The list of the commonly used CI commands is provided at the end of this document.

b. Login the P-870HW-51a v2 via Telnet.

1. Set up your PC/NB IP address to be a DHCP client.
2. Connect to a LAN port of P-870HW-51a v2 via RJ45 Ethernet cable and open your Hyper Terminal software (capable of using TELNET).
3. The default IP of P-870HW-51a v2 is 192.168.1.1 username/password = 1234/1234.
4. Type the command line “atsh” to display the basic information of device.



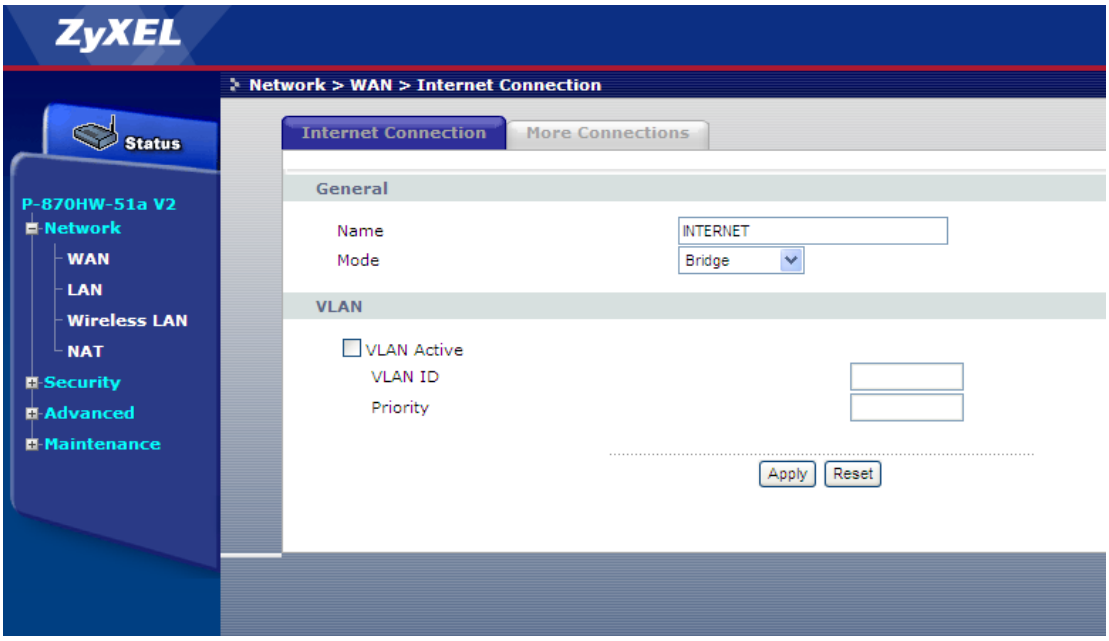
Internet Connection

Bridge Mode

Scenario:
The P-870HW-51a v2 is a CPE bridge.

a. Bridge Mode

1. Go to **Network > WAN > Internet Connection.**
2. Enter the **Name**, e.g. “Internet”.
3. Select the **Mode** to be “Bridge”.
4. Click **Apply.**

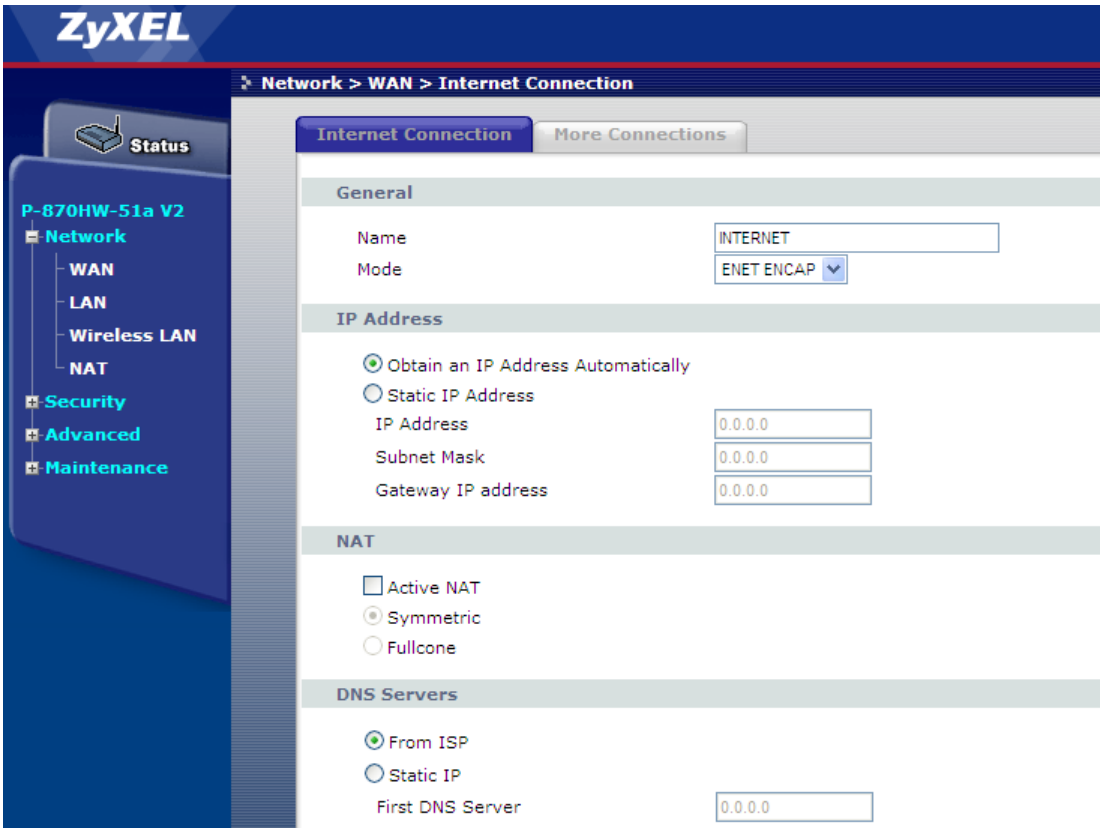


IPoE Mode

Scenario:
The P-870HW-51a v2 is a DHCP client in routing mode.

b. IPoE Mode

1. Go to **Network > WAN > Internet Connection.**
2. Enter the **Name**, e.g. “Internet”.
3. Select the **Mode** to be “ENET ENCAP”.
4. Select **Obtain an IP Address Automatically.**
5. Click **Apply.**

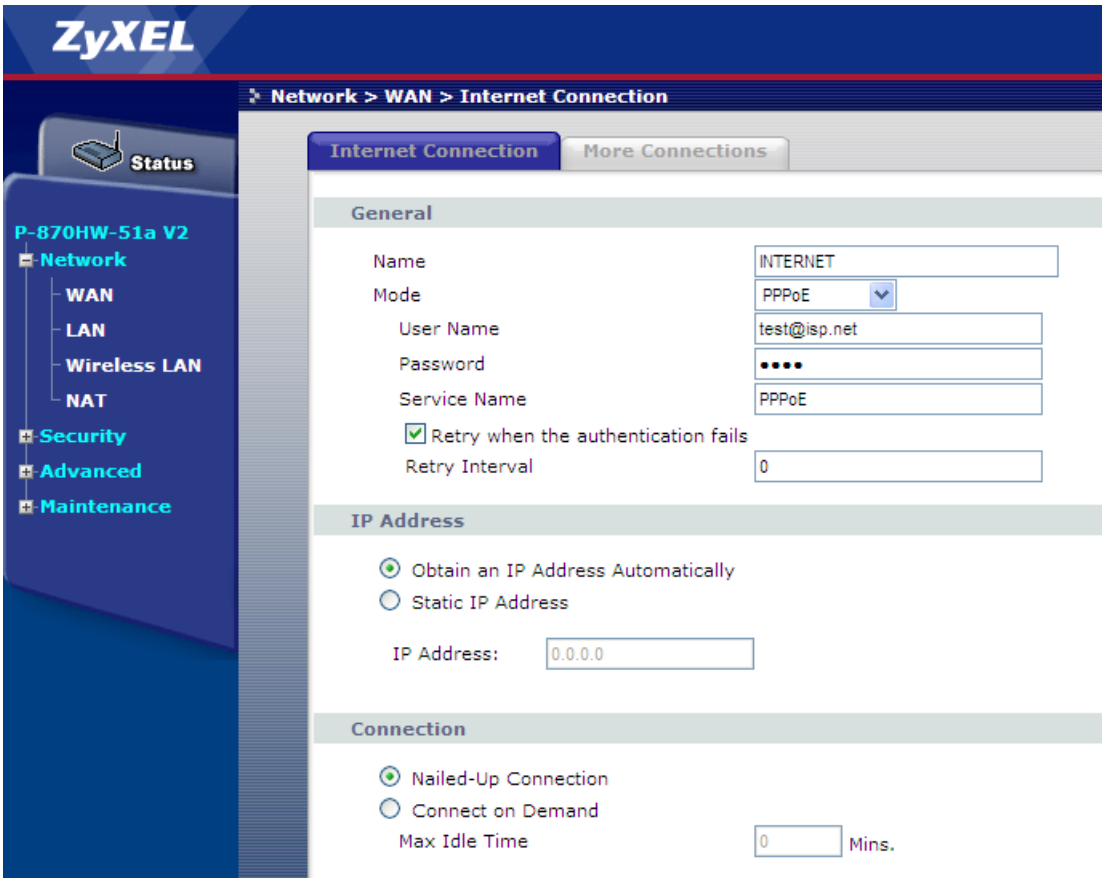


PPPoE Mode

Scenario:
The P-870HW-51a v2 is a PPPoE client.

c. PPPoE Mode

1. Go to **Network > WAN > Internet Connection.**
2. Enter the **Name**, e.g. “Internet”.
3. Select the **Mode** to be “PPPoE”.
4. Enter the **User Name**, e.g. “test@isp.net”.
5. Enter the **Password**, e.g. “1234”.
6. Enter the **Service Name**, e.g. “PPPoE”.
7. Check the **Retry when the authentication fails** box.
8. Enter the **Retry Interval** (in seconds), e.g. “0”.
9. Click **Apply.**

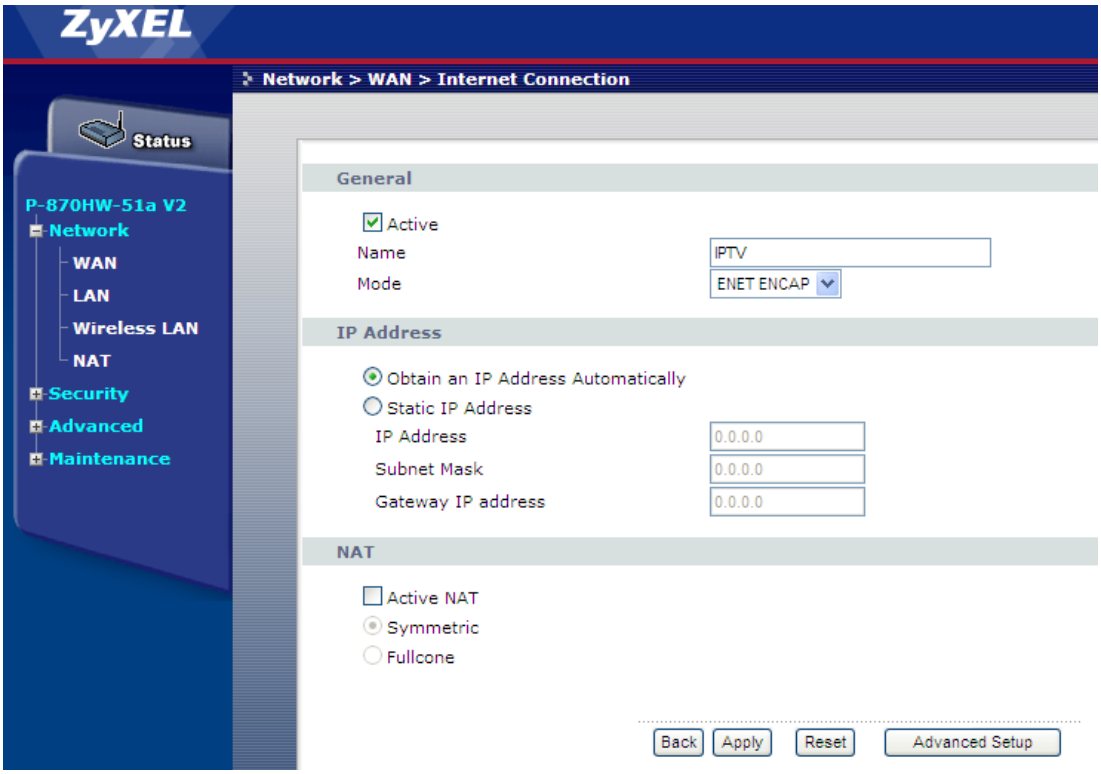


More than One Connection

Scenario:
The P-870HW-51a v2 has more than one remote node (WAN Interface). In this case, the second WAN interface is using the “Ethernet Encapsulation” as its format for its transmission to the Central Office.

d. More than one connection

1. Go to **Network > WAN > Internet Connection.**
2. Click A**dd.**
3. Select **Active.**
4. Enter the **Name**, e.g. “IPTV”.
5. Select the **Mode** to be “ENET ENCAP”.
6. Select **Obtain an IP Address Automatically.**
7. Click **Apply.**



IP Multicast

IP Multicast Introduction

- What is the IP Multicast?

Traditionally, the IP packets are transmitted in two ways: unicast or broadcast. Multicast is a third way to deliver the IP packets to a group of hosts. Host groups are identified by the class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

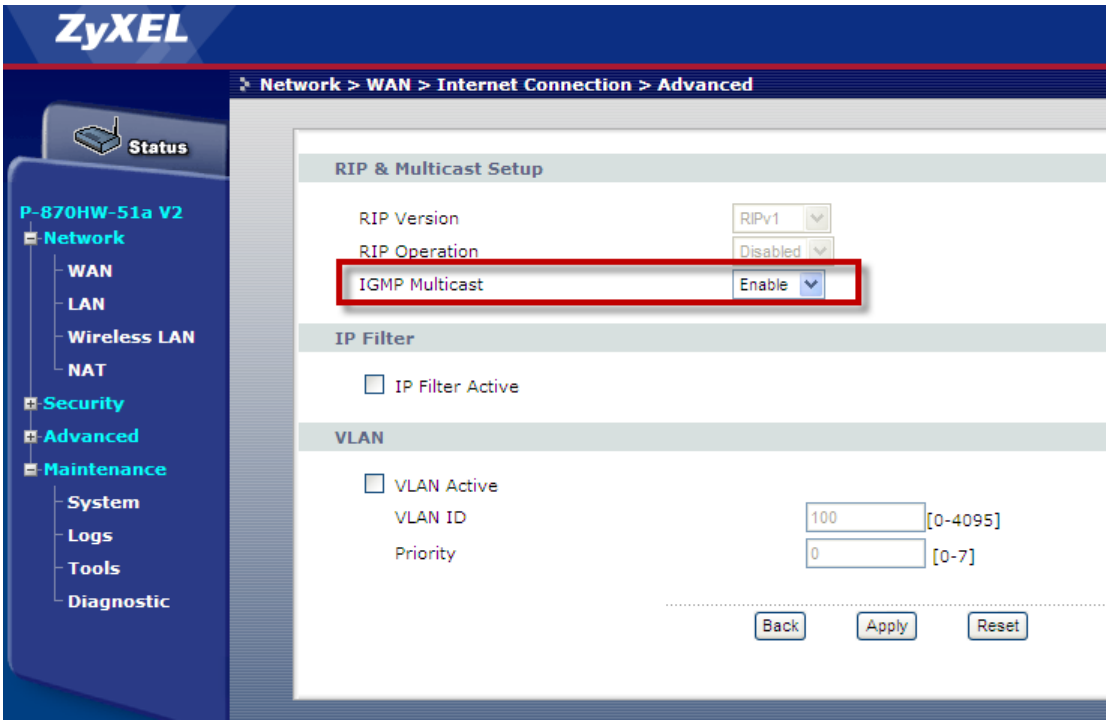
The IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (See RFC2236). The IP hosts use the IGMP to report their multicast group membership to any immediate-neighbor multicast routers, so the multicast routers can decide if a multicast packet needs to be forwarded. At the start-up, the Prestige queries all directly connect networks to gather group membership.

After that, the CPE updates the information by periodic queries. The device implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on the Ethernet and remote nodes.

IP Multicast Configuration

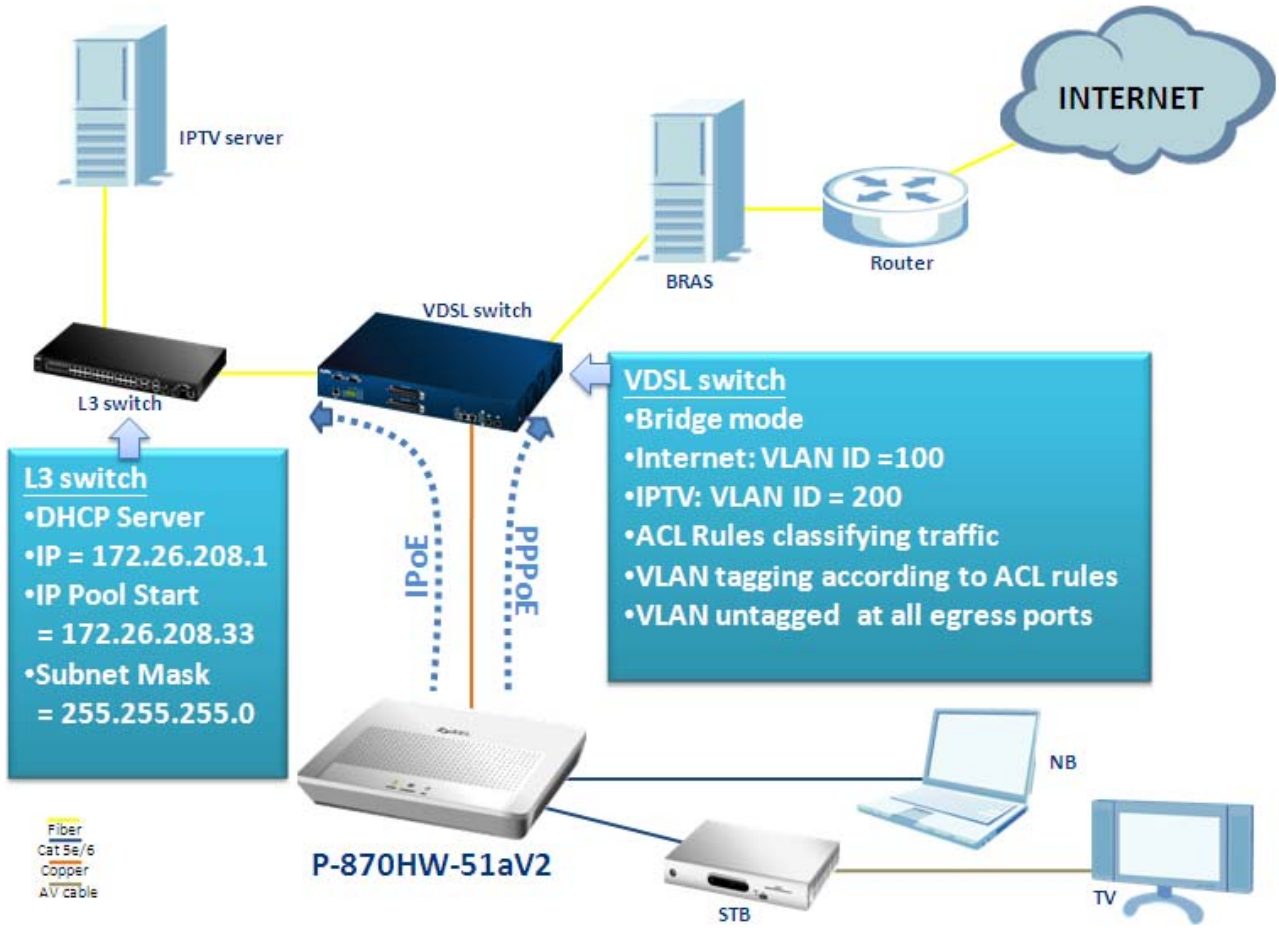
a. IP Multicast

1. Go to **Network > WAN > Internet Connection > Advanced Setup**
2. Select “Enable” for **IGMP Multicast.**
3. Click **Apply.**



Protocol Based Scenario

Environment

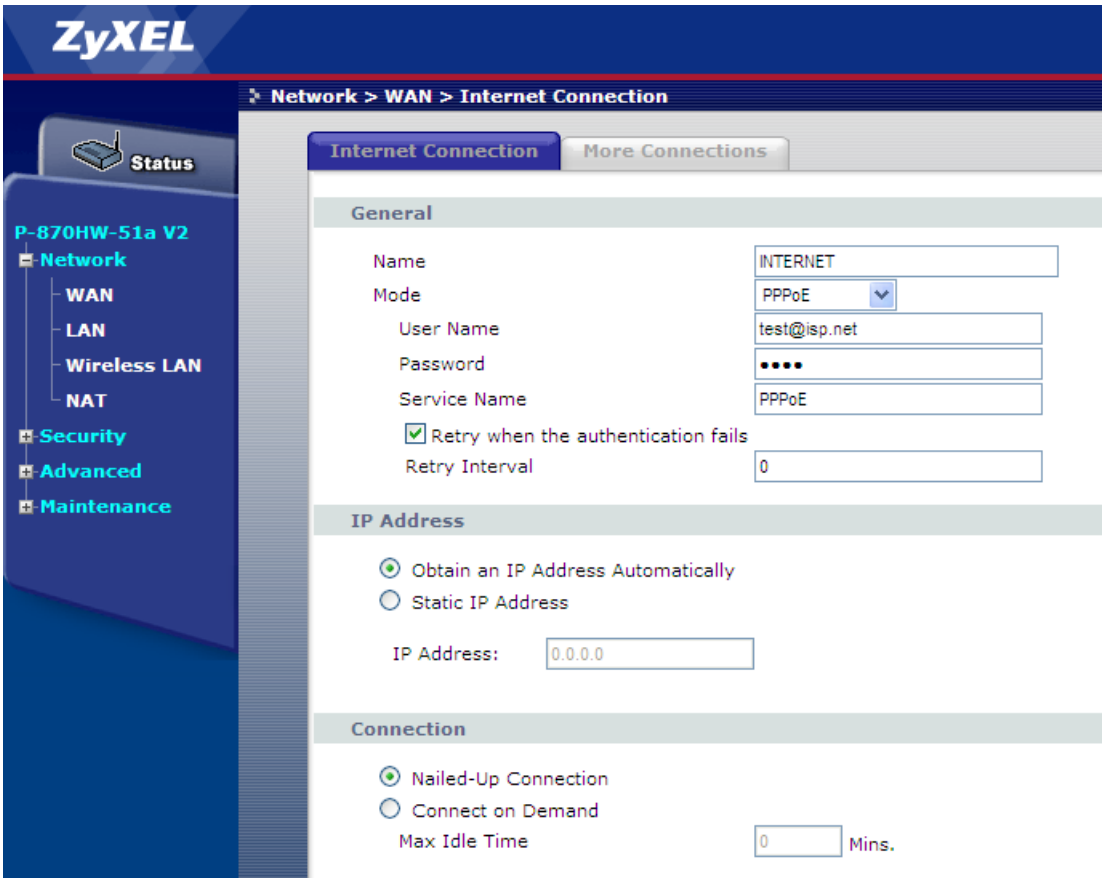


The Network structure of Central Office depends on the deployment of different ISP (Internet Service Provider) in different environments in different countries. One of the commonly known methods for separating different types of traffic is by classifying their transmitting protocols. In the case of the aforementioned diagram, the INTERNET traffic is encapsulated in the PPPoE and the IPTV traffic is encapsulated in the IPoE. The COE (VDSL switch) has the ability to distinguish those 2 traffics and assign the dedicated ACL rules to them. So, how should we configure the P-870HW-51aV2 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

WAN Configuration

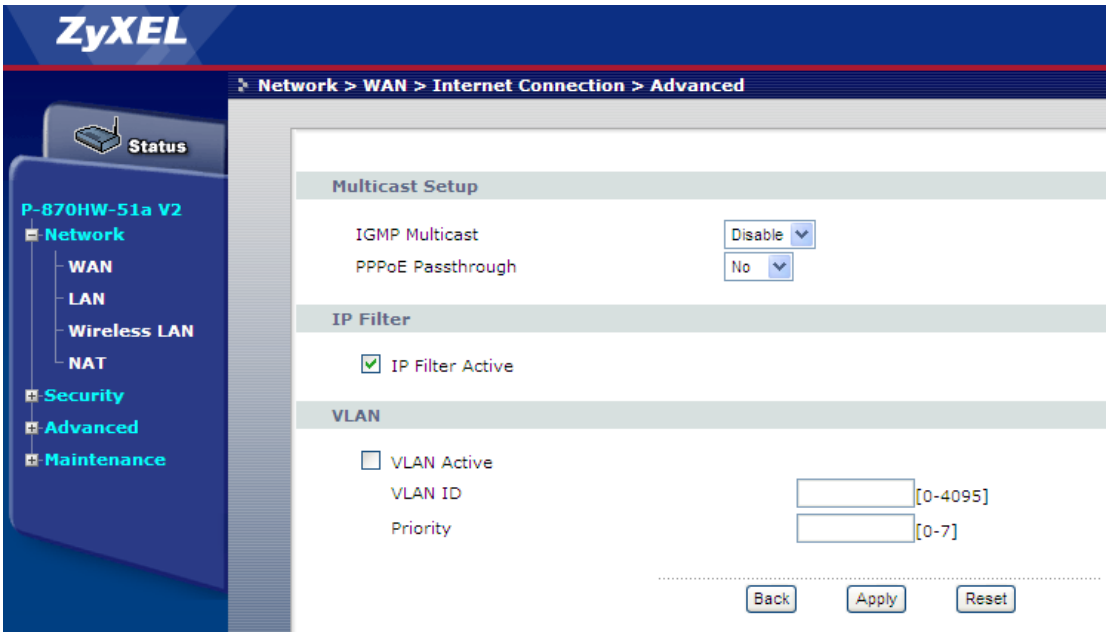
a. INTERNET Service

1. Go to **Network > WAN > Internet Connection.**
2. Enter the **Name**, e.g. “Internet”.
3. Select the **Mode** to be “PPPoE”.
4. Enter the **User Name**, e.g. “test@isp.net”.
5. Enter the **Password**, e.g. “1234”.
6. Enter the **Service Name**, e.g. “PPPoE”.
7. Check the **Retry when the authentication fails** box.
8. Enter the **Retry Interval** (in seconds), e.g. “0”.
9. Click **Apply.**



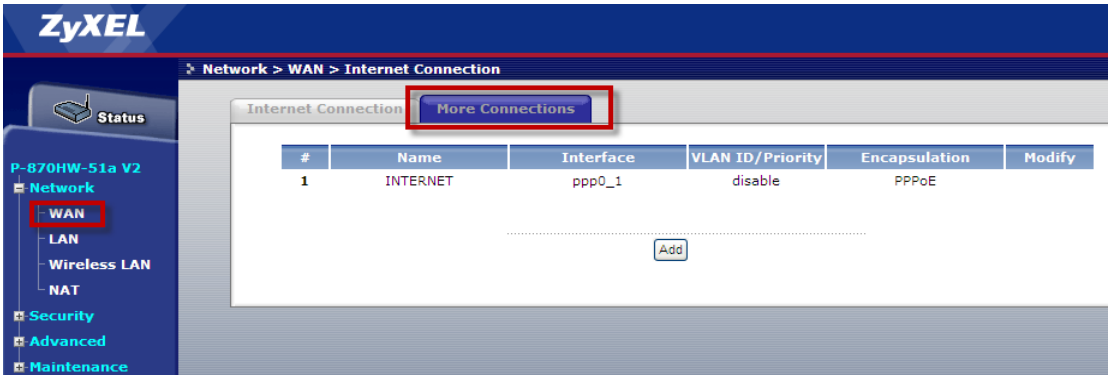
10. Click on **Advanced Setup.**

11. Select “Disable” for **IGMP Multicast.**
12. Select “No” for **PPPoE Passthrough.**
13. Check the **IP Filter Active** box.
14. Click on **Apply.**

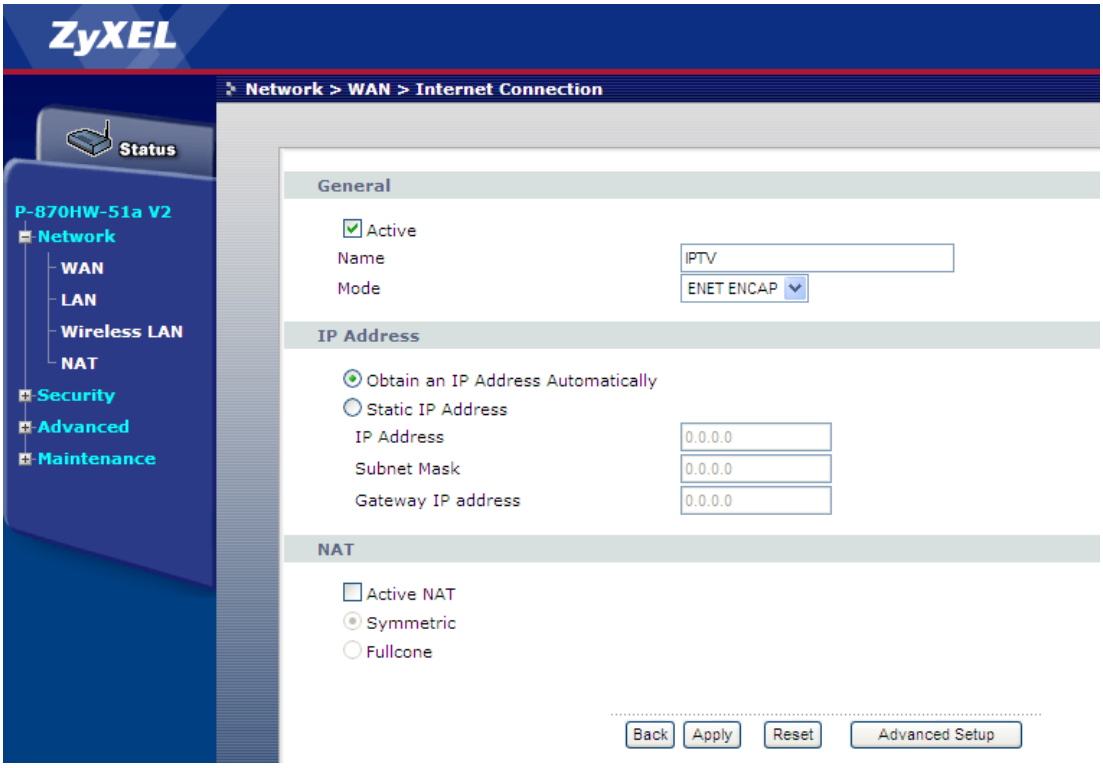


b. IPTV Service

1. Go to **Network > WAN > More Connection.**
2. Click on A**dd.**



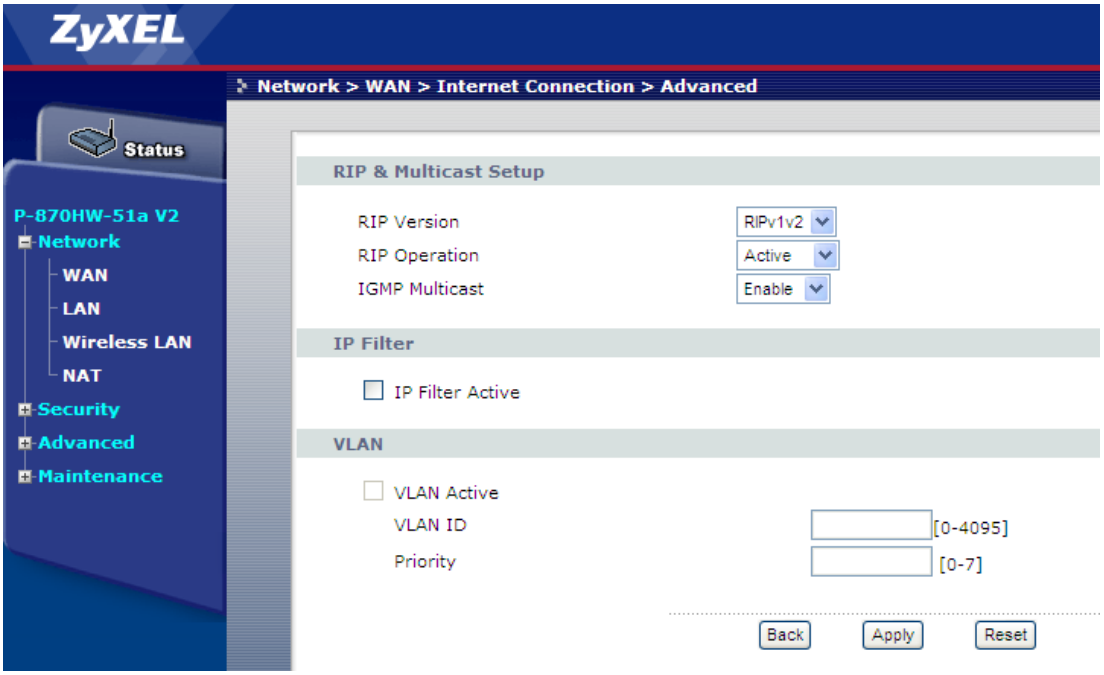
3. Select **Active.**
4. Enter the **Name**, e.g. “IPTV”.
5. Select the **Mode** to be “ENET ENCAP”.
6. Select **Obtain an IP Address Automatically.**
7. Click **Apply.**



8. Click **Apply.**

9. Click **Advanced Setup.**

10. Select “RIPv1v2” for **RIP Version.**
11. Select “Active” for **RIP Operation.**
12. Select “Enable” for **IGMP Multicast.**
13. Click **Apply.**

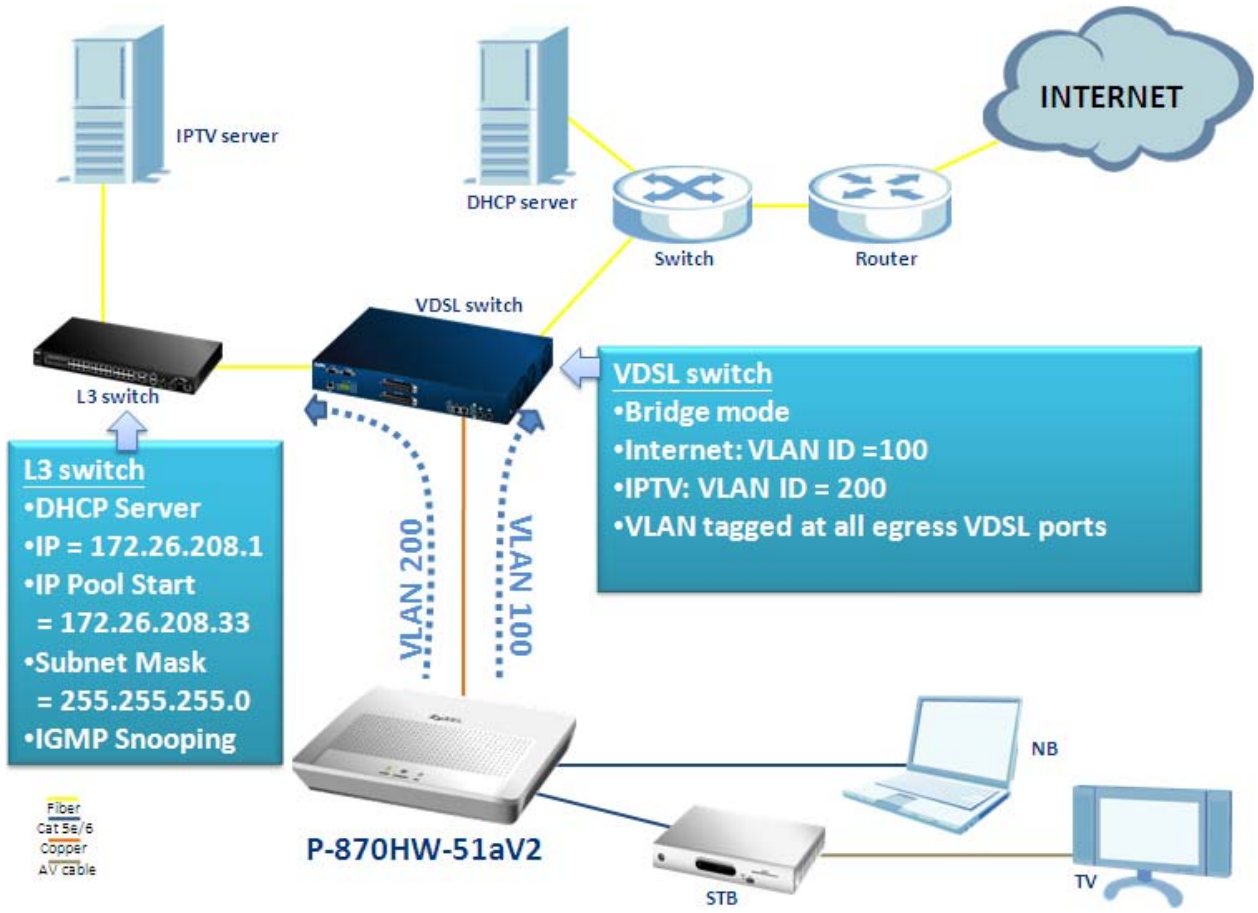


c. Verify the Status

As we can see from the following figure, the WAN1 and WAN2 are assigned with the dedicated IP successfully.

VLAN Based Scenario

Environment

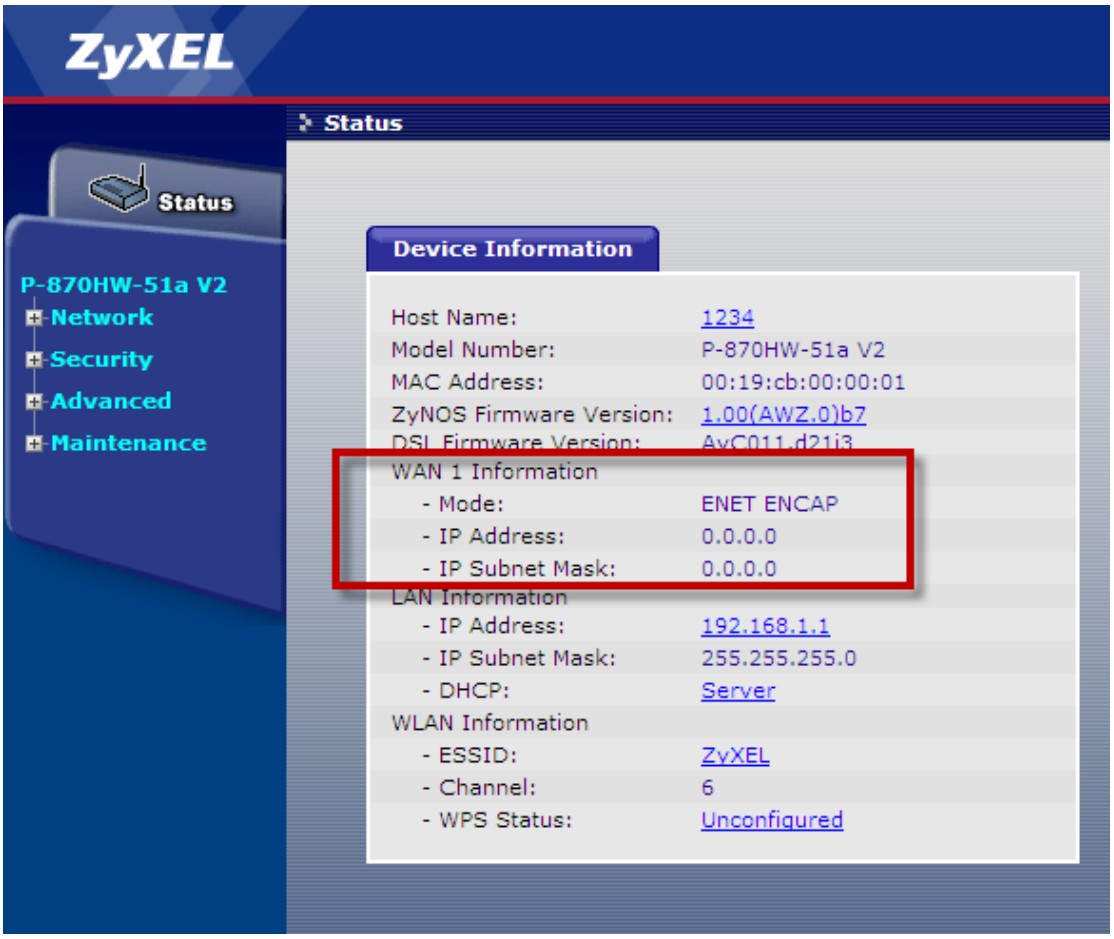


The Network structure of Central Office depends on the deployment of different ISP (Internet Service Provider) in different environments in different countries. One of the commonly known methods for separating different types of traffic is by classifying their VLAN ID. In the case of the aforementioned diagram, the INTERNET traffic is tagged with a VID=100 and the IPTV traffic is tagged with a VID=200. The COE (VDSL switch) receives the already VLAN tagged traffic from the CPE, and handles them according to their VID values. So how should we configure the P-870HW-51aV2 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

WAN Configuration

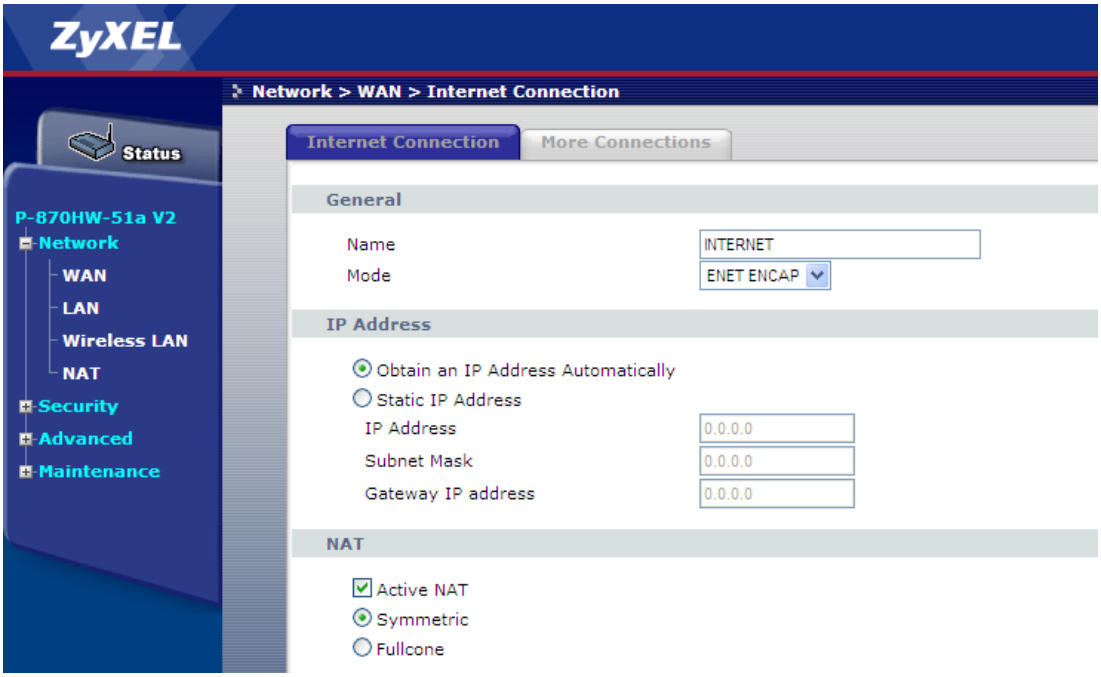
a. Check the WAN interface at default status.

1. Click **Status.**



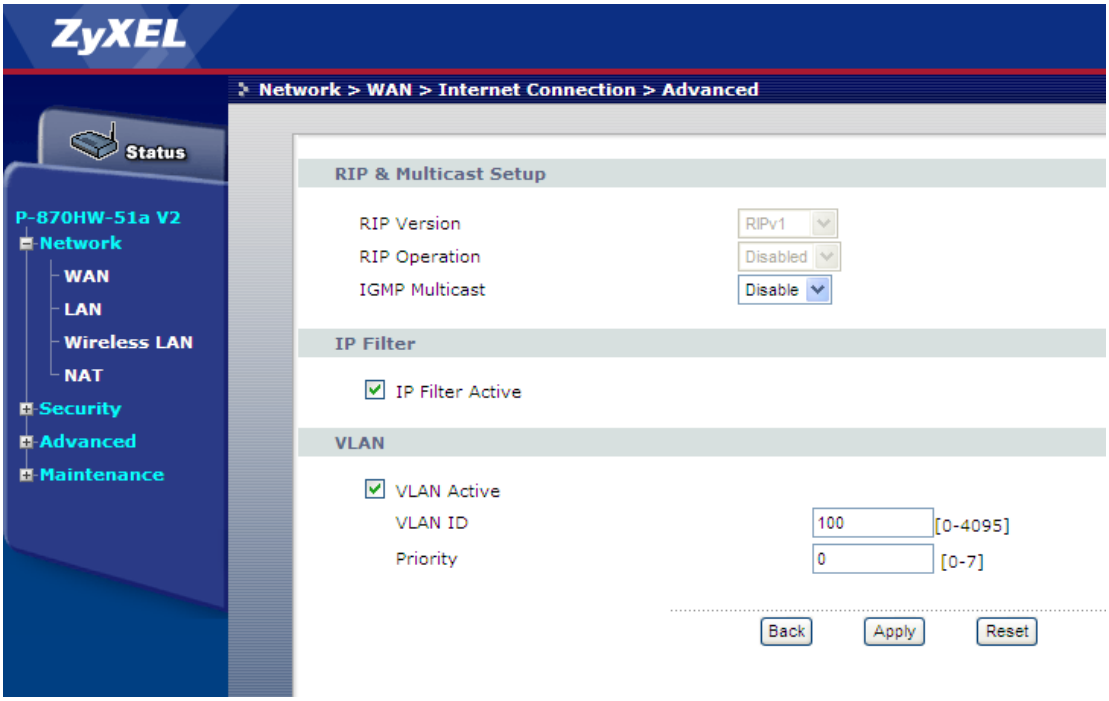
b. INTERNET Service

2. Go to **Network > WAN > Internet Connection.**
3. Enter the **Name**, e.g. “Internet”.
4. Select the **Mode**, e.g. “ENET ENCAP”.
5. Check the **Obtain an IP Address Automatically** box.
6. Click **Apply.**



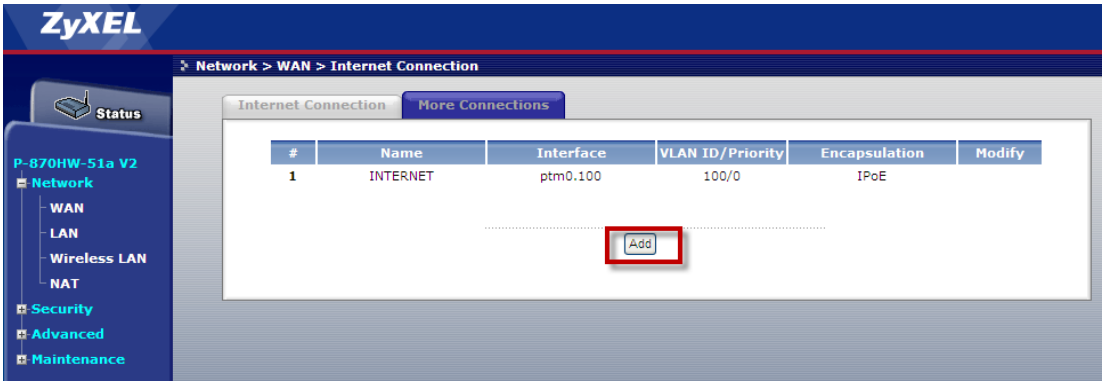
c. Internet Advanced Setup

1. Go to **Network > WAN > Internet Connection > Advanced.**
2. Select the **IGMP Multicast**, e.g. “Disable”.
3. Check the **IP Filter Active** box.
4. Check the **VLAN Active** box.
5. Enter the **VLAN ID**, e.g. “100”.
6. Enter the **Priority**, e.g. “0”.
7. Click **Apply.**

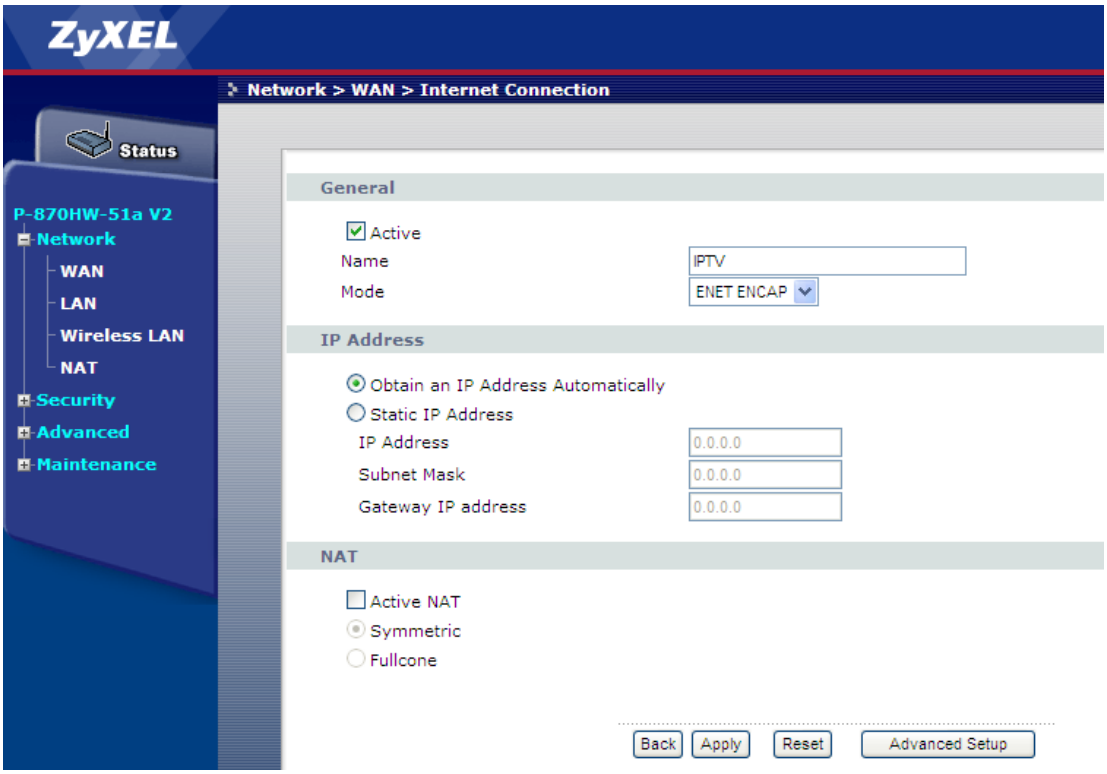


d. IPTV Service

1. Go to **Network > WAN > More connection.**
2. Click **Add.**



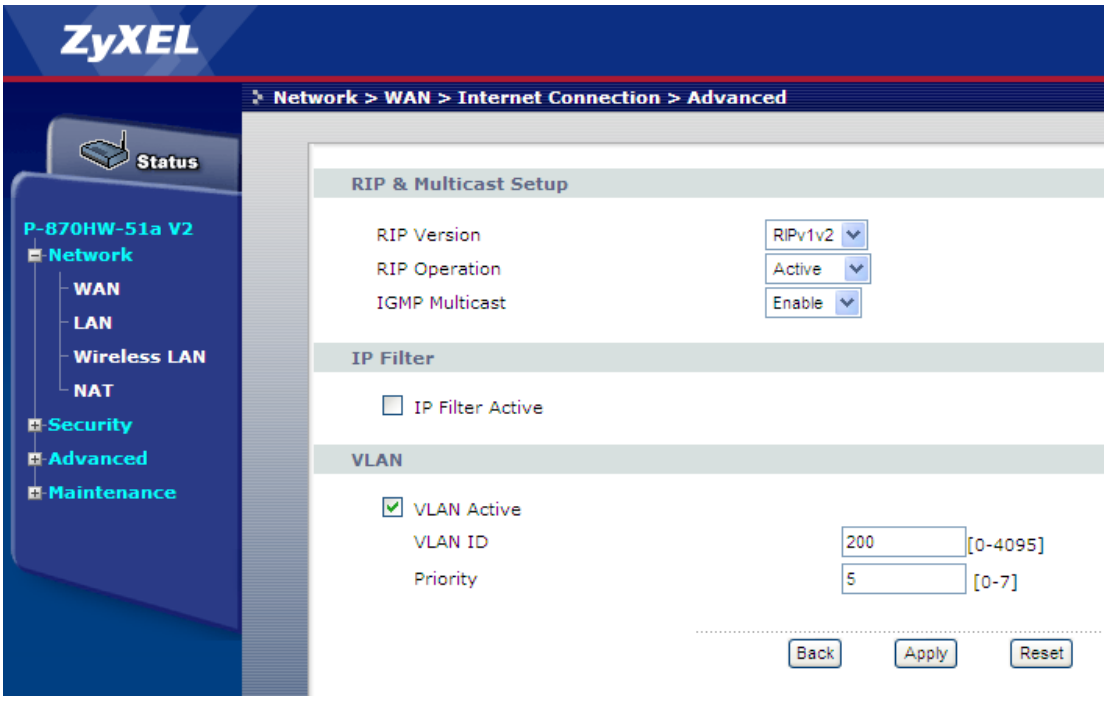
3. Check the **Active** box.
4. Enter the **Name**, e.g. “IPTV”.
5. Select the **Mode** to be “ENET ENCAP”.
6. Check the **Obtain an IP Address Automatically.**



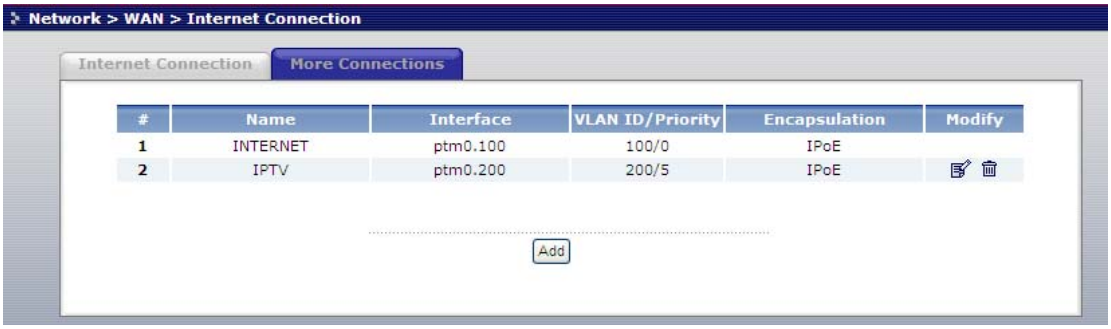
7. Click **Advanced Setup.**

Note: Do NOT click **Apply** yet!

8. Click **Advanced Setup.**
9. Select the **RIP Version**, e.g. “RIPv1v2”.
10. Select the **RIP Operation**, e.g. “Active”.
11. Select the **IGMP Multicast**, e.g. “Enable”.
12. Check the **VLAN Active** box.
13. Enter the **VLAN ID**, e.g. “200”.
14. Enter the **Priority**, e.g. “5”.
15. Click **Apply.**

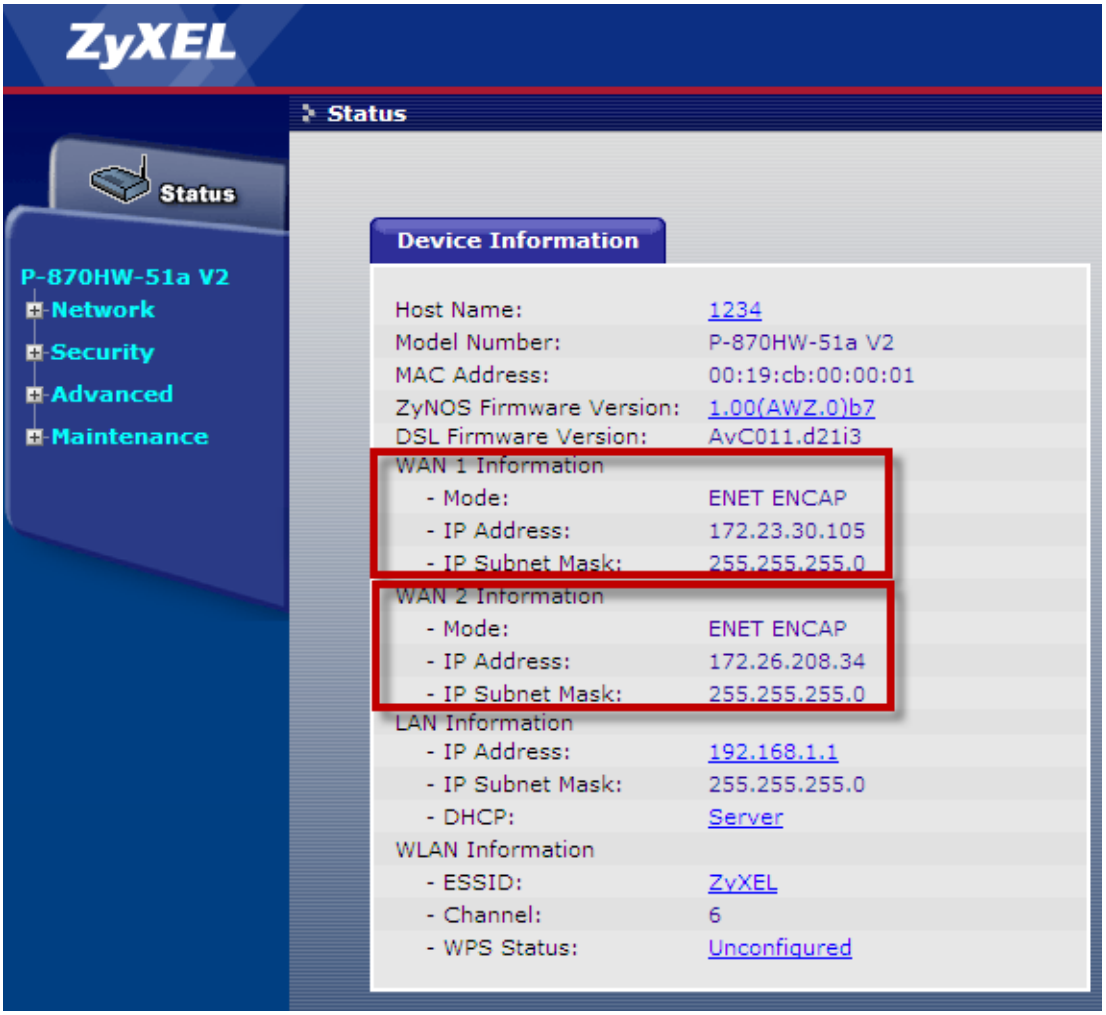


16. Check if the following status is correct.



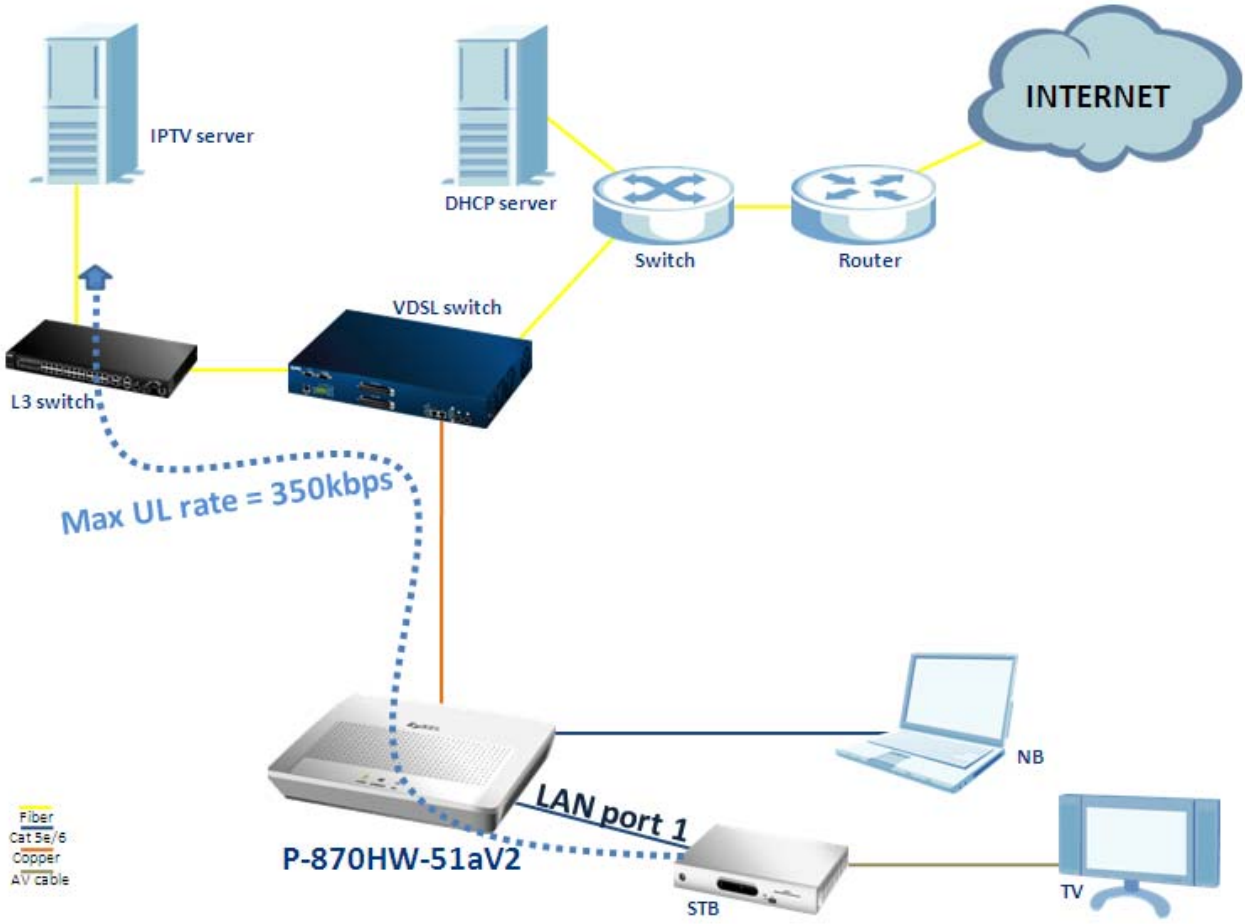
e. Check if the 2 WAN interfaces are assigned with their dedicated IPs.

1. Click **Status.**



Quality of Service

Environment

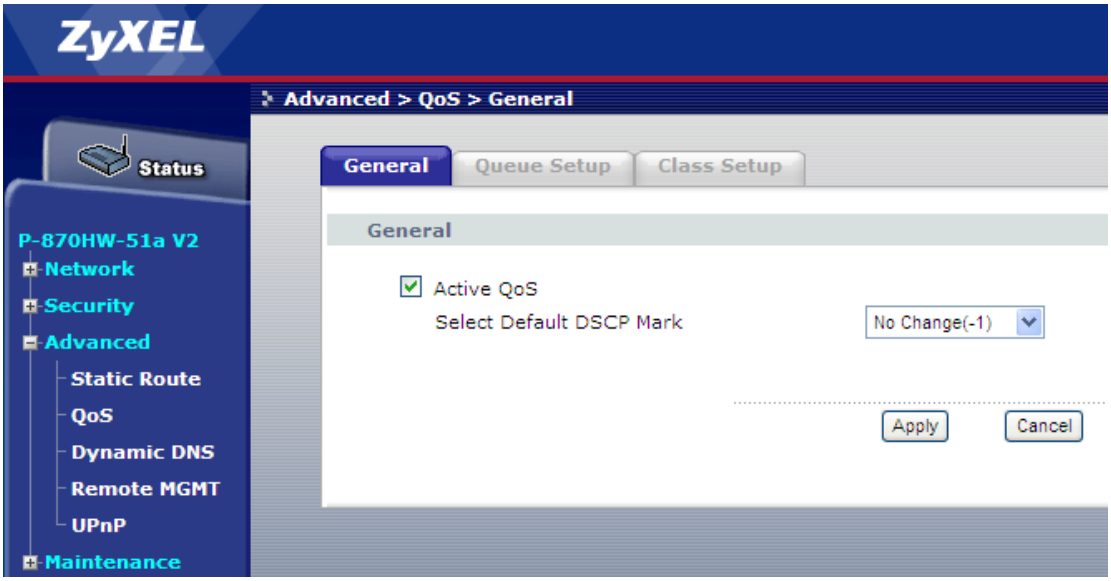


The “Quality of Service” feature in P-870HW-51aV2 has the ability to assign different task in accordance with the chosen type of traffic. In the case of the aforementioned diagram, we would like to limit the maximum upload rate of the IPTV service to 350 kbps. So how should we configure the P-870HW-51aV2 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

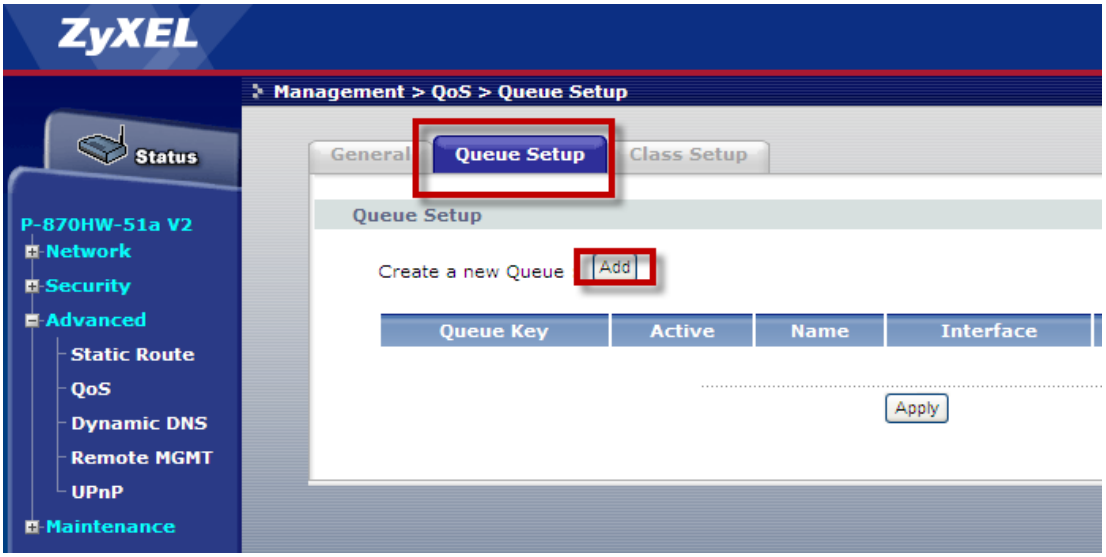
QoS configuration

a. Enable QoS

1. Go to **Advanced > QoS > General.**
2. Check the **Active QoS** box.

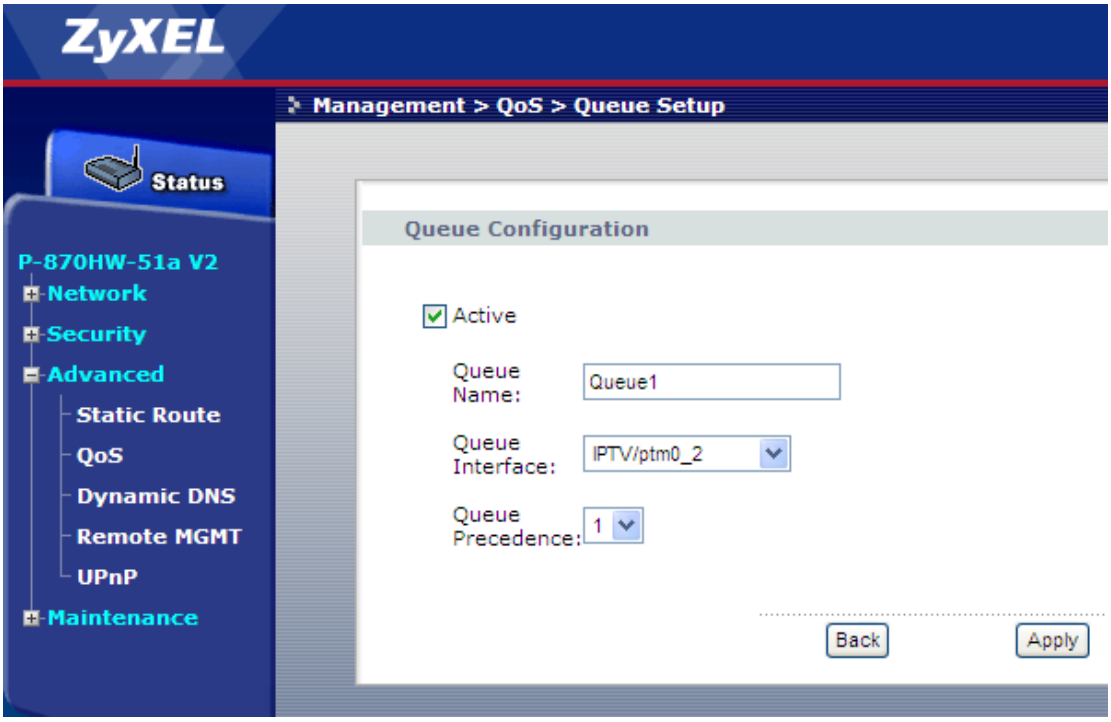


3. Go to **Management > QoS > Queue Setup.**
4. Click **Add.**

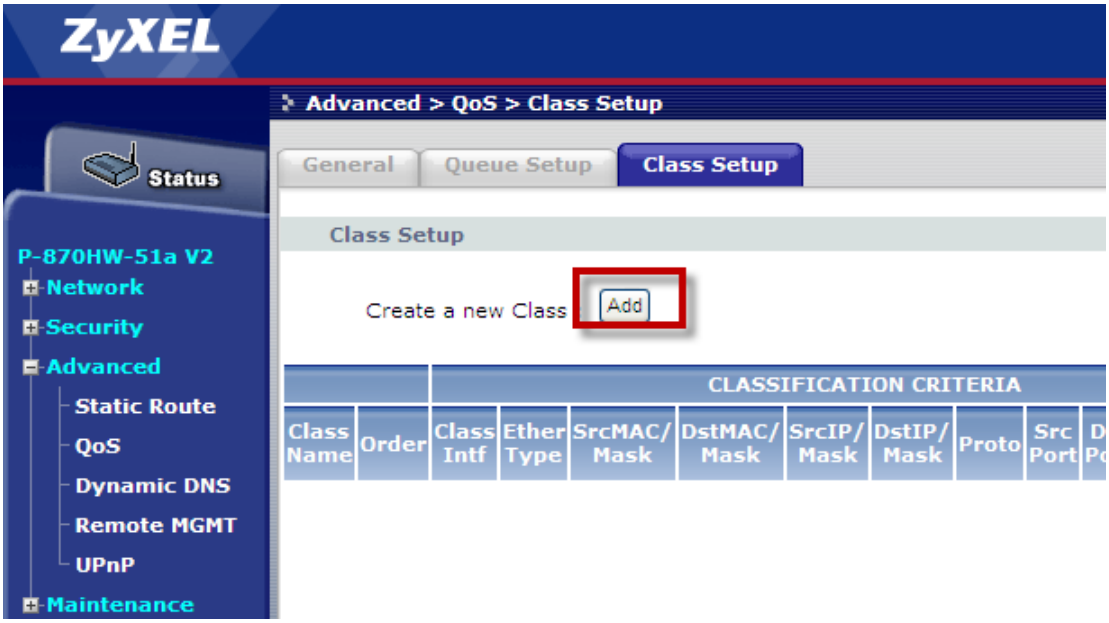


b. Configure the Video traffic.

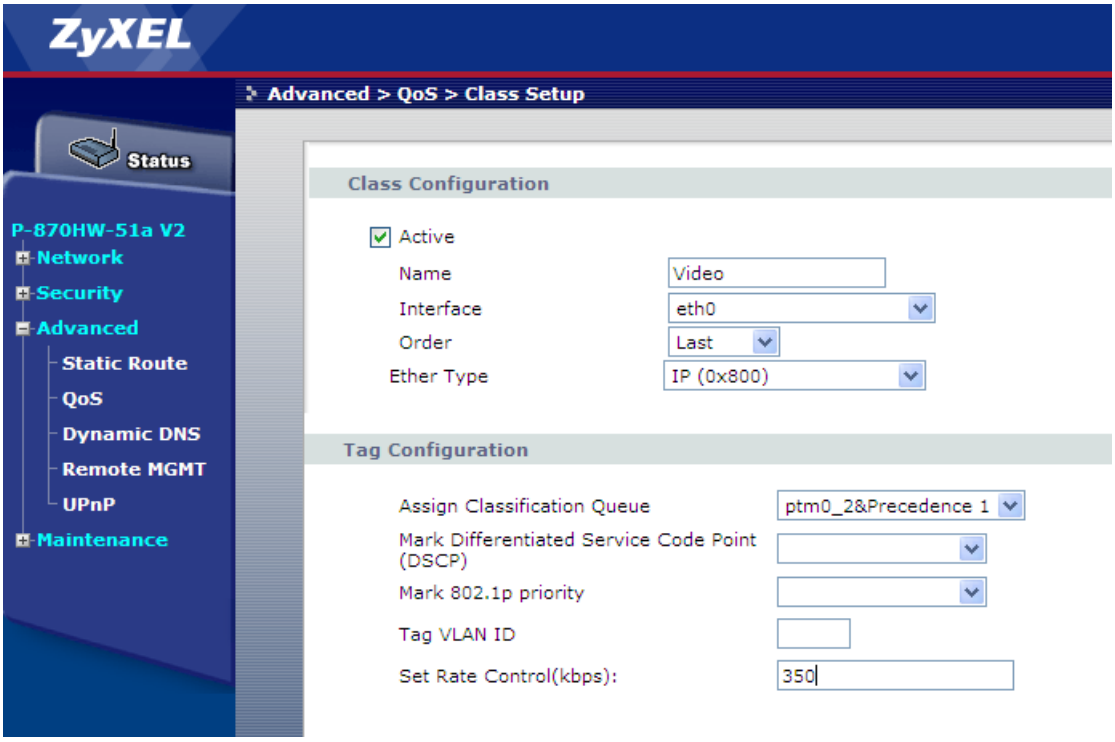
1. Check the **Active** box.
2. Enter the **Queue Name** box, e.g. “Queue1”.
3. Select the **Queue Interface**, e.g. “IPTV/ptm0_2”.
4. Select the **Queue Precedence** as “1”.
5. Click **Apply.**



6. Go to **Advanced > QoS > Class Setup.**
7. Click **Add.**



8. Check the **Active** box.
9. Enter the **Name**, e.g. “Video”.
10. Select the **Interface**, e.g. “eth0” (for LAN port 1).
11. Select the **Order** to be “last”.
12. Select the **Ether Type** to be “IP (0x800)”.
13. Select the **Assign Classification Queue** to be “ptm0_2&Precedence 1”.
14. Enter the **Set Rate Control(kbps)**, e.g. “350”.
15. Click **Apply.**

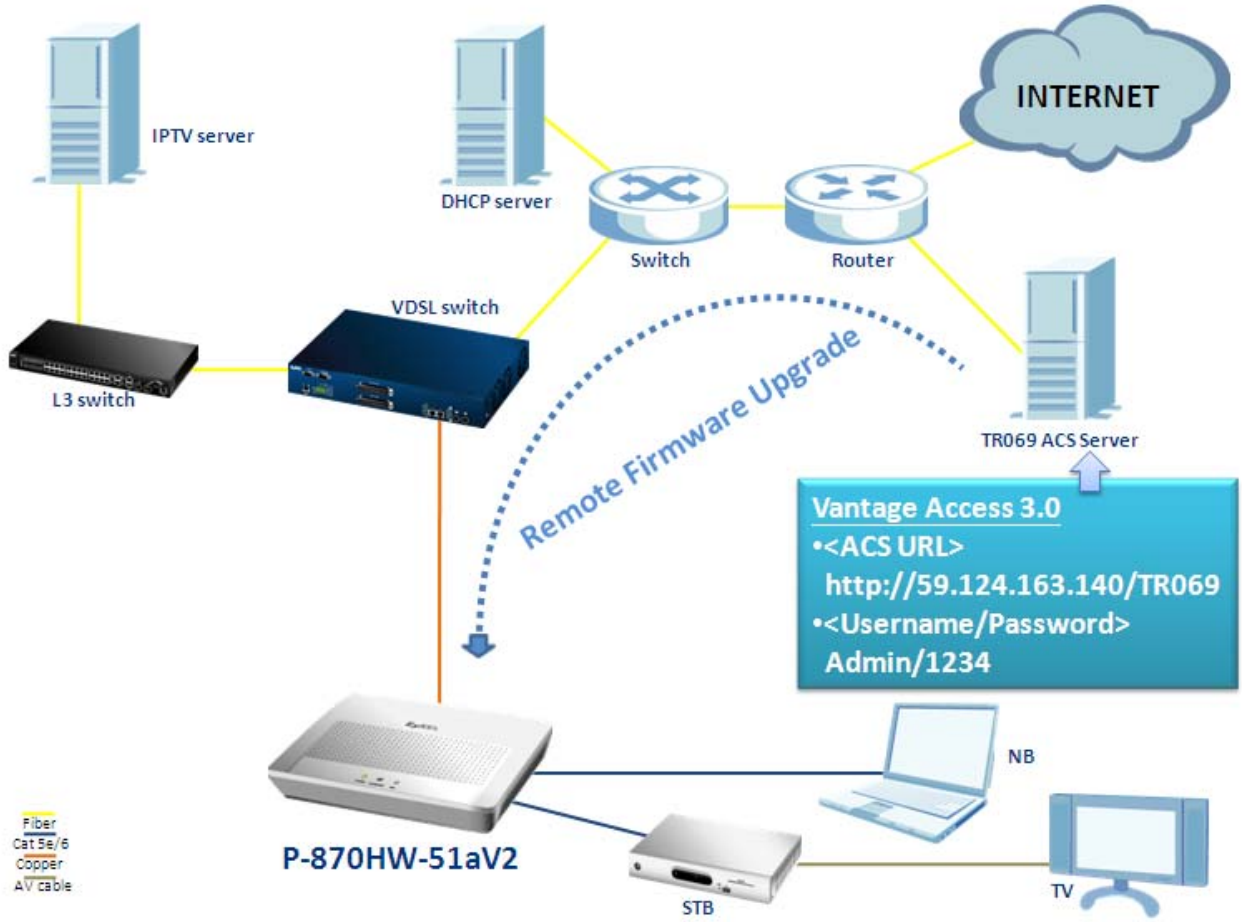


16. Check the results to be as followed.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)
Video	1	eth0	IP										3				350

TR069 – Remote Firmware Upgrade

Environment



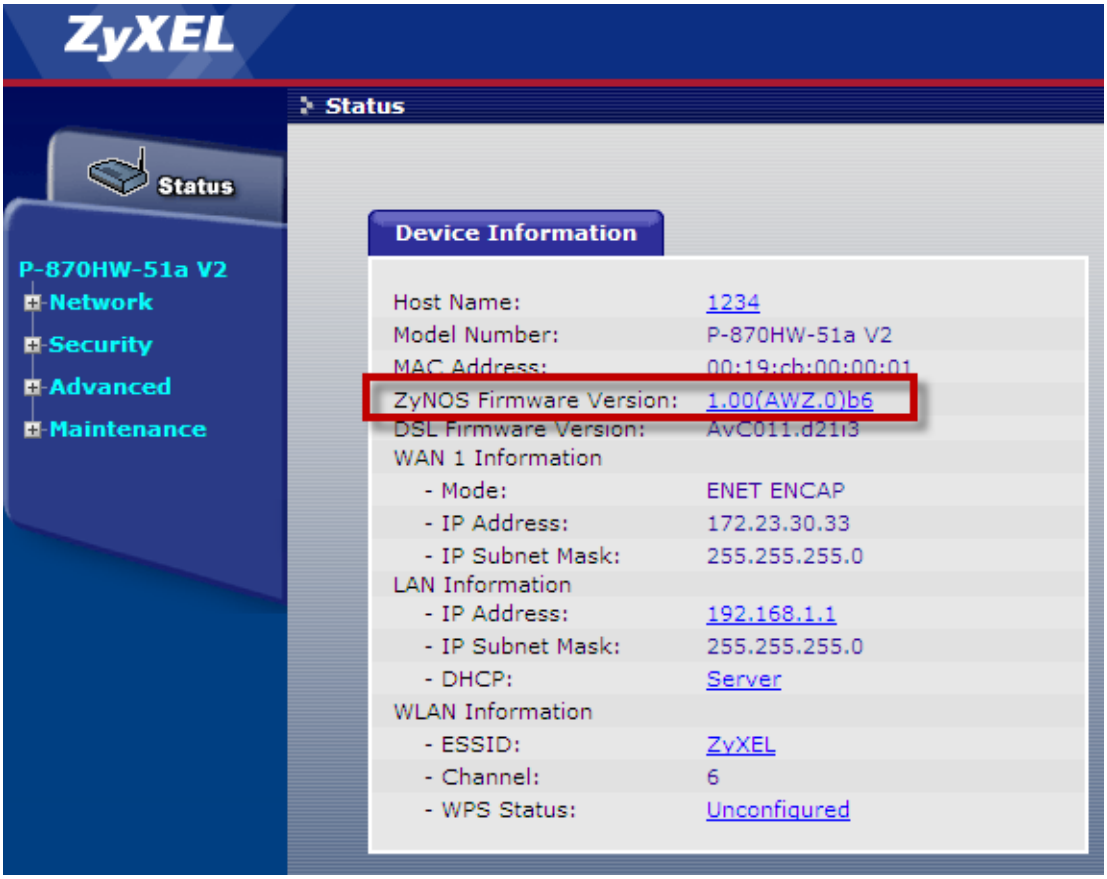
The P-870HW-51a v2 provides the TR-069 remote management feature; it could speed up the deployment of CPEs and ease our supporting costs. It can also help the VDSL ISP (Internet Service Provider) to reduce operation effort as well as enhance customer satisfaction. In the case of the aforementioned diagram, the TR069 ACS server remote upgrades the firmware of CPE. So how should we configure the P-870HW-51aV2 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

Note: This document uses a ZyXEL ACS server, Vantage Access 3.0, as a reference.

TR069 Configuration

a. Check the current firmware version.

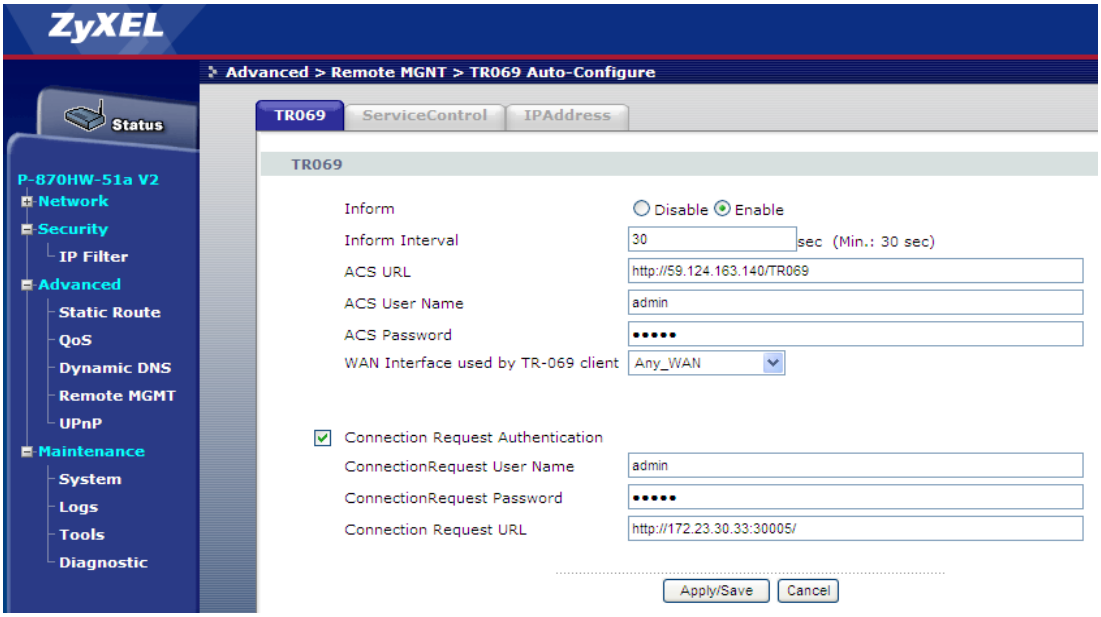
1. Click **Status.**



As we can see, the Firmware Version is 1.00(AWZ.0)b6.

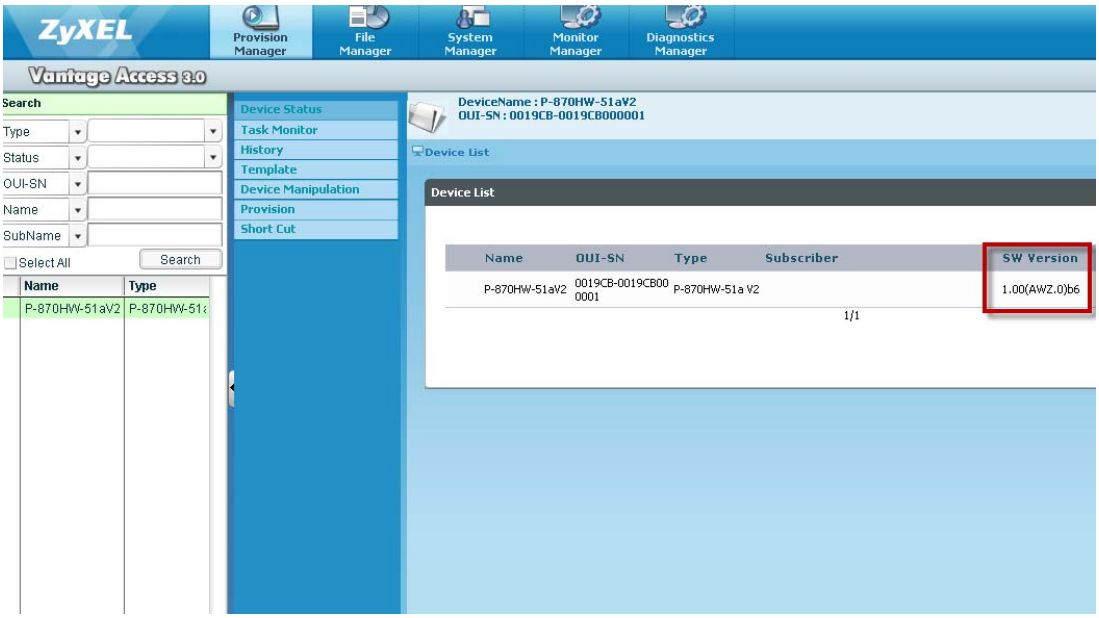
b. Configure the required TR069 parameters for the ACS server.

2. Go to **Advanced > Remote MGNT > TR069**
3. Check the **Enable** box.
4. Enter the **Inform Interval**, e.g. “30” seconds.
5. Enter the **ACS URL**, e.g. “http://59.124.163.140/TR069”.
6. Enter the **ACS User Name**, e.g. “admin”.
7. Enter the **ACS Password**, e.g. “1234”.
8. Select the **WAN Interface used by TR-069 client**, e.g. “Any_WAN”.
9. Click **Apply.**



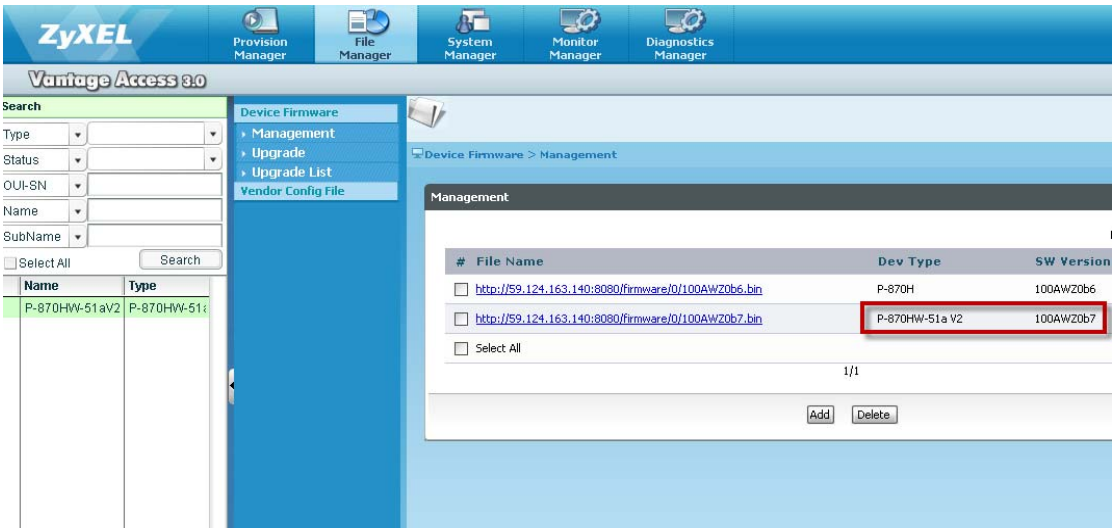
ACS server (Vantage Access 3.0)

Make sure that the P-870HW-51aV2 is correctly subscribed on the ACS server.



As we can see, a P-870HW-51aV2 is subscribed on the server and the SW Version is 1.00(AWZ.0)b6.

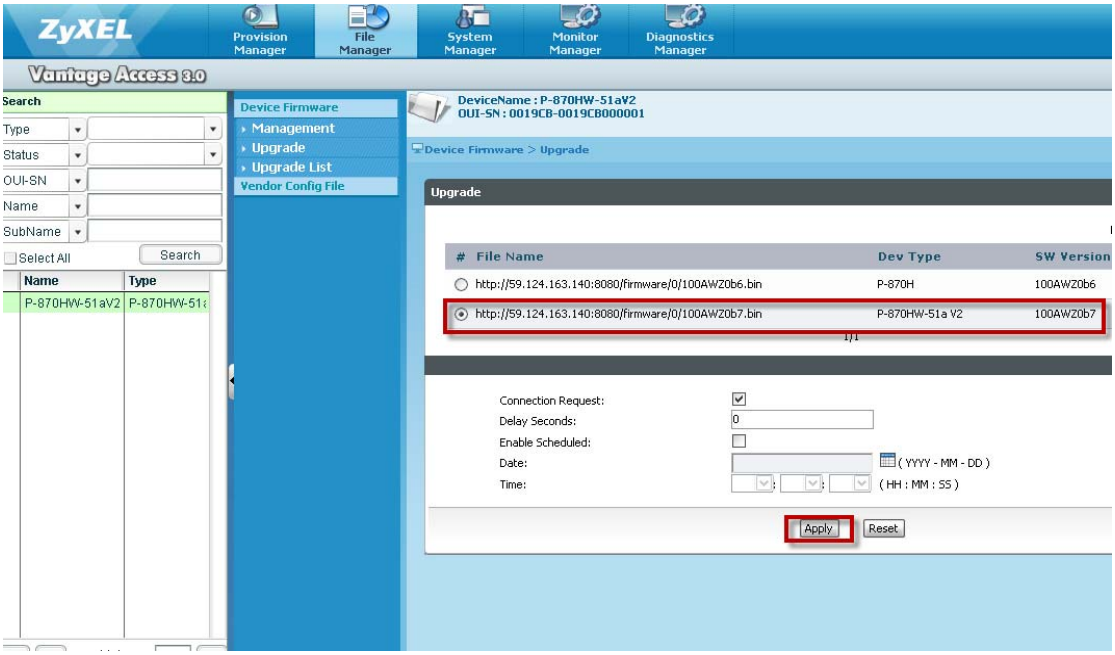
Next, we should be sure that the dedicated firmware should be properly uploaded to the ACS server in order to proceed to the remote firmware upgrade. In this case, it's 1.00(AWZ.0)b7.



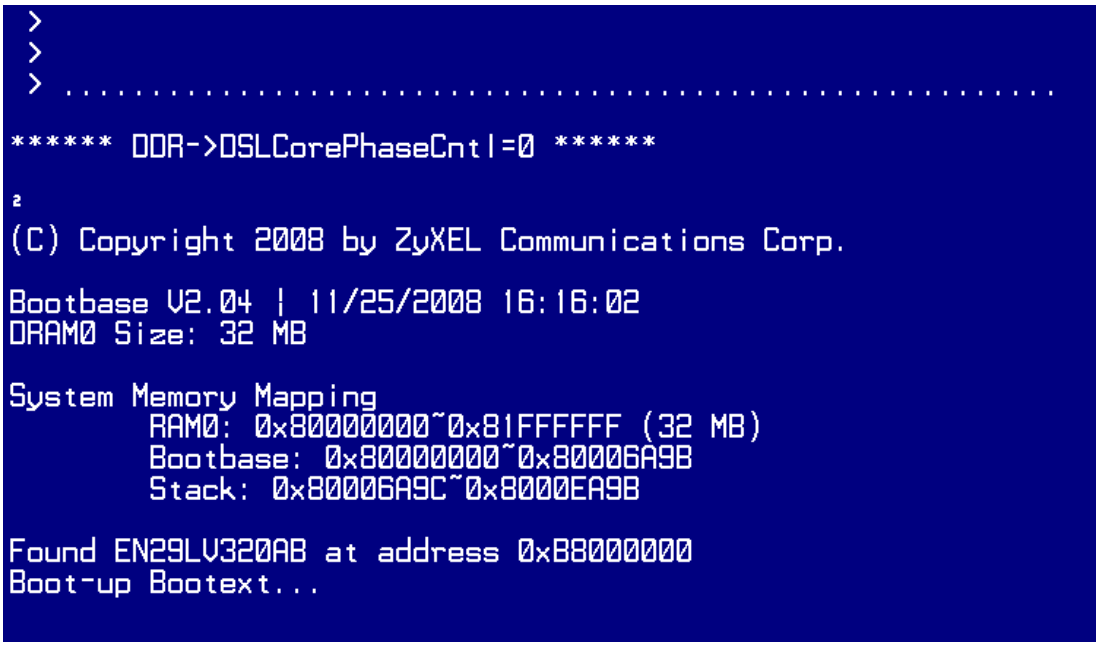
As we can see, the 1.00(AWZ.0)b7 is properly uploaded.

Now, we can execute the remote firmware upgrade by selecting the correct firmware,

and click Apply.

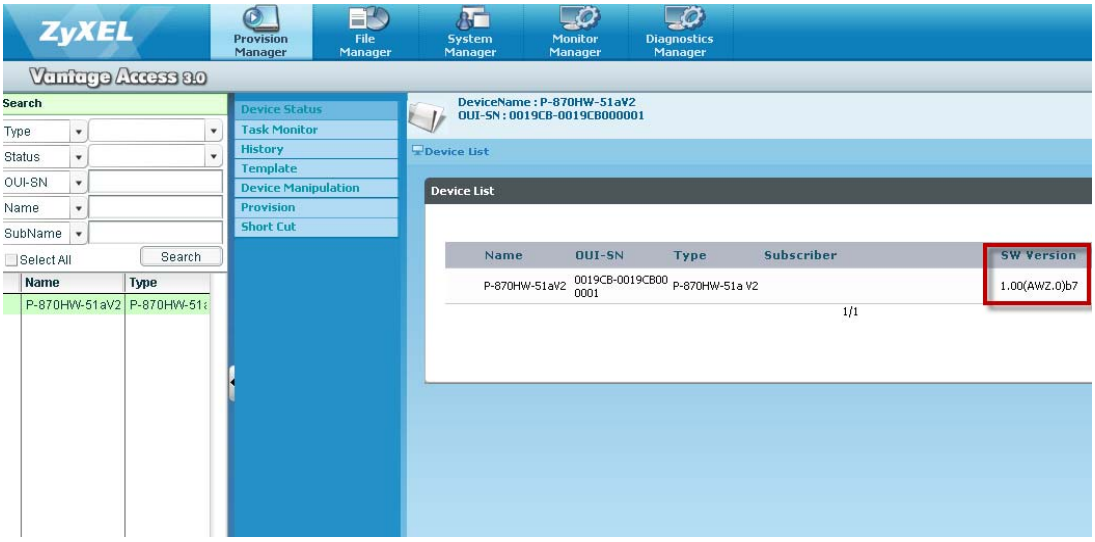


If we have a console cable connected to the P-870HW-51aV2 with a HyperTerminal software turned on, we should be able to see the CPE upgrading the firmware and rebooting once finished as in the following figure:



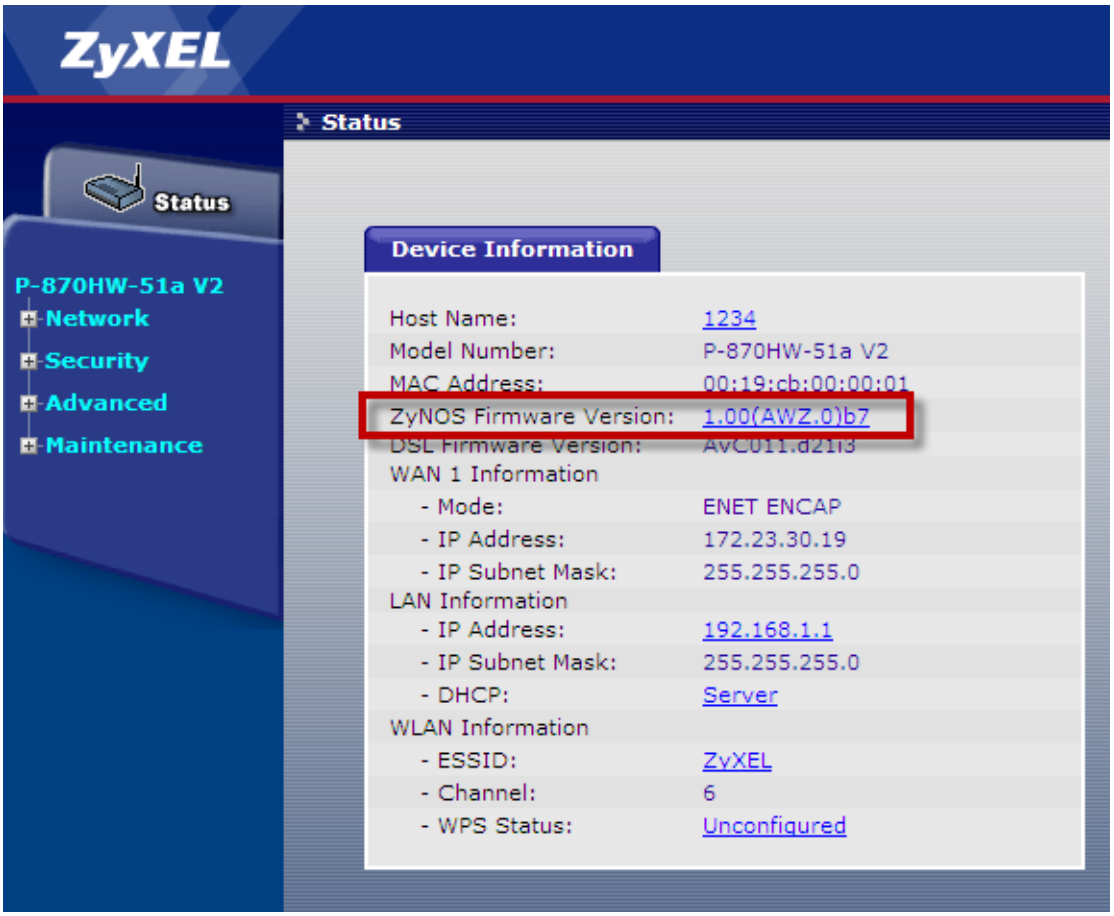
After the whole process is done, the SW version in Vantage Access 3.0 should be

1.00(AWZ.0)b7:



c. Check the firmware Version again.

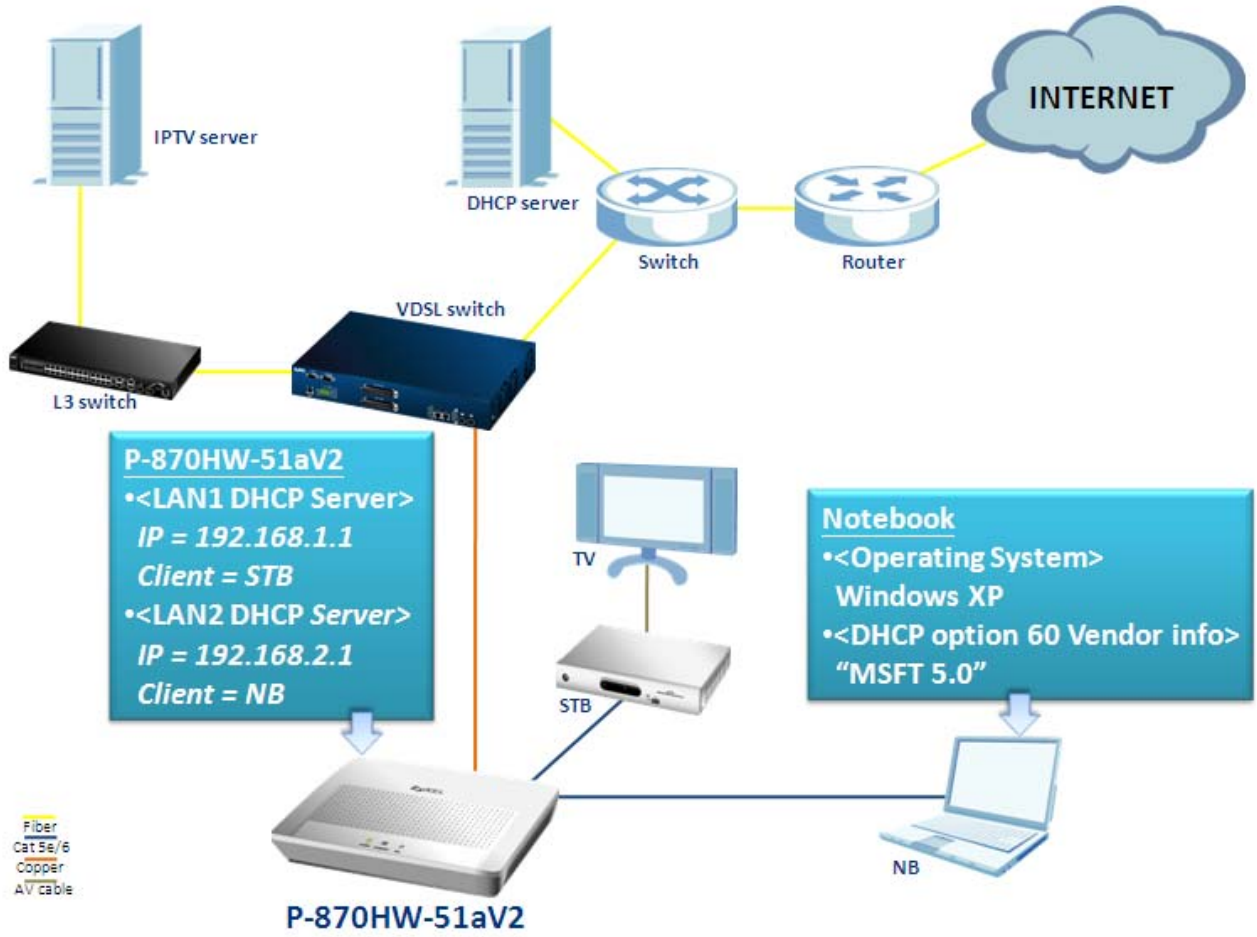
1. Click **Status.**



As we can see, the Firmware Version now is changed to 1.00(AWZ.0)b7.

DHCP Option 60

Environment



The P-870HW-51a v2 supports the DHCP Option 60 feature, which allows the DHCP server to differentiate between two kinds of client machines and process the requests from the two types of "strings" appropriately. In the case of the aforementioned diagram, we would like the notebook to get an IP from the LAN2 DHCP server. We already know that the VCI (Vendor Class Identifier) of notebook (with Windows XP installed) is "MSFT 5.0". How should we configure the P-870HW-51aV2 to use such information and assign an IP for the notebook from LAN2 DHCP server? The following step-by-step procedure instructs us the method.

DHCP Option 60 Configuration

a. Show information on the LAN interface.

1. Login the device by telnet.
2. Type the command “lan show”.

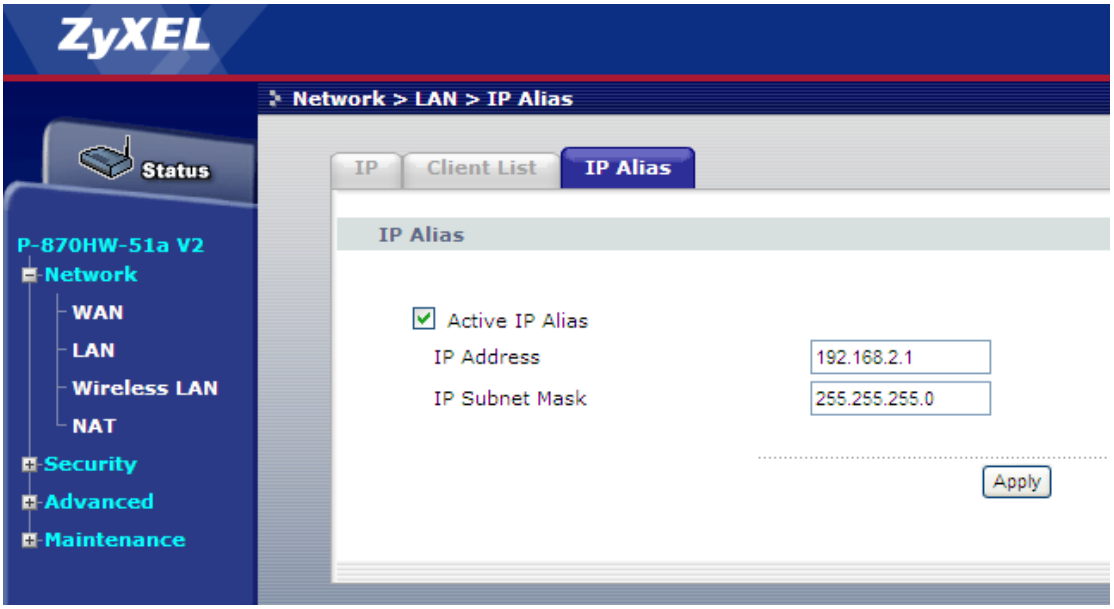
```
> lan show
br0             Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                RX packets:3191 errors:0 dropped:0 overruns:0 frame:0
                TX packets:3436 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:0
                RX bytes:332773 (324.9 KiB)  TX bytes:1920623 (1.8 MiB)

br0:0           Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

br0:1           Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

As we can see, only br0 representing LAN1 is activated with IP = 192.168.1.1. The other LAN interfaces (br0:0 and br0:1) are not activated; thus they do NOT have any IPs.

Note: The DHCP Option 60 is only available on interface br0:0.

b. Enable the IP Alias.

1. Go to **Network > LAN > IP Alias.**
2. Check the **Active IP Alisa** box.
3. Enter the **IP Address**, e.g. “192.168.2.1”.
4. Enter the **IP Subnet Mask**, e.g. “255.255.255.0”.
5. Click **Apply.**



c. Show information on the LAN interface.

1. Login the device by Telnet.
2. Type the command “lan show”.

```
 > lan show
br0             Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                RX packets:3398 errors:0 dropped:0 overruns:0 frame:0
                TX packets:3660 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:0
                RX bytes:355210 (346.8 KiB)  TX bytes:2046056 (1.9 MiB)

br0:0           Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

br0:1           Link encap:Ethernet  HWaddr 00:19:CB:00:00:01
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Now we can see that br0:0 is activated and possess an IP = 192.168.2.1.

d. Enable the DHCP server on the IP Alias.

1. Login the device by Telnet.
2. Type the command “dhcpiprange2 show”.

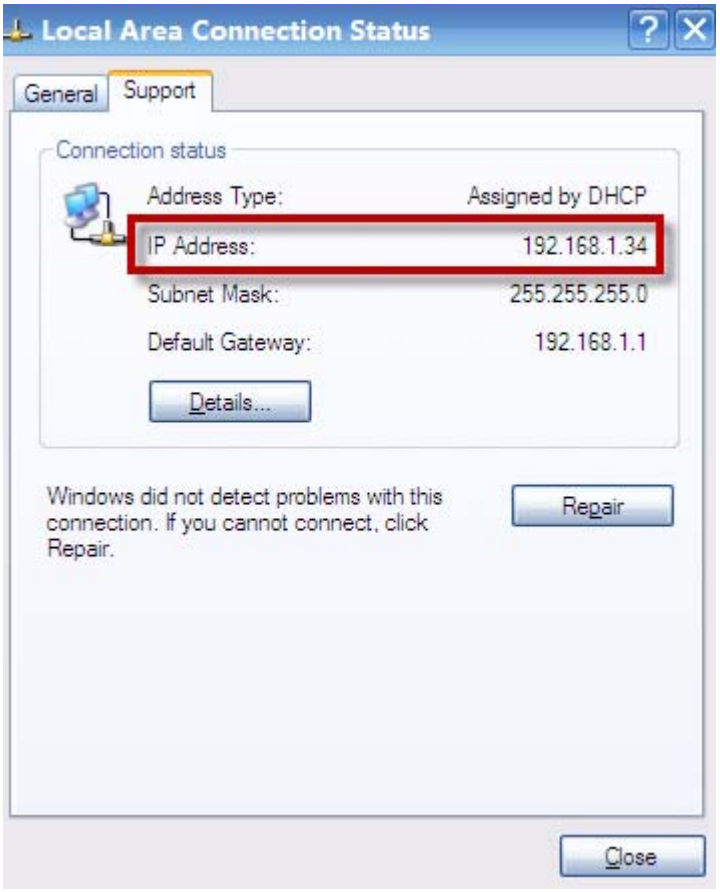
```
 > dhcpiprange2 show
Interface: br0:0
dhcpserver2: disable
dhcpserver2 ip address: 192.168.2.1
dhcpiprange2 start ip address: 0.0.0.0
dhcpiprange2 end ip address: 0.0.0.0
leased time: 24 housrs
```

3. Type the command “dhcpiprange2 enable”.
4. Type the command “dhcpiprange2 show”.

```
 > dhcpiprange2 enable
 > dhcpiprange2 show
Interface: br0:0
dhcpserver2: enable
dhcpserver2 ip address: 192.168.2.1
dhcpiprange2 start ip address: 0.0.0.0
dhcpiprange2 end ip address: 0.0.0.0
leased time: 24 housrs
```

Note: “dhcpiprange” represents interface br0, and “dhcpiprange2” represents interface br0:0.

Check the assigned IP on the notebook.



We can see that it is 192.168.1.34.

e. Input the dedicated string for the DHCP Option 60 on LAN2.

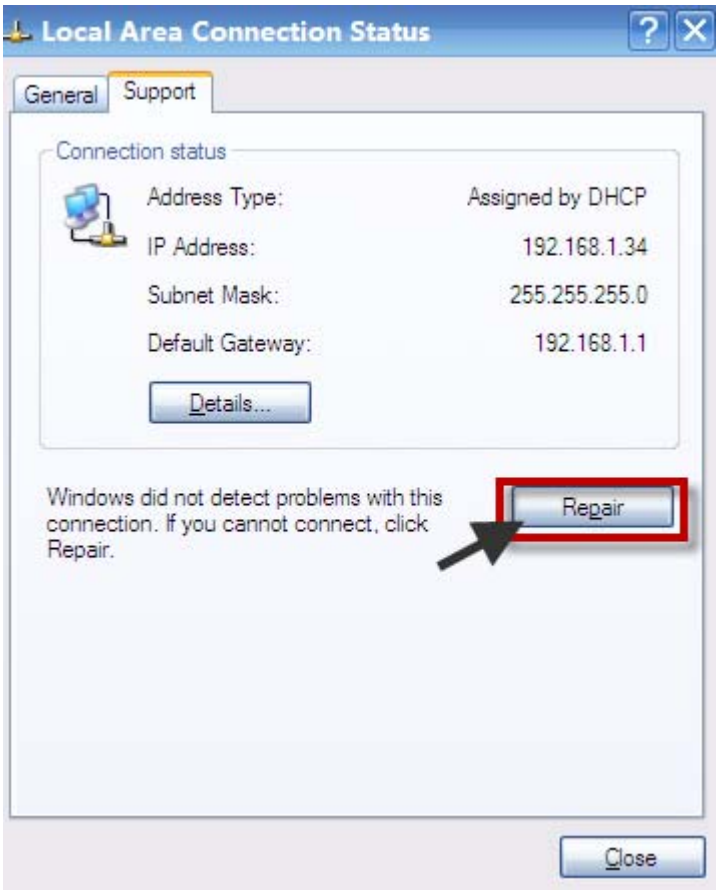
1. Login the device by Telnet.
2. Type the command “dhcpdopt config 60 MSFT 5.0”.
3. Type the command “dhcpdopt show”.

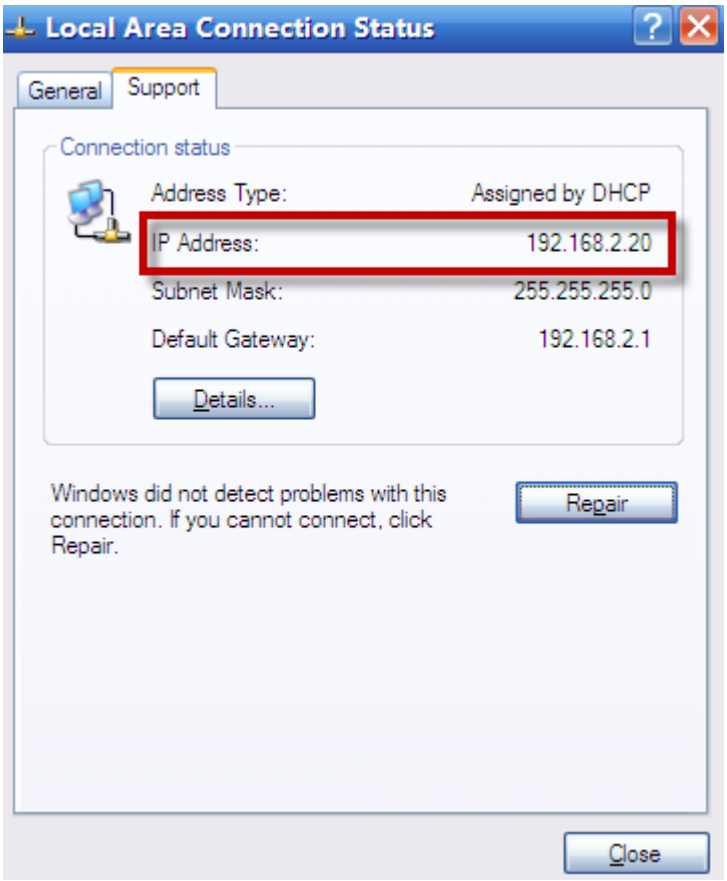
```
 >
 > dhcpdopt config 60 MSFT 5.0
dhcpdopt: set dhcpdopt operation successfully on 'MSFT 5.0'
 > dhcpdopt show
option 60 = MSFT 5.0
 >
```

We can see that the string of the DHCP Option 60 is now changed to “MSFT 5.0”.

Go back to the notebook and click Repair in the “Local Area Connection Status”

window to release the old IP and renew one.





We can see now that the IP is 192.168.2.20, which obviously was assigned by the LAN2 DHCP server (192.168.2.1).

NAT Portforwarding

NAT/Multi-NAT Introduction

- What is Multi-NAT?

The NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated as the *inside* network and the other is the *outside*. Typically, one company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on the incoming packets back into local IP addresses. The IP addresses for NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a Web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, the NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the CPE, thus preventing intruders from probing your network.

For more information on the IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How NAT works?

If we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA), see the following figure. The term 'inside' refers to the set of networks that are subject to translation. The NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers) and then forwards each packet to the Internet ISP, thus making them appear as if they came from the NAT system itself (e.g., the CPE router). The CPE keeps track of the original addresses and port numbers, so the incoming reply packets can have their original values restored.

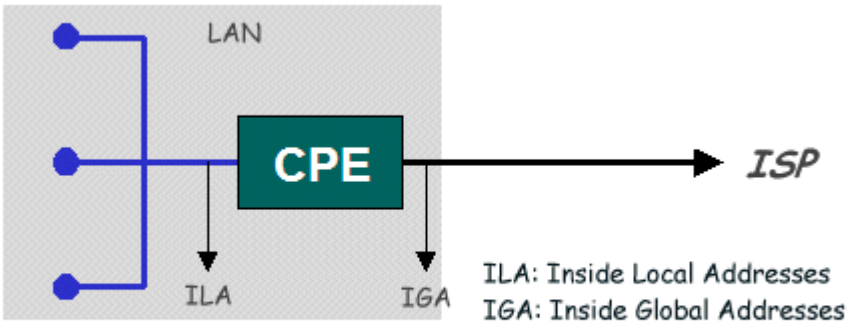


Figure1: Local/Global IP Addresses

- NAT Mapping Types

The NAT supports five types of IP/port mapping. They are:

1. **One to One**

In One-to-One mode, the Prestige maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the CPE maps multiple ILAs to one IGA.

3. **Many to Many Overload**

In Many-to-Many Overload mode, the CPE maps the multiple ILAs to shared IGA.

4. **Many to Many No Overload**

In Many-to-Many No Overload mode, the CPE maps each ILA to unique IGA.

- Server (DMZ host)

In Server mode (DMZ host), the CPE maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note: If you want to map each server to one unique IGA, please use the One-to-One mode.

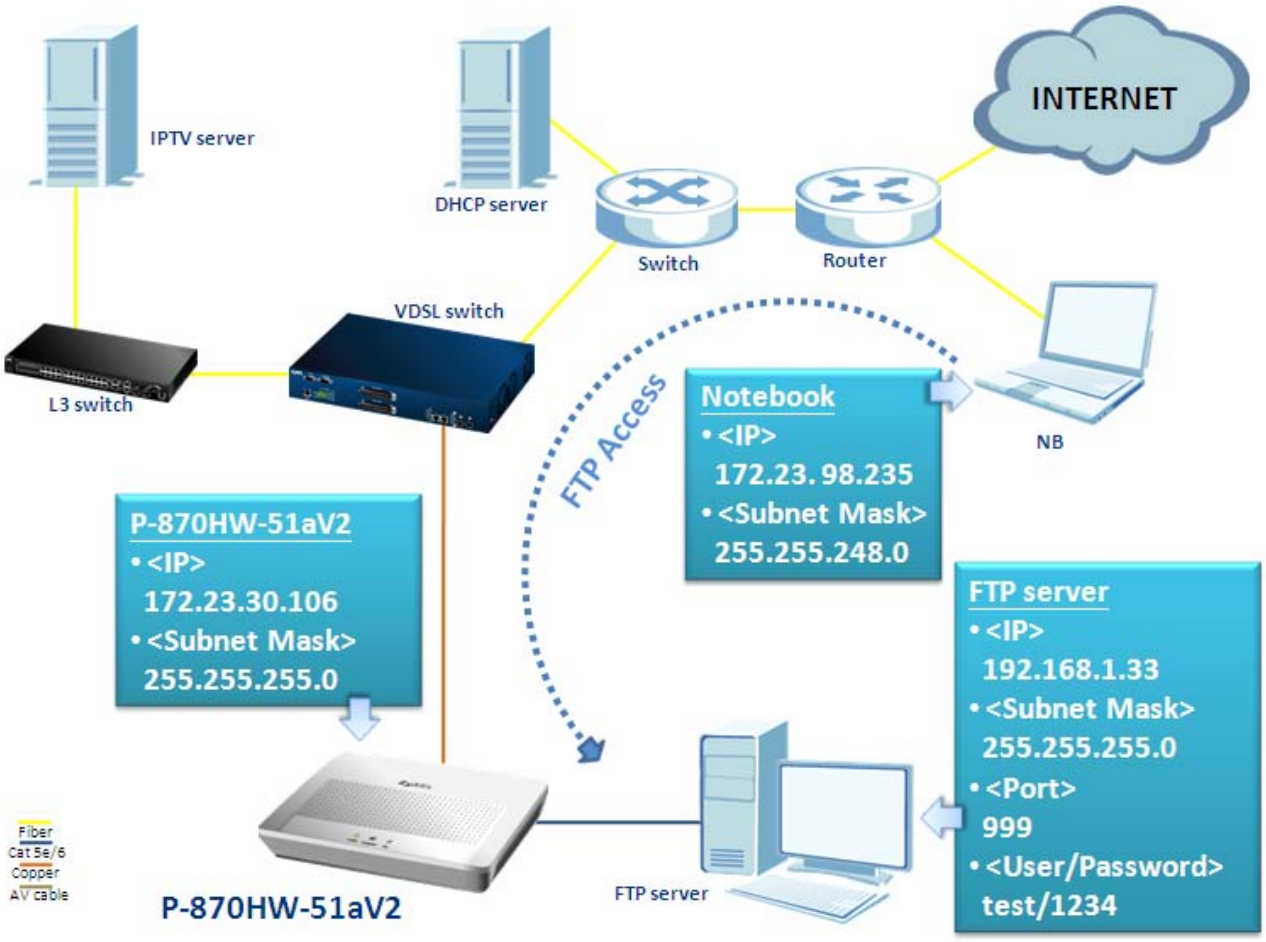
The following table summarizes these types.

NAT Type	IP Mapping	Mapping Direction
One-to-One	ILA1<--->IGA1	Both
Many-to-One	ILA1---->IGA1 ILA2---->IGA1 ...	Outgoing
Many-to-Many Overload	ILA1---->IGA1 ILA2---->IGA2 ILA3---->IGA1 ILA4---->IGA2 ...	Outgoing
Many-to-Many No Overload (Allocate by Connections)	ILA1---->IGA1 ILA2---->IGA3 ILA3---->IGA2 ILA4---->IGA4 ...	Outgoing
Server	Server 1 IP<----IGA1 Server 2 IP<----IGA1	Incoming

- Port numbers for some services:

Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

Environment

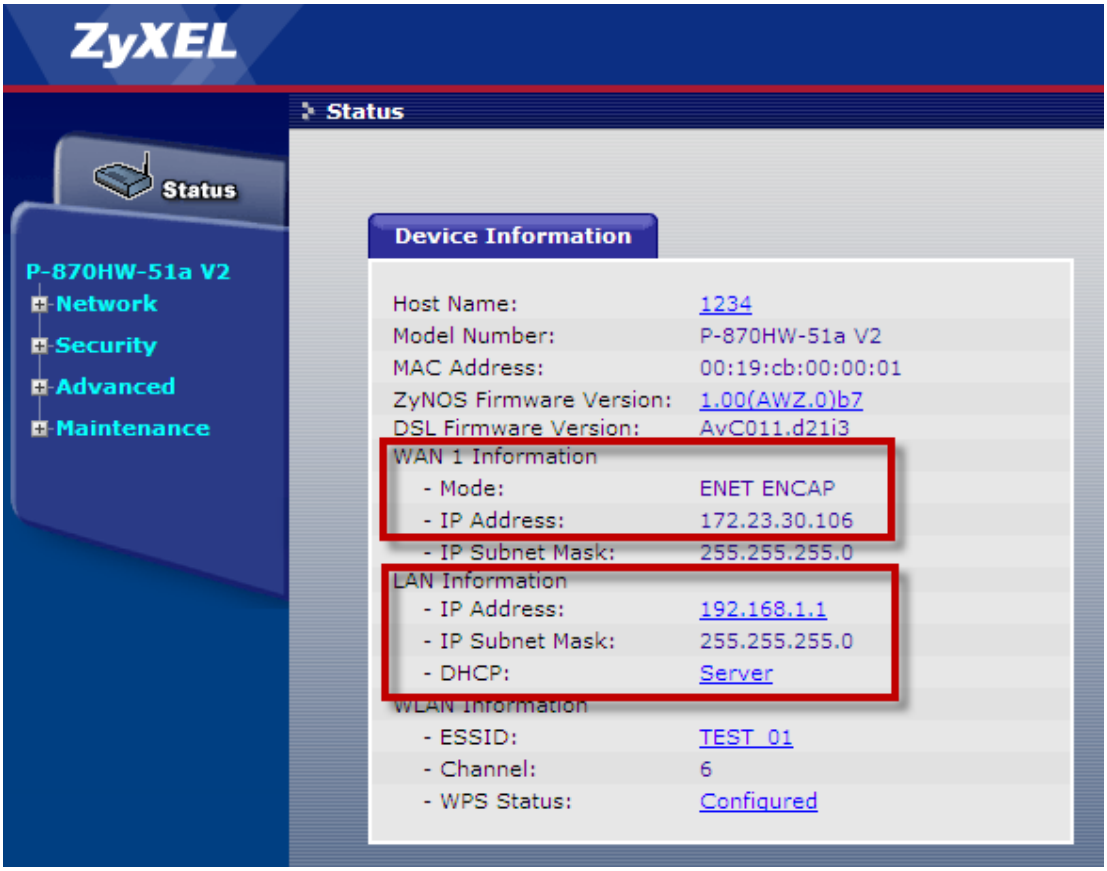


The NAT provides system administrators an easy solution to create a private IP network for security and IP management. Powered by NAT technology, the P-870HW-51aV2 supports complete the NAT mapping and most popular Internet multimedia applications. This feature is the best described with the NAT port forwarding feature implemented in the CPE. In the case of the above diagram, we have a FTP server installed behind the CPE with an IP assigned by the local DHCP server (192.168.1.33). How should we configure the P-870HW-51aV2, so that the notebook at the WAN site can access the FTP server? The following step-by-step procedure instructs us the method.

Port Forwarding Configuration

a. Show the device information.

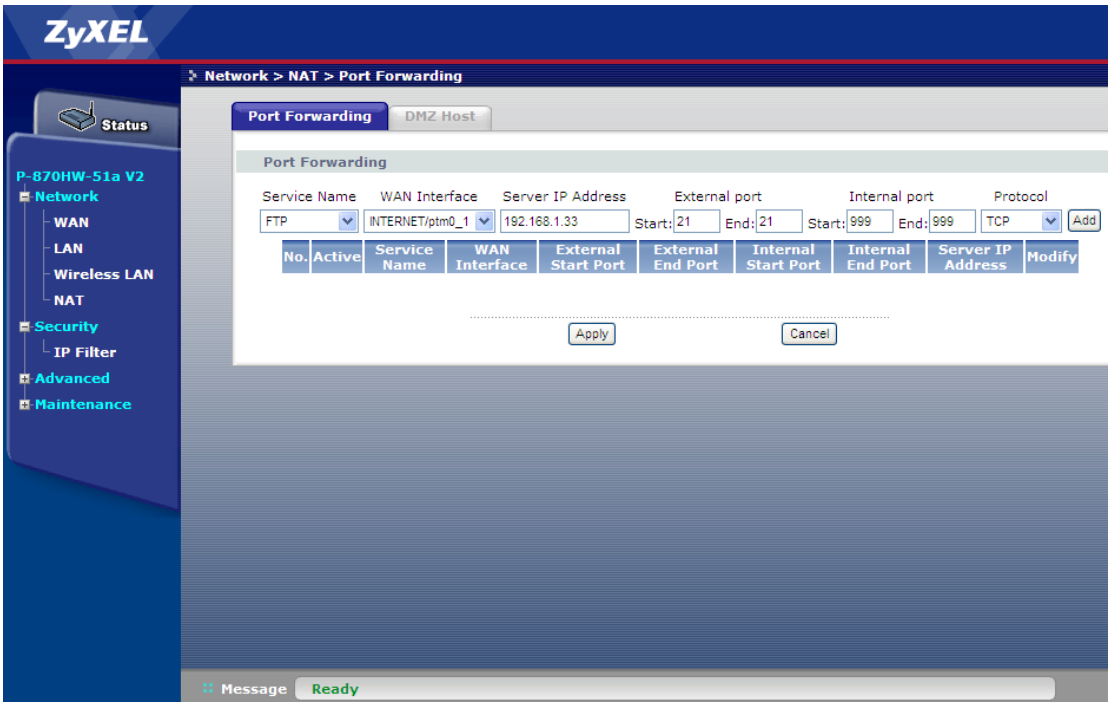
1. Click **Status.**



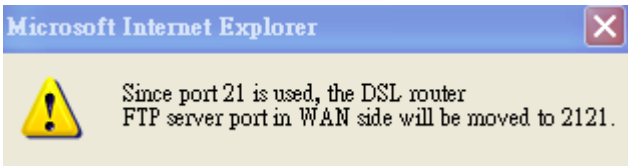
We can see that the WAN1 is assigned with IP = 172.23.30.106/24.

b. Create a port forwarding rule for the FTP server.

1. Go to **Network > NAT > Port Forwarding.**
2. Select the **Service Name**, e.g. “FTP”.
3. Select the **WAN Interface**, e.g. “INTERNET/ptm0_1”.
4. Enter the **Server IP Address**, e.g. “192.168.1.33”.
5. Enter the **External port Start**, e.g. “21”.
6. Enter the **External port End**, e.g. “21”.
7. Enter the **Internal port Start**, e.g. “999”.
8. Enter the **Internal port End**, e.g. “999”.
9. Select the **Protocol**, e.g. “TCP”.
10. Click **Add.**

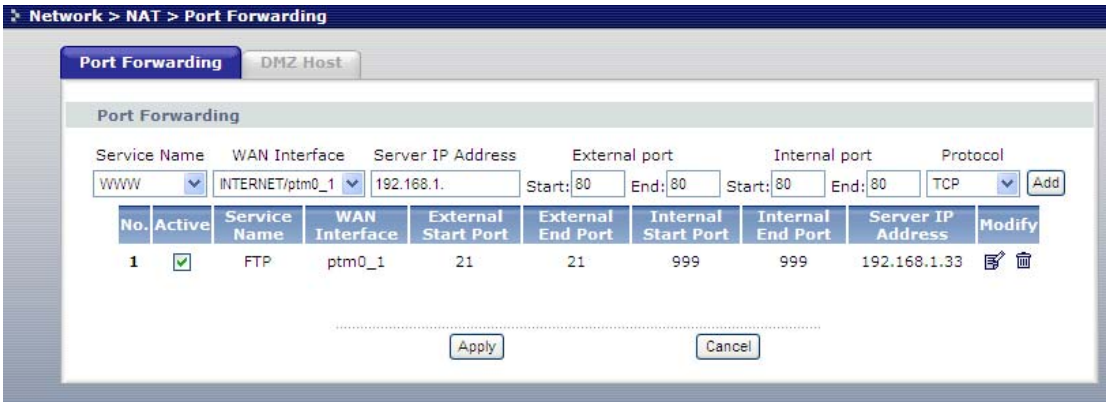


A warning message as followed will pop up:



This phenomenon is normal, because the CPE itself can be accessed by the FTP, which the port is also 21. Since we are creating a new rule using port 21, the default port number of the CPE’s FTP server port will automatically be moved to 2121.

A new port forwarding rule is now created.



Show the IP configuration of notebook:

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . : zyxel.com.tw
        IP Address. . . . . . . . . . . . : 172.23.98.235
        Subnet Mask . . . . . . . . . . . : 255.255.248.0
        Default Gateway . . . . . . . . . : 172.23.97.1
```

Use the notebook to access the FTP server with IP = 172.23.30.106.

```
C:\>ftp 172.23.30.106
Connected to 172.23.30.106.
220 FTP Server 2.0 Ready.
User (172.23.30.106:(none)): test
331 User name okay, need password.
Password:
230 User logged in
ftp>
```

Show the history log of FTP server.

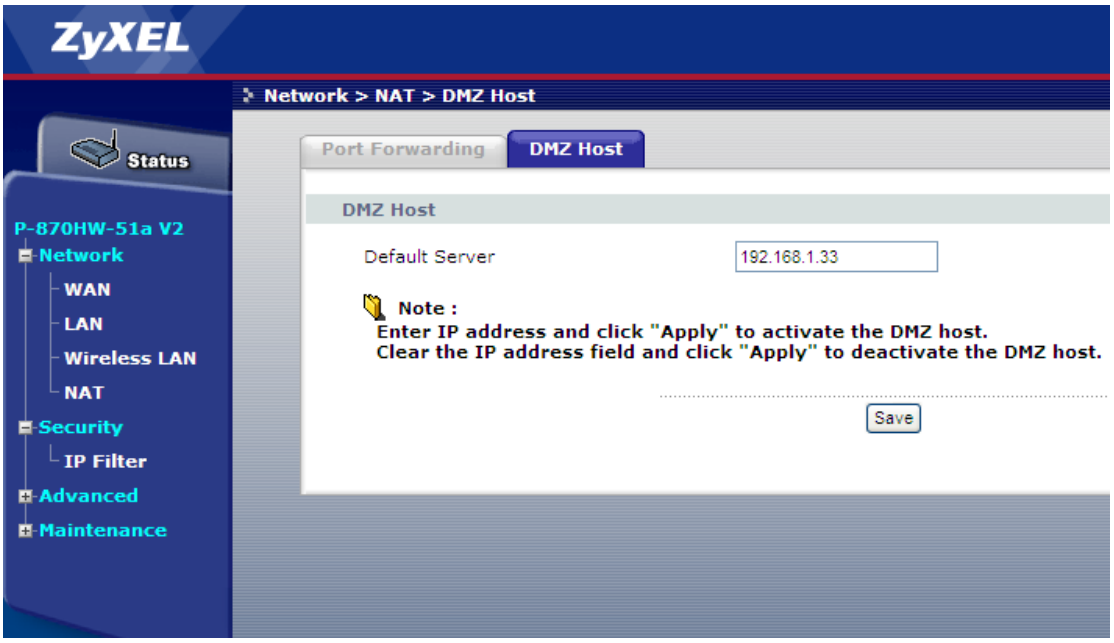
We can see that the client (notebook with IP = 172.23.98.235) is in fact logged into the FTP server.

DMZ Host Configuration

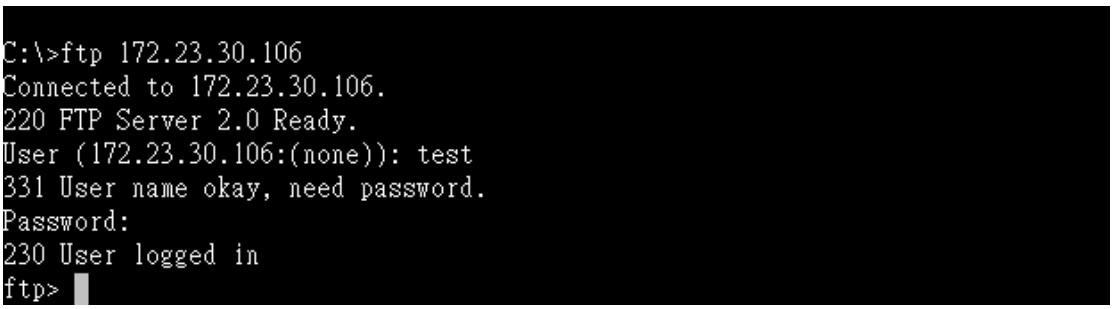
If we enable the DMZ host, it will open up all the internal ports to the dedicated Server IP (in this case, IP = 192.168.1.33) allowing client at the WAN side to access the FTP server via port forwarding.

a. Create a DMZ host.

1. Go to **Network > NAT > DMZ host.**
2. Enter the IP of the **Default Server**, e.g. “192.168.1.33”.
3. Click **Save.**



Use the notebook to access the FTP server with IP = 172.23.30.106.

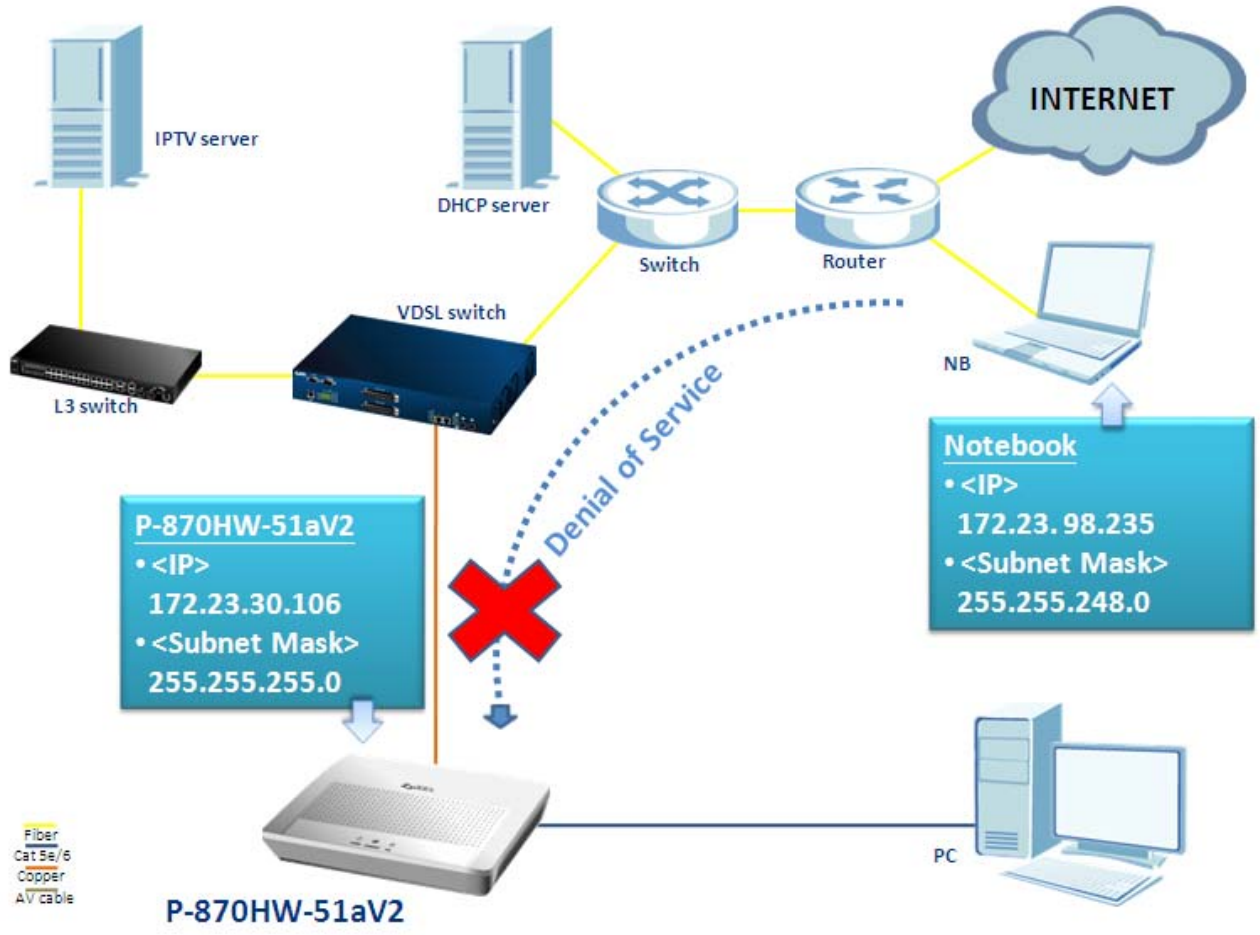


Show the history log of FTP server.

We can see that the client (notebook with IP = 172.23.98.235) is in fact logged into the FTP server.

IP Filter

Environment

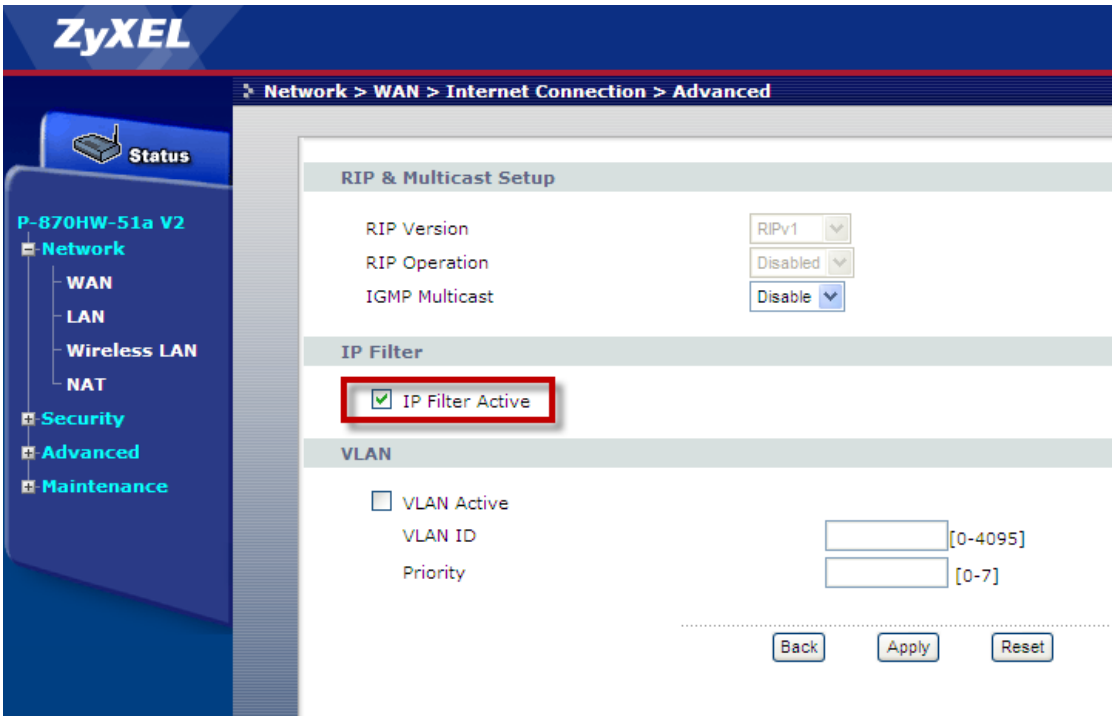


The P-870HW-51aV2 has stateful packet Inspection and Denial of service (DoS) function; it provides the first line of defense against hackers, network intruders and other hazardous threats. In the case of the above scenario, we would like to have the CPE filter all the traffic coming from notebook. How should we configure the P-870HW-51aV2 to fit this scenario? The following step-by-step procedure instructs us the method.

IP Filter Configuration

a. Check the setting of the WAN interface.

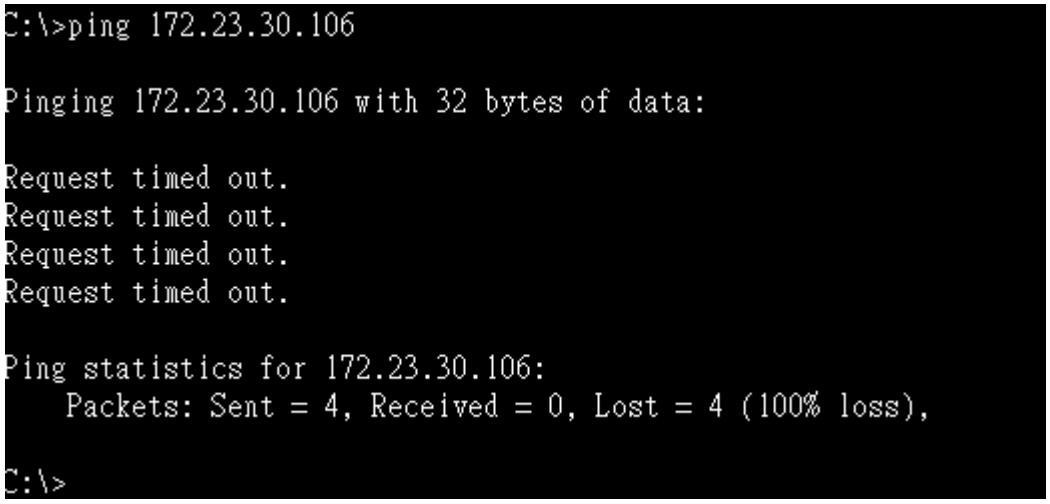
1. Go to **Network > WAN > Internet Connection > Advanced Setup.**
2. Check the **IP Filter Active** box.
3. Click **Apply.**



Show the IP configuration of notebook:

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . : zyxel.com.tw
        IP Address. . . . . . . . . . . . : 172.23.98.235
        Subnet Mask . . . . . . . . . . . : 255.255.248.0
        Default Gateway . . . . . . . . . : 172.23.97.1
```

Use the notebook to ping the P-870HW-51aV2 with IP = 172.23.30.106.

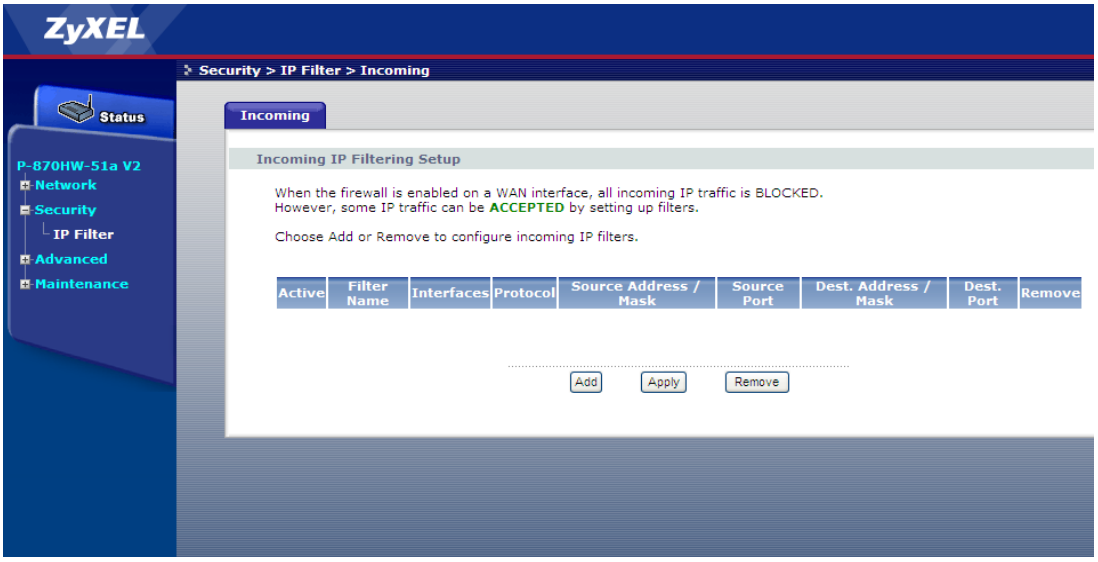


We can see that the ICMP packets do not come back; it is clearly that the ping request packets have all been filtered out by the CPE.

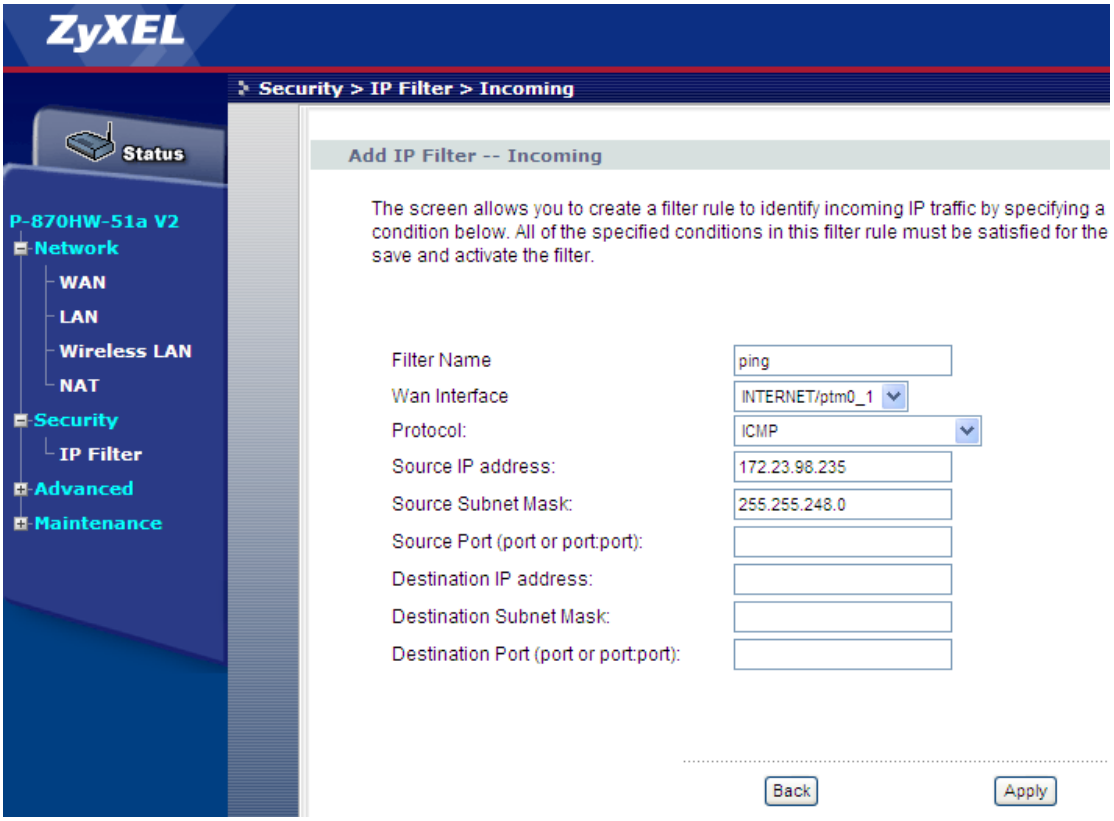
Configuration of Accepting Incoming Traffic

b. Configure the IP Filtering Setup.

1. Go to **Security > IP Filter > Incoming.**
2. Click **Add.**

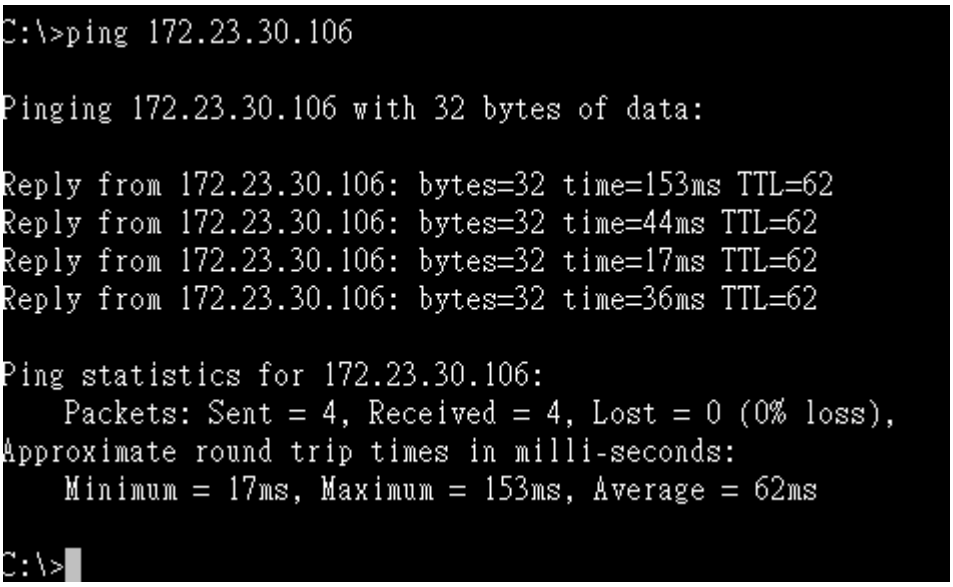


3. Enter the **Filter Name**, e.g. “ping”.
4. Select the **Wan Interface**, e.g. “INTERNET/ptm0_1”.
5. Select the **Protocol**, e.g. “ICMP”.
6. Enter the **Source IP address**, e.g. “172.23.98.235”.
7. Enter the **Source Subnet Mask**, e.g. “255.255.248.0”.
8. Click **Apply.**



We can see the newly created rule as followed:

Use the notebook to ping the P-870HW-51aV2 with IP = 172.23.30.106.



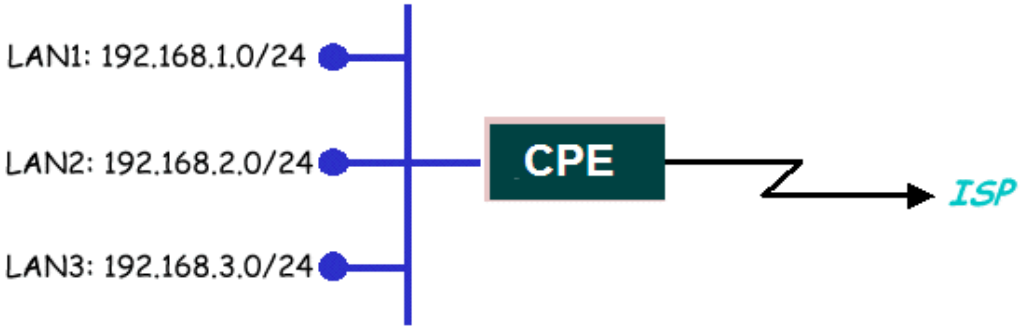
We can see that the ICMP request was successful, thus proving that the CPE is now accepting the traffic coming from notebook.

LAN Connection

IP Alias Introduction

- What is the IP Alias?

In a typical environment, a LAN router is required to connect two local networks. The device can connect three local networks to the ISP or a remote node; we call this function as **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using CPE's single user account. See the following figure.



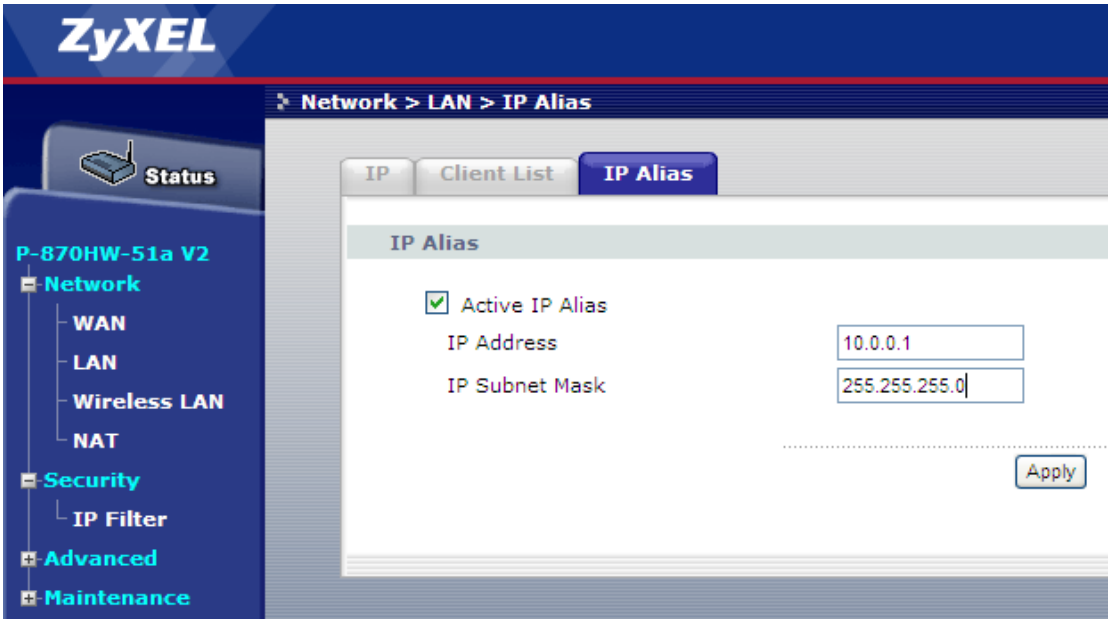
IP Alias connects three local networks to the Internet

The CPE supports three virtual LAN interfaces via its single physical Ethernet interface. As to the second and third networks, we call **'IP Alias 1'** and **'IP Alias 2'**.

IP Alias Configuration

a. IP Alias

1. Go to **Network > LAN > IP Alias.**
2. Check the **Active IP Alias** box.
3. Enter the **IP Address**, e.g. “10.0.0.1”.
4. Enter the **IP Subnet Mask**, e.g. “255.255.255.0”.
5. Click **Apply.**

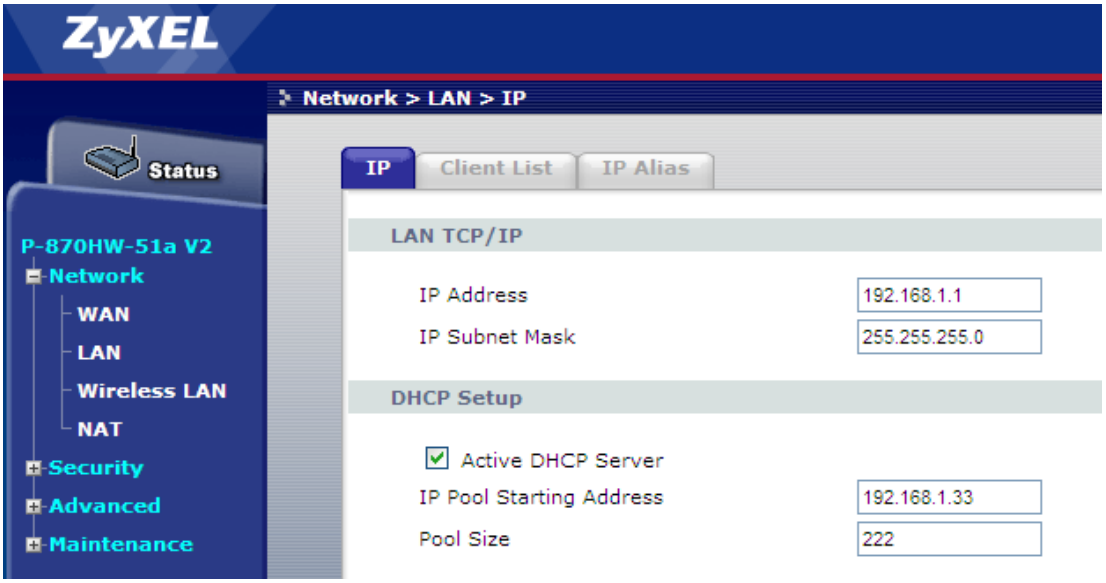


Client List Configuration

We can manually assign a particular IP to a DHCP client with the specific MAC address.

a. Enable the DHCP server.

1. Go to **Network > LAN > IP.**
2. Enter the **IP Address**, e.g. “192.168.1.1”.
3. Enter the **IP Subnet Mask**, e.g. “255.255.255.0”.
4. Check the **Active DHCP Server** box.
5. Enter the **IP Pool Starting Address**, e.g. “192.168.1.33”.
6. Enter the **Pool Size**, e.g. “222”.

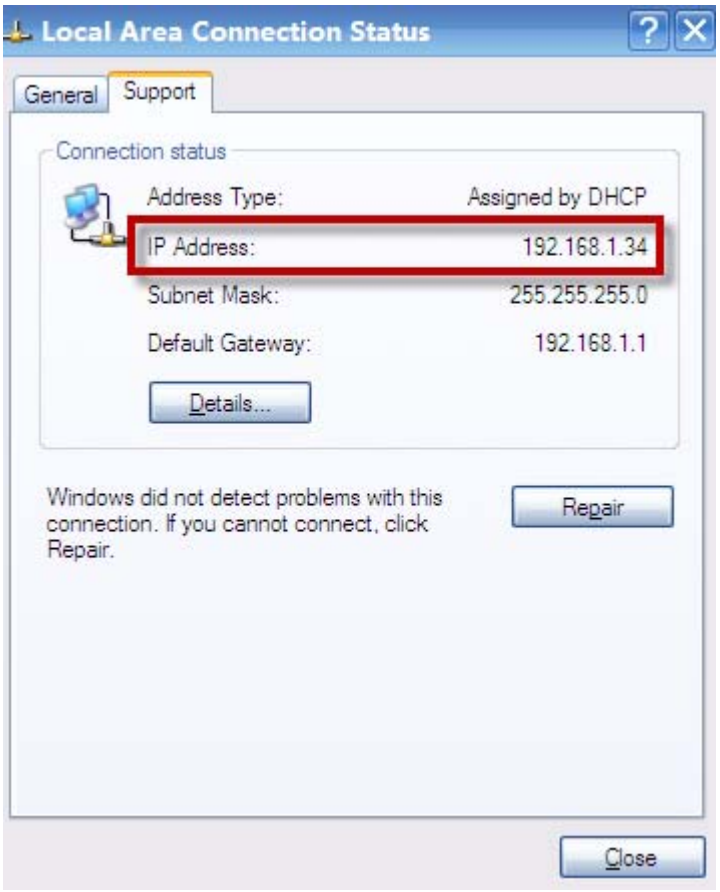


b. Show information on the DHCP server.

1. Login the device by Telnet.
2. Type the command “dhcpiprange show”.

```
 > dhcpiprange show
dhcpserver: enable
start ip address: 192.168.1.33
end ip address: 192.168.1.254
leased time: 24 housrs
 >
```

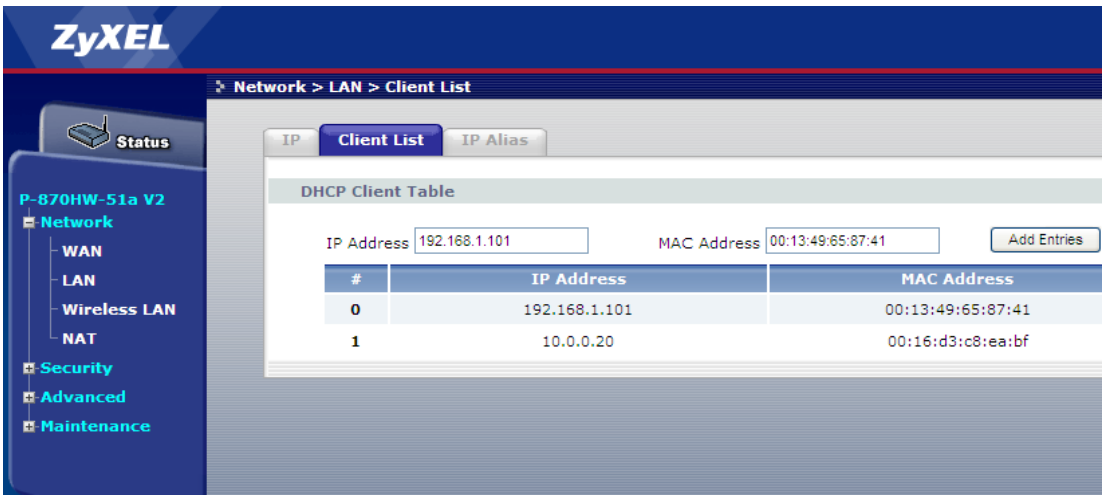
Show the IP of the DHCP client:



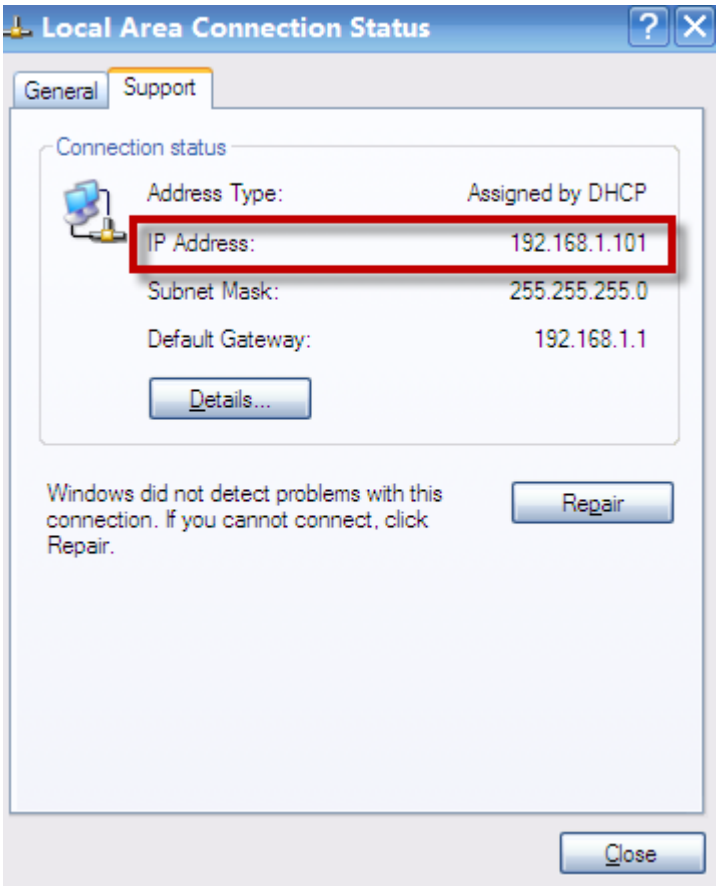
We can see that the DHCP client is assigned with IP = 192.168.1.34.

c. Edit the Client List.

1. Go to **Network > LAN > Client List.**
2. Enter the **IP Address**, e.g. “192.168.1.101”.
3. Enter the **MAC Address**, e.g. “00:13:49:65:87:41”.
4. Click **Add Entries.**



Show the IP of the DHCP client:



We can see that the DHCP client is assigned with IP = 192.168.1.101, which is the particular IP that we specifically assign to this client.

Using Universal Plug n Play (UPnP)

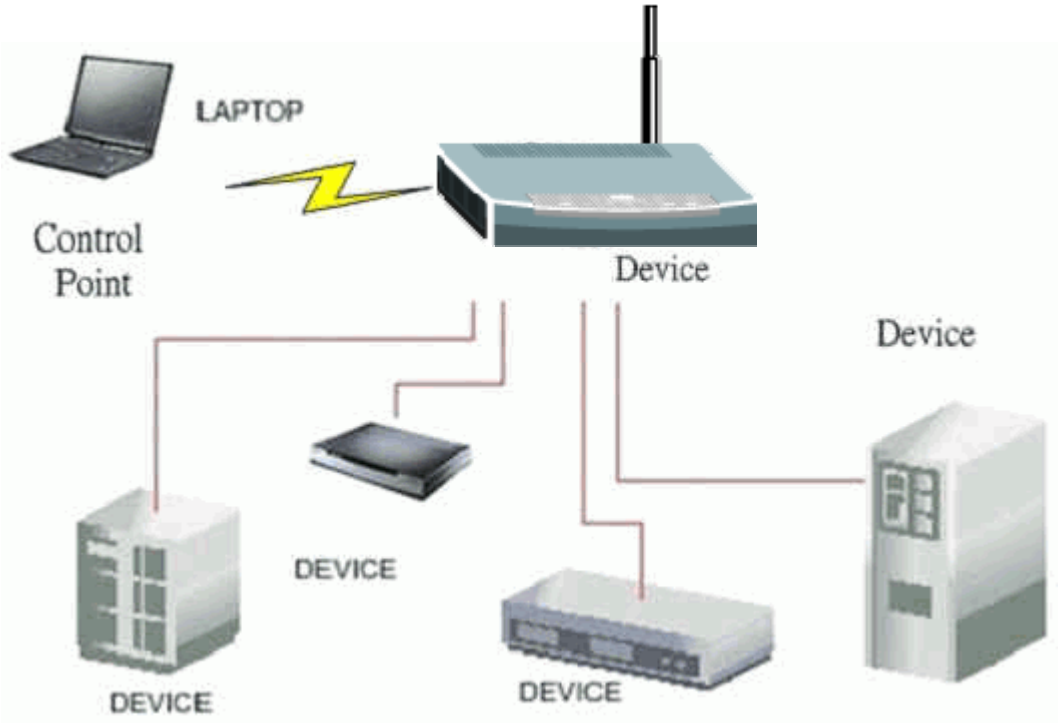
- **1. What is the UPnP?**

The UPnP (Universal Plug and Play) makes the connecting PCs of all form factors, intelligent appliances and wireless devices in the home, office and everywhere in between easier and even automatic by leveraging the TCP/IP and Web technologies. The UPnP can be supported essentially in any operating system and works essentially with any type of physical networking media, wired or wireless.

The UPnP also supports the NAT Traversal which can automatically solve many NAT unfriendly problems. By the UPnP, applications assign the dynamic port mappings to the Internet gateway and delete the mappings when the connections are complete.

The key components in the UPnP are devices, services and control points.

- **Devices**: Network devices, such as networking gateways, TV, refrigerators, printers, etc, which provide services.
- **Services**: Services are provided by devices, such as time services provided by alarm clocks. In the UPnP, services are described in XML format. Control points can set/get services information from devices.
- **Control points**: Control points can manipulate the network devices. When you add a new control point (in this case, a laptop) to a network, the device may ask the network to find the UPnP-enabled devices. These devices respond with their URLs and device descriptions.



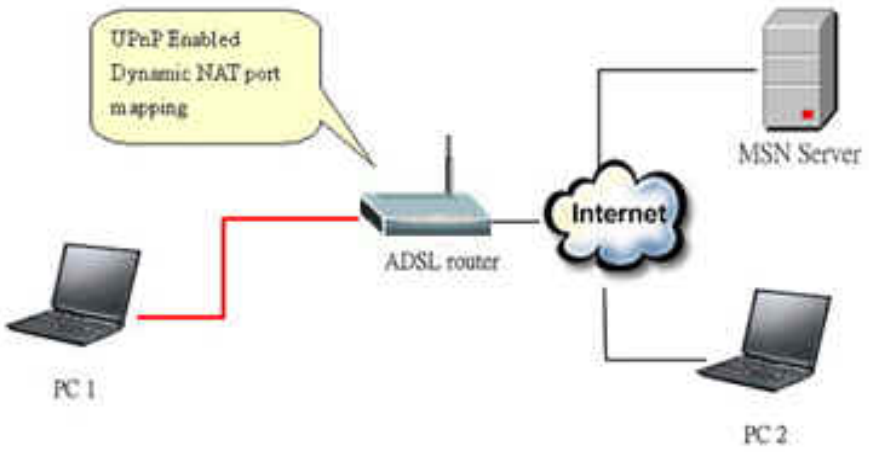
UPnP Operations

- **Addressing**: The UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each device should have the DHCP client. When the device gets connected to the network, it will discover DHCP server on network to get an IP address. If not, then the Auto-IP mechanism should be supported, so that the device can give itself an IP address. (169.254.0.0/16)
- **Discovery**: Whenever a device is added into the network, it will advertise its service over the network. Control point can also discover services provided by devices.
- **Description**: Control points can get more detailed service information from devices' description in XML format. The description may include the product name, model name, serial number, vendor ID and embedded services, etc.
- **Control**: Devices can be manipulated by control points through Control message.
- **Eventing**: Devices can send event message to notify control points, if there is any update on services provided.
- **Presentation**: Each device can provide its own control interface by the URL link. So that users can go to the device's presentation Web page by the URL to control this device.

- **2. Using the UPnP in ZyXEL devices.**

In this example, we will introduce how to enable the UPnP function in ZyXEL devices. Currently, Microsoft MSN is the most popular application exploiting the UPnP, so we take Microsoft MSN application as an example in this support note. You can learn how MSN benefits from the NAT traversal feature in UPnP in this application note.

In the diagram, supposing that PC1 and PC2 both sign in MSN server, they would like to establish a video conference. The PC1 is behind the PPPoE dial-up router which supports the UPnP. Since the router supports the UPnP, we don't need to setup the NAT mapping for PC1. As long as we enable the UPnP function on the router, the PC1 will assign the mapping to the router dynamically. Note that, since the PC1 must support UPnP, we presume that its OS is Microsoft WinME or WinXP.

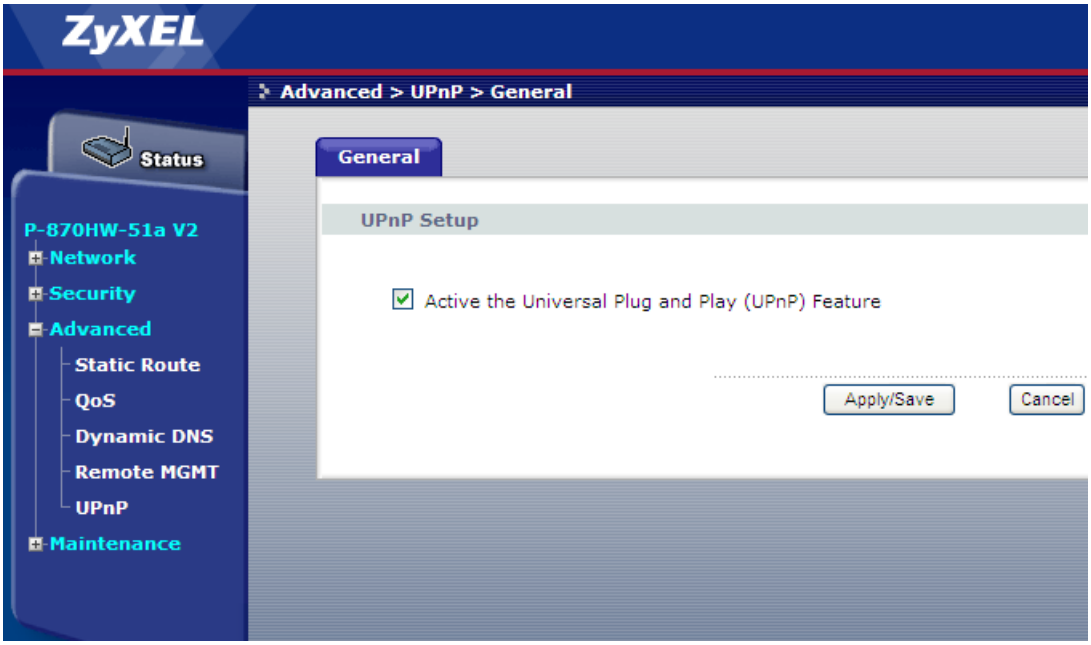


Device: Device Router
Service: NAT function provided by device Router
Control Point: PC1

Universal Plug n Play (UPnP) Configuration

a. Activate the UPnP feature.

1. Go to **Advanced > UPnP > General.**
2. Check the **Active the Universal Plug and Play (UPnP) Feature** box.
3. Click **Apply.**



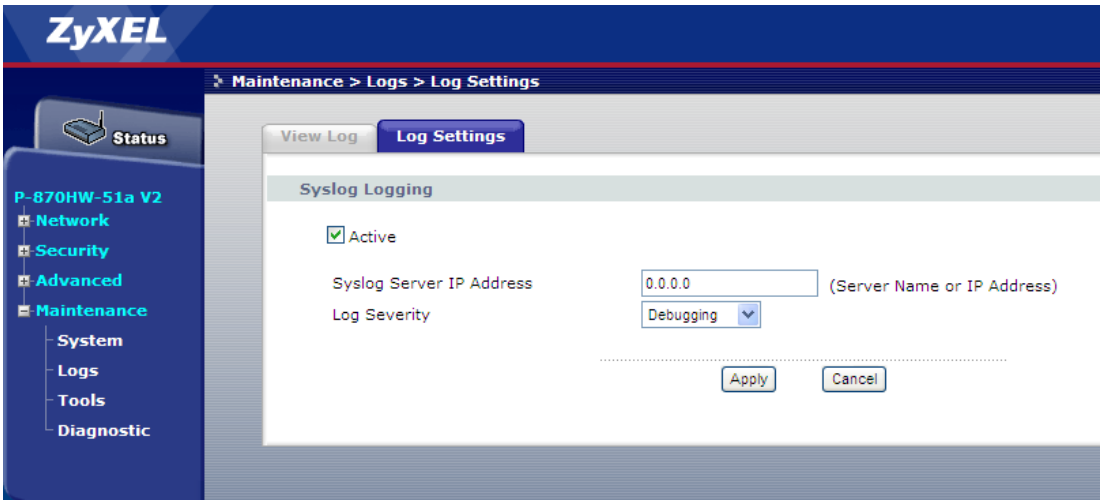
Maintenance Log

Internal Maintenance

The P-870HW-51aV2 has the ability to record the events happening in the CPE into a system log (according to the severity) and maintain this log in itself.

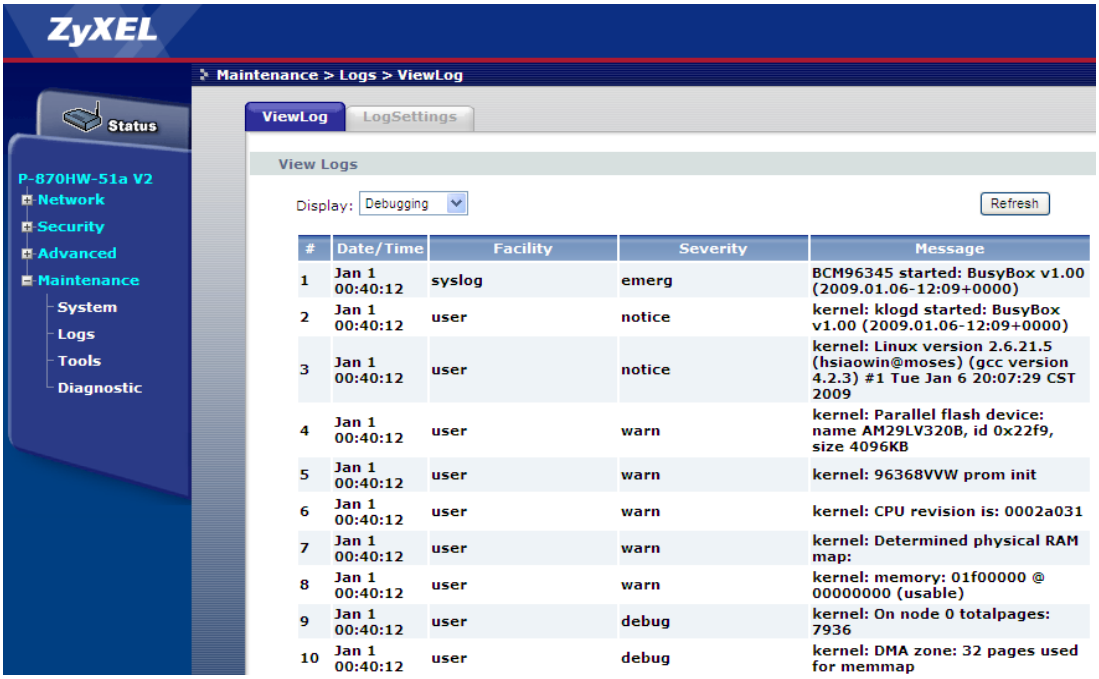
a. Activate the Maintenance Log.

1. Go to **Maintenance > Logs > Log Settings.**
2. Check the **Active** box.
3. Enter the **Syslog Server IP Address** to be “0.0.0.0”.
4. Select the **Log Severity**, e.g. “Debugging”.
5. Click **Apply.**



b. Show the log in the Web GUI.

1. Go to **Maintenance > Logs > ViewLog.**
2. Select the **Display**, e.g. “Debugging”.
3. Click **Refresh.**



c. Show the log by Telnet.

1. Login the device by Telnet,
2. Type the command “syslog dump”.

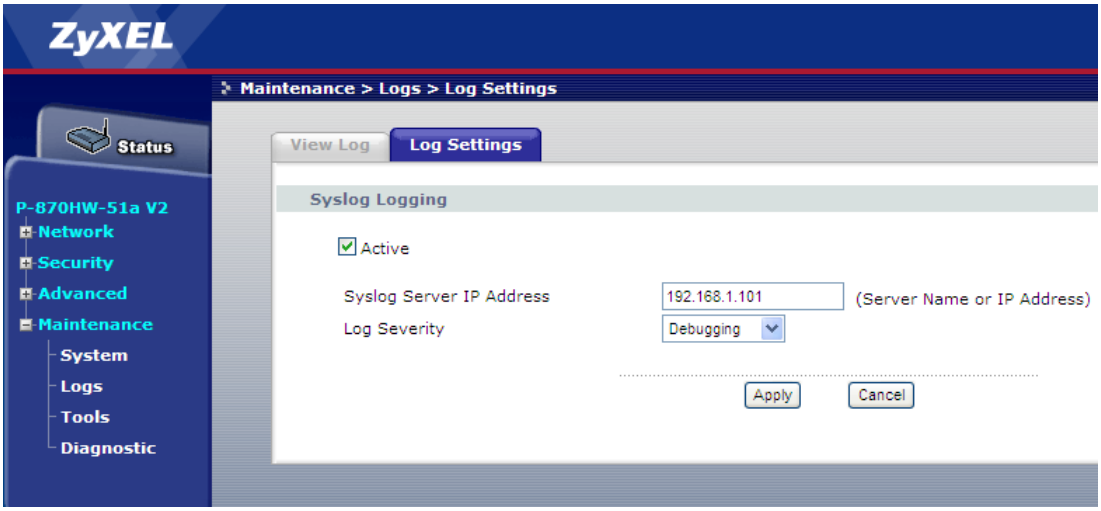
```
 > syslog dump
==== Dump of Syslog ====
Jan  1 00:40:12 (none) syslog.emerg BCM96345  started: BusyBox v1.00 (2009.01.06
-12:09+0000)
Jan  1 00:40:12 (none) user.notice kernel: klogd started: BusyBox v1.00 (2009.01
.06-12:09+0000)
Jan  1 00:40:12 (none) user.notice kernel: Linux version 2.6.21.5 (hsiaowin@mose
s) (gcc version 4.2.3) #1 Tue Jan 6 20:07:29 CST 2009
Jan  1 00:40:12 (none) user.warn kernel: Parallel flash device: name AM29LV320B,
 id 0x22f9, size 4096KB
Jan  1 00:40:12 (none) user.warn kernel: 96368VVW prom init
Jan  1 00:40:12 (none) user.warn kernel: CPU revision is: 0002a031
Jan  1 00:40:12 (none) user.warn kernel: Determined physical RAM map:
Jan  1 00:40:12 (none) user.warn kernel:  memory: 01f00000 @ 00000000 (usable)
Jan  1 00:40:12 (none) user.debug kernel: On node 0 totalpages: 7936
Jan  1 00:40:12 (none) user.debug kernel:   DMA zone: 32 pages used for memmap
Jan  1 00:40:12 (none) user.debug kernel:   DMA zone: 0 pages reserved
Jan  1 00:40:12 (none) user.debug kernel:   DMA zone: 4064 pages, LIFO batch:0
Jan  1 00:40:12 (none) user.debug kernel:   Normal zone: 30 pages used for memma
```

Remote Maintenance

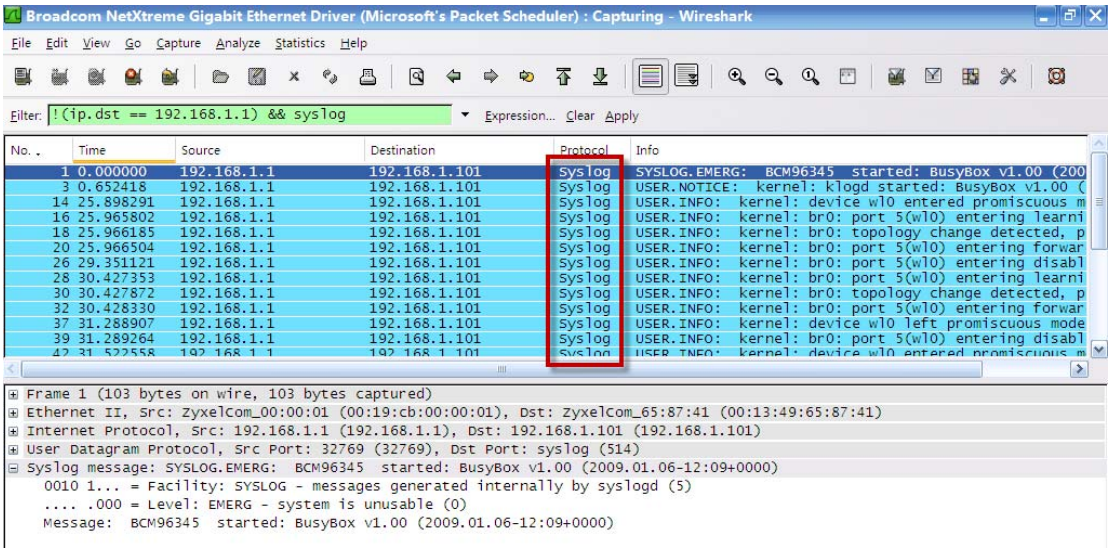
The P-870HW-51aV2 also has the ability to send the system log outside the CPE. Let's say that we want the system log to be sent to the notebook with IP = 192.168.1.101.

a. Activate the Maintenance Log.

1. Go to **Maintenance > Logs > Log Settings.**
2. Check the **Active** box.
3. Enter the **Syslog Server IP Address** to be "192.168.1.101".
4. Select the **Log Severity**, e.g. "Debugging".
5. Click **Apply.**



We can see the system logs being sent from the CPE by opening Ethereal in the notebook.

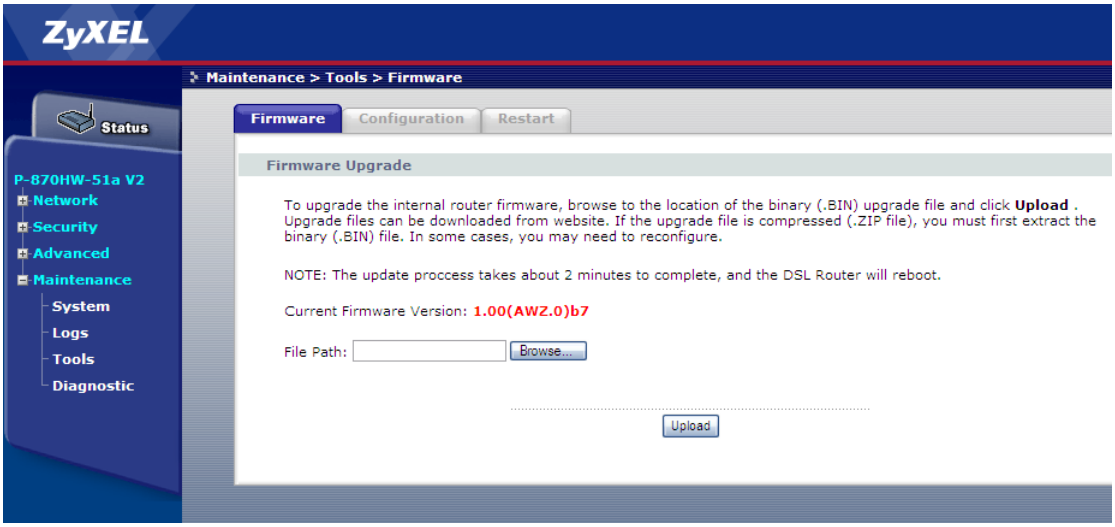


Maintenance Tool

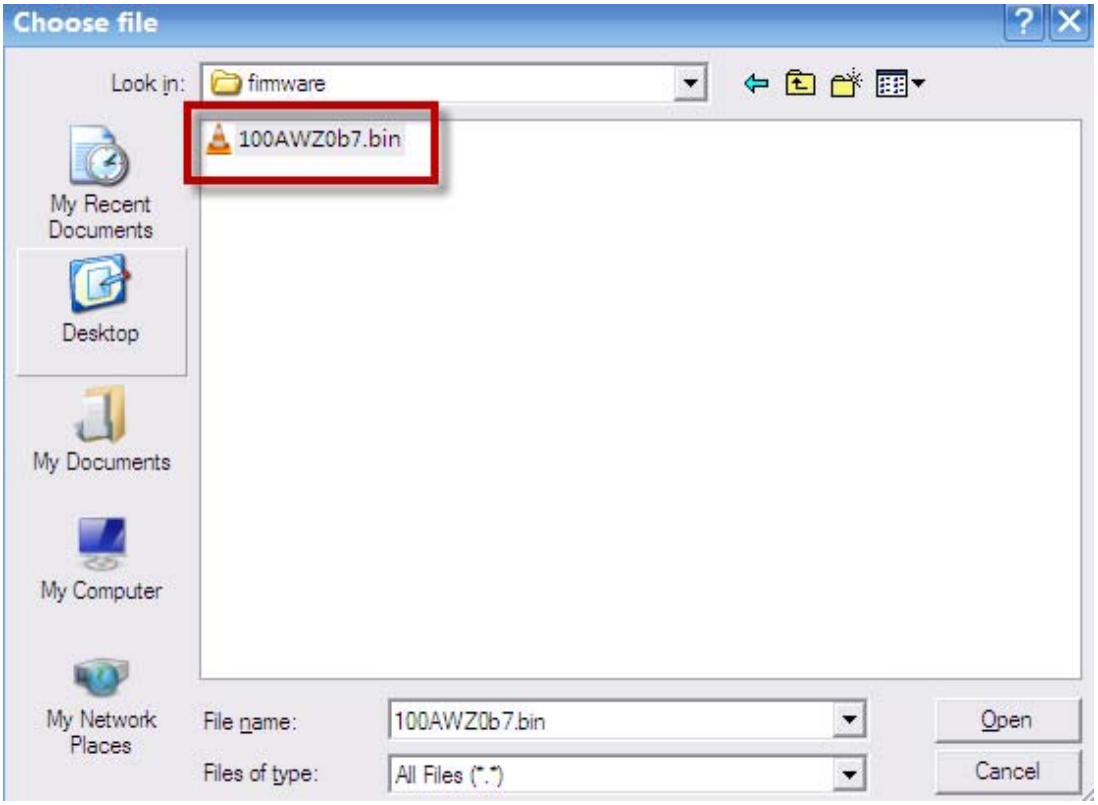
Maintenance Procedure

a. Upload Firmware.

1. Go to **Maintenance > Tools > Firmware.**



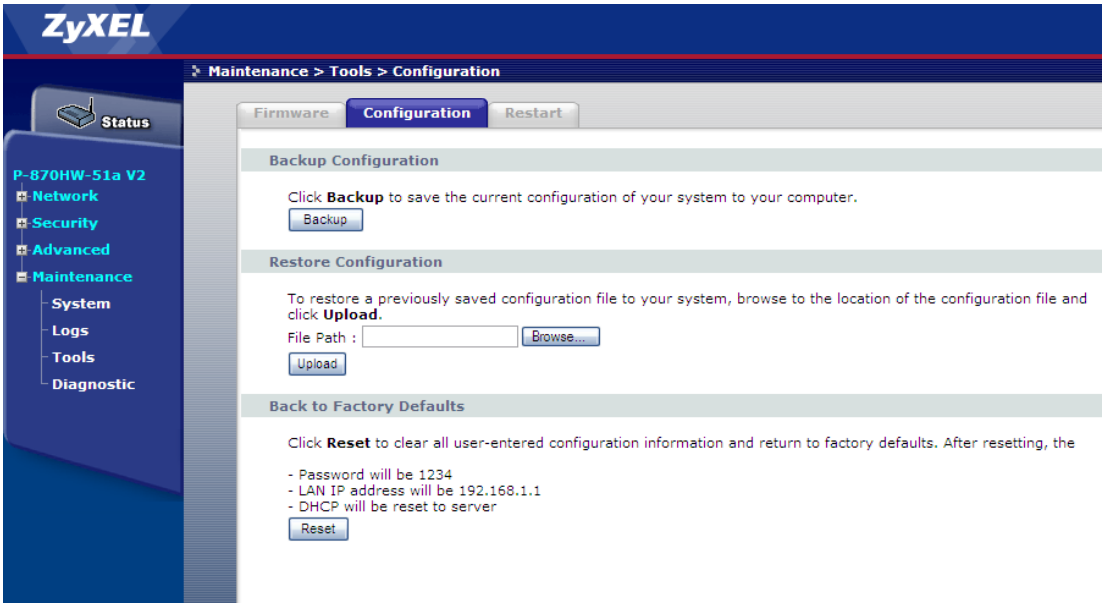
2. Click **Browse.**
3. Select the Firmware to upload and click Open.



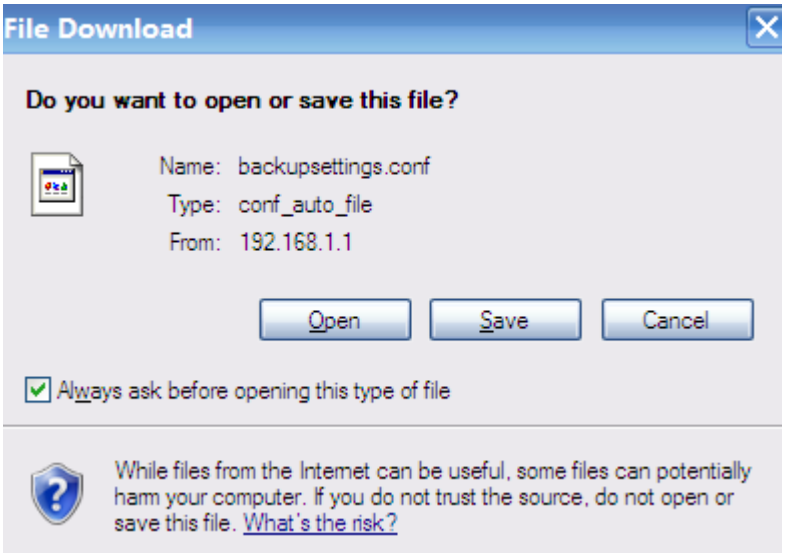
4. Click **Upload.**

b. Save Configuration.

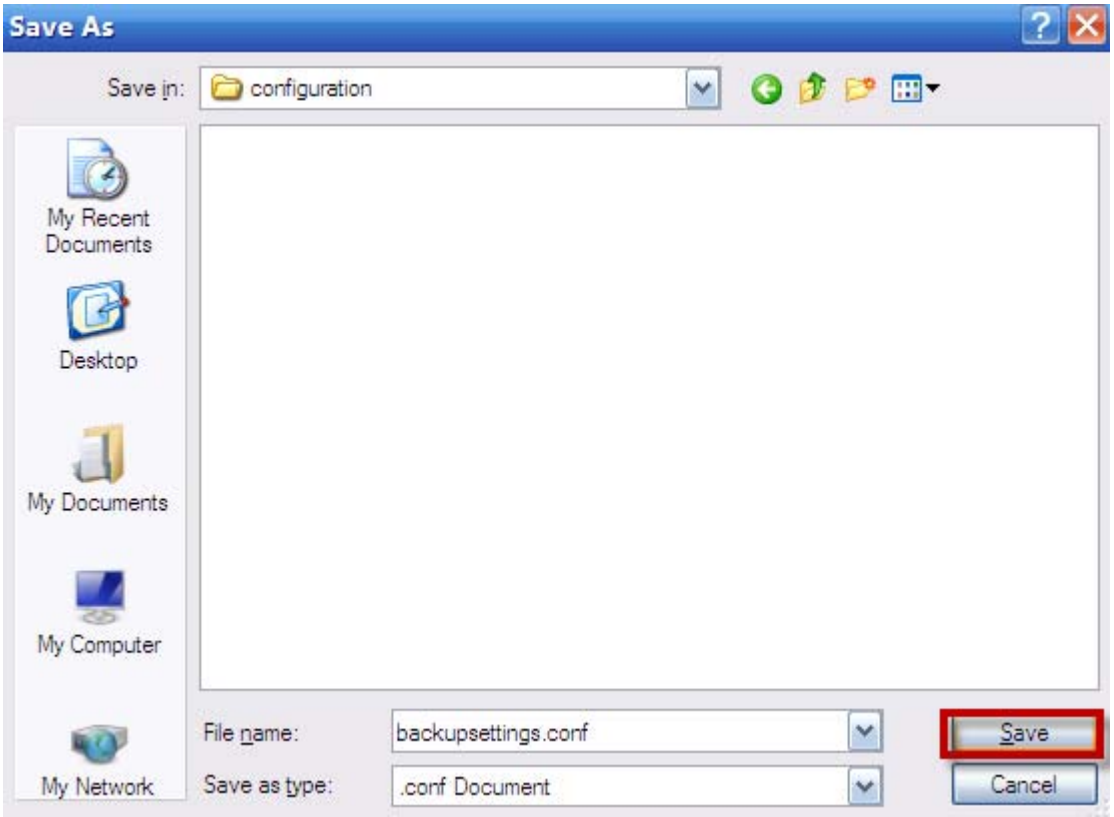
1. Go to **Maintenance > Tools > Configuration.**



2. Click **Backup.**
3. Click **Save.**

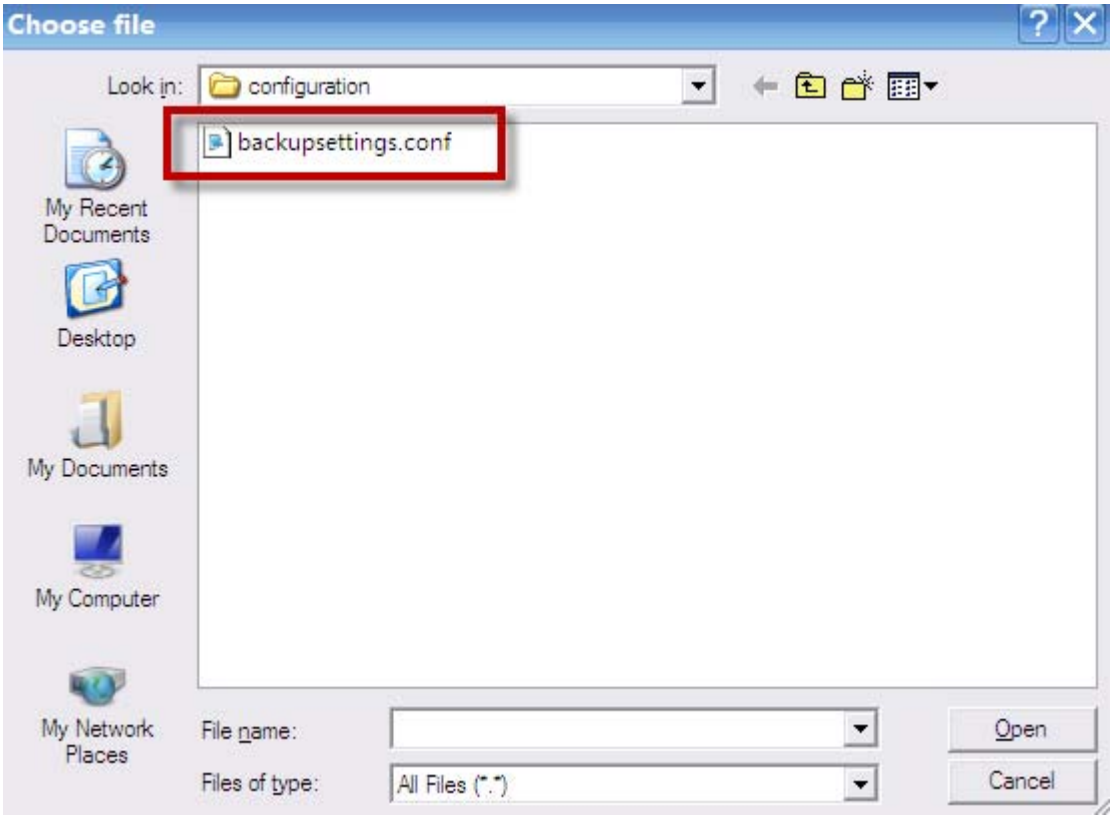


4. Select the directory to save and click Save.



c. Upload Configuration.

1. Go to **Maintenance > Tools > Configuration.**
2. Click **Browse.**
3. Select the configuration file to upload and click Open.



Wireless Application Notes

Wireless Introduction

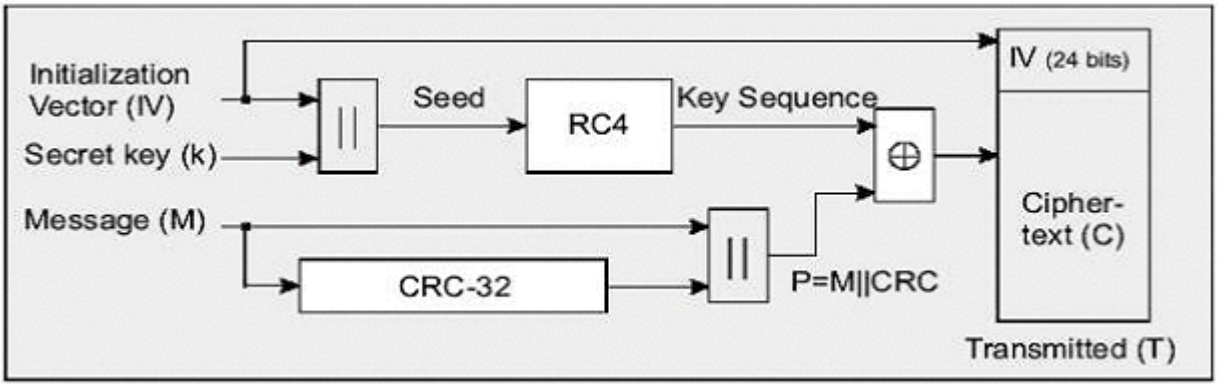
WEP Configuration (Wired Equivalent Privacy) Introduction

The 802.11 standard describes the communication that occurs in the wireless LANs.

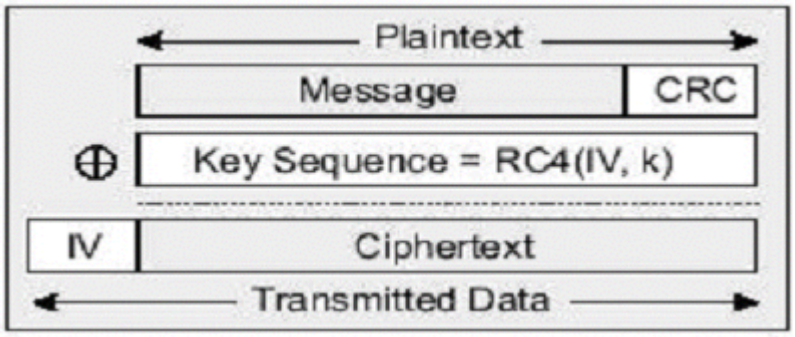
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because the wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium. Everything that is transmitted or received over a wireless network can be intercepted.

The WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packages are not modified during the transition. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points APs.

The WEP employs the key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG). The same key is used to encrypt and decrypt the data.



The WEP has defenses against this attack. To avoid encrypting two cipher texts with the same key stream, an Initialization Vector (IV) is used to augment the shared WEP key (secret key) and produce a different RC4 key for each packet. The IV is also included in the package. The WEP keys (secret key) are available in two types, 64-bits and 128-bits. Many times you will see them referenced as 40-bits and 104-bits instead. The reason for this misnomer is that the WEP key (40/104 bits) is concatenated with the initialization vector (24 bits) resulting in a 64/128 bit total key size.



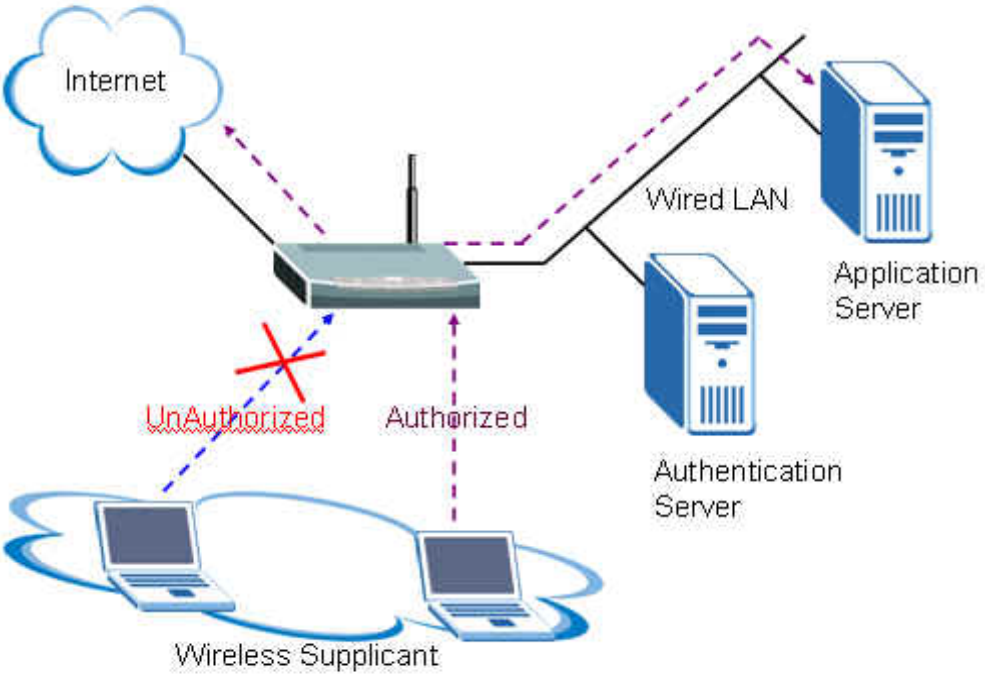
Setting up the Access Point

Most access points and clients have the ability to hold up to the 4 WEP keys simultaneously. You need to specify one of the 4 keys as default Key for data encryption. To set up the Access Point, you will need to set one of the following parameters:

- 64-bit WEP key (secret key) with 5 characters.
- 64-bit WEP key (secret key) with 10 hexadecimal digits.
- 128-bit WEP key (secret key) with 13 characters.
- 128-bit WEP key (secret key) with 26 hexadecimal digits.

IEEE 802.1x Introduction

The IEEE 802.1x port-based authentication is desired to prevent the unauthorized devices (clients) from gaining access to the network. As the LANs extend to hotels, airports and corporate lobbies, the insecure environments could be created. The 802.1x port-based network access control makes use of the physical access characteristics of **IEEE 802 LAN infrastructures**, such as the 802.3 Ethernet, 802.11 Wireless LAN and VDSL LRE (Long Reach Ethernet), in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in case of the failure of authentication process.



The IEEE 802.1x authentication is a client-server architecture delivered with the EAPOL (Extensible Authentication Protocol over LAN). The authentication server authenticates each client connected to an Access Point (for Wireless LAN) or switch port (for Ethernet) before accessing any services offered by the Wireless AP. The 802.1x contains tree major components:

1. Authenticator:

The device (i.e. Wireless AP) facilitates the authentication for supplicant (Wireless client) attached on the Wireless network. Authenticator controls the physical access to the network based on the authentication status of client. The authenticator acts as an intermediary (proxy) between the client and authentication server (i.e. RADIUS server), requesting the identity information from the client, verifying that information with the authentication server and relaying a response to the client.

2. Supplicant:

The station (i.e. Wireless client) is being authenticated by an authenticator attached on the Wireless network. The supplicant requests access to the LAN services and responds to the requests from the authenticator. The station must be running the 802.1x-compliant client software, such as that offered in the Microsoft Windows XP operating system, Meeting House AEGIS 802.1x client and Odyssey 802.1x client.

3. Authentication Server:

The device (i.e. RADIUS server) provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. The authentication server performs the actual authentication of client. It validates the identity of the supplicant. Because the authenticator acts as the proxy, the authentication service is transparent to the supplicant.

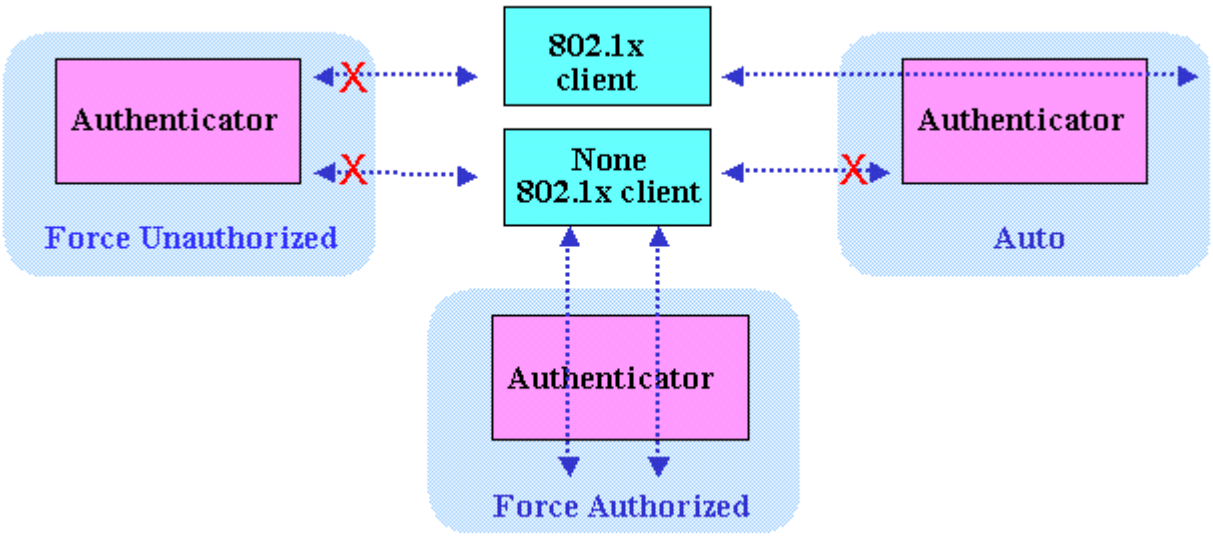
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, therefore the external RADIUS authentication server is not needed. In this case, the Wireless AP is acted as both authenticator and authentication server.

- ***Authentication Port State and Authentication Control***

The port state determines whether or not the supplicant (Wireless Client) is granted access to the network behind Wireless AP. There are two authentication port state on the AP, **authorized state** and **unauthorized state**.

By default, the port starts in the unauthorized state. While in this state, the port disallows all the incoming and outgoing data traffic, except for 802.1x packets. When a supplicant is successfully authenticated, the port transits to the authorized state, allowing all the traffic for client to flow normally. If a client that does not support the 802.1x is connected to an unauthorized 802.1x port, the authenticator requests the client's identity. In this situation, the client does not respond to the 802.1x request; the port remains in the unauthorized state and the client is not granted access to the network.

When the 802.1x is enabled, the authenticator controls the port authorization state by using the following control parameters. The following three authentication control parameters are applied in the Wireless AP.



1. Force Authorized: Disables the 802.1x and causes the port to transit to the authorized state without any authentication exchange required. The port transmits

and receives the normal traffic without the 802.1x-based authentication of client. This is the default port control setting. While the AP is setup as **Force Authorized**, the Wireless client (supported 802.1x client or none-802.1x client) can always access the network.

2. Force Unauthorized: Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the supplicants through the port. While AP is setup as **Force Unauthorized**, Wireless clients (supported 802.1x client or none-802.1x client) never have the access for the network.

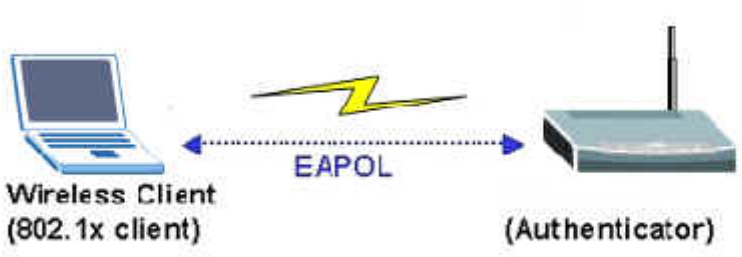
3. Auto: Enables the 802.1x and causes the port to begin in the unauthorized state, allowing only the EAPOL frames to be sent and received through the port. The authentication process begins, when the link state of port transitions from down to up or when an EAPOL-start frame is received requests the identity of the client and begins relaying authentication messages between supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the authenticator by using the client's MAC address. While the AP is setup as **Auto**, only the Wireless client supporting the 802.1x client can access the network.

- ***Re-Authentication***

The administrator can enable the periodic 802.1x client re-authentication and specify how often it occurs. When the re-authentication is time out, the authenticator will send the EAP-Request/Identity to reinitiate authentication process. In the ZyXEL Wireless AP 802.1x implementation, if you do not specify a time period before enabling the re-authentication, the number of seconds between re-authentication attempts is 1,800 seconds (30 minutes).

- ***EAPOL (Extensible Authentication Protocol over LAN)***

The authenticators and supplicants communicate with one another by using the Extensible Authentication Protocol (EAP and RFC-2284). The EAP was originally designed to run over PPP and to authenticate the dial-in users, but the 802.1x defines an encapsulation method for passing the EAP packets over Ethernet frames. This method is referred to as the **EAP over LANs, or EAPOL**. Ethernet type of EAPOL is **88-8E**, two octets in length. The EAPOL encapsulations are described for IEEE 802 compliant environment, such as the 802.3 Ethernet, 802.11 Wireless LAN and Token Ring/FDDI.

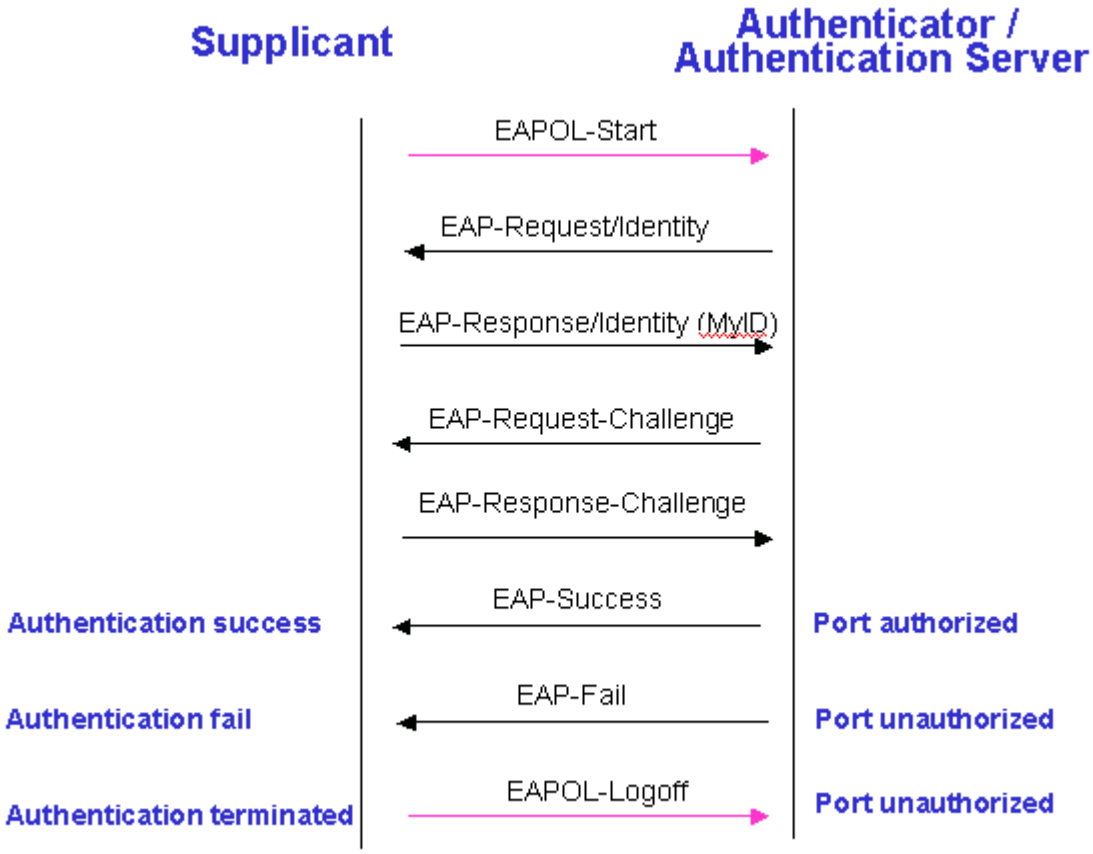


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receives the EAP request, it will reply the associated EAP response. So far, the ZyXEL Wireless AP only supports the MD-5 challenge authentication mechanism, but will support the TLS and TTLS in the future.

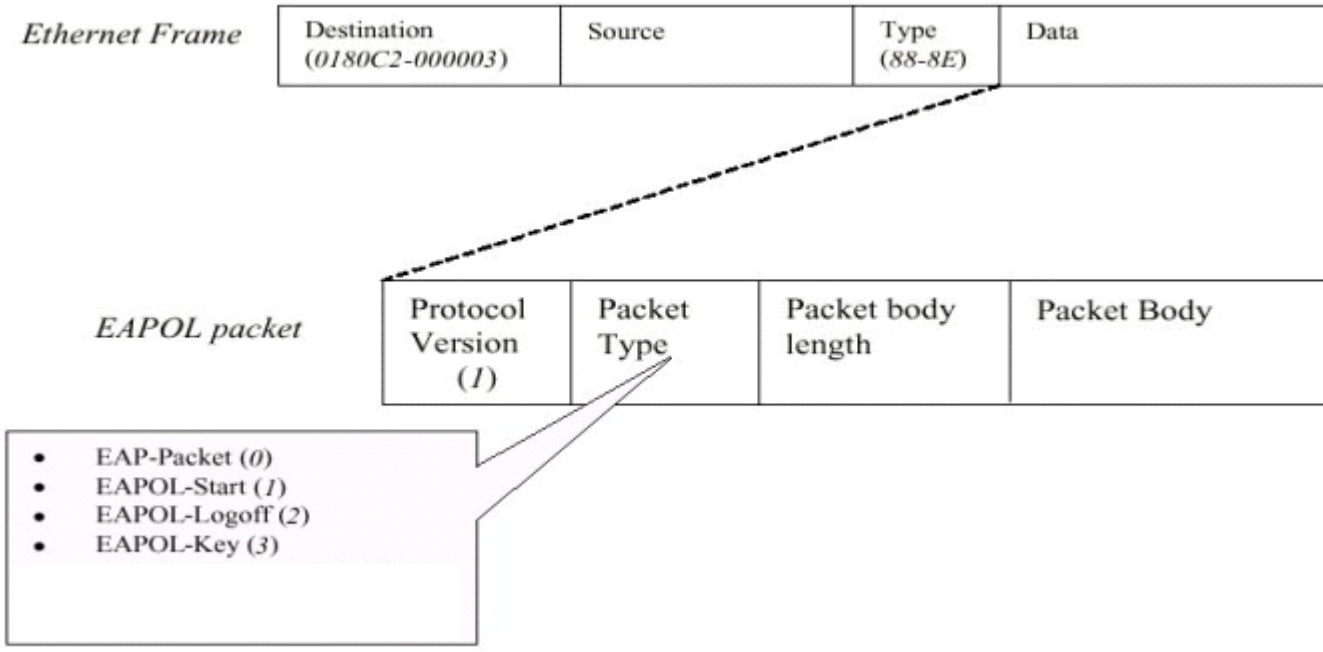
EAPOL Exchange between 802.1x Authenticator and Supplicant

The authenticator or supplicant can initiate the authentication. If you enable the 802.1x authentication on the Wireless AP, the authenticator must initiate authentication, when it determines that the Wireless link state transits from down to up. It then sends an EAP-request/identity frame to the 802.1x client to request its identity. (Typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information.) Upon the receipt of frame, the supplicant responds with an EAP-response/identity frame.

However, if during boot-up, the supplicant does not receive an EAP-request/identity frame from the Wireless AP, the client can initiate the authentication by sending an **EAPOL-Start** frame, which prompts the switch to request the supplicant's identity. In above case, authenticator is co-located with authentication server. When the supplicant supplies its identity, the authenticator directly exchanges the EAPOL to the supplicant until the authentication succeeds or fails. If the authentication succeeds, the port becomes authorized. If the authentication fails, the port becomes unauthorized. When the supplicant does not need the wireless access any more, it sends **EAPOL-Logoff** packet to terminate its 802.1x session and the port state will become unauthorized. The following figure displays the EAPOL exchange ping-pong chart.



The EAPOL packet contains the following fields: protocol version, packet type, packet body length, and packet body. Most of the fields are obvious. The packet type can have four different values and these values are described as followed:



- EAP-Packet: Both the supplicant and authenticator send this packet, when the authentication is taking place. This is the packet that contains either the MD5-Challenge or TLS information required for authentication.
- EAPOL-Start: This supplicant sends this packet, when it wants to initiate the authentication process.
- EAPOL-Logoff: The supplicant sends this packet, when it wants to terminate its 802.1x session.
- EAPOL-Key: This is used for the TLS authentication method. The Wireless AP uses this packet to send the calculated WEP key to the supplicant after the TLS negotiation has completed between the supplicant and RADIUS server.

Wi-Fi Protected Access Introduction

The Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between the WAP and WEP are user authentication and improved data encryption. The WAP applies the IEEE 802.1x Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can not use the P-660HW-Tx v2's local user database for WPA authentication purpose, since the local user database uses the MD5 EAP which can not generate keys.

The WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check and IEEE 802.1x. Temporal Key Integrity Protocol uses 128-bits keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extend initialization vector (IV) with sequencing rules and a re-keying mechanism.

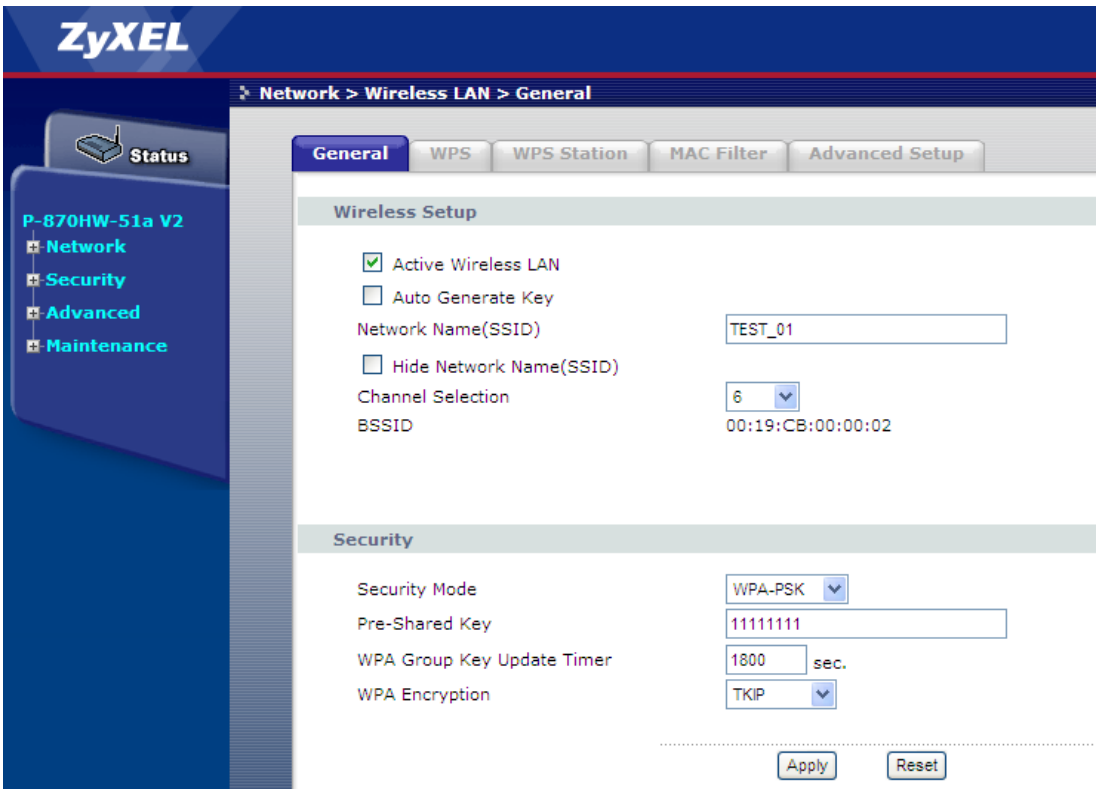
If you do not have an external RADIUS and server, you should use the **WPA-PSK** (WPA Pre-Share Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted to access to a WLAN.

Wireless Configuration

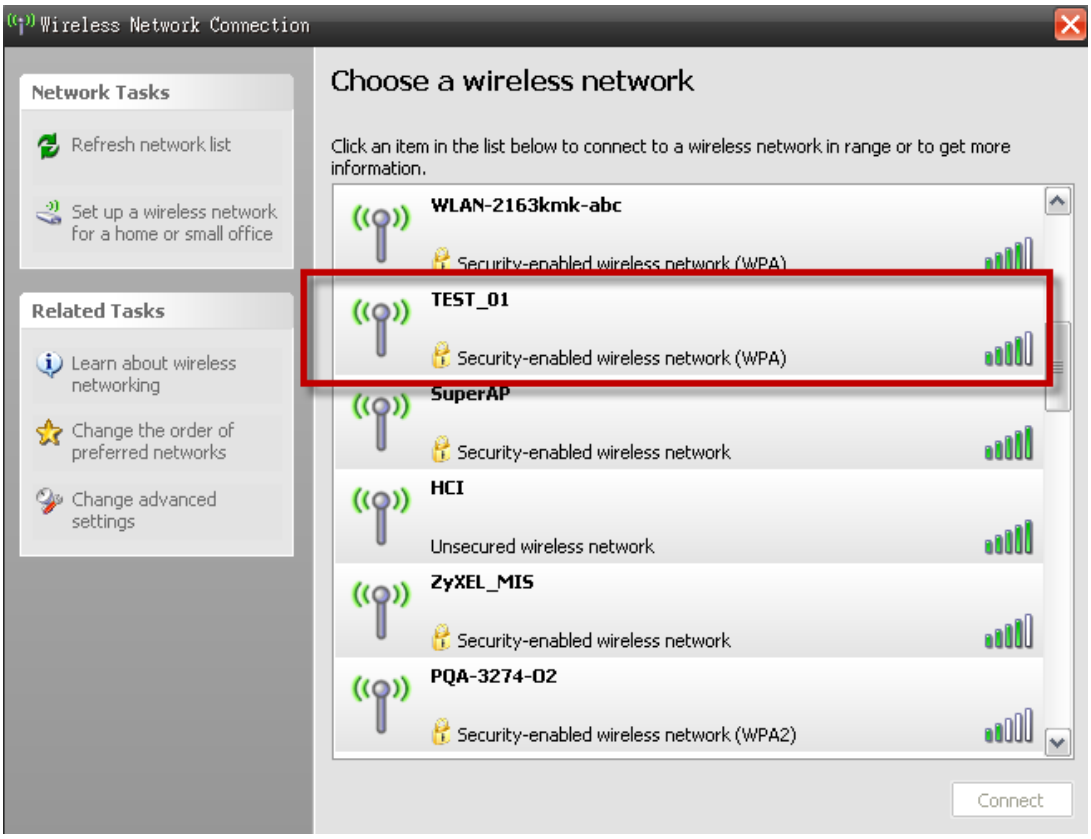
Activate the WLAN interface of the P-870HW-51aV2 and connect the notebook (802.11bg wireless NIC required) under the WPA-PSK as its security mode.

a. Wireless Setup.

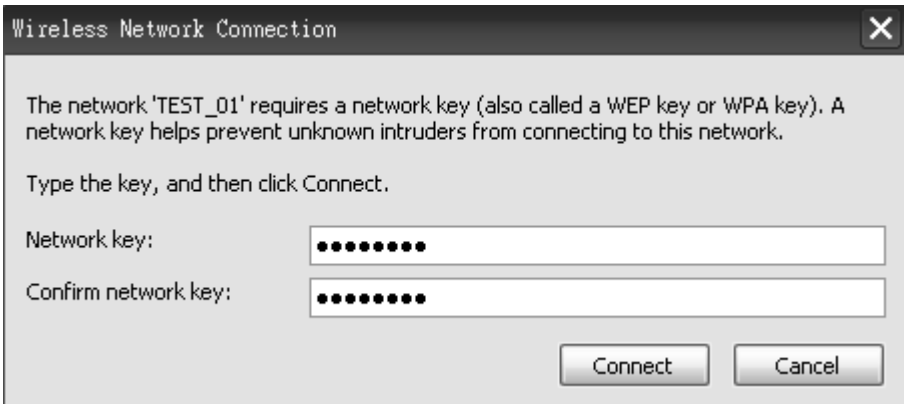
1. Go to **Network > Wireless LAN > General.**
2. Check the **Active Wireless LAN** box.
3. Enter the **Network Name(SSID)**, e.g. “TEST_01”.
4. Select the **Security Mode**, e.g. “WPA-PSK”.
5. Enter the **Pre-Shared Key**, e.g. “11111111”.
6. Enter the **WPA Group Key Update Timer**, e.g. “1800”.
7. Select the **WPA Encryption**, e.g. “TKIP”.
8. Click **Apply.**

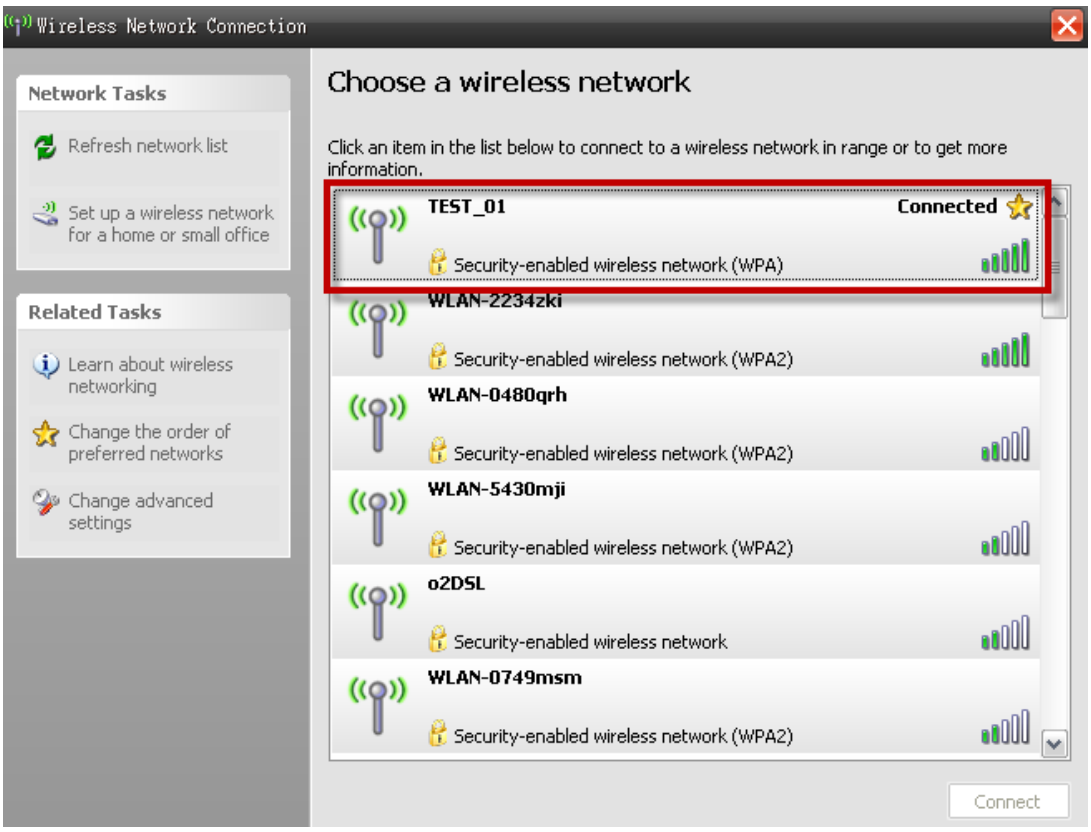


Show all the wireless networks in your notebook (802.11bg wireless NIC required):



Enter the WPA-PSK pre-shared key.

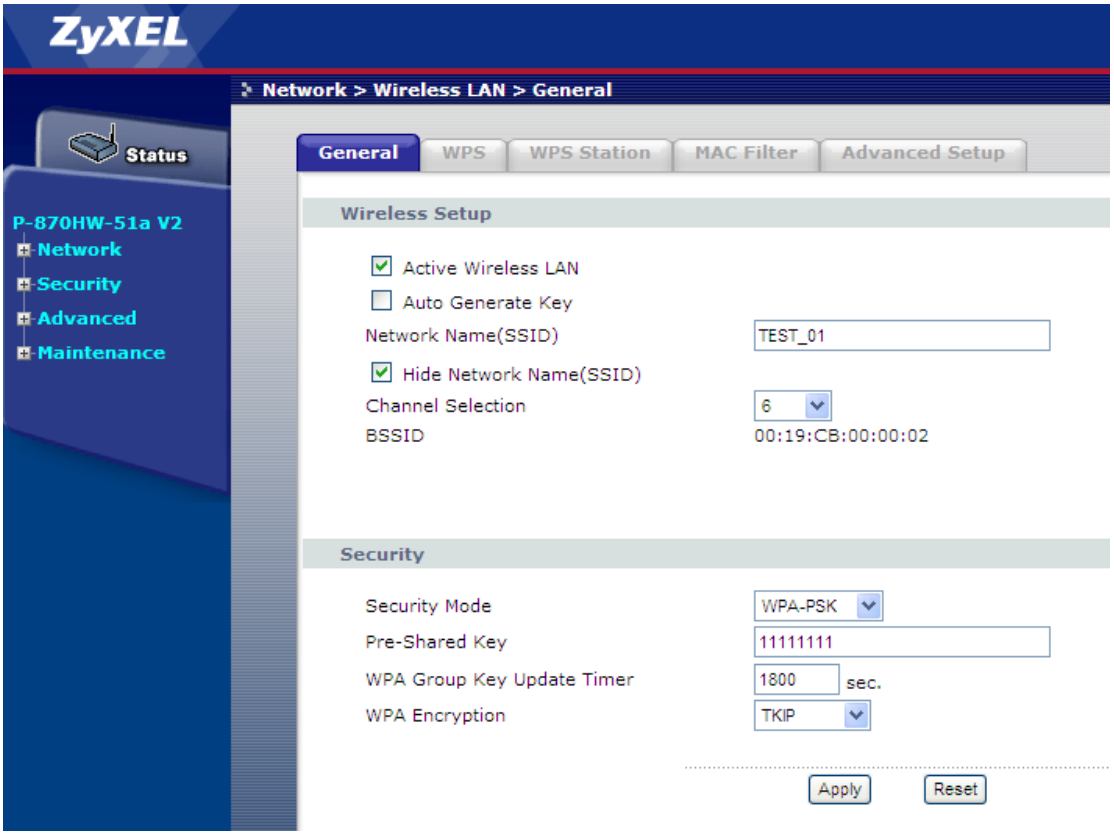




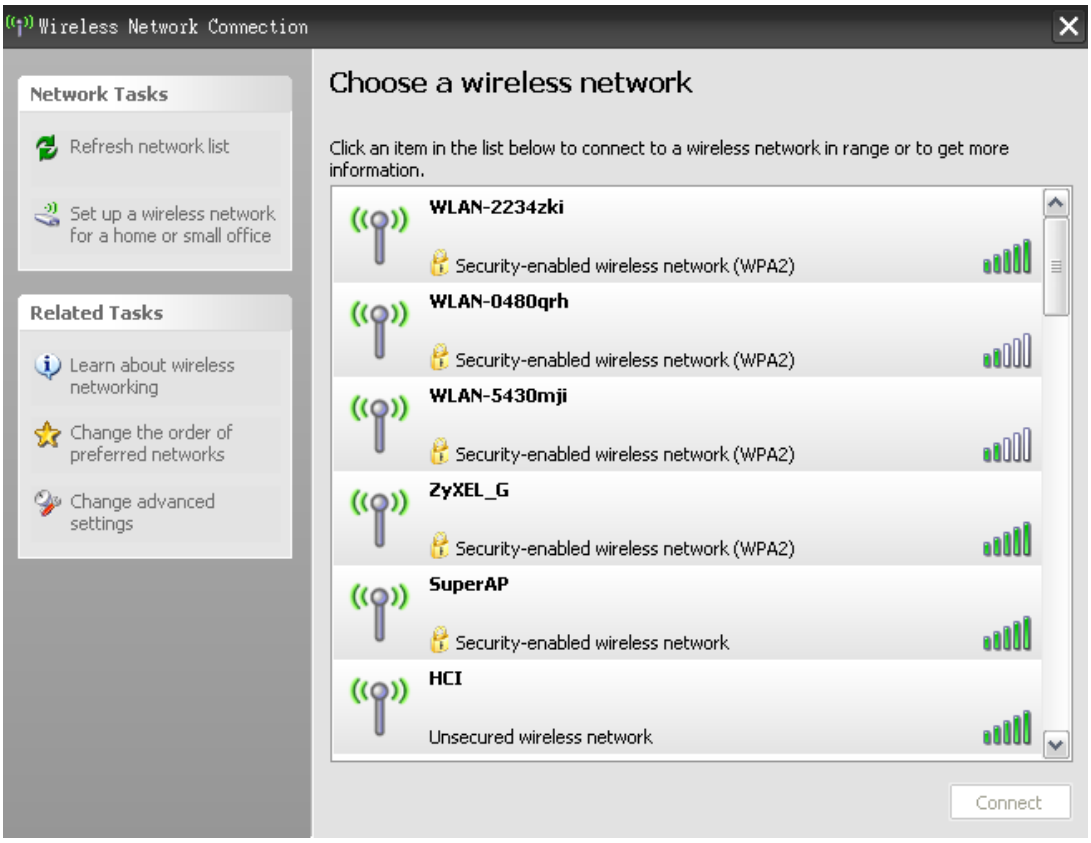
We can see that the notebook is now connected to the WLAN interface of the P-870HW-51aV2.

b. Wireless Setup Hiding the SSID.

1. Go to **Network > Wireless LAN > General.**
2. Check the **Active Wireless LAN** box.
3. Enter the **Network Name(SSID)**, e.g. “TEST_01”.
4. Check the **Hide Network Name(SSID)** box.
5. Select the **Security Mode**, e.g. “WPA-PSK”.
6. Enter the **Pre-Shared Key**, e.g. “11111111”.
7. Enter the **WPA Group Key Update Timer**, e.g. “1800”.
8. Select the **WPA Encryption**, e.g. “TKIP”.
9. Click **Apply.**

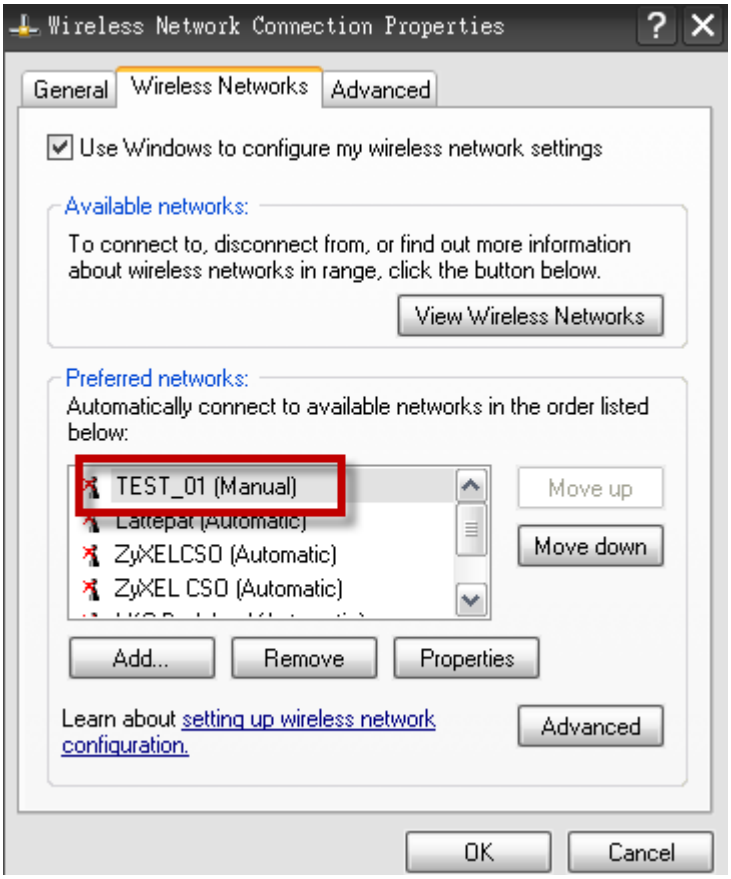


Show all the wireless networks in your notebook:

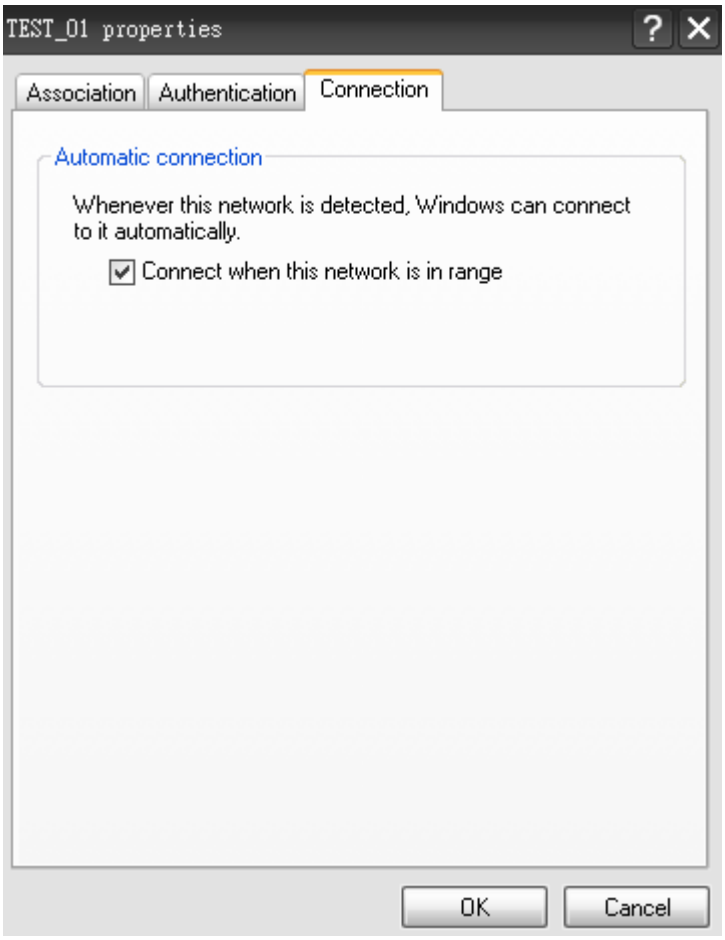


As we can see, we cannot find the SSID “TEST_01”.

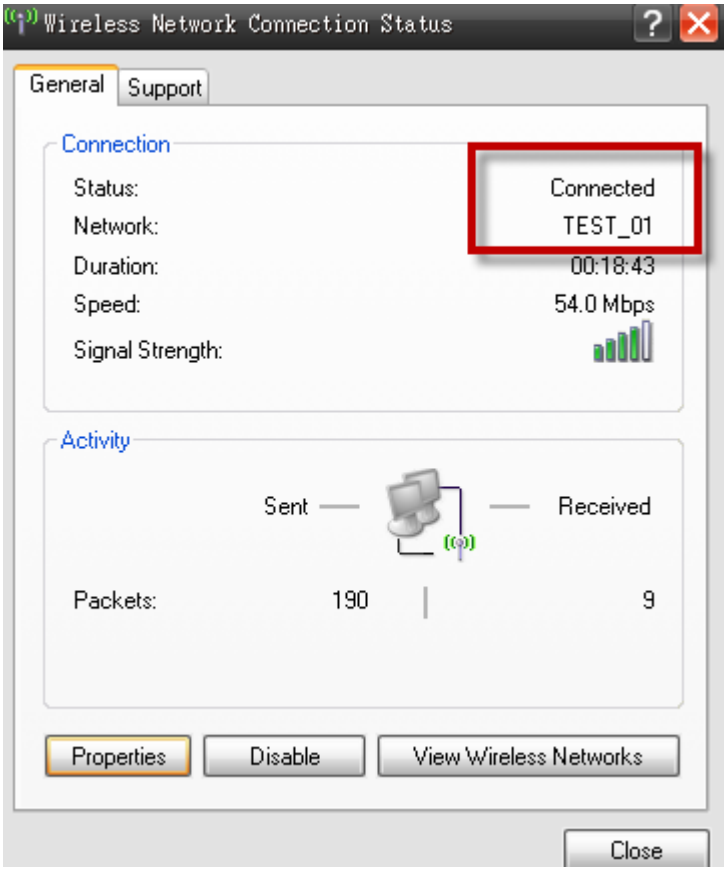
To connect to “TEST_01”, we need to configure the “Wireless Network Connection Properties” of the notebook WLAN interface:



Go “Connection” tab and check the box under the name of “Connect when this network is in range”.

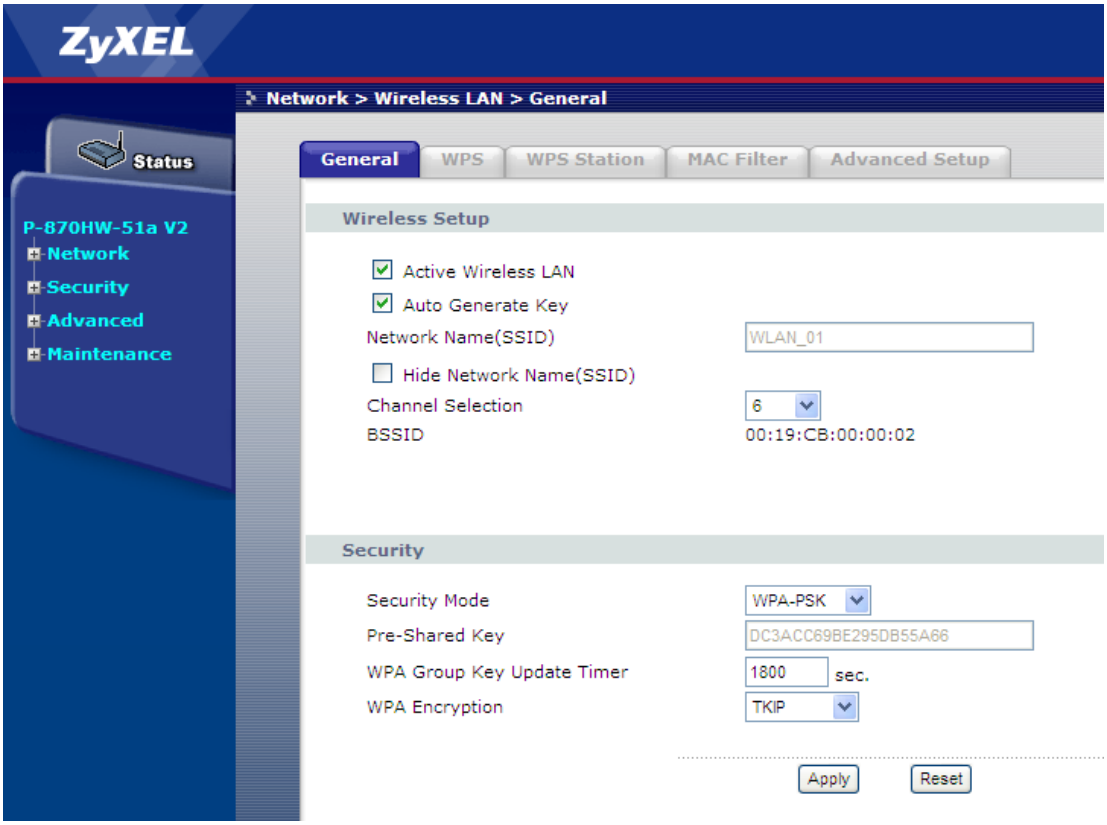


Then we will see the notebook connected to the “TEST_01”, even though the SSID is now displayed in the broadcast list.

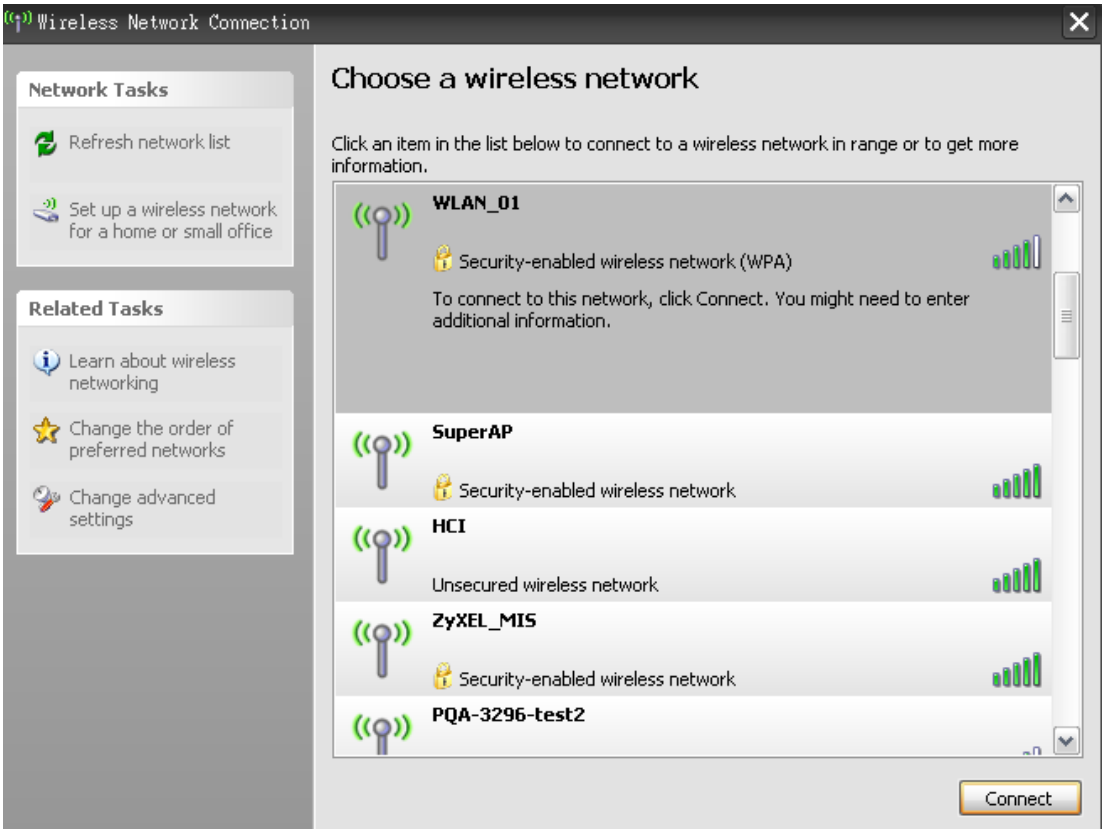


c. Wireless Setup Using “Auto Generate Key”.

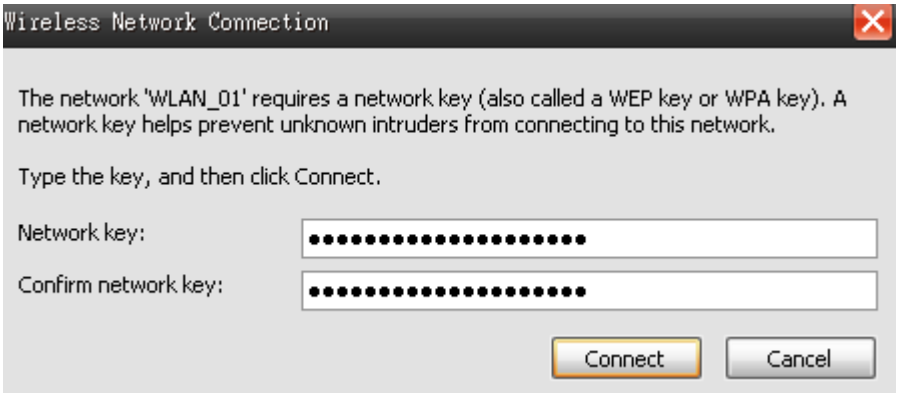
10. Go to **Network > Wireless LAN > General.**
11. Check the **Active Wireless LAN** box.
12. Check the **Auto Generate Key** box.
13. Select the **Security Mode**, e.g. “WPA-PSK”.
14. Enter the **WPA Group Key Update Timer**, e.g. “1800”.
15. Select the **WPA Encryption**, e.g. “TKIP”.
16. Click **Apply.**

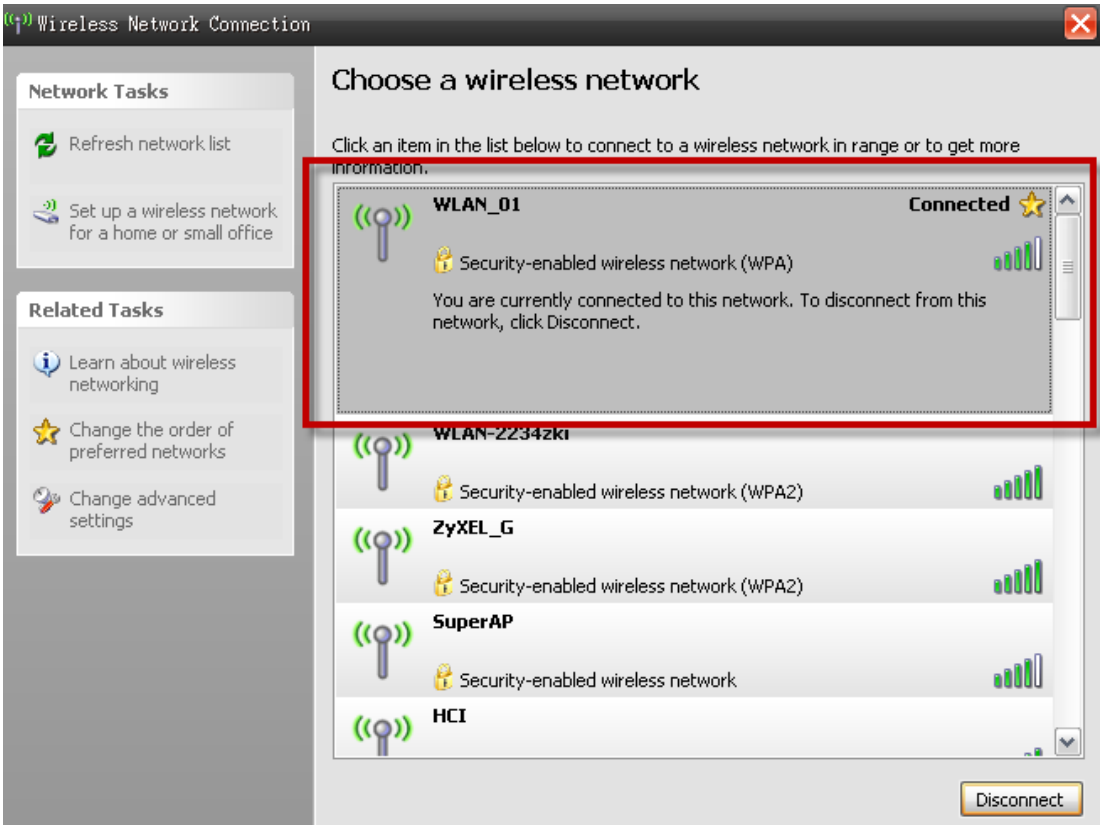


Show all the wireless networks in your notebook:



Enter the WPA-PSK pre-shared key auto-generated by P-870HW-51aV2.





We can see that the notebook is now connected to the WLAN interface of the P-870HW-51aV2.

WPS Application Notes

What is WPS?

Wi-Fi Protected Setup (**WPS**) is a standard created by the Wi-Fi Alliance for easy and secure establishment of a wireless home/office network. The goal of the WPS protocol is to simplify the process for configuring the security of the wireless network, and thus calling the name **Wi-Fi Protected Setup**.

There are several different methods defined in WPS to simplify the process of configuration. P-870HW-51aV2 supports two of those methods, which are the PIN Method and the PBC Method.

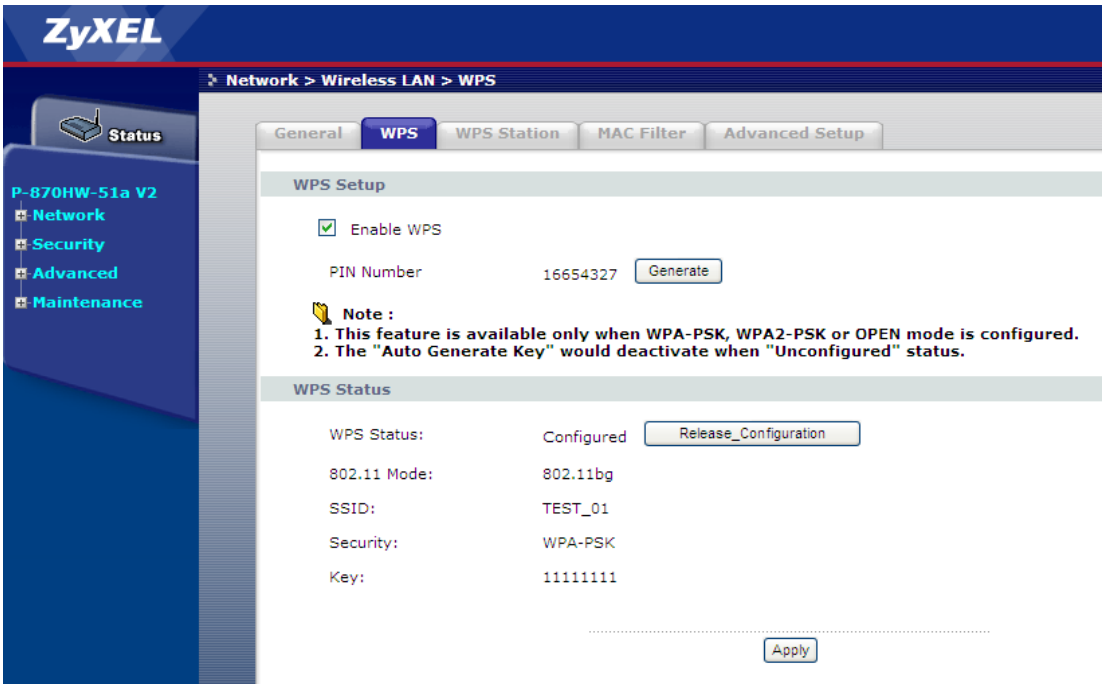
PIN Method:
A PIN (Personal Identification Number) has to be read from either a sticker on the new wireless client device or a display, and entered at either the wireless access point (AP) or a Registrar of the network.

PBC Method:
A simple action of “push button” suffices the process to activate the security of the wireless network and at the same time be subscribed in it.

WPS configuration

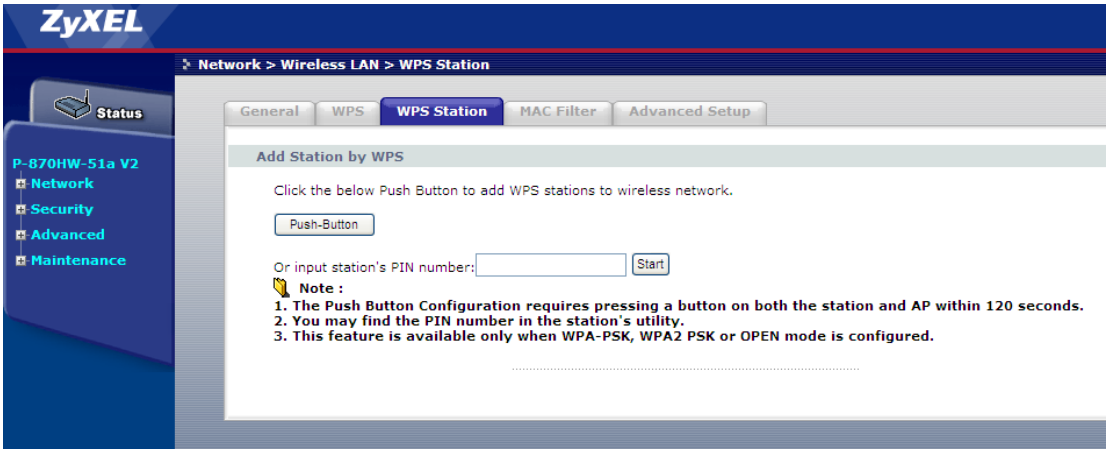
a. WPS Setup

1. Go to **Network > Wireless LAN > WPS.**
2. Check the **Enable WPS** box.
3. Click **Apply.**



b. WPS Station Setup

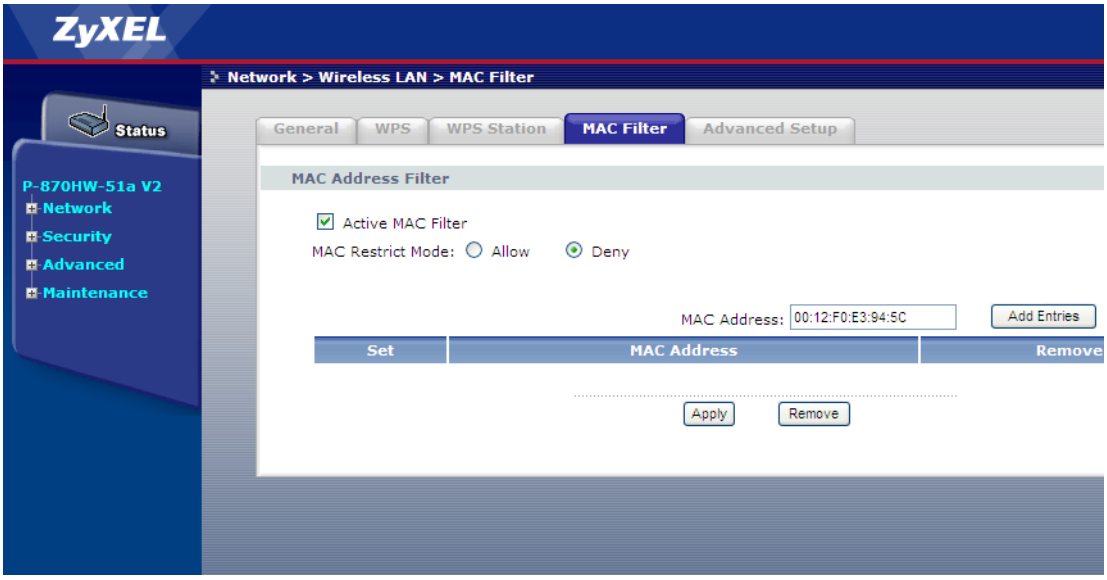
1. Go to **Network > Wireless LAN > WPS Station.**
2. Click the **Push-Button**



Note: You must press the other wireless device's WPS button within 2 minutes of pressing this button.

c. MAC filtering

1. Go to **Network > Wireless LAN > MAC Filter.**
2. Check the **Active MAC Filter** box.
3. Enter the **MAC Address**, e.g. “00:12:F0:E3:94:5C”.
4. Click **Apply.**



Product FAQ

Will the device work with my Internet connection?

P-870HW-51aV2 is designed to be compatible with major ISPs utilize VDSL as a broadband service. P-870HW-51aV2 offers Ethernet ports to connect to your computer so the device is placed in the line between the computer and your ISP. If your ISP supports PPPoE you can also use the device, because PPPoE is supported in the device.

Why do I need to use P-870HW-51aV2?

You need an VDSL modem/router to use with VDSL line, P-870HW-51aV2 is an ideal device for such application. The device has 4 Ethernet ports (LAN ports) and one VDSL WAN port. You should connect the computer to the LAN port and connect the VDSL line to the WAN port. If the ISP uses PPPoE you need the user account to access Internet.

What is PPPoE?

PPPoE stands for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management. There are some service providers running of PPPoE today. Before configuring PPPoE in the device, please make sure your ISP supports PPPoE.

Does the device support PPPoE?

Yes. The device supports PPPoE.

How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the device if the ISP uses PPPoE.

Why does my provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

Which Internet Applications can I use with the device?

Most common applications include MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, QuakeII, QuakeIII, StarCraft, & Quick Time.

How can I configure the device?

a. Telnet remote management- driven user interface for easy remote management
b. Web browser- web server embedded for easy configurations

What network interface does the device support?

The device supports 10/100M Ethernet to connect to the LAN computer or hub/switch and an up to 100M VDSL interface to the ISP.

What can we do with the device?

Browse the World Wide Web (WWW), send and receive individual e-mail, and download software. These are just a few of many benefits you can enjoy when you put the whole office on-line with the device.

Does device support dynamic IP addressing?

The device supports either a static or dynamic IP address from ISP.

What is the difference between the internal IP and the real IP from my ISP?

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP. The Device works like an intelligent router that route between the virtual IP and the real IP.

How does e-mail work through the device?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through the device using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address.

Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through the device using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

Is it possible to access a server running behind SUA from the outside Internet? If possible, how?

Yes, it is possible because the device delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured.

What DHCP capability does the device support?

The device supports DHCP client (Ethernet encap) on the WAN port and DHCP server on the LAN port. The device's DHCP client allows it to get the Internet IP address from ISP automatically if your ISP use DHCP as a method to assign IP address. The device's internal DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

How do I used the reset button, more over what field of parameter will be reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 5 second, the unit will be reset. When the reset button is pressed the devices all parameter will be reset back to factory default include, password, and IP address.

The default IP address is 192.168.1.1, Password 1234.

What network interface does the new device series support?

The new device series support auto MDX/MDIX 10/100M Ethernet LAN port to connect to the computer or Switch on LAN.

How does the device support TFTP?

In addition to the direct console port connection, the device supports the uploading/download of the firmware and configuration file using TFTP (Trivial File Transfer Protocol) over LAN.

Can the device support TFTP over WAN?

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

How fast can the data go?

The speed of the VDSL is only one part of the equation. There are a combination of factors starting with how fast your PC can handle IP traffic, then how fast your PC to cable modem interface is, then how fast the cable modem system runs and how much congestion there is on the cable network, then how big a pipe there is at the head end to the rest of the Internet.

Different models of PCs and Macs are able to handle IP traffic at varying speeds. Very few can handle it at 100 Mbps.

To create the appearance of faster network access, service companies plan to store or "cache" frequently requested web sites and Usenet newsgroups on a server at their head-end. Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? In a perfect world (or lab) they can receive data at speeds up to 100 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall behind the speed that the ISP appointed at the first place.

What is Multi-NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the device, thus preventing intruders from probing your network.

The SUA feature that the device supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The device supports most of the features of the NAT based on RFC 1631, and we call this feature as **'Multi-NAT'**. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

When do I need Multi-NAT?

a. Make local server accessible from outside Internet

When NAT is enabled the local computers are not accessible from outside. You can use Multi-NAT to make an internal server accessible from outside.

a. Support Non-NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. Thus, users on the same network can not login to the same server simultaneously. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address.

What IP/Port mapping does Multi-NAT support?

NAT supports five types of IP/port mapping. They are: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. The details of the mapping between ILA and IGA are described as below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA),

1. **One to One**

In One-to-One mode, the device maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the device maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

3. **Many to Many Overload**

In Many-to-Many Overload mode, the device maps the multiple ILA to shared IGA.

4. **Many to Many No Overload**

In Many-to-Many No Overload mode, the device maps each ILA to unique IGA.

5. **Server**

In Server mode, the device maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note: if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many-to-Many No Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

What is the difference between SUA and Multi-NAT?

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The device now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple severs of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The device supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The device supports 2 sets since there is only one remote node. The default SUA (Read Only) is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

What is BOOTP/DHCP?

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the device is a BOOTP/DHCP server. Win95 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as WWW.DYNDNS.ORG.

Without DDNS, we always tell the users to use the WAN IP of the 312 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the device, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the 312.

When the ISP assigns the device a new IP, the device updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the device sends this IP to the DDNS server for its updates.

Wireless FAQ

What is a Wireless LAN?

Wireless LANs provide all the functionality of wired LANs, without the need for physical connections (wires). Data is modulated onto a radio frequency carrier and transmitted through the ether. Typical bit-rates are 11Mbps and 54Mbps, although in practice data throughput is half of this. Wireless LANs can be formed simply by equipping PC's with wireless NICs. If connectivity to a wired LAN is required an Access Point (AP) is used as a bridging device. AP's are typically located close to the centre of the wireless client population.

What are the advantages of Wireless LANs?

a. Mobility:

Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.

b. Installation Speed and Simplicity:

Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

c. Installation Flexibility:

Wireless technology allows the network to go where wire cannot go.

d. Reduced Cost-of-Ownership:

While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.

e. Scalability:

Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure

networks of thousands of users that enable roaming over a broad area.

What are the disadvantages of Wireless LANs?

The speed of Wireless LAN is still relative slower than wired LAN. The most popular wired LAN is operated in 100Mbps, which is almost 10 times of that of Wireless LAN (10Mbps). A faster wired LAN standard (1000Mbps), which is 100 times faster, becomes popular as well. The setup cost of Wireless LAN is relative high because the equipment cost including access point and PCMCIA Wireless LAN card is higher than hubs and CAT 5 cables.

Where can you find wireless 802.11 networks?

Airports, hotels, and even coffee shops like Starbucks are deploying 802.11 networks so people can wirelessly browse the Internet with their laptops. As these types of networks increase, this will create additional security risk for the remote user if not properly protected.

What is an Access Point?

The AP (access point also known as a base station) is the wireless server that with an antenna and a wired Ethernet connection that broadcasts information using radio signals. AP typically act as a bridge for the clients. It can pass information to wireless LAN cards that have been installed in computers or laptops allowing those computers to connect to the campus network and the Internet without wires.

What is IEEE 802.11?

The IEEE 802.11 is a wireless LAN industry standard, and the objective of IEEE 802.11 is to make sure that different manufactures' wireless LAN devices can communicate to each other.802.11 provides 1 or 2 Mbps transmission in the 2.4 GHz ISM band using either FHSS or DSSS.

What is 802.11b?

802.11b is the first revision of 802.11 standard allowing data rates up to 11Mbps in the 2.4GHz ISM band. Also known as 802.11 High-Rate and Wi-Fi. 802.11b only uses DSSS, the maximum speed of 11Mbps has fallbacks to 5.5, 2 and 1Mbps.

How fast is 802.11b?

The IEEE 802.11b standard has a nominal speed of 11 megabits per second (Mbps). However, depending on signal quality and how many other people are using the wireless ethernet through a particular Access Point, usable speed will be much less (on the order of 4 or 5 Mbps, which is still substantially faster than most dialup, cable and DSL modems).

What is 802.11a?

802.11a the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54Mbps. 802.11a uses OFDM (orthogonal frequency division multiplexing) as opposed to FHSS or DSSS. Higher data rates are possible by combining channels. Due to higher frequency, range is less than lower frequency systems (i.e., 802.11b and 802.11g) and can increase the cost of the overall solution because a greater number of access points may be required. 802.11a is not directly compatible with 802.11b or 802.11g networks. In other words, a user equipped with an 802.11b or 802.11g radio card will not be able to interface directly to an 802.11a access point. Multi-mode NICs will solve this problem.

What is 802.11g?

802.11g is an extension to 802.11b. 802.11g increases 802.11b's data rates to 54 Mbps and still utilise the the 2.4 GHz ISM. Modulation is based upon OFDM (orthogonal frequency division multiplexing) technology. An 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. The range at 54 Mbps is less than for 802.11b operating at 11 Mbps.

Is it possible to use products from a variety of vendors?

Yes. As long as the products comply to the same IEEE 802.11 standard. The Wi-Fi logo is used to define 802.11b compatible products. Wi-Fi5 is a compatibility standard for 802.11a products running in the 5GHz band.

What is Wi-Fi?

The Wi-Fi logo signifies that a product is interoperable with wireless networking equipment from other vendors. A Wi-Fi logo product has been tested and certified by the Wireless Ethernet Compatibility Alliance (WECA). The Socket Wireless LAN Card is Wi-Fi certified, and that means that it will work (interoperate) with any brand of Access Point that is also Wi-Fi certified.

What types of devices use the 2.4GHz Band?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE 802.11b), cordless phones, wireless medical telemetry equipment and Bluetooth™ short-range wireless applications, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

Does the 802.11 interfere with Bluetooth devices?

Any time devices are operated in the same frequency band, there is the potential for interference.
Both the 802.11b and Bluetooth devices occupy the same2.4-to-2.483-GHz unlicensed frequency range-the same band. But a Bluetooth device would not interfere with other 802.11 devices much more than another 802.11 device would interefere. While more collisions are possible with the introduction of a Bluetooth device, they are also possible with the introduction of another 802.11 device, or a new 2.4 GHz cordless phone for that matter. But, BlueTooth devices are usually low-power, so the effects that a Bluetooth device may have on an 802.11 network, if any, aren't far-reaching.

Can radio signals pass through walls?

Transmitting through a wall is possible depending upon the material used in its construction. In general, metals and substances with a high water content do not allow radio waves to pass through. Metals reflect radio waves and concrete attenuates radio waves. The amount of attenuation suffered in passing through concrete will be a function of its thickness and amount of metal re-enforcement used.

What are potential factors that may causes interference among WLAN products?

Factors of interference:

1. Obstacles: walls, ceilings, furniture… etc.
2. Building Materials: metal door, aluminum studs.
3. Electrical devices: microwaves, monitors, electric motors.

Solution :

1.Minimizing the number of walls and ceilings

2.Antenna is positioned for best reception

3.Keep WLAN products away from electrical devices, eg: microwaves, monitors, electric motors,…, etc.

4. Add additional APs if necessary.

What's the difference between a WLAN and a WWAN?

WLANs are generally privately owned, wireless systems that are deployed in a corporation, warehouse, hospital, or educational campus setting. Data rates are high and there are no per-packet charges for data transmission.

WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier. Data rates are low and charges are based on usage. Specialized applications are characteristically designed around short, burst messaging.

What is Ad Hoc mode?

A wireless network consists of a number of stations without access points. Without using an access point or any connection to a wired network.

What is Infrastructure mode?

Infrastructure mode implies connectivity to a wired communications infrastructure. If such connectivity is required the Access Points must be used to connect to the wired LAN backbone. Wireless clients have their configurations set for "infrastructure mode" in order to utilize access points relaying.

How many Access Points are required in a given area?

This depends on the surrounding terrain, the diameter of the client population, and the number of clients. If an area is large with dispersed pockets of populations then extension points can be used for extend coverage.

What is Direct-Sequence Spread Spectrum Technology – (DSSS)?

DSSS spreads its signal continuously over a wide frequency band. DSSS maps the information bearing bit-pattern at the sending station into a higher data rate bit sequence using a "chipping" code. The chipping code (also known as processing gain) introduces redundancy which allows data recovery if certain bit errors occur during transmission. The FCC rules the minimum processing gain should be 10, typical systems use processing gains of 20. IEEE 802.11b specifies the use of DSSS.

What is Frequency-hopping Spread Spectrum Technology – (FHSS)?

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To an unsynchronized receivers an FHSS transmission appears to be short-duration impulse noise. 802.11 may use FHSS or DSSS.

Do I need the same kind of antenna on both sides of a link?

No. Provided the antenna is optimally designed for 2.4GHz or 5GHz operation. WLAN NICs often include an internal antenna which may provide sufficient reception.

Why the 2.4 Ghz Frequency range?

This frequency range has been set aside by the FCC, and is generally labeled the ISM band. A few years ago Apple and several other large corporations requested that the FCC allow the development of wireless networks within this frequency range. What we have today is a protocol and system that allows for unlicensed use of radios within a prescribed power level. The ISM band is populated by Industrial, Scientific and Medical devices that are all low power devices, but can interfere with each other.

What is Server Set ID (SSID)?

SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. SSID from a security point of view acts as a simple single shared password between base stations and clients.

What is an ESSID?

ESSID stands for Extended Service Set Identifier and identifies the wireless LAN. The ESSID of the mobile device must match the ESSID of the AP to communicate with the AP. The ESSID is a 32-character maximum string and is case-sensitive.

How do I secure the data across an Access Point's radio link?

Enable Wired Equivalency Protocol (WEP) or Wi-Fi Protected Access (WPA) to encrypt the payload of packets sent across a radio link.

What is WEP?

Wired Equivalent Privacy. WEP is a security mechanism defined within the 802.11 standard and designed to make the security of the wireless medium equal to that of a cable (wire). WEP data encryption was designed to prevent access to the network by "intruders" and to prevent the capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied by anyone who does not have an assigned key. WEP comes in 40/64-bit and 128-bit encryption key lengths. Note, WEP has shown to have fundamental flaws in its key generation processing.

What is the difference between 40-bit and 64-bit WEP?

40 bit WEP & 64 bit WEP are the same encryption level and can interoperate. The lower level of WEP encryption uses a 40 bit (10 Hex character) as "secret key" (set by user), and a 24 bit "Initialization Vector" (not under user control) (40+24=64). Some vendors refer to this level of WEP as 40 bit, others as 64 bit.

What is a WEP key?

A WEP key is a user defined string of characters used to encrypt and decrypt data.

A WEP key is a user defined string of characters used to encrypt and decrypt data?

128-bit WEP will not communicate with 64-bit WEP or 256-bit WEP Although 128 bit WEP also uses a 24 bit Initialization Vector, but it uses a 104 bit as secret key. Users need to use the same encryption level in order to make a connection.

Can the SSID be encrypted?

WEP, the encryption standard for 802.11, only encrypts the data packets not the 802.11 management packets and the SSID is in the beacon and probe management messages. The SSID is not encrypted if WEP is turned on. The SSID goes over the air in clear text. This makes obtaining the SSID easy by sniffing 802.11 wireless traffic.

By turning off the broadcast of SSID, can someone still sniff the SSID?

Many APs by default have broadcasting the SSID turned on. Sniffers typically will find the SSID in the broadcast beacon packets. Turning off the broadcast of SSID in the beacon message (a common practice) does not prevent getting the SSID; since the SSID is sent in the clear in the probe message when a client associates to an AP, a sniffer just has to wait for a valid user to associate to the network to see the SSID.

What are Insertion Attacks?

The insertion attacks are based on placing unauthorized devices on the wireless network without going through a security process and review.

What is Wireless Sniffer?

An attacker can sniff and capture legitimate traffic. Many of the sniffer tools for Ethernet are based on capturing the first part of the connection session, where the data would typically include the username and password. An intruder can masquerade as that user by using this captured information. An intruder who monitors the wireless network can apply this same attack principle on the wireless.

What is the difference between Open System and Shared Key of Authentication Type?

Open System:
The default authentication service that simply announces the desire to associate with another station or access point. A station can authenticate with any other station or access point using open system authentication if the receiving station designates open system authentication.

Share Key:
The optional authentication that involves a more rigorous exchange of frames, ensuring that the requesting station is authentic. For a station to use shared key authentication, it must implement WEP.

What is 802.1x?

IEEE 802.1x Port-Based Network Access Control is an IEEE (Institute of Electrical and Electronics Engineers) standard, which specifies a standard mechanism for authenticating, at the link layer (Layer 2), users' access to IEEE 802 networks such as Ethernet (IEEE 802.3) and Wireless LAN (IEEE 802.11). For IEEE 802.11 WLAN, IEEE 802.1x authentication can be based on username/password or digital certificate.

What is the difference between No authentication required, No access allowed and Authentication required?

No authentication required—disables 802.1X and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
No access allowed—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
Authentication required—enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

What is AAA?

AAA is the acronym for Authentication, Authorization, and Accounting and refers to the idea of managing subscribers by controlling their access to the network, verifying that they are who they say they are (via login name and password or MAC address) and accounting for their network usage.

What is RADIUS?

RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is a standard that has been implemented into several software packages and networking devices. It allows user information to be sent to a central database running on a RADIUS Server, where it is verified. RADIUS also provides a mechanism for accounting.

What is WPA?

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i security sepcification draft. Key difference between WPA and WEP are user authentication and improve data encryption.

What is WPA-PSK?

WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) can be used if user do not have a Radius server but still want to benefit from it. Because WPA-PSK only requires a single password to be entered on wireless AP/gateway and wireless client. As long as the passwords match, a client will be granted access to the WLAN.

Trouble Shooting

In case of problems happening to the P-870HW-51aV2, we are able to check the device with more detailed information by entering the “shell mode”. Those statistics may help the engineer to pinpoint the problem more easily.

How to enter the “Shell mode”

Login to the device by telnet
Execute “sh”

```
ZyXEL xDSL Router
Login: 1234
Password:
 > sh


BusyBox v1.00 (2009.01.14-02:33+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

#
```

CPU usage

Command:
#top

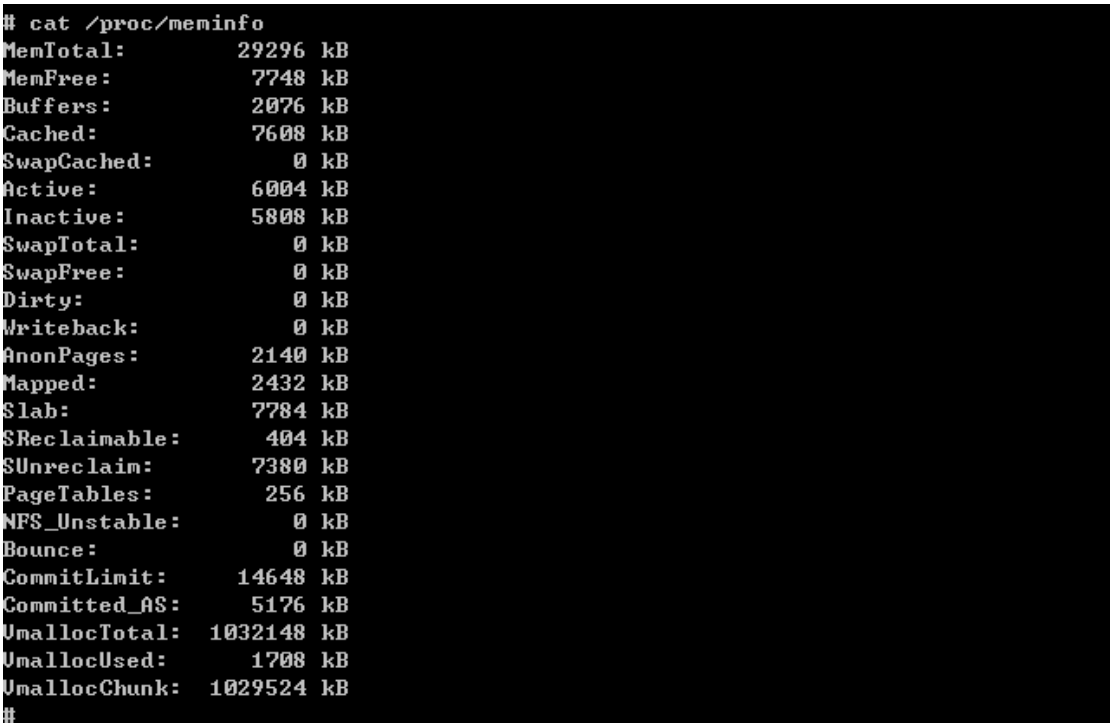
```
Mem: 21512K used, 7784K free, 0K shrd, 2076K buff, 7608K cached
Load average: 0.11, 0.08, 0.08    (State: S=sleeping R=running, W=waiting)

  PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
12404 1234     R        324 12323  0.1  1.1 exe
  114 1234     S       1680   113  0.0  5.7 ssk
  326 1234     S       1368   113  0.0  4.6 wlmngr
12320 1234     S        612   113  0.0  2.0 telnetd
12321 1234     S        564 12320  0.0  1.9 telnetd
  113 1234     S        548    54  0.0  1.8 smd
  412 1234     S        488     1  0.0  1.6 nas
  706 1234     S        480   113  0.0  1.6 pppd
 1003 1234     S        400   113  0.0  1.3 ripd
  246 1234     S        388   113  0.0  1.3 dhcpd
   54 1234     S        360     1  0.0  1.2 sh
12323 1234     S        352 12322  0.0  1.2 exe
 1002 1234     S        348   113  0.0  1.1 zebra
  932 1234     S        332   113  0.0  1.1 igmp
12322 1234     S        320 12321  0.0  1.0 sh
    1 1234     S        316     0  0.0  1.0 init
  949 1234     S        296   113  0.0  1.0 dnsproxy
  913 1234     S        272   113  0.0  0.9 dhcpc
   42 1234     SW         0     1  0.0  0.0 mtdblockd
    3 1234     SW<        0     1  0.0  0.0 events/0
```

(press Ctrl+C to exit)

Memory usage

Command:

cat /proc/meminfo



Current processes

Command:

#ps

```
# ps
  PID  Uid     VmSize Stat Command
    1 1234        316 S    init
    2 1234            SWN [ksoftirqd/0]
    3 1234            SW< [events/0]
    4 1234            SW< [khelper]
    5 1234            SW< [kthread]
   14 1234            SW< [kblockd/0]
   28 1234            SW  [pdflush]
   29 1234            SW  [pdflush]
   30 1234            SW< [kswapd0]
   31 1234            SW< [aio/0]
   42 1234            SW  [mtdblockd]
   54 1234        360 S    -sh
   96 1234            SW  [bcmsw]
  113 1234        548 S    smd
  114 1234       1680 S    ssk
  246 1234        388 S    dhcpd
  326 1234       1368 S    wlmngr -m 0
  412 1234        488 S    nas -P /var/wl0nas.lan0.pid -H 34954 -l br0 -i wl0 -A
  706 1234        480 S    pppd -c ppp0.100 -i ptm0.100 -u test -p ****** -f 0
  913 1234        272 S    dhcpc -f -i ptm0.200
  932 1234        332 S    igmp ptm0.200
  949 1234        296 S    dnsproxy -D Home
 1002 1234        348 S    zebra -f /var/zebra/zebra.conf
 1003 1234        400 S    ripd -f /var/zebra/ripd.conf
12320 1234        612 S    telnetd
12321 1234        564 S    telnetd
12322 1234        320 S    sh -c sh
12323 1234        356 S    sh
12678 1234        300 R    ps
#
```

NAT session table

Command:

#cat /proc/net/ip_conntrack

```
# cat /proc/net/ip_conntrack
tcp      6 424835 ESTABLISHED src=10.59.1.47 dst=172.23.5.49 sport=1526 dport=11
35 [UNREPLIED] src=172.23.5.49 dst=10.59.1.47 sport=1135 dport=1526 use=1
unknown  2 543 src=172.26.208.34 dst=224.0.0.22 [UNREPLIED] src=224.0.0.22 dst=1
72.26.208.34 use=1
tcp      6 424838 ESTABLISHED src=10.59.1.47 dst=172.23.5.50 sport=1514 dport=11
86 [UNREPLIED] src=172.23.5.50 dst=10.59.1.47 sport=1186 dport=1514 use=1
unknown  2 598 src=10.0.0.33 dst=224.7.7.7 [UNREPLIED] src=224.7.7.7 dst=10.0.0.
33 use=1
udp      17 29 src=172.26.208.1 dst=224.0.0.9 sport=520 dport=520 [UNREPLIED] sr
c=224.0.0.9 dst=172.26.208.1 sport=520 dport=520 use=1
tcp      6 421514 ESTABLISHED src=10.59.1.47 dst=172.23.5.2 sport=3698 dport=102
6 [UNREPLIED] src=172.23.5.2 dst=10.59.1.47 sport=1026 dport=3698 use=1
udp      17 88 src=172.26.208.35 dst=168.95.1.1 sport=60320 dport=53 [UNREPLIED]
 src=168.95.1.1 dst=172.26.208.35 sport=53 dport=60320 use=1
udp      17 88 src=172.26.208.35 dst=172.23.5.1 sport=60320 dport=53 [UNREPLIED]
 src=172.23.5.1 dst=172.26.208.35 sport=53 dport=60320 use=1
udp      17 29 src=172.26.208.35 dst=224.7.7.7 sport=2503 dport=1234 [UNREPLIED]
 src=224.7.7.7 dst=172.26.208.35 sport=1234 dport=2503 use=1
tcp      6 421649 ESTABLISHED src=10.59.1.47 dst=64.15.120.162 sport=3720 dport=
80 [UNREPLIED] src=64.15.120.162 dst=10.59.1.47 sport=80 dport=3720 use=1
tcp      6 424921 ESTABLISHED src=10.59.1.47 dst=64.15.120.162 sport=1590 dport=
80 [UNREPLIED] src=64.15.120.162 dst=10.59.1.47 sport=80 dport=1590 use=1
tcp      6 424923 ESTABLISHED src=10.59.1.47 dst=172.23.5.49 sport=1589 dport=11
35 [UNREPLIED] src=172.23.5.49 dst=10.59.1.47 sport=1135 dport=1589 use=1
unknown  2 598 src=10.0.0.33 dst=224.8.8.8 [UNREPLIED] src=224.8.8.8 dst=10.0.0.
33 use=1
```

IGMP table

Command:

#cat /proc/net/igmp

```
# cat /proc/net/igmp
Idx     Device    : Count Querier       Group    Users Timer    Reporter
1       lo        :     0      V2
                                E0000001     1 0:00000000               0
2       ifb0      :     1      V2
                                E0000001     1 0:00000000               0
8       eth0      :     1      V2
                                E0000001     1 0:00000000               0
9       eth1      :     1      V2
                                E0000001     1 0:00000000               0
10      eth2      :     1      V2
                                E0000001     1 0:00000000               0
11      eth3      :     1      V2
                                E0000001     1 0:00000000               0
12      wl0       :     1      V2
                                E0000001     1 0:00000000               0
13      br0       :     4      V2
                                E0000009     1 0:00000000               0
                                E0000016     1 0:00000000               1
                                E0000002     1 0:00000000               1
                                E0000001     1 0:00000000               0
19      ptm0      :     6      V2
                                E0000001     1 0:00000000               0
20      ptm0.100  :     1      V2
                                E0000001     1 0:00000000               0
21      ppp0.100  :     0      V2
                                E0000001     1 0:00000000               0
22      ptm0.200  :     6      V2
                                EFFFFFFA     1 0:00000000               1
                                E0000009     1 0:00000000               0
                                E0090909     1 0:00000000               1
                                E0080808     1 0:00000000               1
                                E0070707     1 0:00000000               1
                                E0000001     1 0:00000000               0
#
```

Packets statistics

Command:
#cat /proc/net/dev

```
# cat /proc/net/dev
Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes    packe
ts errs drop fifo colls carrier compressed
    lo:    7736      92    0    0    0     0          0         0     7736
92    0    0    0     0       0          0
  ifb0: 4043846    3729    0    0    0     0          0         0  4043846    37
29    0    0    0     0       0          0
  ifb1:       0       0    0    0    0     0          0         0        0
 0    0    0    0     0       0          0
  dsl0:       0       0    0    0    0     0          0         0        0
 0    0    0    0     0       0          0
 bcmsw:56914755   58830    0    0    0     0          0         0 1457217511 109
1888    0    0    0     0       0          0
pktcmf_sw_sar:       0       0    0    0    0     0          0         0
0       0    0    0    0     0       0          0
pktcmf_sar_sw:       0       0    0    0    0     0          0         0
0       0    0    0    0     0       0          0
  eth0:  400970    5867    0    0    0     0          0         0 1441674402 105
0331    0    0    0     0       0          0
  eth1:       0       0    0    0    0     0          0         0    89720    11
35    0    0    0     0       0          0
  eth2:56513785   52963    0    0    0     0          0         0 15363797   392
89    0    0    0     0       0          0
  eth3:       0       0    0    0    0     0          0         0    89592    11
33    0    0    0     0       0          0
   wl0:       0       0    0    0    0 34706          0         0        0
 0   19    0    0     0       0          0
   br0: 6048351   26378    0    0    0     0          0      6534 1448441607 106
8670    0    0    0     0       0          0
 wl0.1:       0       0    0    0    0 34706          0         0        0
 0   19    0    0     0       0          0
 wl0.2:       0       0    0    0    0 34706          0         0        0
 0   19    0    0     0       0          0
 wl0.3:       0       0    0    0    0 34706          0         0        0
 0   19    0    0     0       0          0
  ptm0:1446356465 1073793    0    0    0     0          0   1049839        0   4
0564    0    0    0     0       0          0
ptm0.100:  344990    2601    0    0    0     0          0         0   136016
1623    0    0    0     0       0          0
ppp0.100:  298339    2197    0    0    0     0          0         0    90399
1236    0    0    0     0       0          0
ptm0.200:1427016925 1050776    0    0    0     0          0   1049647  4065259
  3827    0    0    0     0       0          0
```

Physical layer statistics

Command:

#adslctl info --stats

```
# adslctl info --stats
adslctl: ADSL driver and PHY status
Status: Showtime
Retrain Reason: 0
Max:    Upstream rate = 21902 Kbps, Downstream rate = 159508 Kbps
Path:   0, Upstream rate = 988 Kbps, Downstream rate = 29998 Kbps

Link Power State:       L0
Mode:                   VDSL2 Annex A
VDSL2 Profile:          Profile 17a
TPS-TC:                 PTM Mode
Trellis:                U:OFF /D:ON
Line Status:            No Defect
Training Status:        Showtime
                Down            Up
SNR (dB):        32.6            42.9
Attn(dB):        0.0             0.0
Pwr(dBm):        1.3            -5.9
                        VDSL2 framing
                        Path 0
B:              239             31
M:              1               1
T:              64              1
R:              0               16
S:              0.2545          1.0000
L:              7543            384
D:              1               1
I:              240             24
N:              240             48
                        Counters
                        Path 0
OHF:            2956298         711017
OHFErr:         0               0
RS:             0               1104519
RSCorr:         0               0
RSUnCorr:       0               0
```

CLI Command List

The latest CI command list is available in release notes of every ZyXEL firmware release. Please go to ZyXEL public WEB site http://www.zyxel.com/web/support_download.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.