P-2812HNU(L)-Fx

802.11n Wireless VDSL2 VoIP Combo WAN IAD

(Green Product)

Support Notes

March 2011

Edition 1.0

Content

General Application Notes

This support note is applied for two different products types P-2812HNU-Fx and P-2812HNUL-Fx, the difference is P-2812HNUL-Fx supports lifeline.
P-2812HNU(L)-Fx support note is applied to both P-2812HNU(L)-F1, and P-2812HNU(L)-F3 models. The differences between these two models are:

- F1 supports Annex A, and F3 supports Annex B.
- For F1, the DSL line connector is RJ-11, and for F3, the DSL line connector is RJ-45.

Why use the P-2812HNU(L)-Fx?

- **Key features of the P-2812HNU(L)-Fx**

  The P-2812HNU(L)-Fx is an VDSL2 integrated access device (IAD), which provides high-speed VDSL Internet access in cooperation with major service providers to meet the worldwide market requirements of triple-play services. This model also features built-in 802.11n WLAN which allows for simple on-site deployment without additional wires. Two lines of telephony service (P-2812HNUL-Fx) are provided using VoIP technology with SIP signaling protocol. Additionally, the device incorporates dual WAN functionality, suitable for Switch/DSLAM or WiMAX users. Users may also leverage the built-in USB interface for file sharing or together with a 3G USB dongle for 3G backup connectivity.

- **Dual WAN to Simplify the Logistics for ISP**

  When a customer migrates from ADSL2+ or VDSL2 to PON or WiMAX, the ISP only needs to install a simple and relatively cheap bridge-device to terminate the physical connection and provide an Ethernet-interface towards the customer. The customer's existing P-2812HNU(L)-Fx will still able to be used for terminating the IP-connection, but now via the Ethernet WAN-interface. The end-users can still enjoy the services provided by their original CPE, without having to change the CPE due to the different physical connection.

- **Dual mode VDSL2/ADSL2+ functionality**

P-2812HNU(L)-Fx series supports dual-mode functionality that enables service providers to support ATM or PTM on the same device. It offers bi-directional high speed VDSL2, VDSL connection with speed of up to 100/45Mbps in PTM mode and 24/1Mbps ADSL2+, ADSL2 and ADSL connection in ATM mode. This powerful feature ensures the service provider can support connections not only on the IP network but also on the legacy ATM network without changing the CPE.

- **Internet Access through 3G Networks**

The P-2812HNU(L)-Fx with a USB interface for 3G USB dongles provides convenient Internet access through 3G networks to eliminate the restrictions of wired networks and to further extend last-mile connectivity. In Internet-challenged environments, such as rural or mountain areas, 3G connectivity may be the only viable solution; and it can be used to provide temporary Internet access to places such as exhibition booths as well. Furthermore, 3G access can be used as a WAN backup for high-availability Internet connections in office environments.

- **Quality of Service (QoS)**

The P-2812HNU(L)-Fx series comes equipped with both ATM and IP QoS features. The service provider can base its QoS policy on the service plan to freely design and prioritize mission-critical services such as IPTV and VoIP. This increases the network efficiency and productivity to enable the service provider to bring real multi-play into residential user’s life.

- **TR-069 Remote Management**

With TR-069 standard management specifications, the service provider is able to manage and configure the client devices remotely without end-user’s manual intervention. This unique feature not only offers user truly “plug-and-play” experience but also reduces the complexity of deployment and therefore saves service provider’s operating and maintenance costs.

- **PPP over Ethernet**

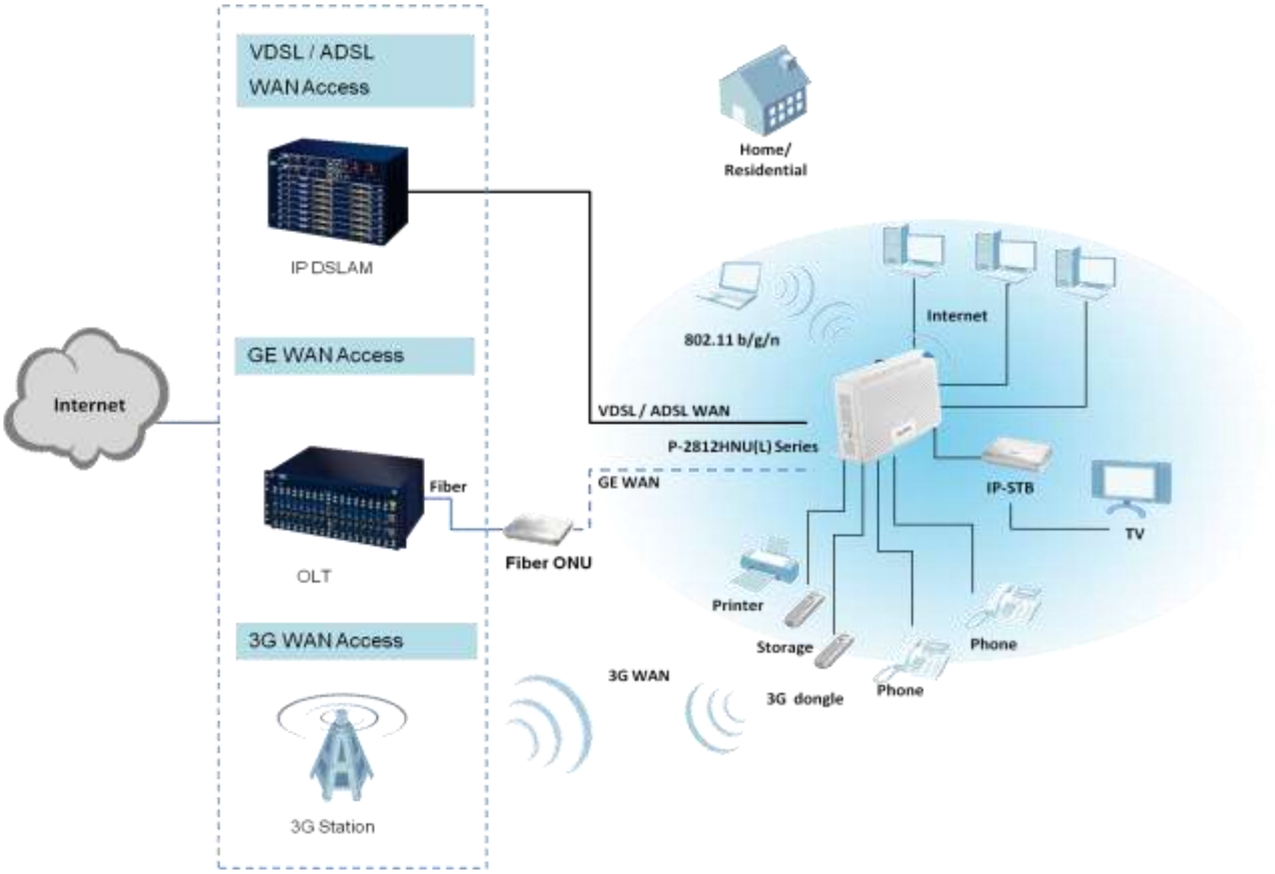
Since PPPoE benefits both Telco's and ISPs, the P-2812HNU(L)-Fx implements this feature and has tested it thoroughly with PPPoE servers.

- **NAT**

  NAT provides system administrators with an easy solution to create a private IP network for security and IP management. Powered by NAT technology, the P-2812HNU(L)-Fx supports 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.

Key Application Scenario

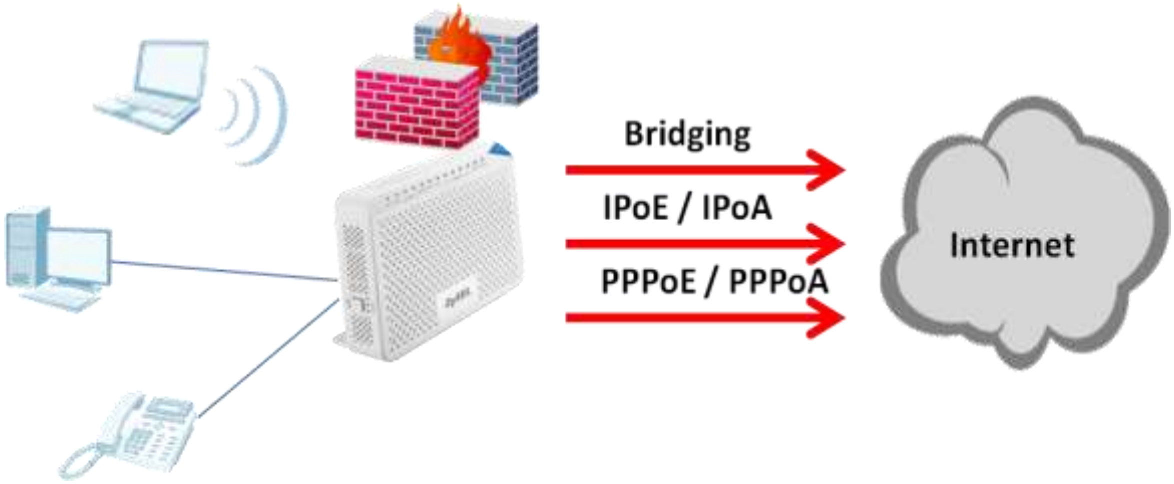
■ Multi-Service application Scenario



The ZyXEL device provides shared Internet Access by connecting the DSL port to the DSL or Modem jack on a splitter or your telephone jack. The P-2812HNU(L)-Fx serves as a home gateway, providing high speed Internet service, VoIP and High Quality IPTV service.

Internet Connection

A typical Internet access application of the P-2812HNU(L)-Fx is shown below. For a small office, some components need to be checked before accessing the Internet.



- 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 user's username/password = user/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 protocol, 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 list of 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 any 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.

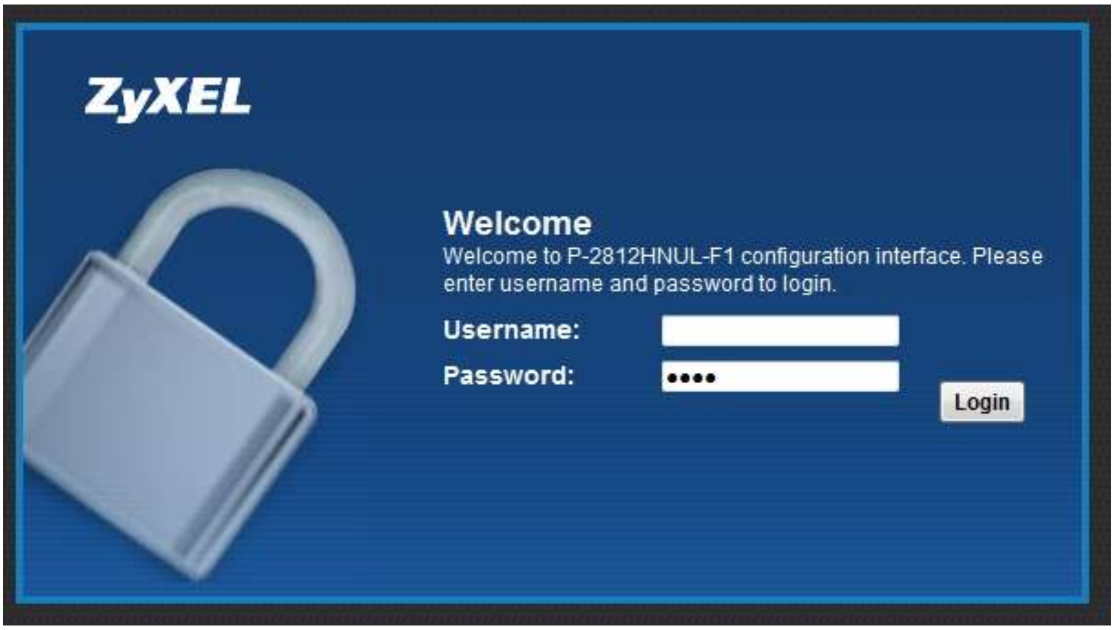
Access Application Notes

Web GUI

The following procedure describes the most typical operation of the device using a browser. The device features an embedded Web server that allows you to use Web browser to configure it. Please make sure there is no Telnet or Console login session before configuring the router using a browser.

- Accessing the Prestige Web

Please enter the LAN IP address of the Prestige router in the URL location to retrieve the web screen from the device. The default LAN IP of the device is 192.168.1.1. See the example below.



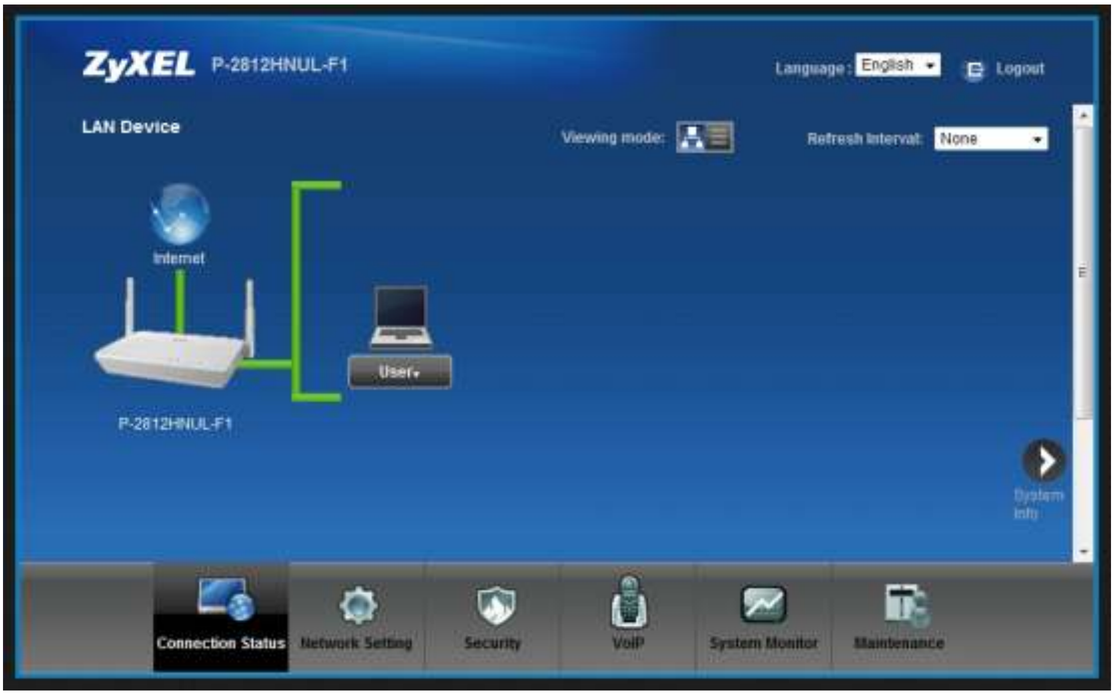
Welcome

Welcome to P-2812HNUL-F1 configuration interface. Please enter username and password to login.

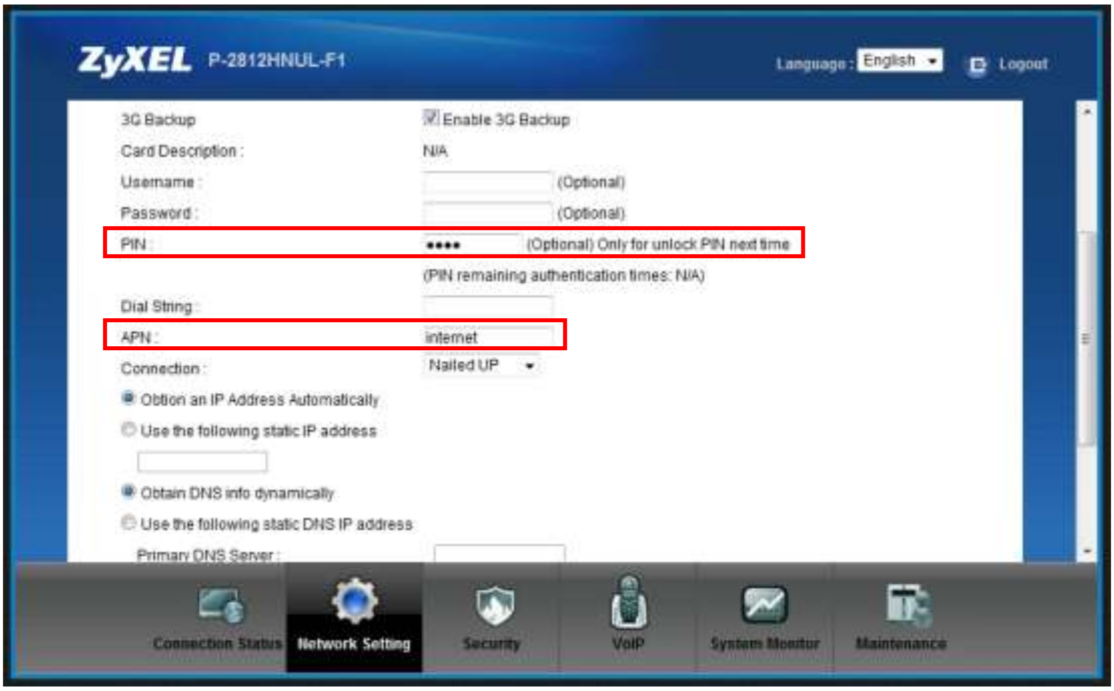
Username:

Password: ●●●●

- Log into the P-2812HNU(L)-Fx via Web GUI.
    1. Set up your PC/NB IP address to be a DHCP client.
    2. Connect to a LAN port of P-2812HNU(L)-Fx via RJ45 Ethernet cable and open your Web browser.
    3. The default IP of P-2812HNU(L)-Fx is 192.168.1.1
       Username/password = admin/1234



3G Backup connection



3G Backup ☑ Enable 3G Backup

Card Description : N/A

Username : (Optional)

Password : (Optional)

PIN : •••• (Optional) Only for unlock PIN next time

(PIN remaining authentication times: N/A)

Dial String :

APN : internet

Connection : Nailed UP

● Obtion an IP Address Automatically

○ Use the following static IP address

● Obtain DNS info dynamically

○ Use the following static DNS IP address

Primary DNS Server :

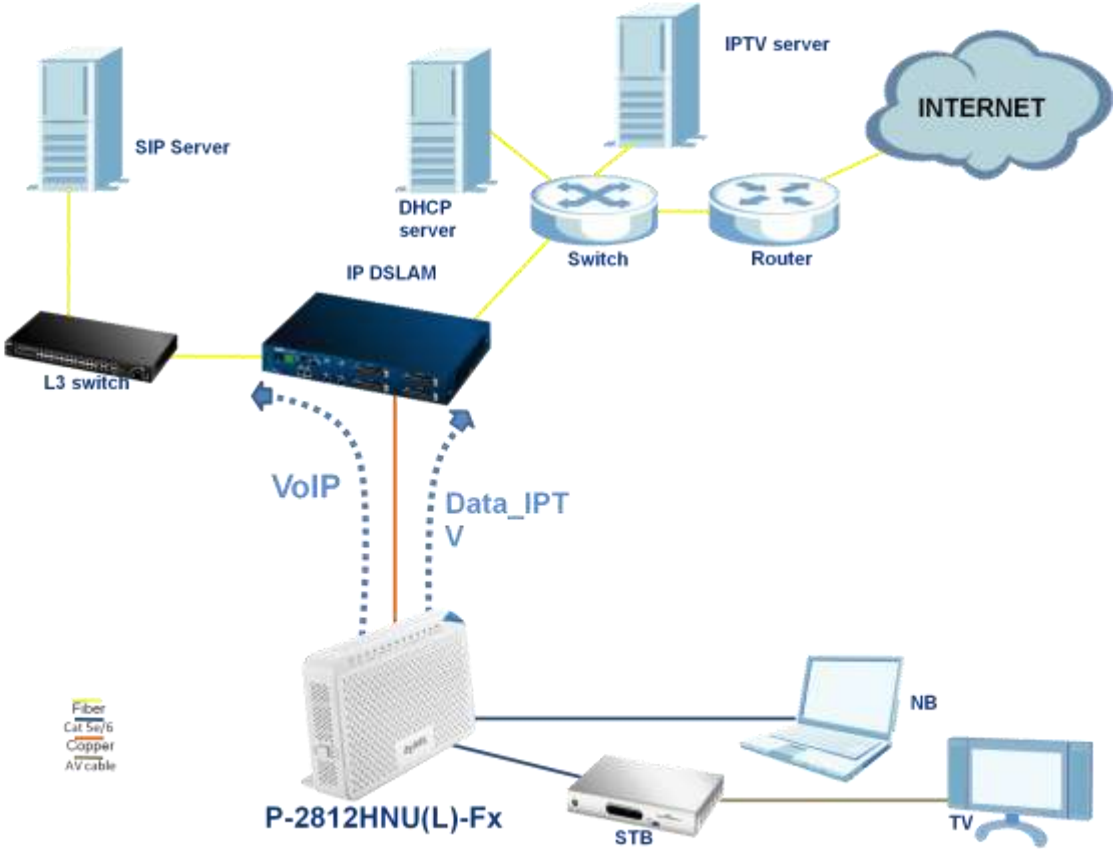
1. Go to **Network Setting> Broadband > 3G Backup**.
2. Select the check box ***Enable 3G Backup.***

3. Card Description will show what dongle model is plugged into P-2812HNU(L)-Fx Series .
4. If P-2812HNU(L)-Fx Series supports that dongle, ***3G status*** will read Enable.
5. Fill in the PIN number.
6. Enter the APN string or number.

Application Scenario

The following example demonstrates a Triple Play service configuration running Data, VoIP and IPTV. The step by step guide beneath the following scenario illustration will take you through the setup of the WAN Interface, NAT Port forwarding (using FTP service to demonstrate Data service), VoIP configuration (to demonstrate VoIP service), Quality of Service and WLAN setting (to demonstrate WPS setup).

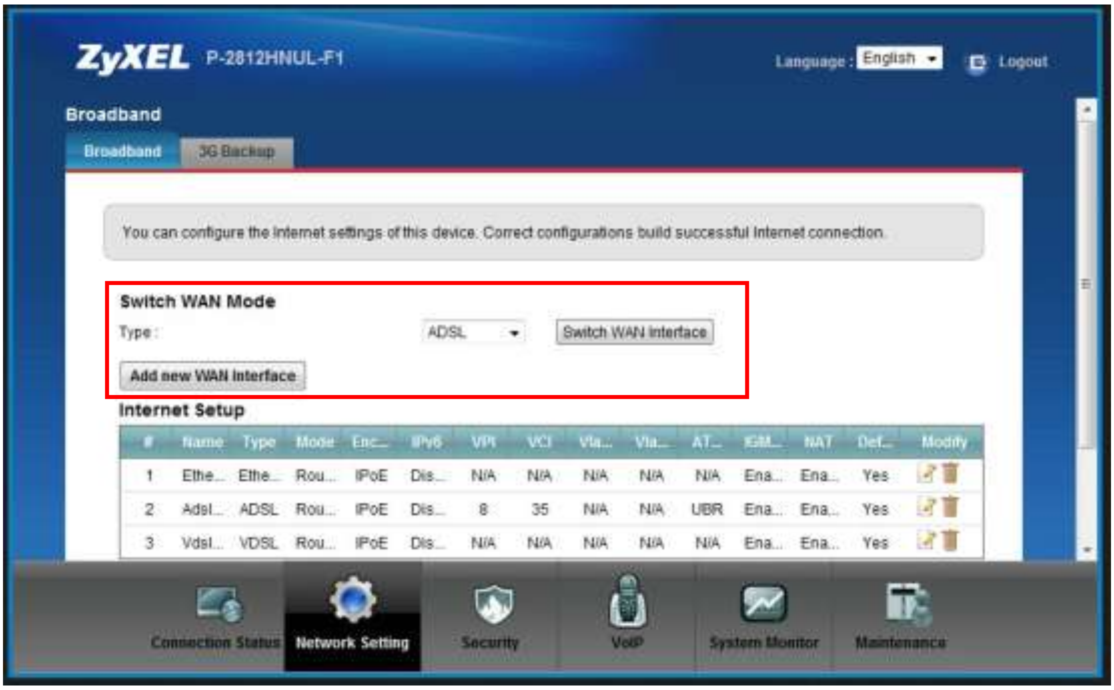
The following figure is a simplified overall scenario diagram of WAN interface configuration.



ADSL 2+ WAN Mode

In the ADSL WAN mode, we will set up two WAN interfaces: for data/IPTV and for VoIP services. Based on the current implementation, the IPTV service will go through the data WAN interface in routing mode.

1. Go to **Networking Setting > Broadband** and select **Broadband** tag.
2. Change the **WAN switch mode** to type: **ADS**L, then **click Switch WAN Interface**. The system would require rebooting.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

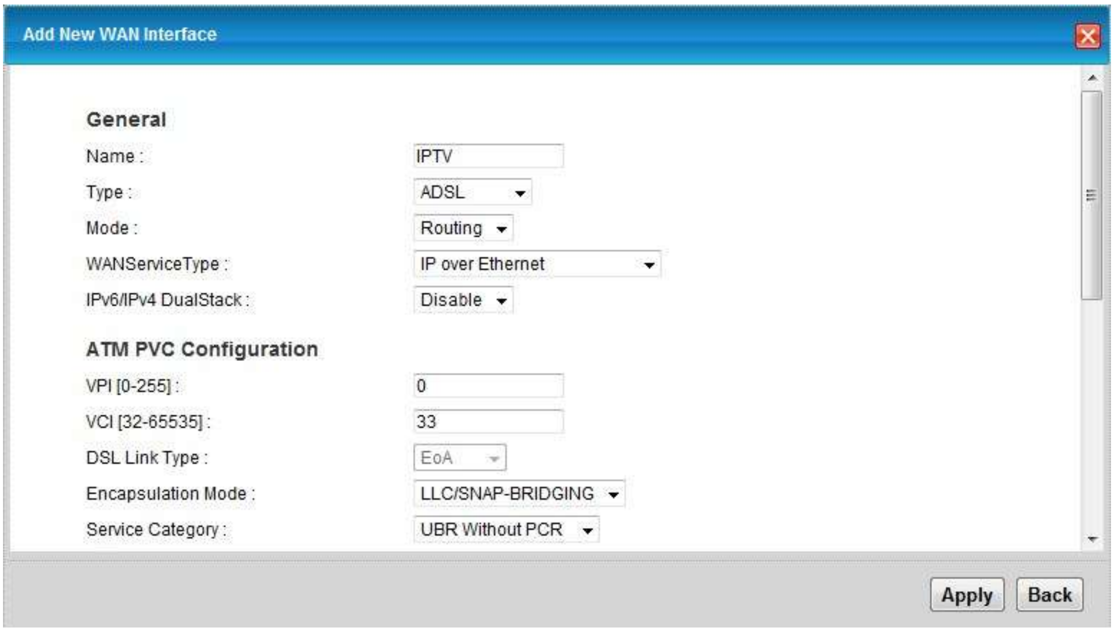
Switch WAN Mode

Type : ADSL

Internet Setup

#	Name	Type	Mode	Enc...	IPv6	VPI	VCI	Vla...	Vla...	AT...	IGM...	NAT	Def...	Modify
1	Ethe...	Ethe...	Rou...	IPoE	Dis...	N/A	N/A	N/A	N/A	N/A	Ena...	Ena...	Yes	
2	Adsl...	ADSL	Rou...	IPoE	Dis...	8	35	N/A	N/A	UBR	Ena...	Ena...	Yes	
3	Vdsl...	VDSL	Rou...	IPoE	Dis...	N/A	N/A	N/A	N/A	N/A	Ena...	Ena...	Yes	

3. After restarted, go to **Networking Setting > Broadband** and select **Broadband** tag again.
4. Click "**Add new WAN Interface**" button to create the data WAN interface.
5. In **Add New Interface**, give this interface a name (e.g. IPTV) and select the **ADSL** interface Type.
6. Set interface Mode to **Routing**.
7. Choose **IP over Ethernet** WAN service Type**.**
8. Configure the PVC parameters (VPI/VCI). In this example, set 0/33.
9. Please set **Service Category** to "UBR without PCR" for Data and IPTV service for medium priority.



Add New WAN Interface

General

Name : IPTV

Type : ADSL

Mode : Routing

WANServiceType : IP over Ethernet

IPv6/IPv4 DualStack : Disable

ATM PVC Configuration

VPI [0-255] : 0

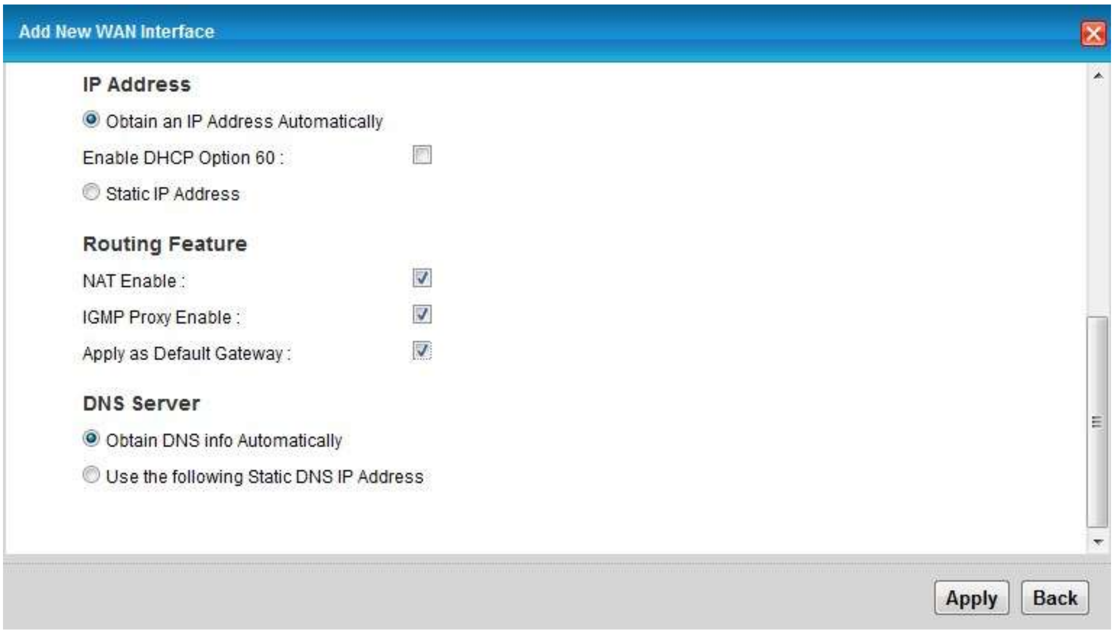
VCI [32-65535] : 33

DSL Link Type : EoA

Encapsulation Mode : LLC/SNAP-BRIDGING

Service Category : UBR Without PCR

10. Set IP Address to “**Obtain an IP Address Automatically**”.
11. Enable all Routing Features: select **NAT Enable**, **IGMP Proxy Enable** and **Apply as Default Gateway.**
12. For DNS Server setting, choose “**Obtain DNS info Automatically**”.
13. Click **Apply**.



Add New WAN Interface

IP Address

● Obtain an IP Address Automatically

Enable DHCP Option 60 : □

○ Static IP Address

Routing Feature

NAT Enable : ☑

IGMP Proxy Enable : ☑

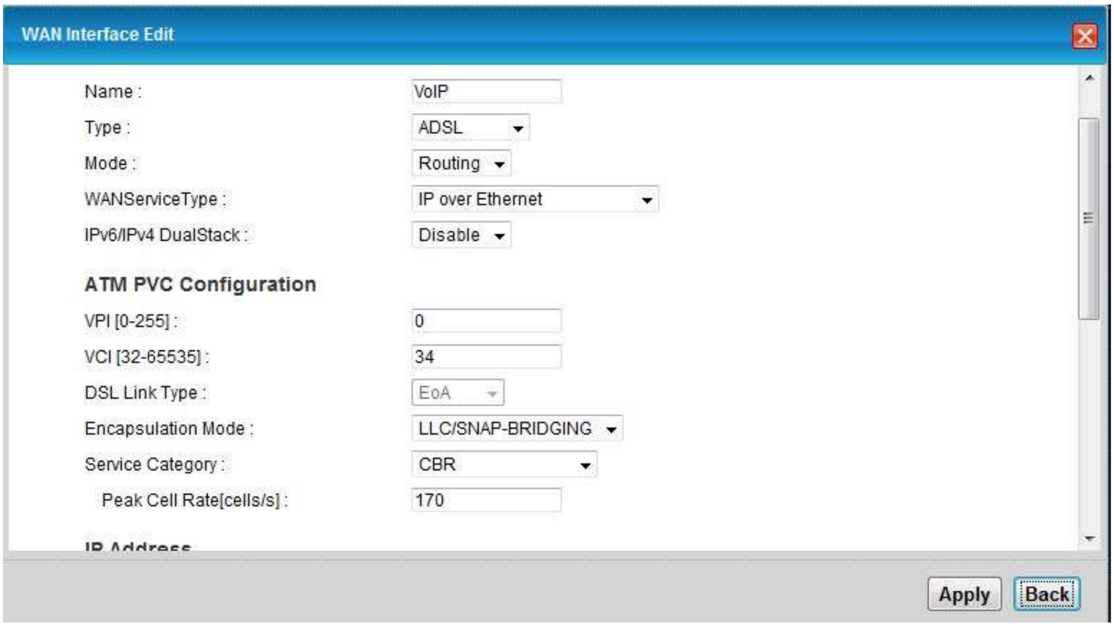
Apply as Default Gateway : ☑

DNS Server

● Obtain DNS info Automatically

○ Use the following Static DNS IP Address

14. Please repeat steps 1–13 to create the second data WAN interface for VoIP, named “VoIP”. Set VCI to 34 and select “CBR” and set cell rate “170” this time.



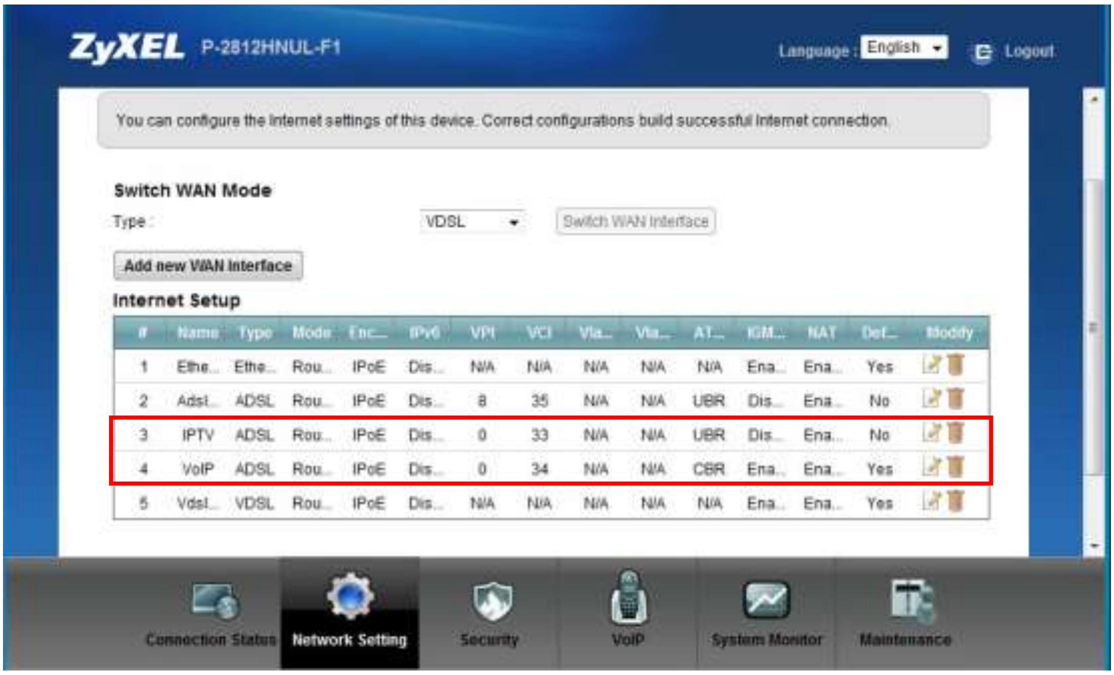
Name :	VoIP
Type :	ADSL
Mode :	Routing
WANServiceType :	IP over Ethernet
IPv6/IPv4 DualStack :	Disable

ATM PVC Configuration

VPI [0-255] :	0
VCI [32-65535] :	34
DSL Link Type :	EoA
Encapsulation Mode :	LLC/SNAP-BRIDGING
Service Category :	CBR
Peak Cell Rate[cells/s] :	170

IP Address

After completion, you will see two new WAN interfaces as shown in the following screenshot.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

Switch WAN Mode

Type : VDSL

Internet Setup

#	Name	Type	Mode	Enc...	IPv6	VPI	VCI	Vla...	Vla...	AT...	IGM...	NAT	Def...	Modify
1	Ethe...	Ethe...	Rou...	IPoE	Dis...	N/A	N/A	N/A	N/A	N/A	Ena...	Ena...	Yes	
2	Adsl...	ADSL	Rou...	IPoE	Dis...	8	35	N/A	N/A	UBR	Dis...	Ena...	No	
3	IPTV	ADSL	Rou...	IPoE	Dis...	0	33	N/A	N/A	UBR	Dis...	Ena...	No	
4	VoIP	ADSL	Rou...	IPoE	Dis...	0	34	N/A	N/A	CBR	Ena...	Ena...	Yes	
5	Vdsl...	VDSL	Rou...	IPoE	Dis...	N/A	N/A	N/A	N/A	N/A	Ena...	Ena...	Yes	

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.

NAT Introduction

- What is 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 as 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 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.

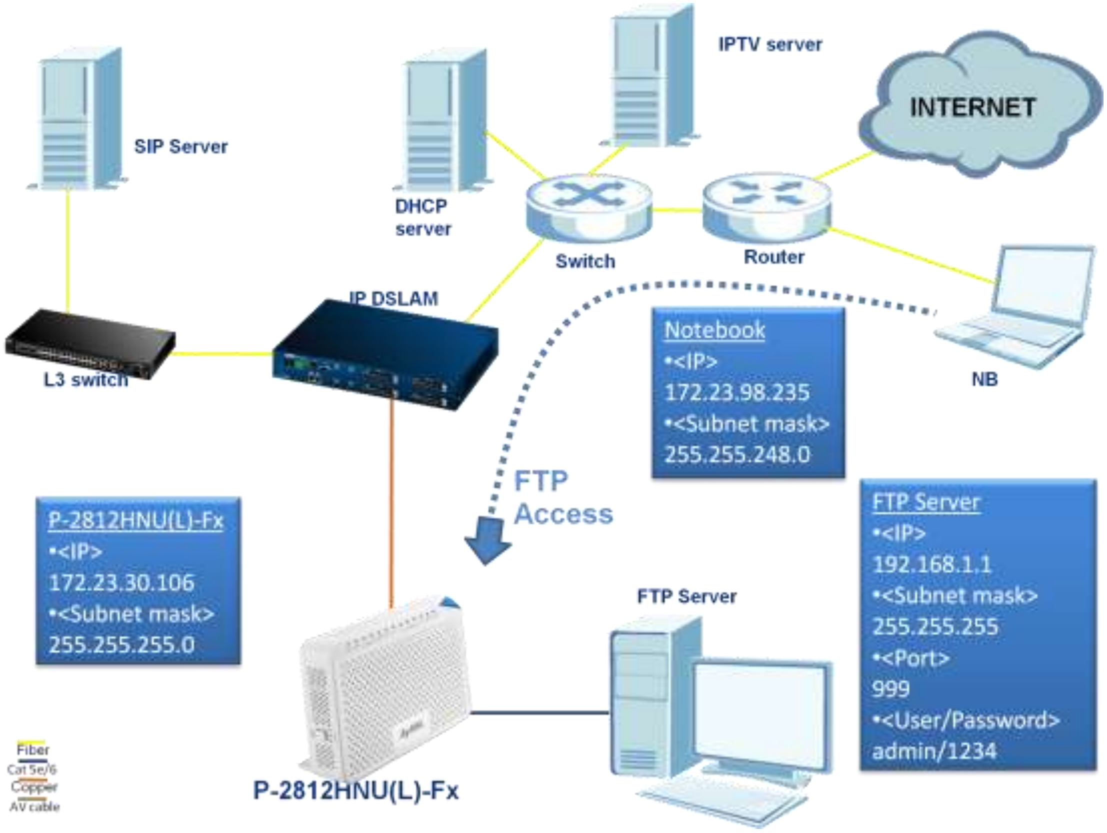
For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How does NAT work?

According to the following figure, we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Addresses (IGA). 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.

Data Service FTP Downloading Scenario

- **Topology**



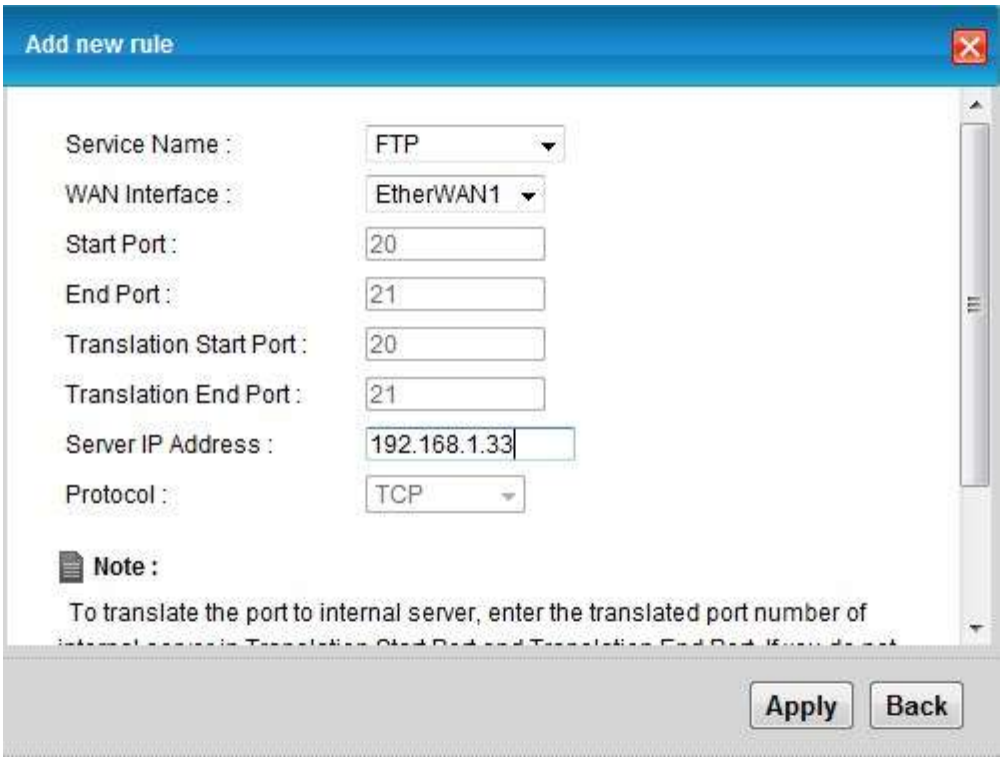
NAT provides system administrators with an easy solution to create a private IP network for security and IP management. Powered by NAT technology, the P-2812HNU(L)-Fx supports complete NAT mapping and most popular Internet multimedia applications. This feature is best demonstrated with the NAT port forwarding feature implemented in the CPE. In a scenario shown in the above diagram, we have an 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-2812HNU(L)-Fx, so that the notebook at the WAN site can access the FTP server? The following step-by-step guide illustrates the setup.

PS: Make sure that NAT is enabled on the WAN interface.

Port Forwarding Configuration

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

1. Go to **Network Setting**> **NAT** > **Port Forwarding** and click “**add new rule**”.
2. Select the Service Name, e.g. “FTP”.
3. Select the WAN Interface, e.g. “EtherWAN1”.
4. Enter the Server IP Address, e.g. “192.168.1.33”.
5. Click **Apply.**



Add new rule

Service Name :	FTP
WAN Interface :	EtherWAN1
Start Port :	20
End Port :	21
Translation Start Port :	20
Translation End Port :	21
Server IP Address :	192.168.1.33
Protocol :	TCP

Note :

To translate the port to internal server, enter the translated port number of

VoIP Configuration

Setting up an SIP Account

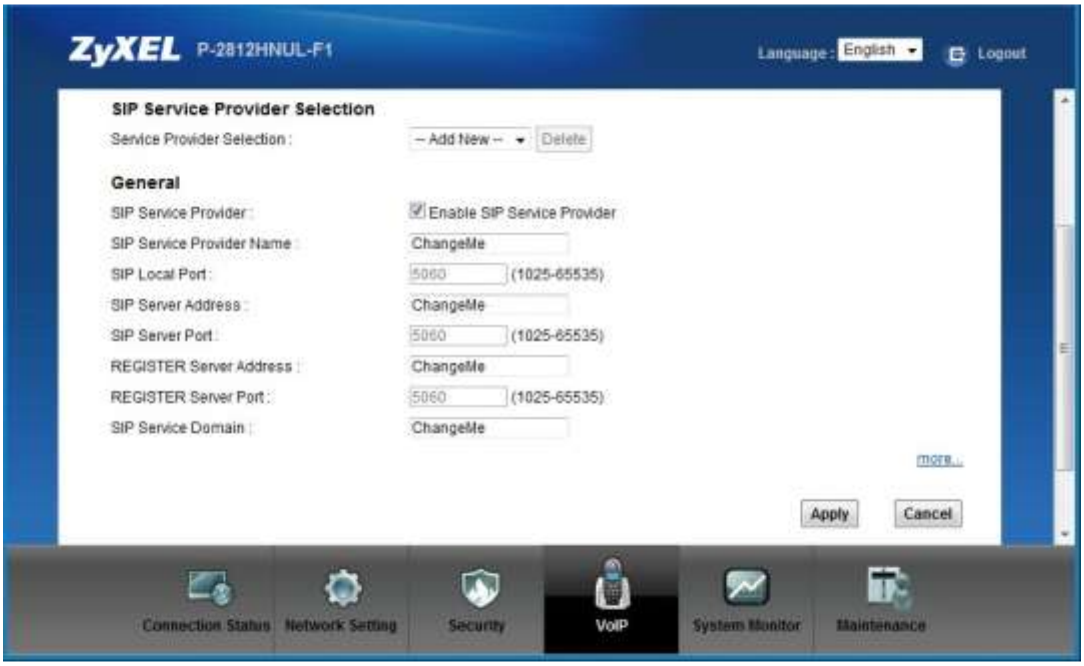
The VoIP technology sends voice signals over the Internet Protocol. This allows users to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network.

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks. The Prestige can hold up to two SIP account simultaneously. Please follow the instructions below to configure the SIP accounts properly.

Note: You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configuring a SIP account on the unit.

With the account information supplied by your ITSP provider at hand you may start the setup procedure.

1. Go to **VoIP** >**SIP**, select “**Add New**” for the Service selection and enter the SIP server IP address supplied by your SIP service provider.



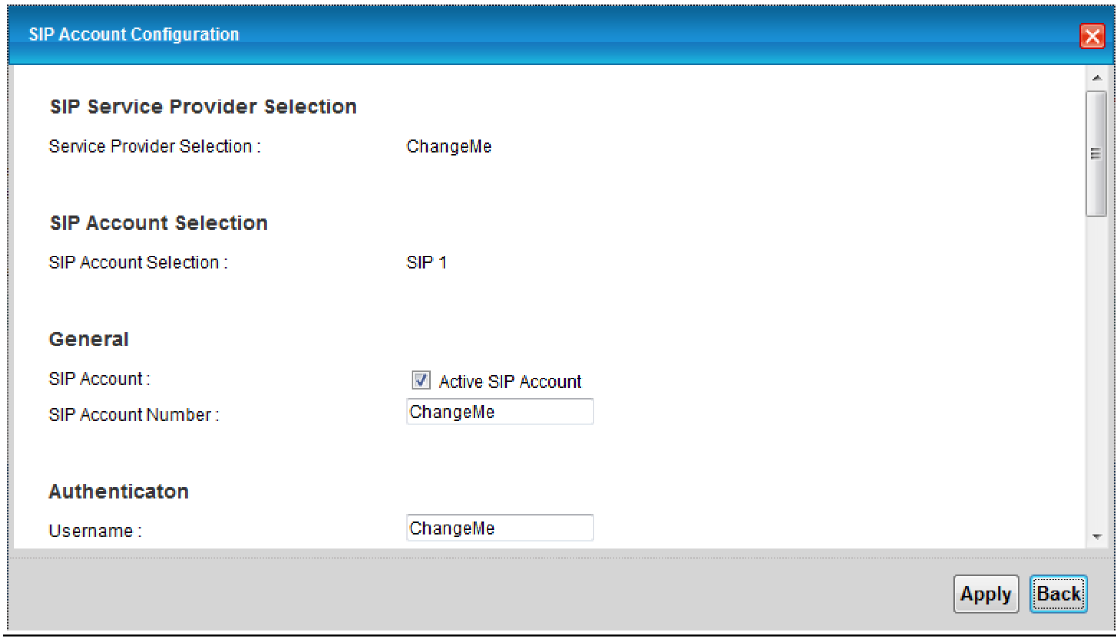
SIP Service Provider Selection

Service Provider Selection :	-- Add New -- Delete

General

SIP Service Provider :	☑ Enable SIP Service Provider
SIP Service Provider Name :	ChangeMe
SIP Local Port :	5060 (1025-65535)
SIP Server Address :	ChangeMe
SIP Server Port :	5060 (1025-65535)
REGISTER Server Address :	ChangeMe
REGISTER Server Port :	5060 (1025-65535)
SIP Service Domain :	ChangeMe

2. Click on the "**SIP Account**" tab to configure the SIP account.
3. Click Edit icon for "**SIP1**" and configure the SIP account.



SIP Account Configuration

SIP Service Provider Selection

Service Provider Selection : ChangeMe

SIP Account Selection

SIP Account Selection : SIP 1

General

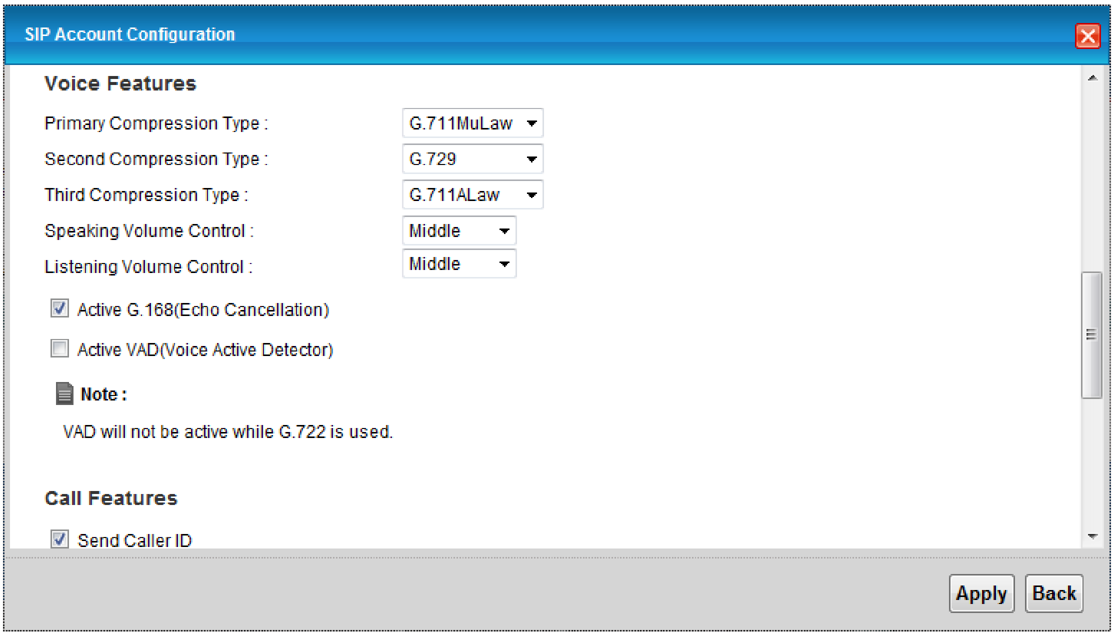
SIP Account : ☑ Active SIP Account

SIP Account Number : ChangeMe

Authenticaton

Username : ChangeMe

4. Fill in the SIP number and the account username and password. Leave the Advanced setting unchanged.



SIP Account Configuration

Voice Features

Primary Compression Type : G.711MuLaw

Second Compression Type : G.729

Third Compression Type : G.711ALaw

Speaking Volume Control : Middle

Listening Volume Control : Middle

☑ Active G.168(Echo Cancellation)

☐ Active VAD(Voice Active Detector)

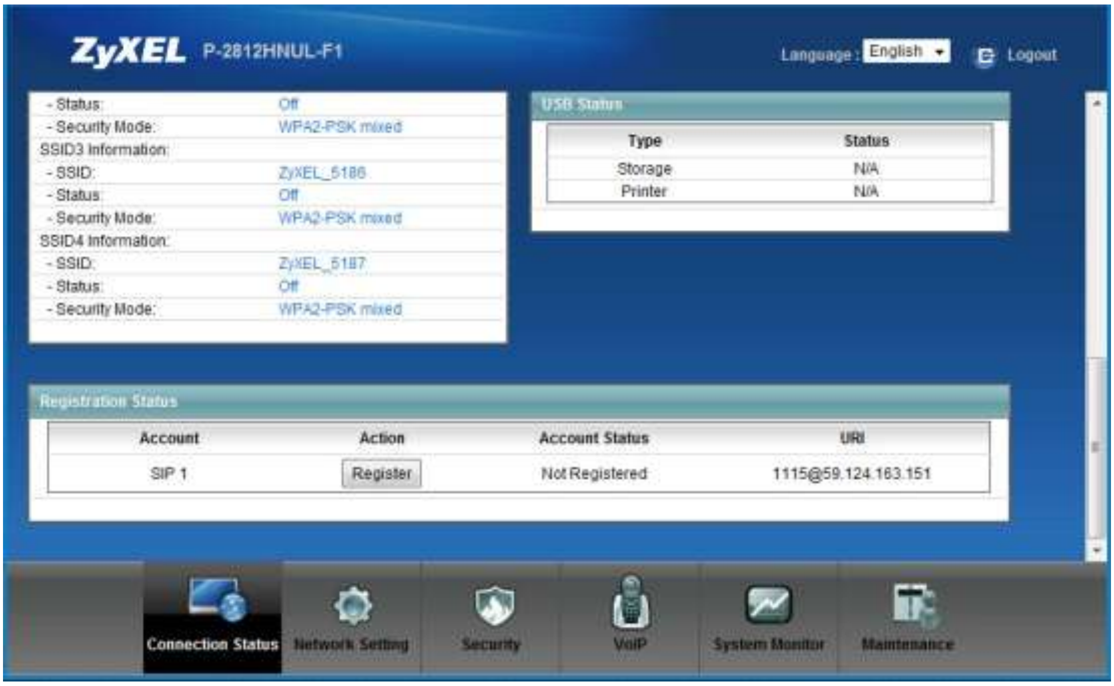
Note :

VAD will not be active while G.722 is used.

Call Features

☑ Send Caller ID

After the SIP account is properly configured, the P-2812HNU(L)-Fx will automatically register the configured SIP account with assigned SIP server. If it does not, you can go to the Status page, scroll down to the SIP account status section, and click “**Register**” to register the SIP account manually.



- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID3 Information:	
- SSID:	ZyXEL_5186
- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID4 Information:	
- SSID:	ZyXEL_5187
- Status:	Off
- Security Mode:	WPA2-PSK mixed

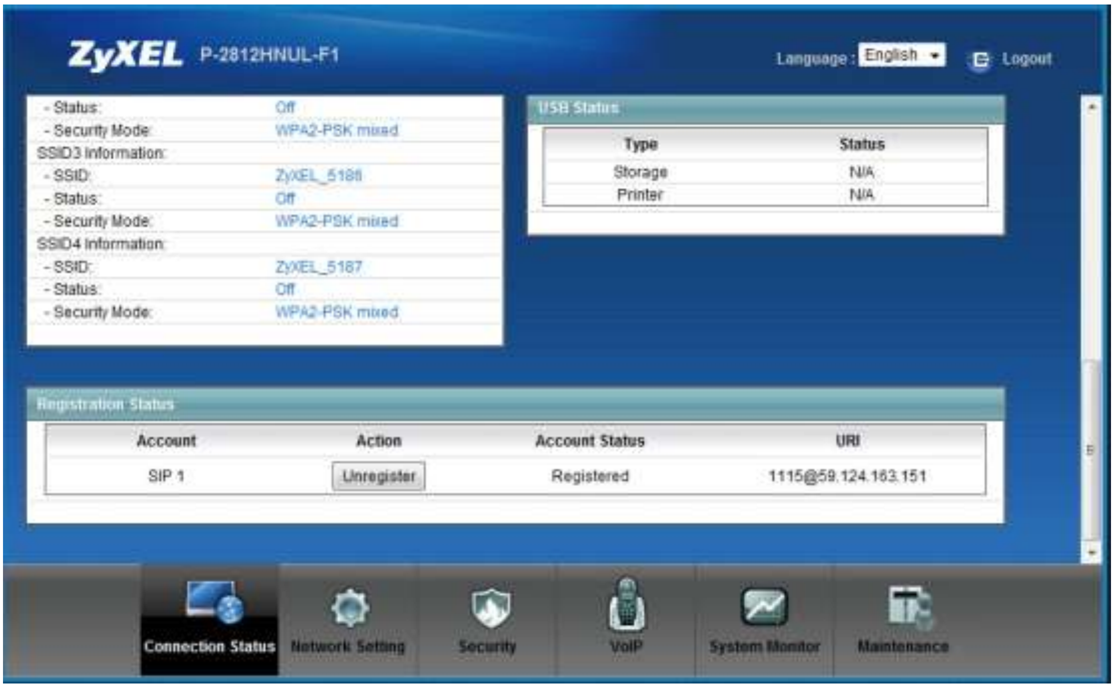
USB Status

Type	Status
Storage	N/A
Printer	N/A

Registration Status

Account	Action	Account Status	URI
SIP 1	Register	Not Registered	1115@59.124.163.151

Or you can also click “**Unregister**” to unregister the SIP account manually.



- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID3 Information:	
- SSID:	ZyXEL_5186
- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID4 Information:	
- SSID:	ZyXEL_5187
- Status:	Off
- Security Mode:	WPA2-PSK mixed

USB Status

Type	Status
Storage	N/A
Printer	N/A

Registration Status

Account	Action	Account Status	URI
SIP 1	Unregister	Registered	1115@59.124.163.151

FXO Lifeline Application Notes

This FXO Lifeline application notes section is for P-2812HNUL-Fx only. Here we use P-2812HNUL-F1 as example

Usage of FXO Lifeline

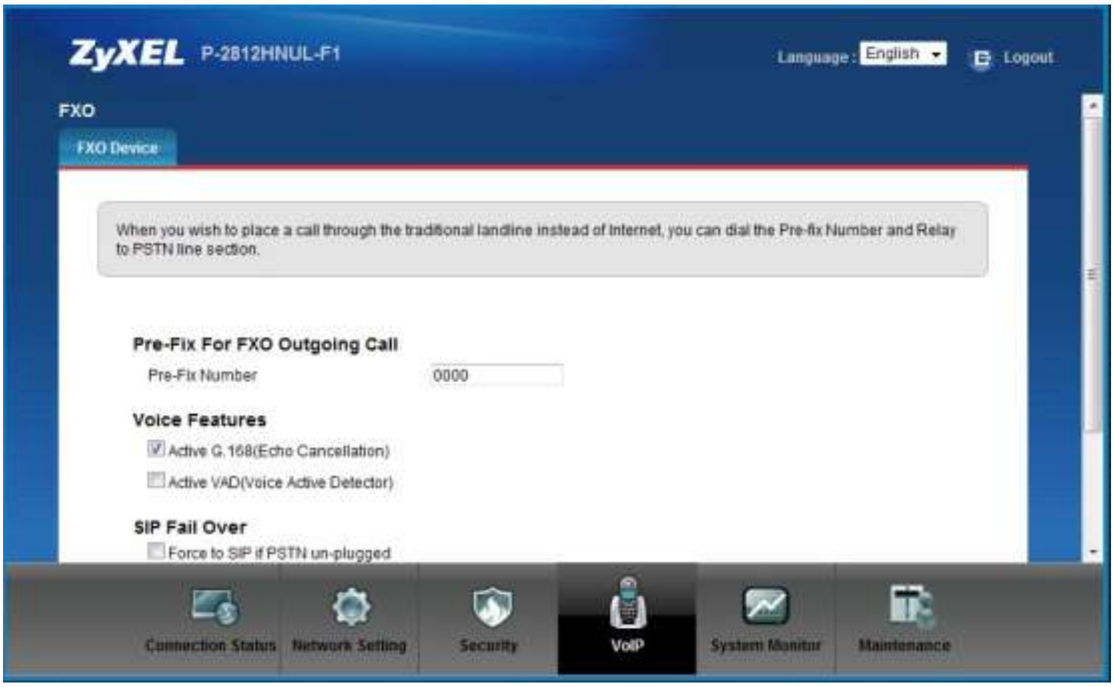
By using the FXO lifeline function, you can make and receive regular FXO phone calls in coexistence with the VoIP service on the same phone set. This can be done by simply assigning a prefix number (by default the prefix for FXO dial out is 0000 and can be changed to any desired value) and dialing this prefix to switch over to the FXO line, rather than dialing the FXO number as usual.

Furthermore, when the P-2812HNUL-Fx experiences power loss such as in the case of earthquake and other natural hazard that causes power loss, it will automatically switch to the FXO line and allow you to dial a regular phone number without dialing the prefix number.

This can be applied in emergency situations such as for contacting police, fire or emergency medical services during a power outage. The following section illustrates how to configure the lifeline in P-2812HNUL-Fx Web GUI.

Lifeline configuration

To configure the lifeline in P-2812HNUL-Fx, click on **FXO Line** to display the following screen.



When you wish to place a call through the traditional landline instead of Internet, you can dial the Pre-fix Number and Relay to PSTN line section.

Pre-Fix For FXO Outgoing Call

Pre-Fix Number: 0000

Voice Features

☑ Active G.168(Echo Cancellation)

□ Active VAD(Voice Active Detector)

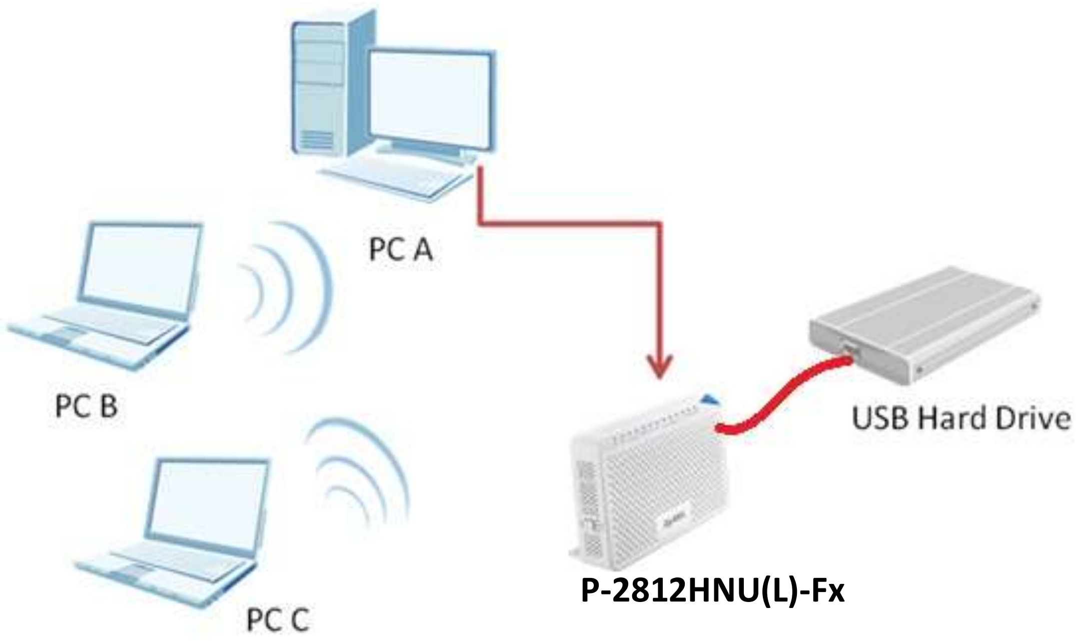
SIP Fail Over

□ Force to SIP if PSTN un-plugged

You can specify a prefix number in the prefix field. This number will be used to switch from VoIP to the FXO system when you wish to make a call to an FXO destination. For example, when you want to dial out to an FXO destination, you would first pick up the phone, and when you hear a dial tone, you would push in the prefix number as defined in the prefix field. In this case, it would be 0000; the device would then switch over to the FXO line. At this moment you would hear a dial tone from FXO again, allowing you to dial out to FXO as you would on a regular FXO system.

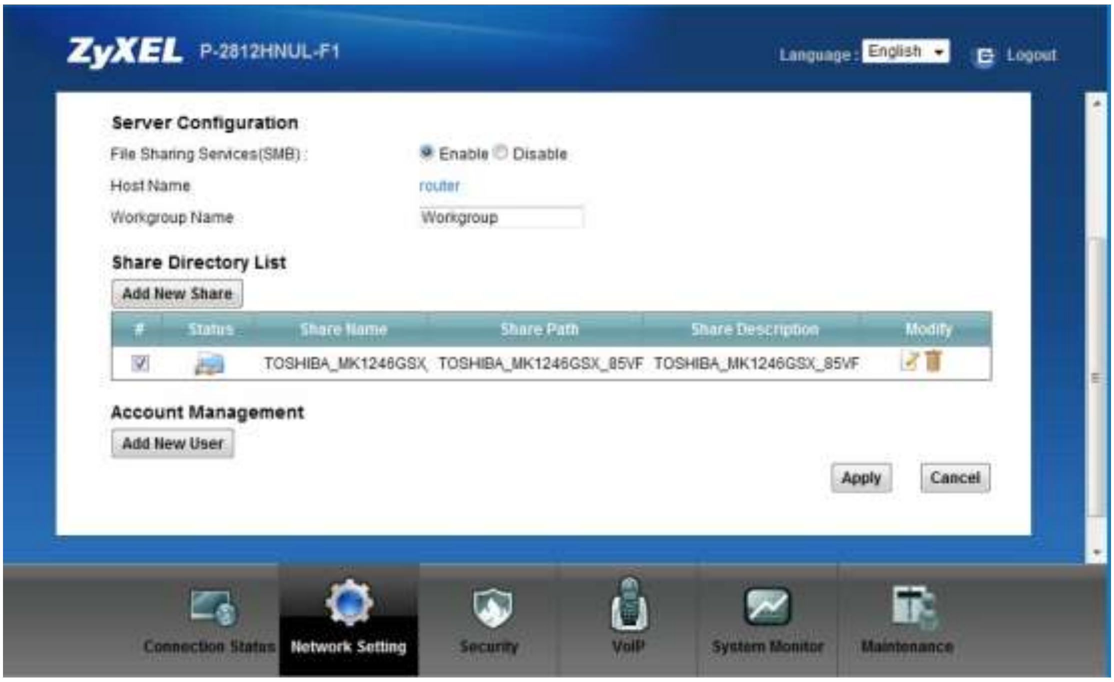
File Sharing

This feature allows sharing files on a USB memory stick or hard drive connected to the P-2812HNU(L)-Fx with other users on the network. The topology shown below allows PC A, B & C to access files on the USB Hard drive.



1. Plug a Flash disk into the USB port.
2. Go to **Network Setting > Home Networking**.
3. Select “**Enable**” of File Sharing Service(SMB) function.
4. Set the Workgroup name (e.g. Workgroup)
5. Select the Folder for sharing.
6. Click on “**Apply**”.

When the File Sharing feature is enabled, P-2812HNU(L)-Fx will find the attached USB hard drive.



Server Configuration

File Sharing Services(SMB) : ● Enable ○ Disable

Host Name router

Workgroup Name Workgroup

Share Directory List

Add New Share

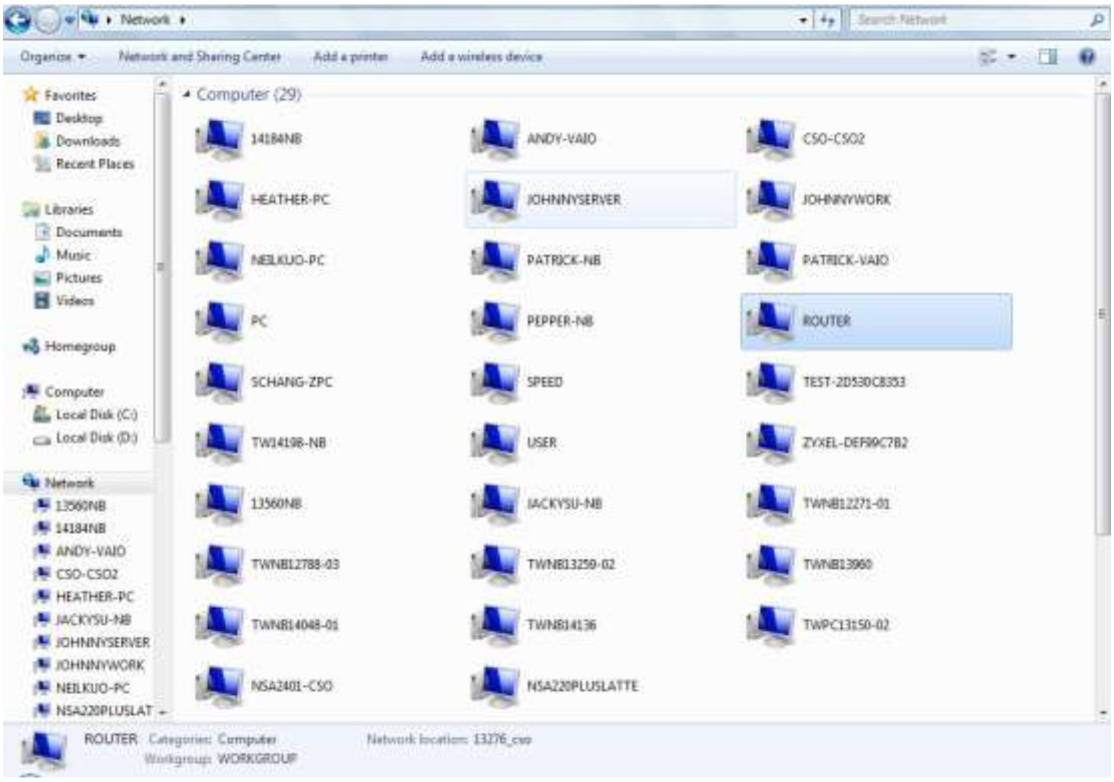
#	Status	Share Name	Share Path	Share Description	Modify
☑		TOSHIBA_MK1246GSX	TOSHIBA_MK1246GSX_85VF	TOSHIBA_MK1246GSX_85VF	

Account Management

Add New User

Apply Cancel

7. Go to Network, you can find “Router” is in your group.

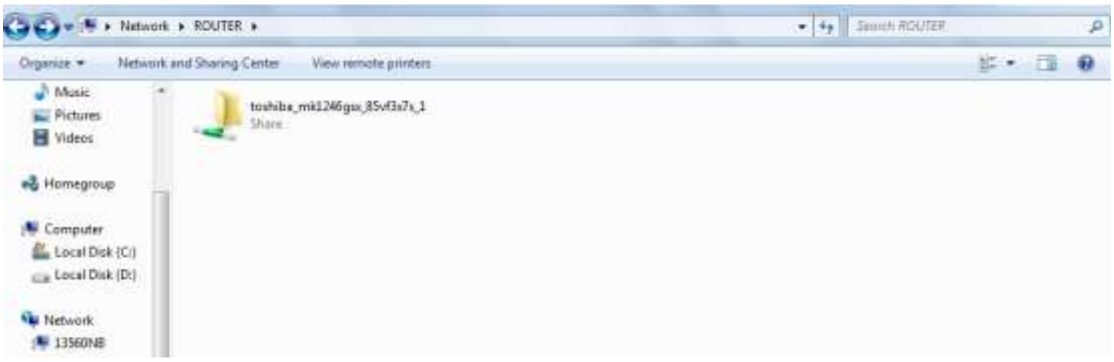


Computer (29)

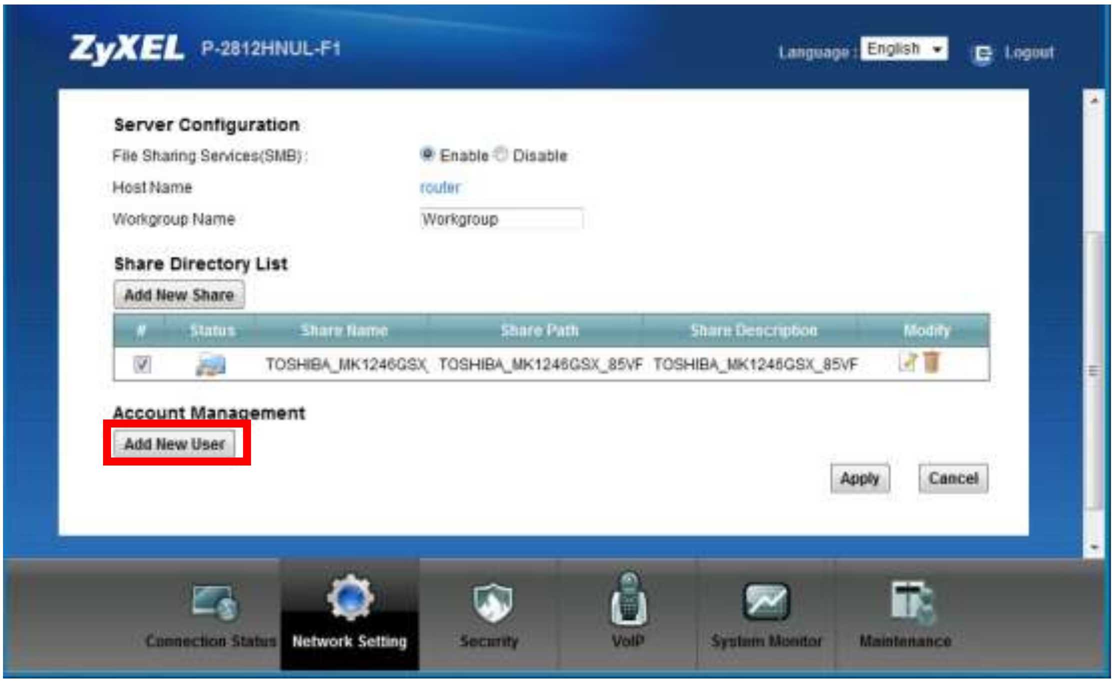
14184NB	ANDY-VAIO	CSO-CSO2
HEATHER-PC	JOHNNYSERVER	JOHNNYWORK
NEILKUO-PC	PATRICK-NB	PATRICK-VAIO
PC	PEPPER-NB	ROUTER
SCHANG-ZPC	SPEED	TEST-2D530C8353
TW14198-NB	USER	ZYXEL-DEF99C7B2
13560NB	JACKYSU-NB	TWNB12271-01
TWNB12788-03	TWNB13259-02	TWNB13960
TWNB14048-01	TWNB14136	TWPC13150-02
NSA2401-CSO	NSA220PLUSLATTE	

ROUTER Categories: Computer Network location: 13276_cso
Workgroup: WORKGROUP

8. Simply click “Router”, the contents of the USB hard drive will be displayed.



9. Set security level for shared folder. Go to **Network Setting > Home Networking.** Click “**Add New User**” to create file sharing users.



Server Configuration

File Sharing Services(SMB) : ● Enable ○ Disable

Host Name: router

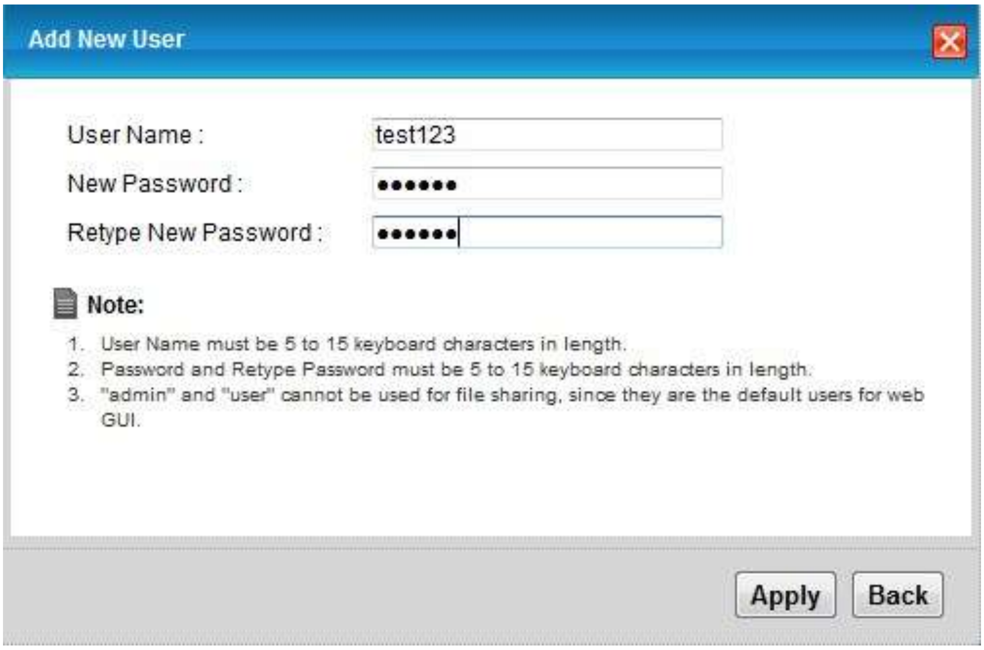
Workgroup Name: Workgroup

Share Directory List

#	Status	Share Name	Share Path	Share Description	Modify
☑		TOSHIBA_MK1246GSX_	TOSHIBA_MK1246GSX_85VF	TOSHIBA_MK1246GSX_85VF	

Account Management

10. Input the user name and password, then click “**Apply**”.



Add New User

User Name : test123

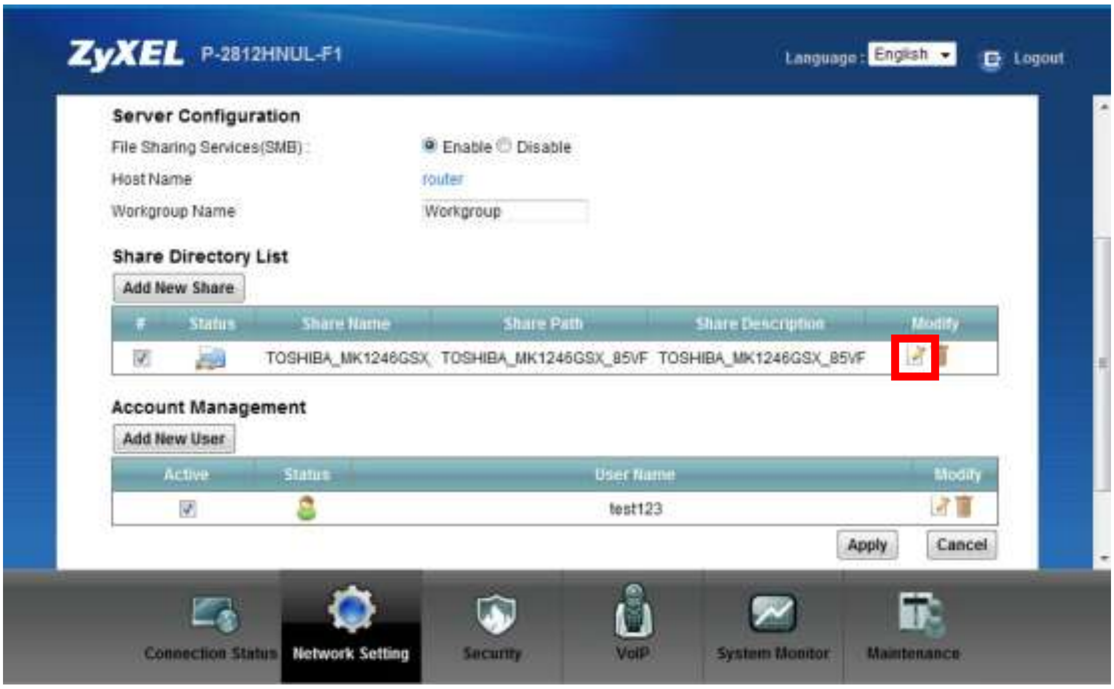
New Password : ●●●●●●

Retype New Password : ●●●●●●

Note:

1. User Name must be 5 to 15 keyboard characters in length.
2. Password and Retype Password must be 5 to 15 keyboard characters in length.
3. "admin" and "user" cannot be used for file sharing, since they are the default users for web GUI.

11. Click the “**Edit**” icon of the shared folder.



Server Configuration

File Sharing Services(SMB) : ● Enable ○ Disable

Host Name router

Workgroup Name Workgroup

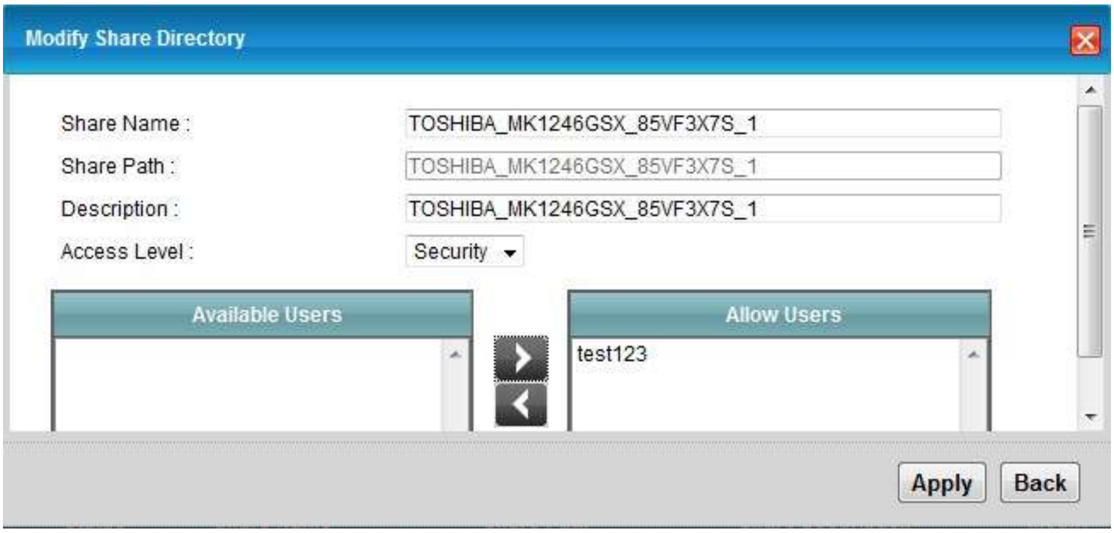
Share Directory List

#	Status	Share Name	Share Path	Share Description	Modify
☑		TOSHIBA_MK1246GSX_	TOSHIBA_MK1246GSX_85VF	TOSHIBA_MK1246GSX_85VF	

Account Management

Active	Status	User Name	Modify
☑		test123	

12. Set Access Level to “**Security**” and move the user account which allowed to access to “**Allow Users**” box, then “**Apply**”



Modify Share Directory

Share Name : TOSHIBA_MK1246GSX_85VF3X7S_1

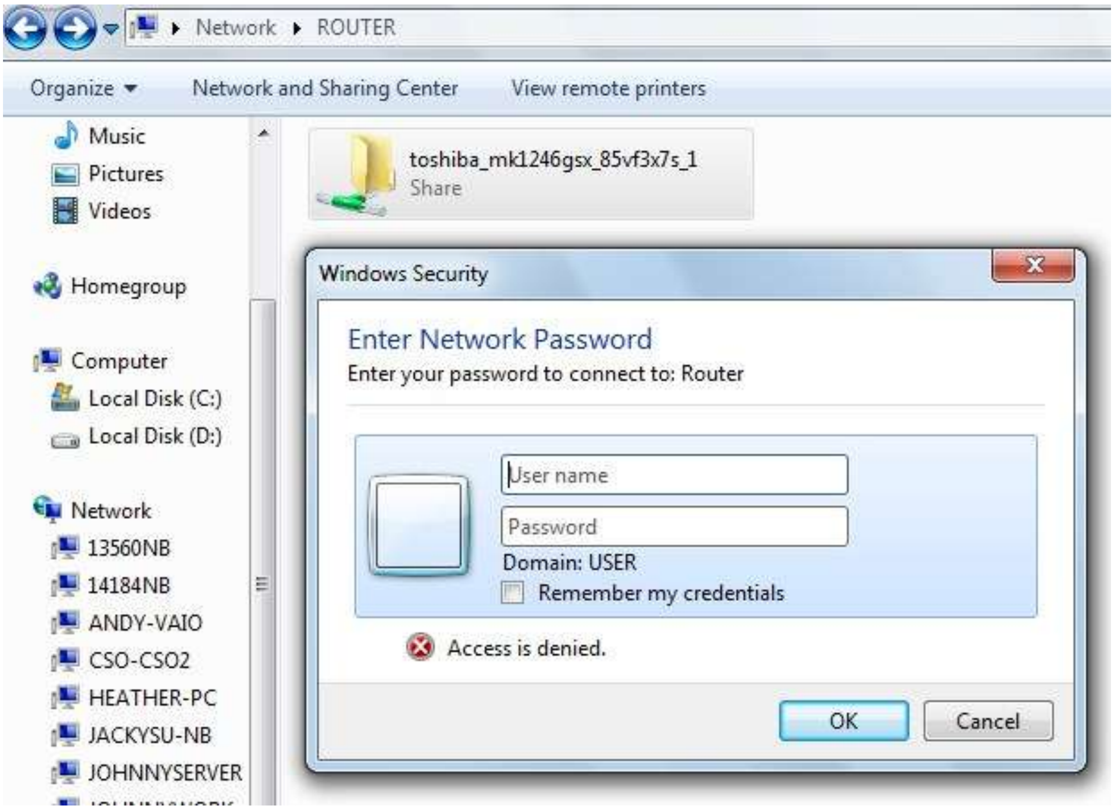
Share Path : TOSHIBA_MK1246GSX_85VF3X7S_1

Description : TOSHIBA_MK1246GSX_85VF3X7S_1

Access Level : Security

Available Users	Allow Users
	test123

13. Then the system would need authentication to access the shared folder.



Windows Security

Enter Network Password

Enter your password to connect to: Router

User name

Password

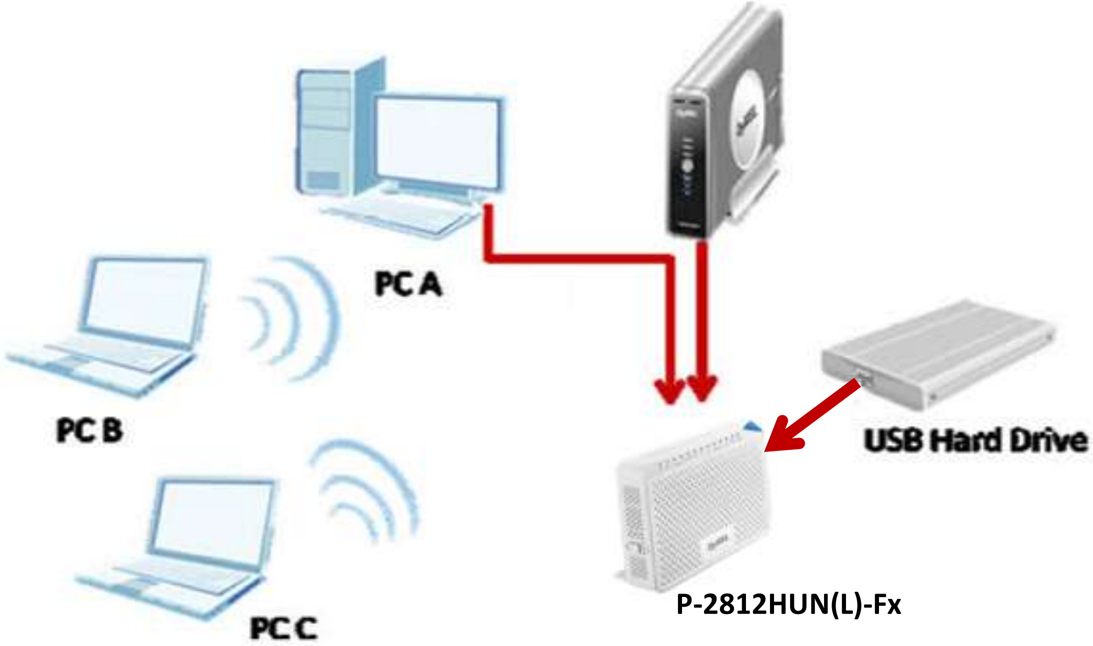
Domain: USER

□ Remember my credentials

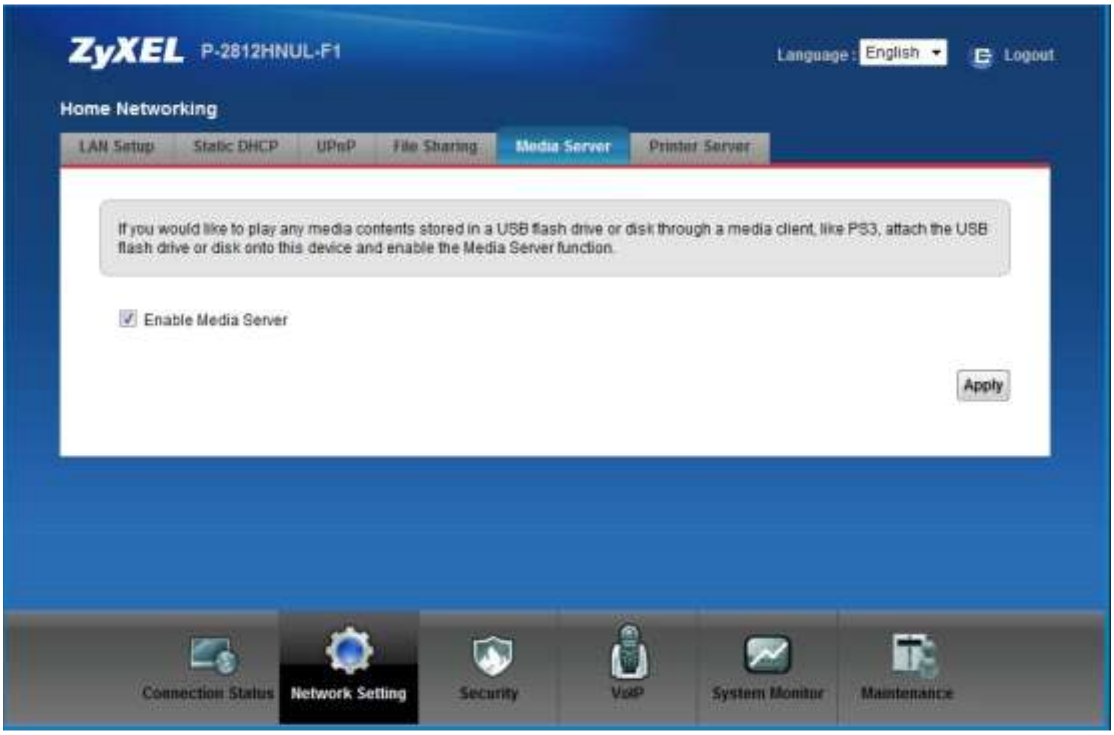
Access is denied.

- ## Media Server Feature

Using the media server feature to play media files on a the PC, this section shows you how the media server feature works with the Windows Media Player in windows 7 (if user do not have media player as User Guide suggested) to play music or video from USB disk and NSA-210 which is connecting to the LAN port.



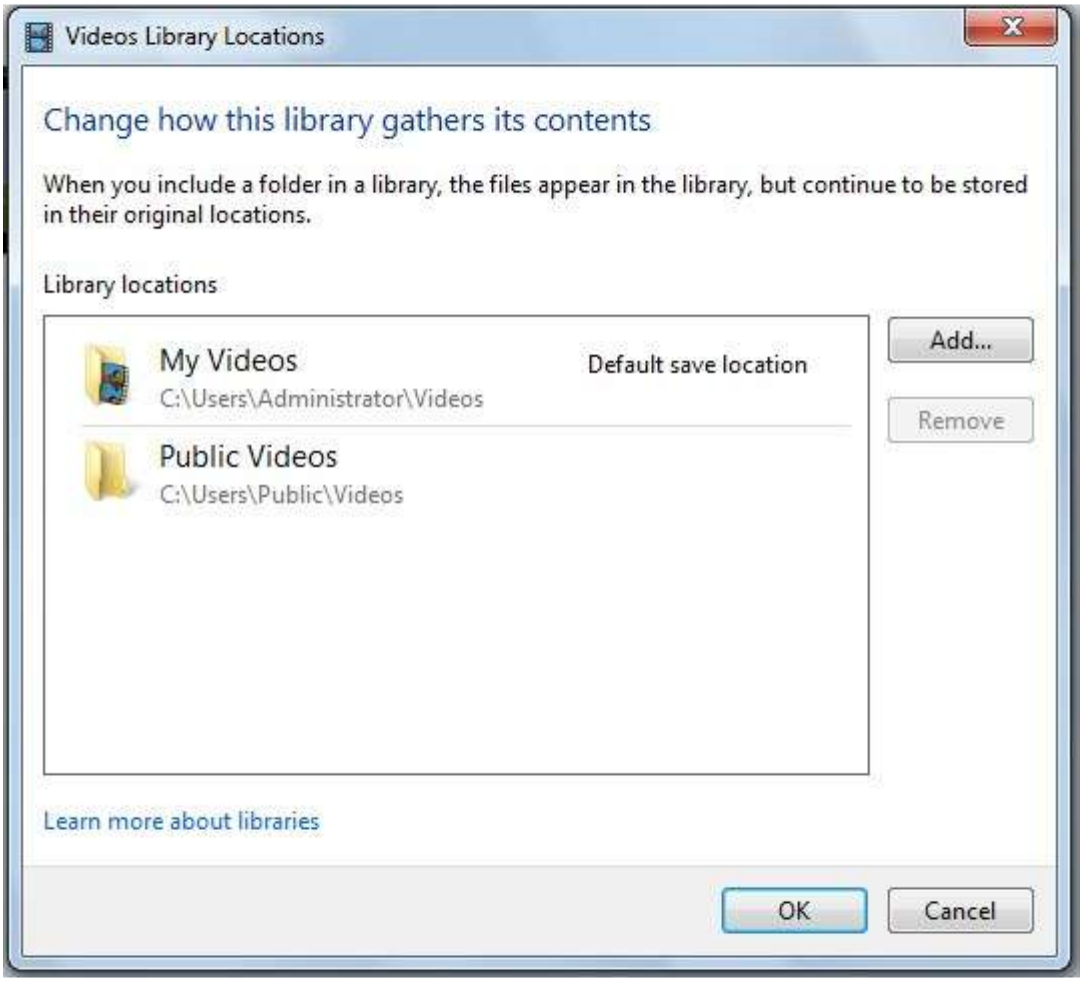
1. Go to **Network Setting > Home Networking > Media Server.**
2. Click on "**Enable Media Server".**



If you would like to play any media contents stored in a USB flash drive or disk through a media client, like PS3, attach the USB flash drive or disk onto this device and enable the Media Server function.

☑ Enable Media Server

3. Run Windows Media Player on PC and go to **Organize > Manage libraries > Videos**, then click “**Add**” to add folders to Videos.



Videos Library Locations

Change how this library gathers its contents

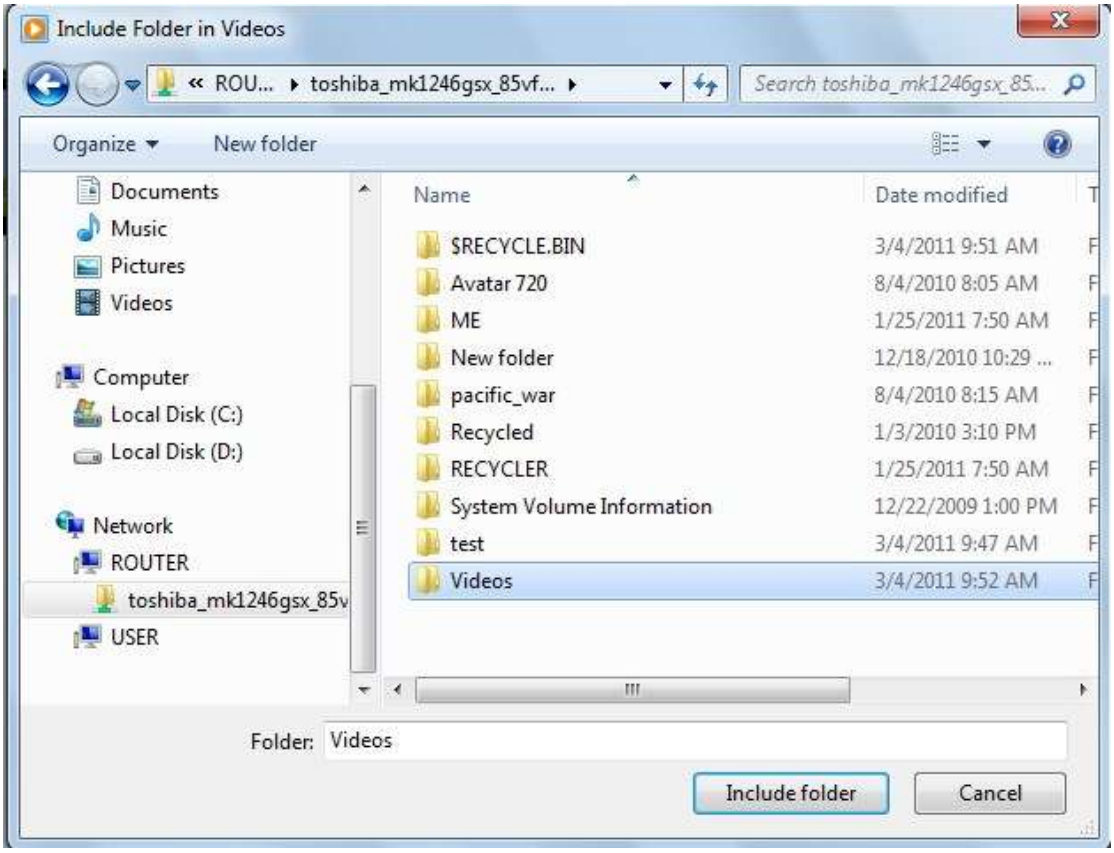
When you include a folder in a library, the files appear in the library, but continue to be stored in their original locations.

Library locations

My Videos Default save location
C:\Users\Administrator\Videos

Public Videos
C:\Users\Public\Videos

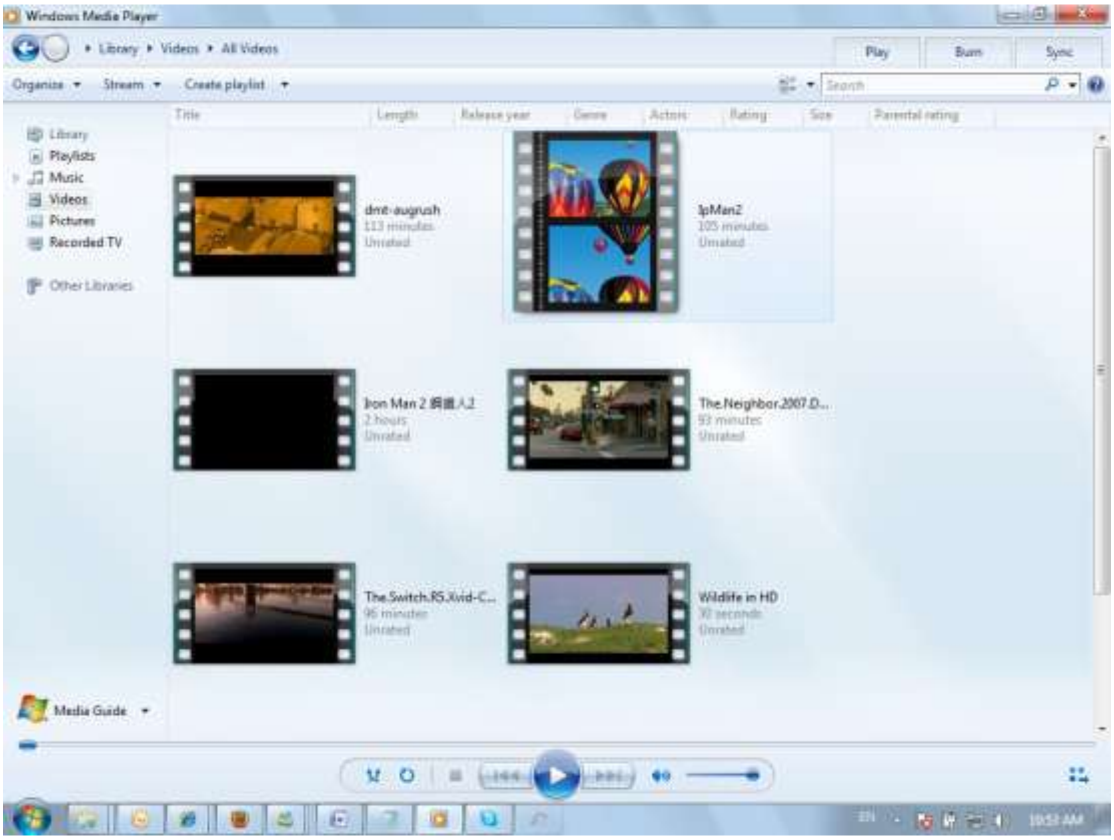
4. Select the folder on the shared USB disk that you would like to add to the Videos list, then click **“Include folder”** and “**OK**”**.**



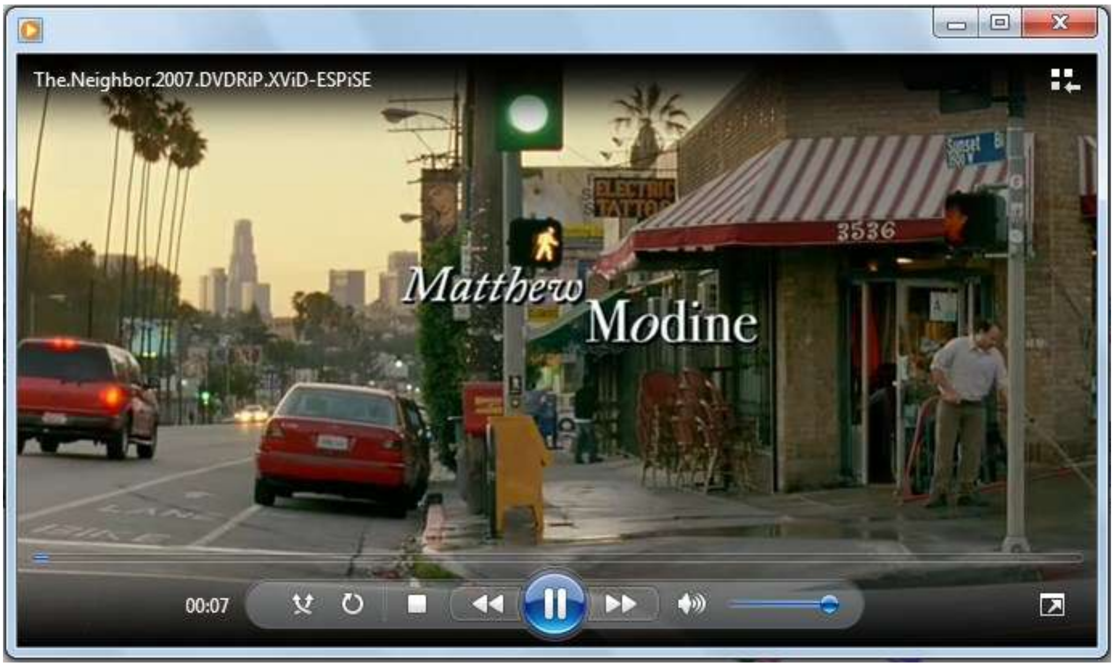
Name	Date modified	T
$RECYCLE.BIN	3/4/2011 9:51 AM	F
Avatar 720	8/4/2010 8:05 AM	F
ME	1/25/2011 7:50 AM	F
New folder	12/18/2010 10:29 ...	F
pacific_war	8/4/2010 8:15 AM	F
Recycled	1/3/2010 3:10 PM	F
RECYCLER	1/25/2011 7:50 AM	F
System Volume Information	12/22/2009 1:00 PM	F
test	3/4/2011 9:47 AM	F
Videos	3/4/2011 9:52 AM	F

Folder: Videos

5. Click “**Videos**” on Windows Media Player, Media Player would search the video files and add to the video library automatically.



6. All the videos on the library are able to play remotely.



You can also play the media contents in the NAS210 as well following the same steps.

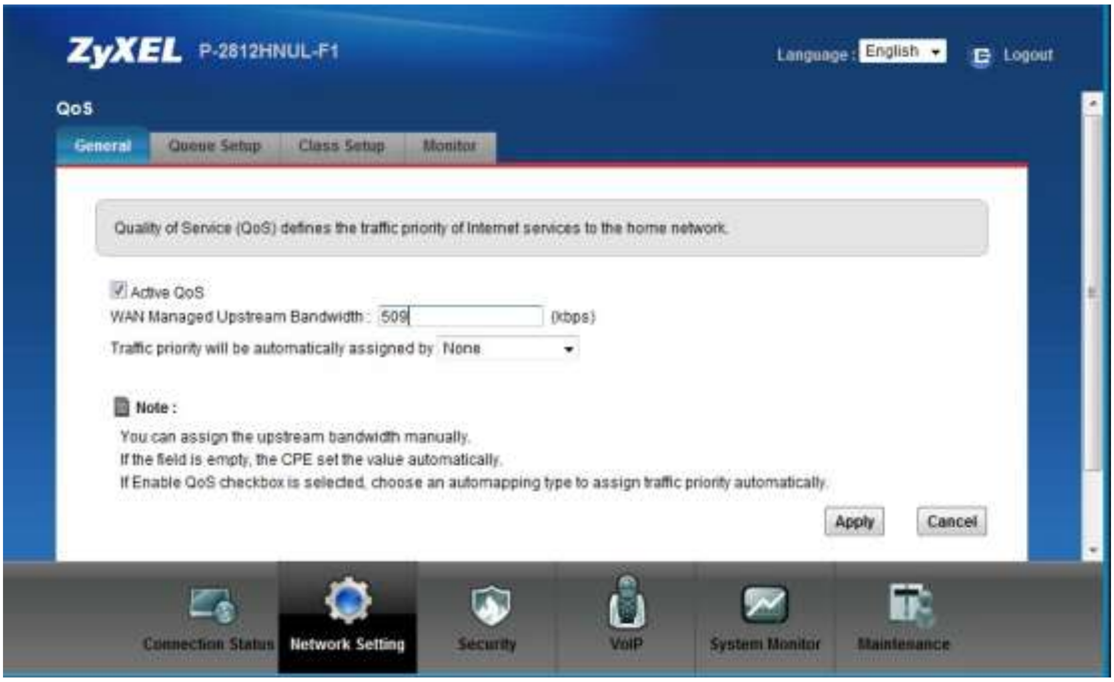
QoS Support

Introduction of QoS

- Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and to the networking methods used to control the use of bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

- Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network unfit for time critical applications such as video-on-demand and VoIP.

1. Click **Network Setting > QoS > General**, and activate the QoS service, then set the Maximum Upstream bandwidth value to 509 to fully utilize WAN bandwidth.



Quality of Service (QoS) defines the traffic priority of Internet services to the home network.

☑ Active QoS

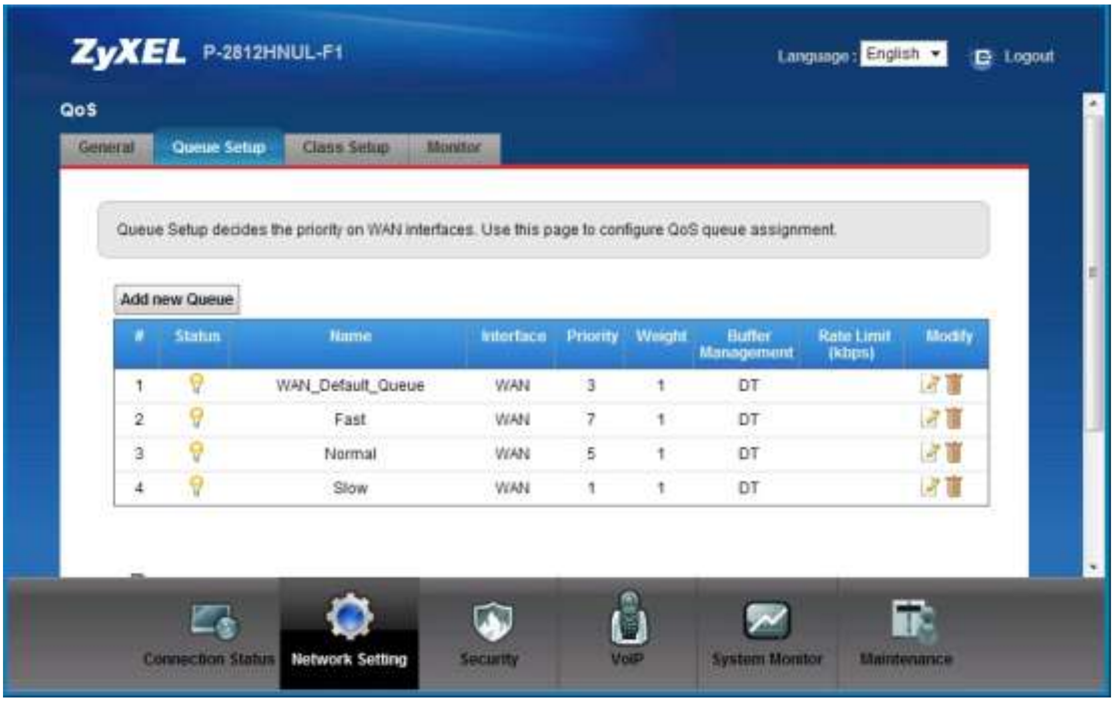
WAN Managed Upstream Bandwidth : 509 (kbps)

Traffic priority will be automatically assigned by None

Note :

You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.

2. Click on "**Queue Setup**".
3. You can "**Add new Queue**" or "**Edit**" the Queues displayed in the screenshot. The Priority and Weight can be adjusted



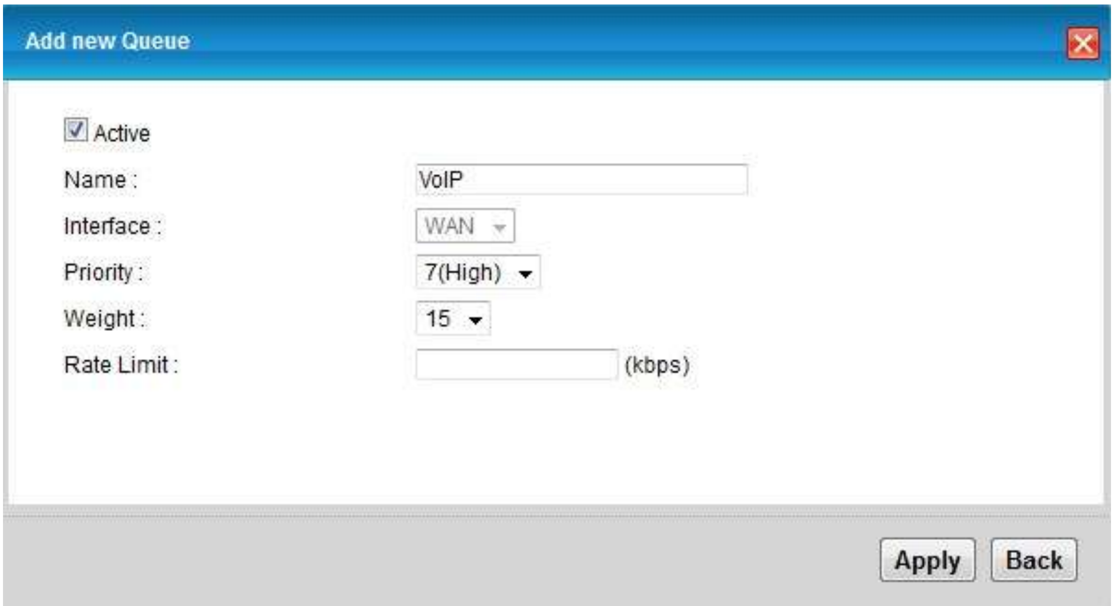
QoS

Queue Setup decides the priority on WAN interfaces. Use this page to configure QoS queue assignment.

Add new Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1		WAN_Default_Queue	WAN	3	1	DT		
2		Fast	WAN	7	1	DT		
3		Normal	WAN	5	1	DT		
4		Slow	WAN	1	1	DT		

4. You can add new Queues for VoIP and IPTV. Click "**Add new Queue**", active the new queue, named "VoIP", set priority as 7 and weight as 15.



☑ Active

Name : VoIP

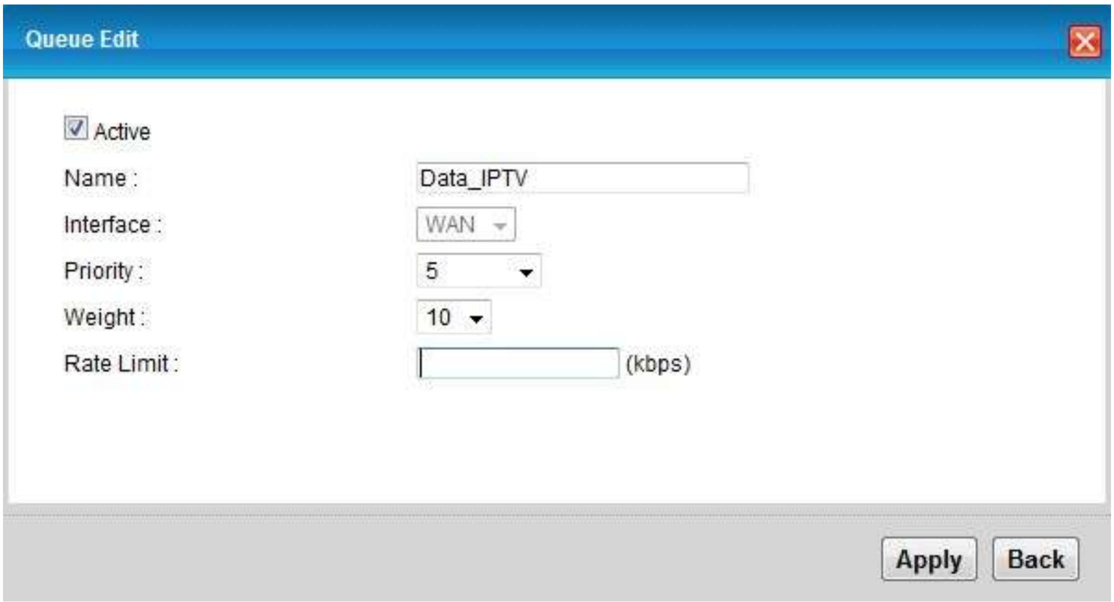
Interface : WAN

Priority : 7(High)

Weight : 15

Rate Limit : (kbps)

5. Again, Click "**Add new Queue**", active the new queue, named "Dat_IPTV", set priority as 5 and weight as 10



Queue Edit

☑ Active

Name : Data_IPTV

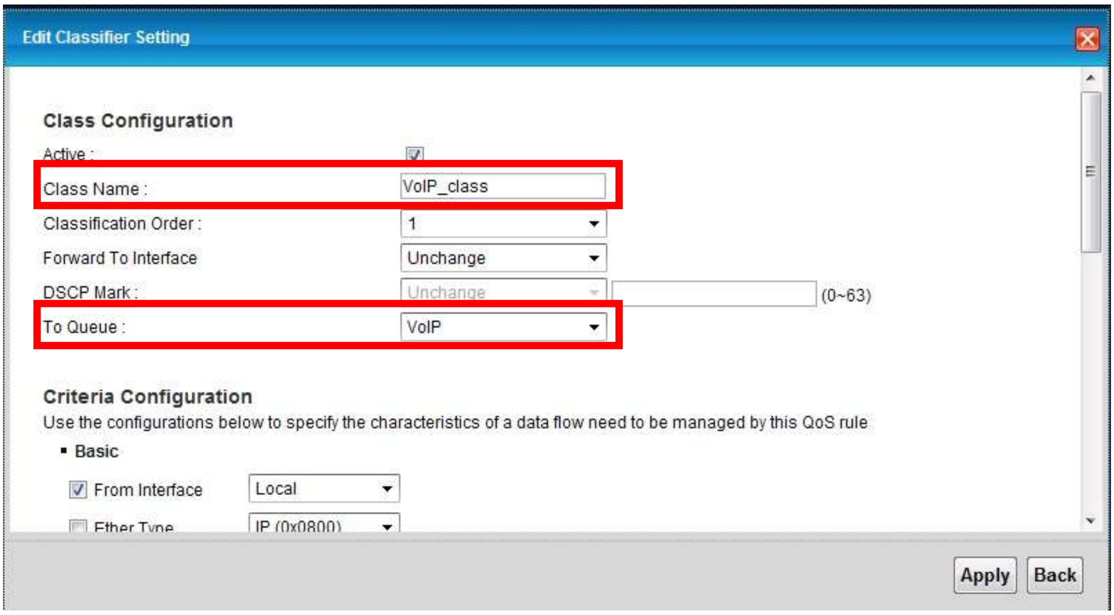
Interface : WAN

Priority : 5

Weight : 10

Rate Limit : (kbps)

6. Click on the “**Class Setup**” tab to set up QoS Classifiers
7. Configure the first Class rule for VoIP. Select “**VoIP**” in “To Queue:” and input a name for it. E.g. “VoIP_test” as follows:



Edit Classifier Setting

Class Configuration

Active : ☑

Class Name : VoIP_class

Classification Order : 1

Forward To Interface Unchange

DSCP Mark : Unchange (0~63)

To Queue : VoIP

Criteria Configuration

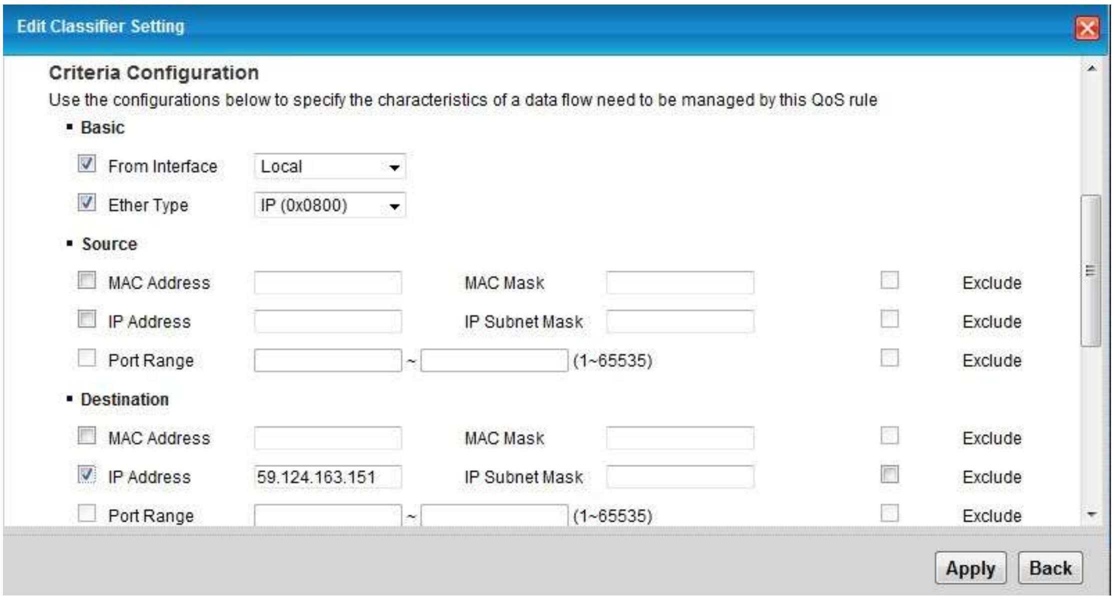
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic

☑ From Interface Local

□ Ether Type IP (0x0800)

8. Enable the **From Interface** and set to “Local”, and **Ether Type** criteria and set them accordingly.
9. Set the **Destination IP address** to the SIP server’s IP address.



Edit Classifier Setting

Criteria Configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic

☑ From Interface	Local				
☑ Ether Type	IP (0x0800)				

- Source

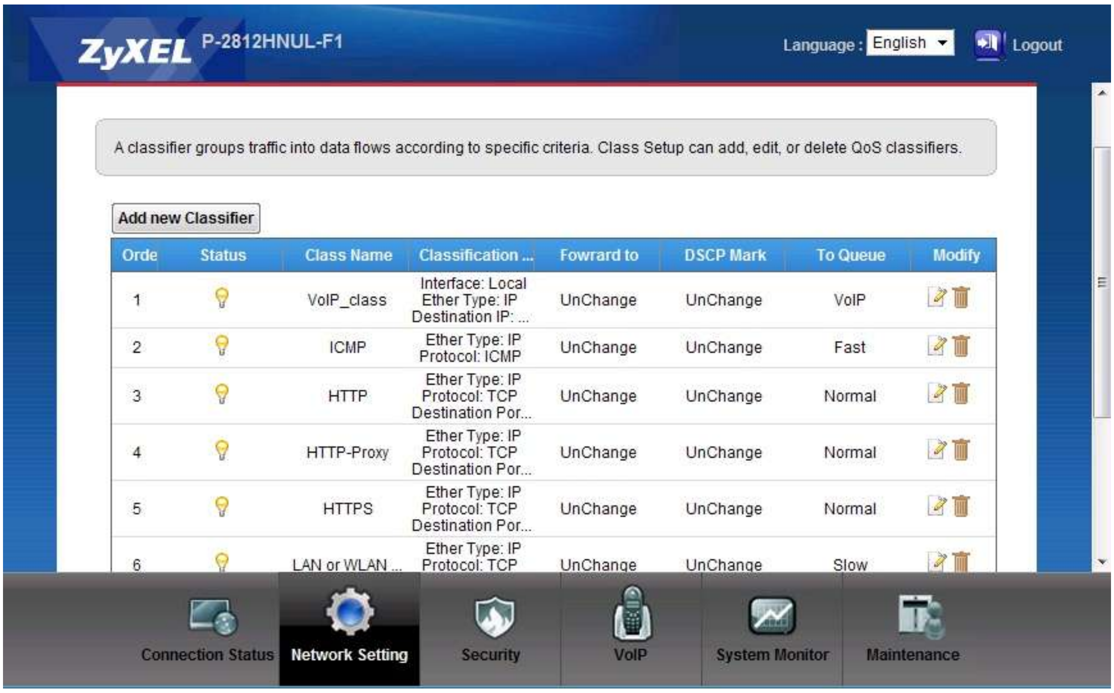
□ MAC Address		MAC Mask		□	Exclude
□ IP Address		IP Subnet Mask		□	Exclude
□ Port Range	~	(1~65535)		□	Exclude

- Destination

□ MAC Address		MAC Mask		□	Exclude
☑ IP Address	59.124.163.151	IP Subnet Mask		□	Exclude
□ Port Range	~	(1~65535)		□	Exclude

10. Click “**Apply**”. Now we have completed the Class rule for VoIP service, and the next step is to configure the second class rule for the Data_IPTV service.

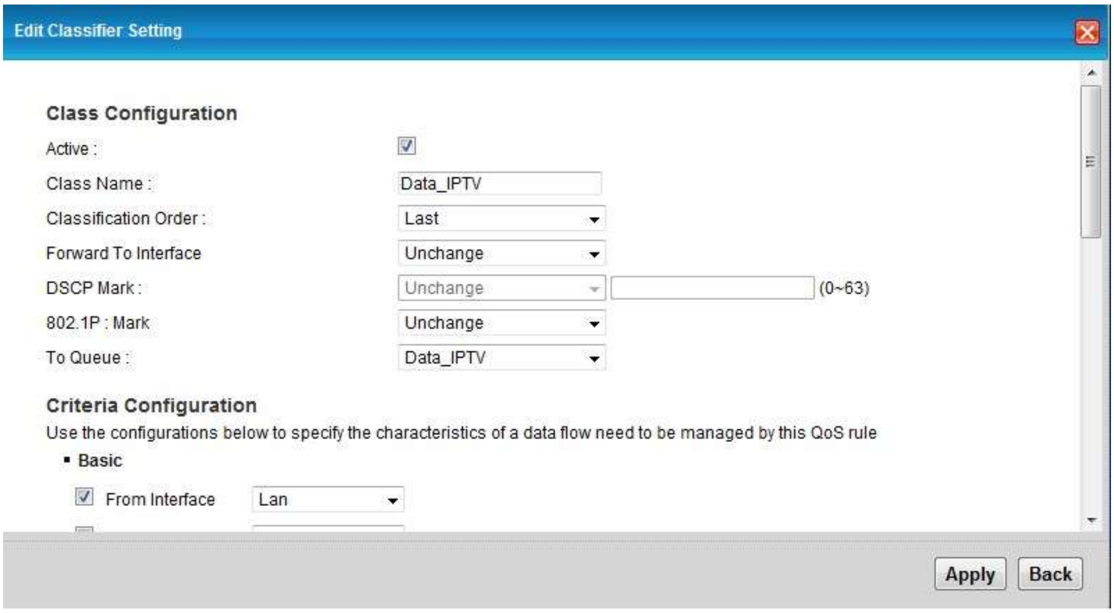
11. Click “**Add new Classifier**” to add the second class rule.



A classifier groups traffic into data flows according to specific criteria. Class Setup can add, edit, or delete QoS classifiers.

Orde	Status	Class Name	Classification ...	Fowrard to	DSCP Mark	To Queue	Modify
1		VoIP_class	Interface: Local Ether Type: IP Destination IP: ...	UnChange	UnChange	VoIP	
2		ICMP	Ether Type: IP Protocol: ICMP	UnChange	UnChange	Fast	
3		HTTP	Ether Type: IP Protocol: TCP Destination Por...	UnChange	UnChange	Normal	
4		HTTP-Proxy	Ether Type: IP Protocol: TCP Destination Por...	UnChange	UnChange	Normal	
5		HTTPS	Ether Type: IP Protocol: TCP Destination Por...	UnChange	UnChange	Normal	
6		LAN or WLAN ...	Ether Type: IP Protocol: TCP	UnChange	UnChange	Slow	

12. Configure the second Class rule as follows:



Class Configuration

Active :	☑
Class Name :	Data_IPTV
Classification Order :	Last
Forward To Interface	Unchange
DSCP Mark :	Unchange (0~63)
802.1P : Mark	Unchange
To Queue :	Data_IPTV

Criteria Configuration

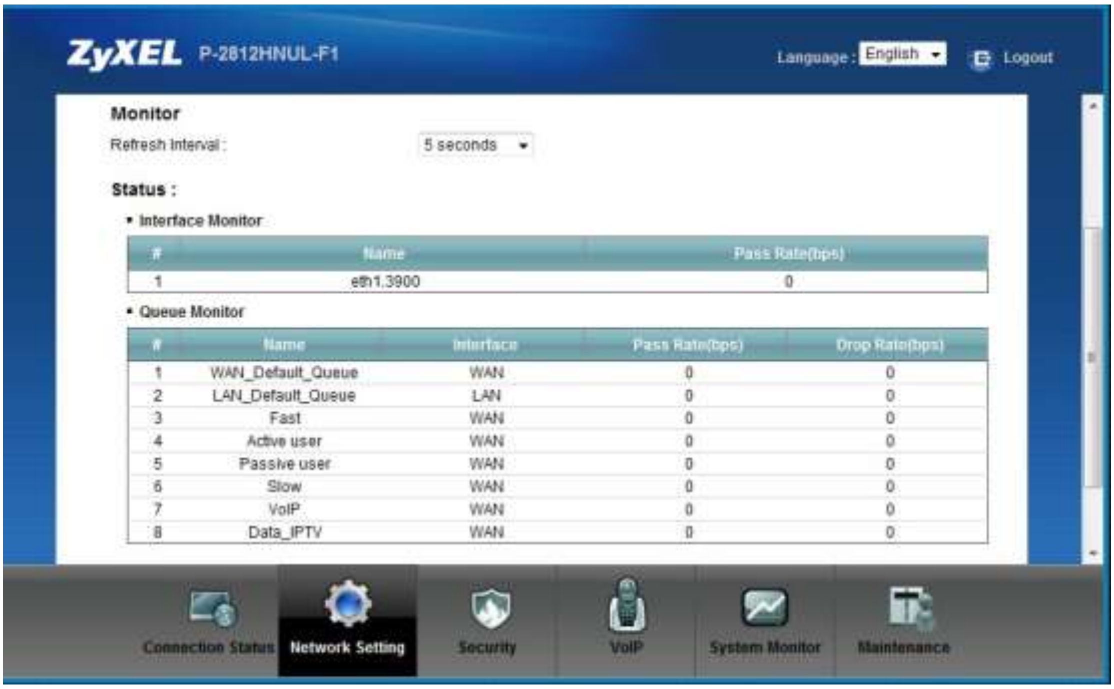
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic

☑ From Interface Lan

13. Enable the "**From Interface**" criteria and set it to "**LAN**" and Select "**Data_IPTV**" in "To Queue:". Then click "**Apply**".
14. To make sure the Class rules are correctly configured, you can go to **Network Setting > QoS > Monitor**.

5. Select **5 sec** as the refresh interval time, and monitor the ZyXEL device's QoS packet statistics.



Monitor

Refresh Interval : 5 seconds

Status :

- Interface Monitor

#	Name	Pass Rate(bps)
1	eth1.3900	0

- Queue Monitor

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	0	0
3	Fast	WAN	0	0
4	Active user	WAN	0	0
5	Passive user	WAN	0	0
6	Slow	WAN	0	0
7	VoIP	WAN	0	0
8	Data_IPTV	WAN	0	0

Wireless Application Notes

Wireless Introduction

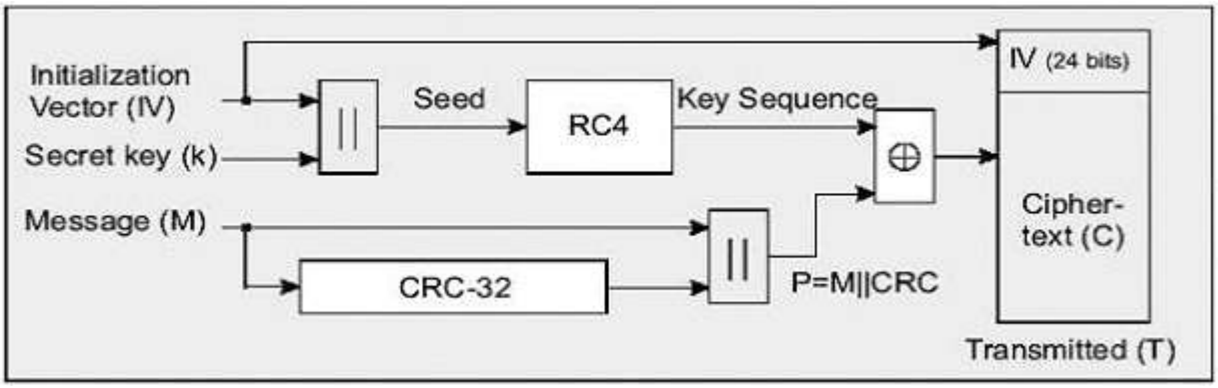
WEP Configuration (Wired Equivalent Privacy) Introduction

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

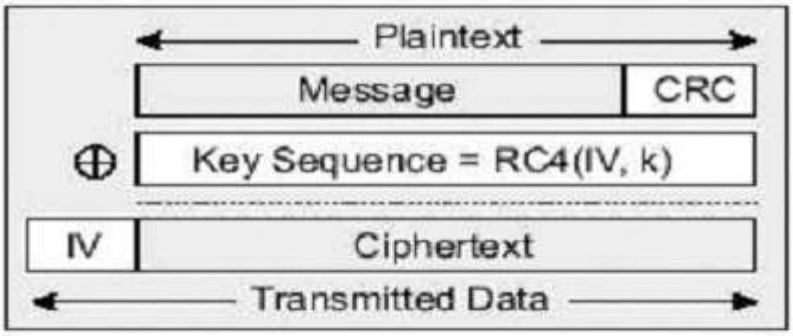
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because the wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium. Everything that is transmitted or received over a wireless network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



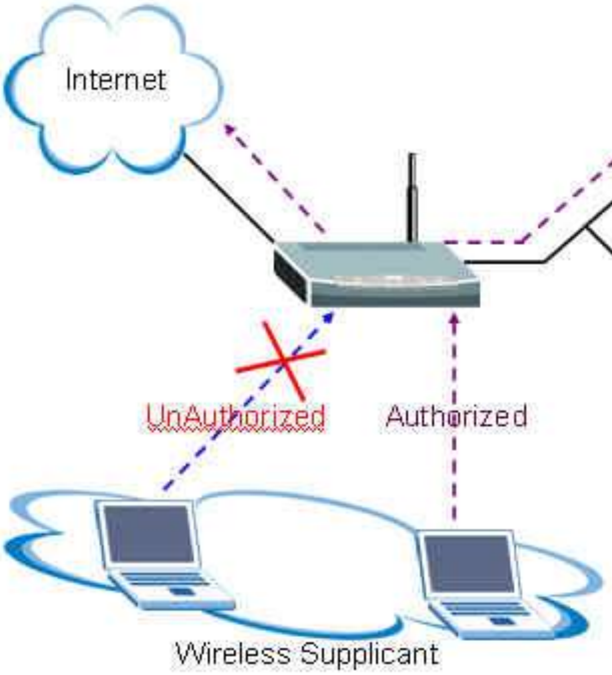
Setting up the Access Point

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 ADSL 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.

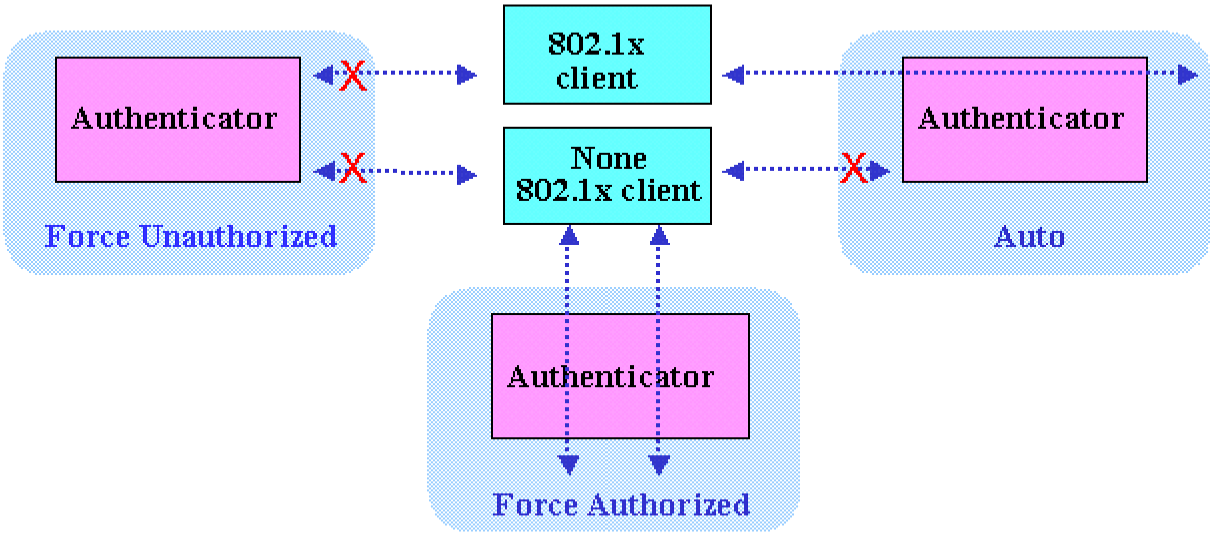
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, therefore the external RADIUS authentication server is not needed. In this case, the Wireless AP is acted as both authenticator and authentication server.

- ***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.

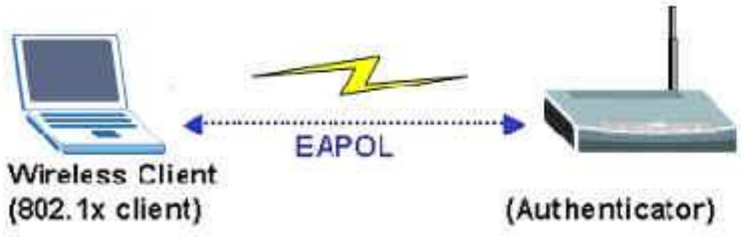
3. Auto: Enables the 802.1x and causes the port to begin in the unauthorized state, allowing only the EAPOL frames to be sent and received through the port. The authentication process begins, when the link state of port transitions from down to up or when an EAPOL-start frame is received requests the 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.

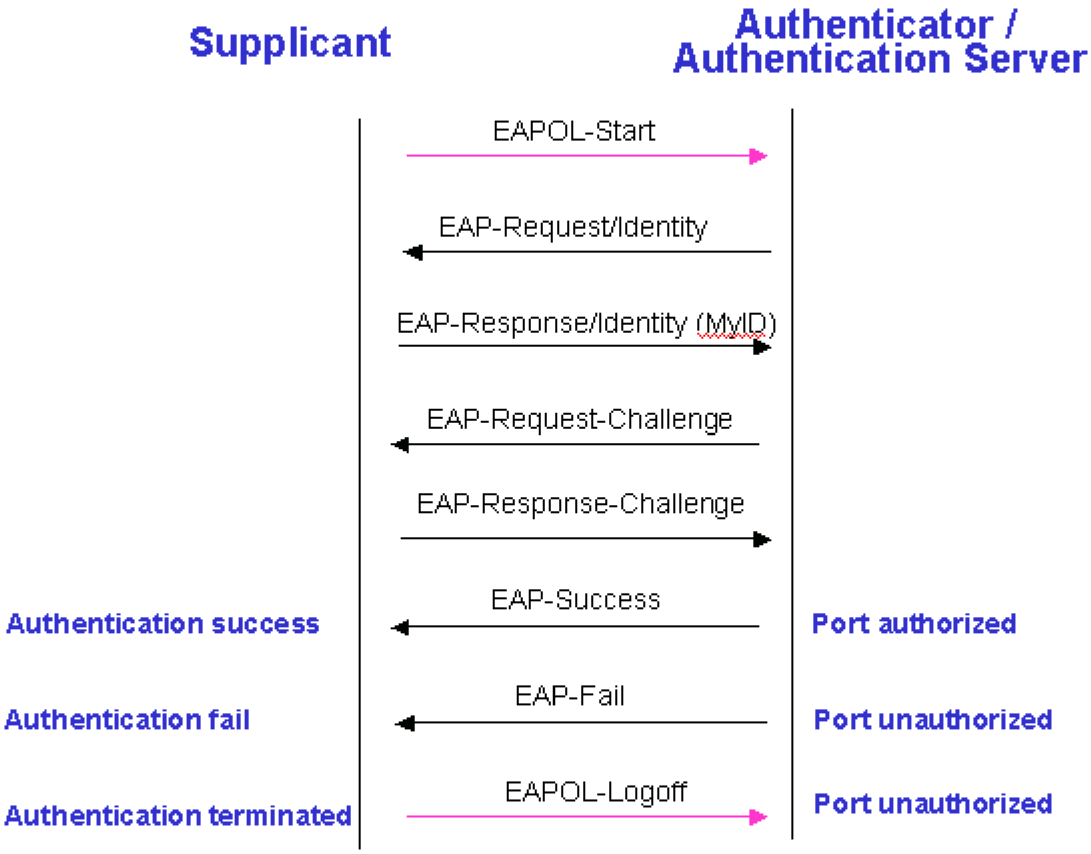


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receives 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.

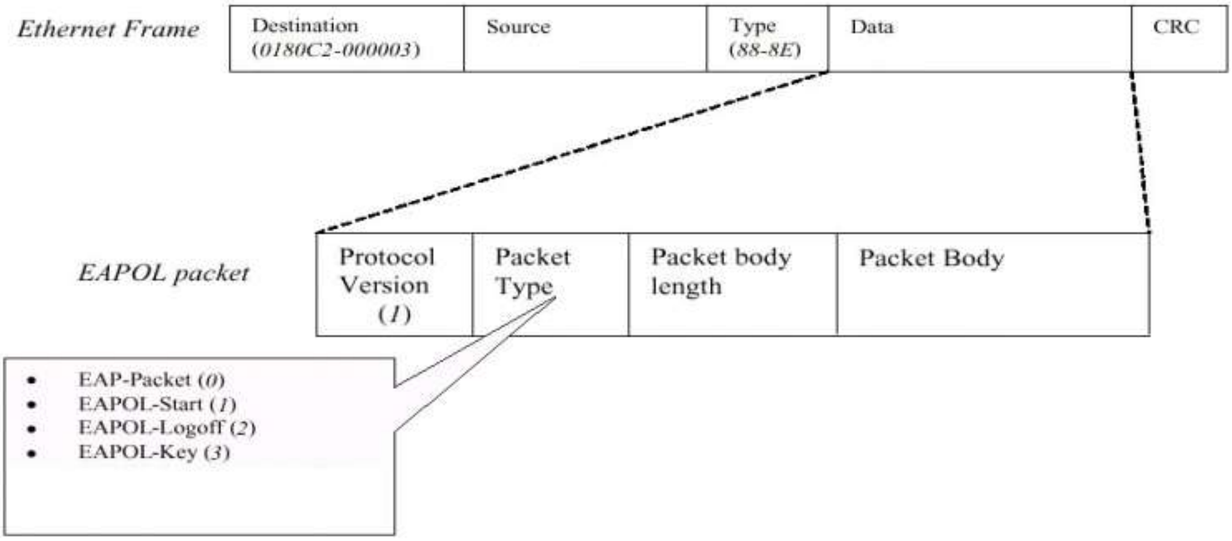
EAPOL Exchange between 802.1x Authenticator and Supplicant

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.

Brief in WPA2

WPA2 (Wi-Fi Protected Access 2) is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 implements the

National Institute of Standards and Technology (NIST) which security is a higher level then WPA, cause it brings AES-base algorithm and Cipher Block Chaining Message Authentication Code Protocol (CCMP) in it and offers stronger encryption then WPA uses (TKIP). WPA2 encryption keys that are used for each client on the network are unique and specific to that client. Eventually, each packet which is sent over the air is encrypted with a unique key. The higher security is enhanced with the use of a new and unique encryption key because there is no key reuse.

WPA &WPA2

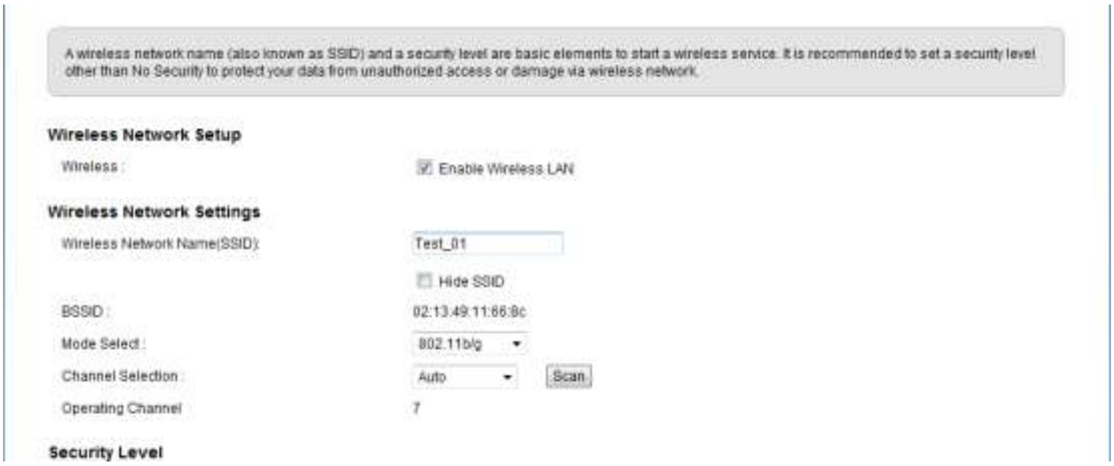
Both WPA & WPA2 offer a high level security for end users and administrators, which utilize EAP (Extensible authentication Protocol) for authentication, both of them all support Personal and Enterprise mode. Because WPA2 provides a stronger encryption mechanism through AES (Advanced Encryption Standard), WPA2's level and standard is requirement for some corporate and government users.

Wireless Configuration

Activate the WLAN interface of the P-2812HNU(L)-Fx and connect the notebook (802.11bg wireless NIC required) under the WPA-PSK security mode.

a. Wireless Setup.

1. Go to **Network Setting** > **Wireless** > **General**.
2. Check the Active Wireless LAN box.
3. Enter the Network Name(SSID), e.g. "Test_01".



A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless : ☑ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID): Test_01

□ Hide SSID

BSSID : 02:13:49:11:66:8c

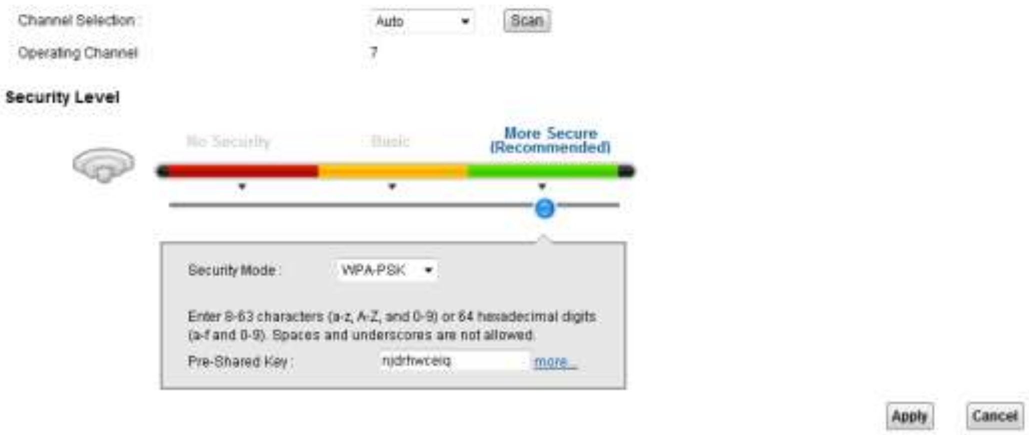
Mode Select : 802.11b/g

Channel Selection : Auto

Operating Channel 7

Security Level

4. Select the Security Mode, e.g. "WPA-PSK".
5. Enter the Pre-Shared Key, e.g. "njdrhwceiq".
6. Click Apply.



Channel Selection : Auto

Operating Channel 7

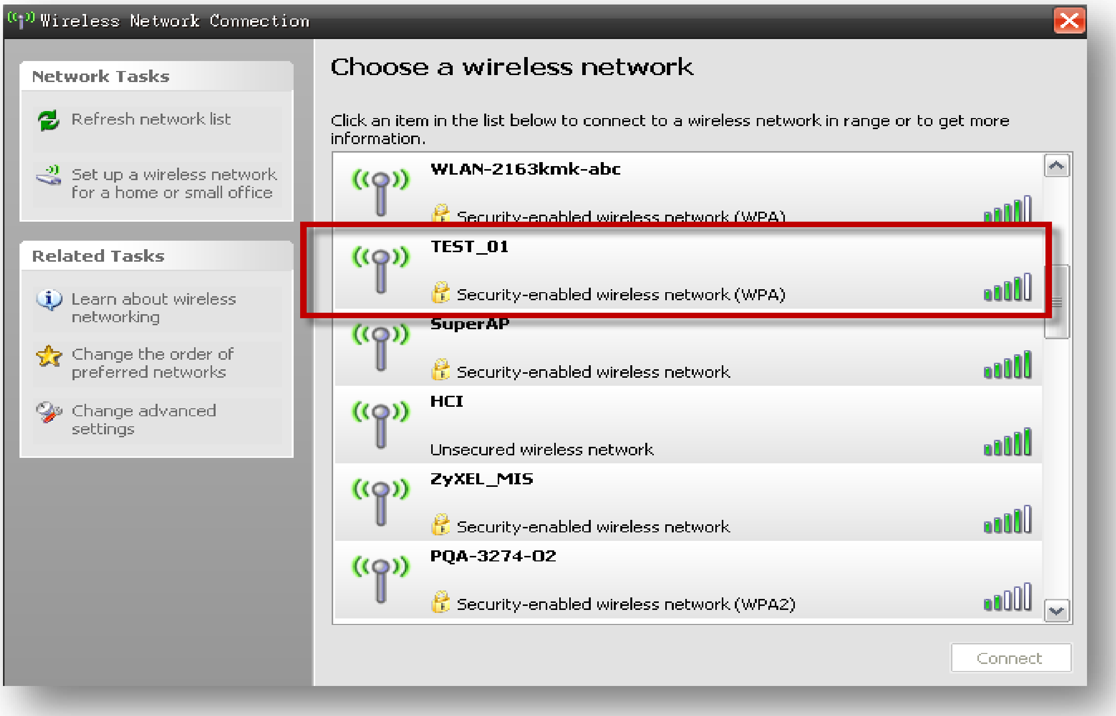
Security Level

Security Mode : WPA-PSK

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f and 0-9). Spaces and underscores are not allowed.

Pre-Shared Key : njdrfwceiq

View all the available wireless networks on your notebook (802.11bg wireless NIC required):



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

WLAN-2163kmk-abc
Security-enabled wireless network (WPA)

TEST_01
Security-enabled wireless network (WPA)

SuperAP
Security-enabled wireless network

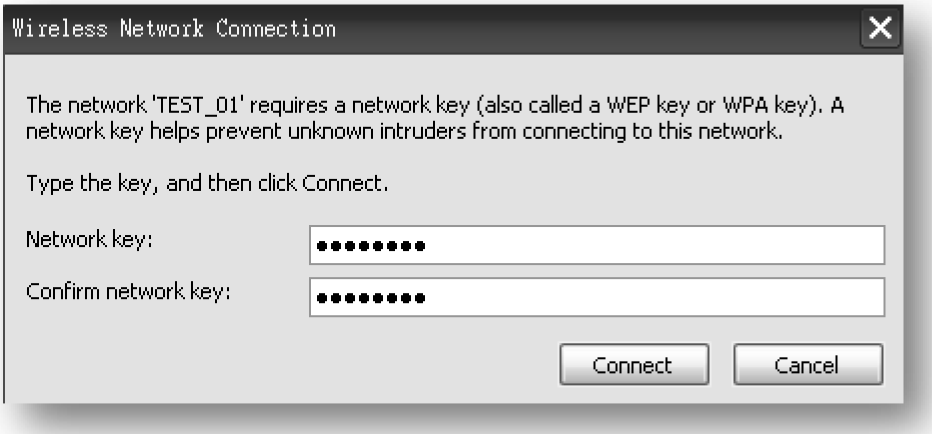
HCI
Unsecured wireless network

ZyXEL_MIS
Security-enabled wireless network

PQA-3274-02
Security-enabled wireless network (WPA2)

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Enter the WPA-PSK pre-shared key.

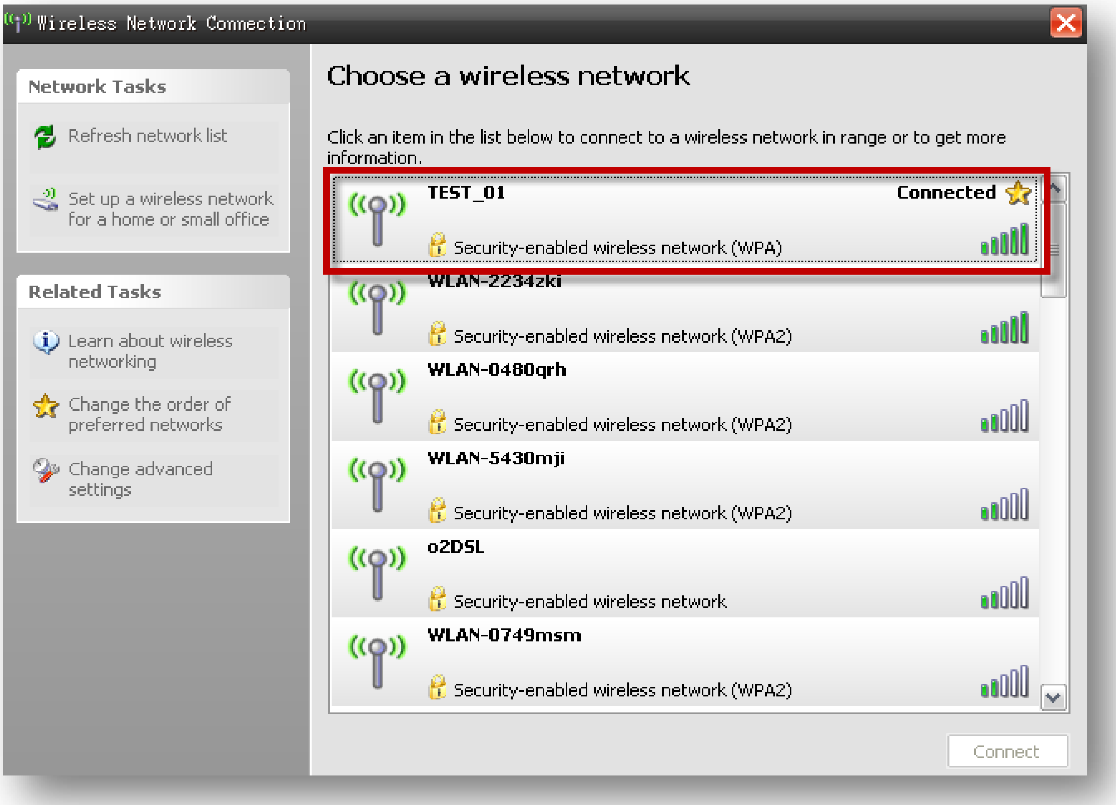


The network 'TEST_01' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

TEST_01 Connected ☆
Security-enabled wireless network (WPA)

WLAN-2234zki
Security-enabled wireless network (WPA2)

WLAN-0480qrh
Security-enabled wireless network (WPA2)

WLAN-5430mji
Security-enabled wireless network (WPA2)

o2DSL
Security-enabled wireless network

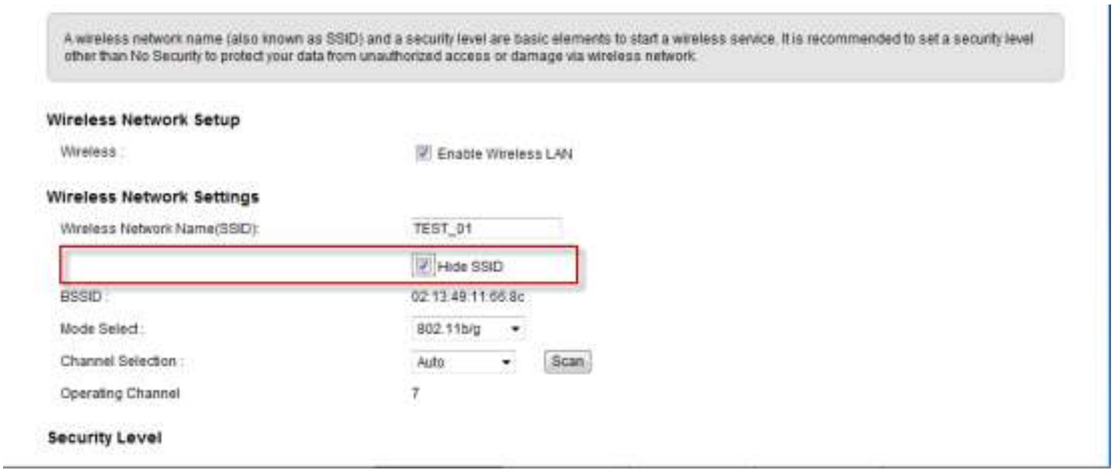
WLAN-0749msm
Security-enabled wireless network (WPA2)

We can see that the notebook is now connected to the WLAN interface of the P-2812HNU(L)-Fx.

b. Wireless Setup Hiding the SSID.

1. Go to **Network Setting > Wireless LAN > General**.
2. Check the **Enable Wireless LAN** box.
3. Enter the **Wireless Network Name (SSID)**, e.g. “TEST_01”.
4. Check the **Hide SSID** box

5. Select the **Security Mode**, e.g. “WPA2-PSK”.
6. Enter the **Pre-Shared Key**, e.g. “RKW7ENKNM49VW ”.
7. Click **Apply**.



A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless : ☑ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID): TEST_01

☑ Hide SSID

BSSID : 02:13:49:11:66:8c

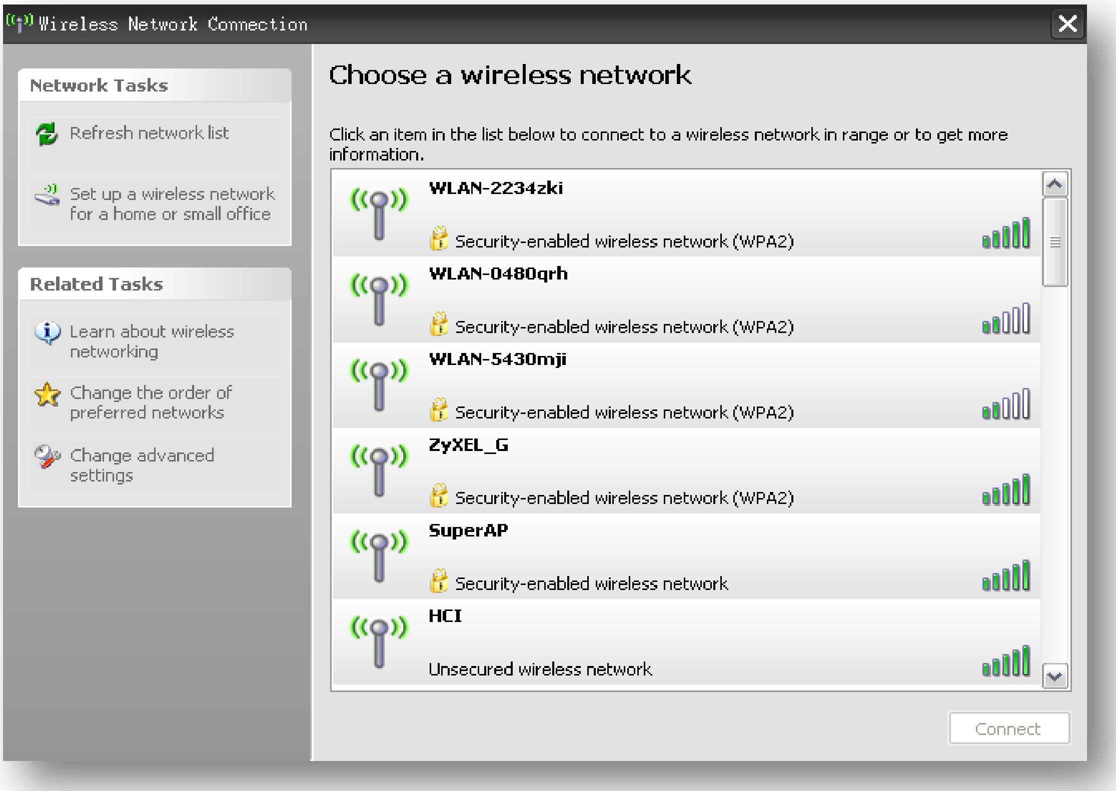
Mode Select : 802.11b/g

Channel Selection : Auto

Operating Channel 7

Security Level

View all the available wireless networks on your notebook:



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

WLAN-2234zki
Security-enabled wireless network (WPA2)

WLAN-0480qrh
Security-enabled wireless network (WPA2)

WLAN-5430mji
Security-enabled wireless network (WPA2)

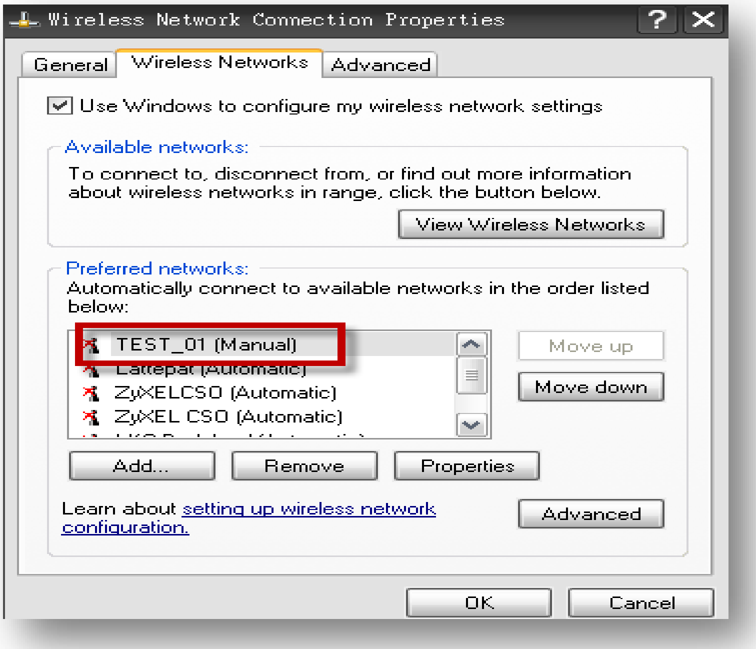
ZyXEL_G
Security-enabled wireless network (WPA2)

SuperAP
Security-enabled wireless network

HCI
Unsecured wireless network

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:



Wireless Network Connection Properties

General | Wireless Networks | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

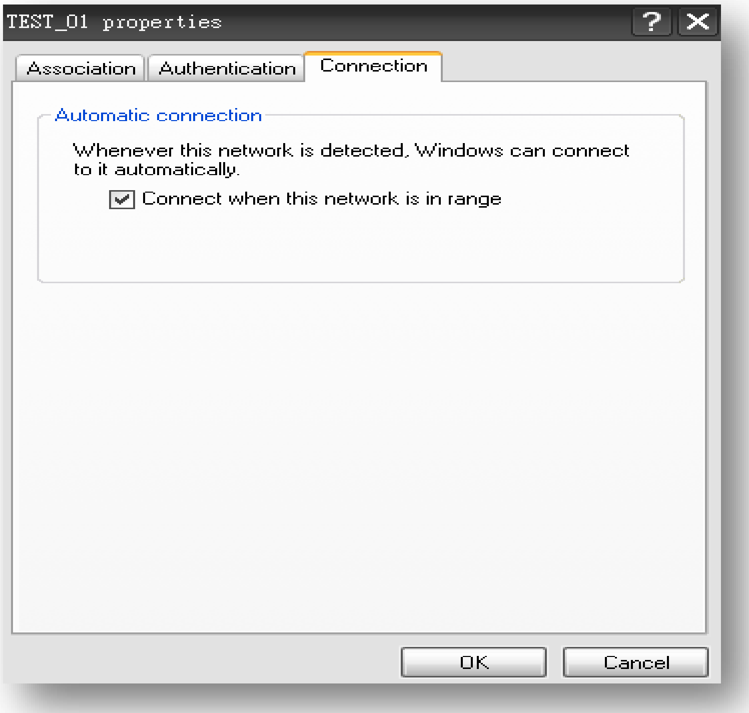
Preferred networks:

Automatically connect to available networks in the order listed below:

TEST_01 (Manual)
Lattepat (Automatic)
ZyXELCSO (Automatic)
ZyXEL CSO (Automatic)

Learn about setting up wireless network configuration.

Go to the “Connection” tab and check “Connect when this network is in range” checkbox.



TEST_01 properties

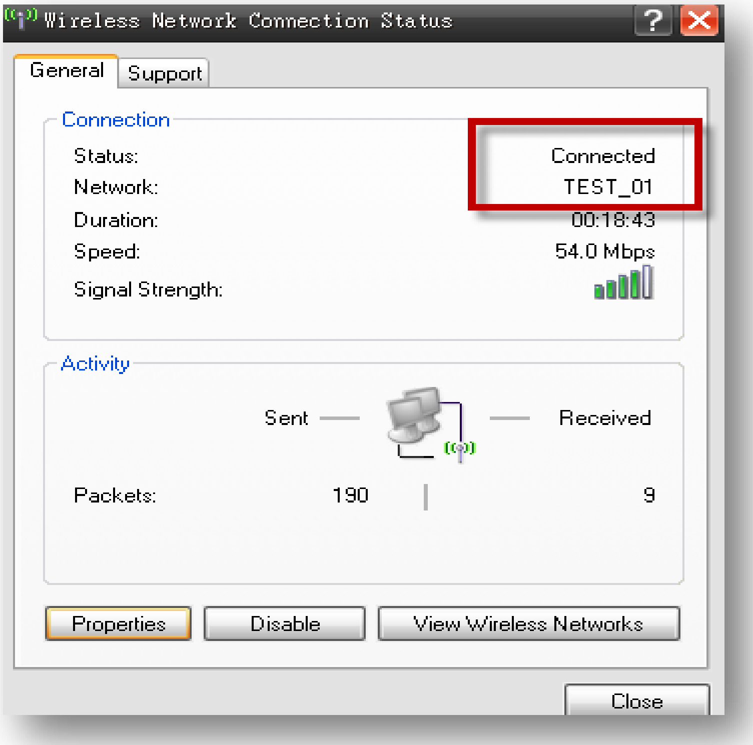
Association | Authentication | Connection

Automatic connection

Whenever this network is detected, Windows can connect to it automatically.

☑ Connect when this network is in range

We can then see the notebook connected to the “TEST_01”, even though the SSID is not displayed in the broadcast network list.



Connection

Status: Connected

Network: TEST_01

Duration: 00:18:43

Speed: 54.0 Mbps

Signal Strength:

Activity

	Sent	Received
Packets:	190	9

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**.

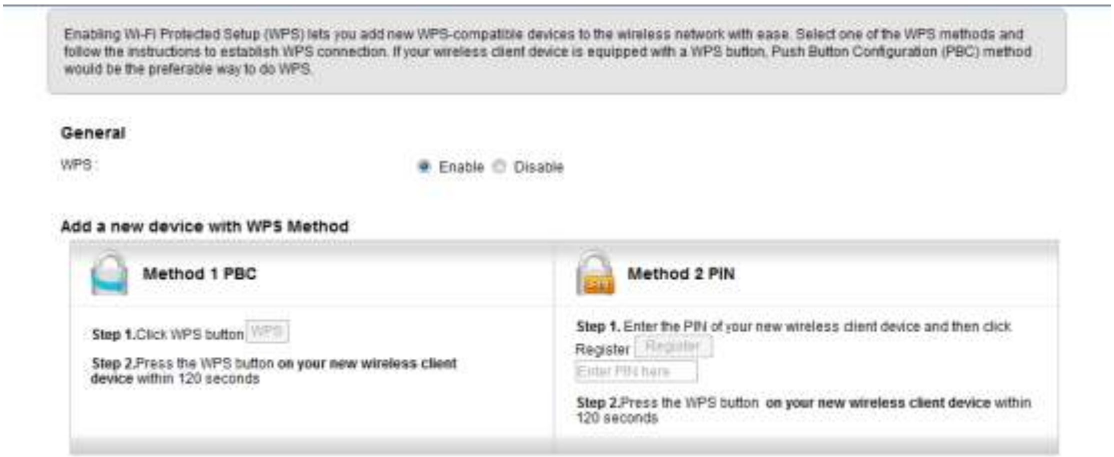
There are several different methods defined in WPS to simplify the process of configuration. P-2812HNU(L)-Fx supports two of those methods, which are the PIN Method and the PBC Method.

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 Setting** > **Wireless** > **WPS**.
    2. Check the "**Enable**" box for WPS.
    3. Click Apply.



Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General

WPS : ● Enable ○ Disable

Add a new device with WPS Method

Method 1 PBC

Step 1. Click WPS button

Step 2. Press the WPS button **on your new wireless client device** within 120 seconds

Method 2 PIN

Step 1. Enter the PIN of your new wireless client device and then click Register

Step 2. Press the WPS button **on your new wireless client device** within 120 seconds

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

Maintenance Log

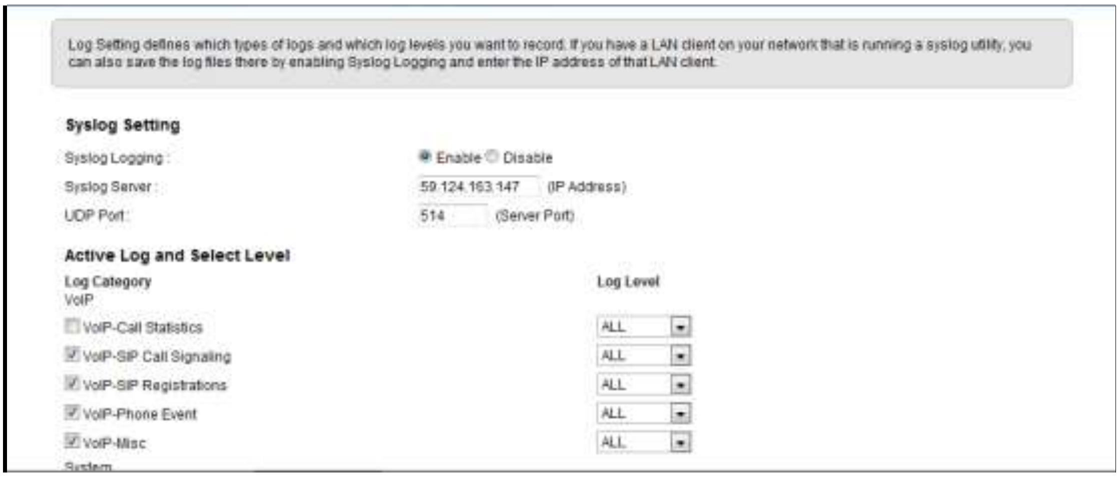
Internal Maintenance

The P-2812HNU(L)-Fx has the ability to record the events occurring in the CPE in a system log (according to the severity) and maintain this log in itself.

At this point, the P-2812HNU(L)-Fx only can logs VoIP service events.

a. Activate the Maintenance Log.

1. Go to **Maintenance** > **Log setting**.
2. Select “Enable” for **Syslog Logging**.
3. Insert the parameters, for example the syslog server address.
4. Select the logging conditions according to user’s needs.
5. Click “**Apply**”



Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging : ● Enable ○ Disable

Syslog Server : 59.124.163.147 (IP Address)

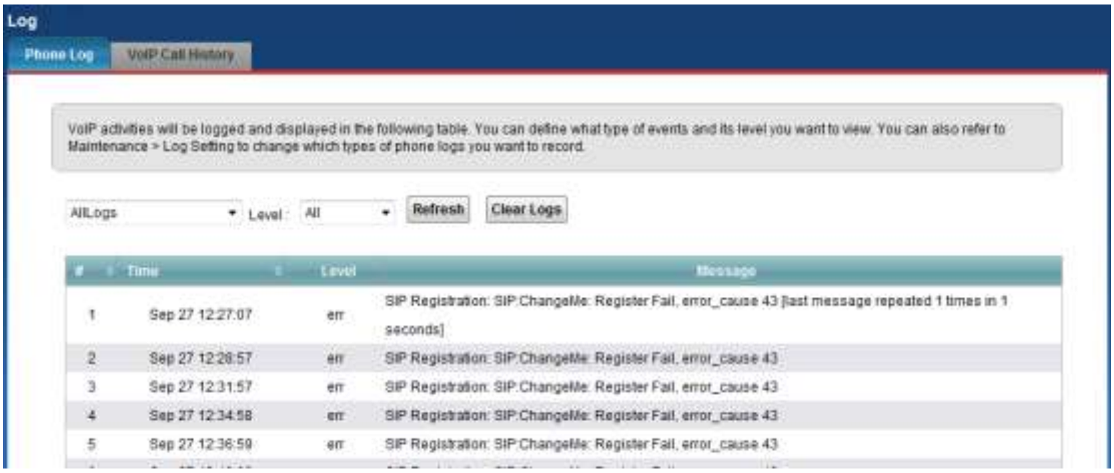
UDP Port : 514 (Server Port)

Active Log and Select Level

Log Category	Log Level
VoIP	
□ VoIP-Call Statistics	ALL
☑ VoIP-SIP Call Signaling	ALL
☑ VoIP-SIP Registrations	ALL
☑ VoIP-Phone Event	ALL
☑ VoIP-Misc	ALL
System	

b. View the log in the Web GUI.

1. Go to **System Monitor** > **Log**.



VoIP activities will be logged and displayed in the following table. You can define what type of events and its level you want to view. You can also refer to Maintenance > Log Setting to change which types of phone logs you want to record.

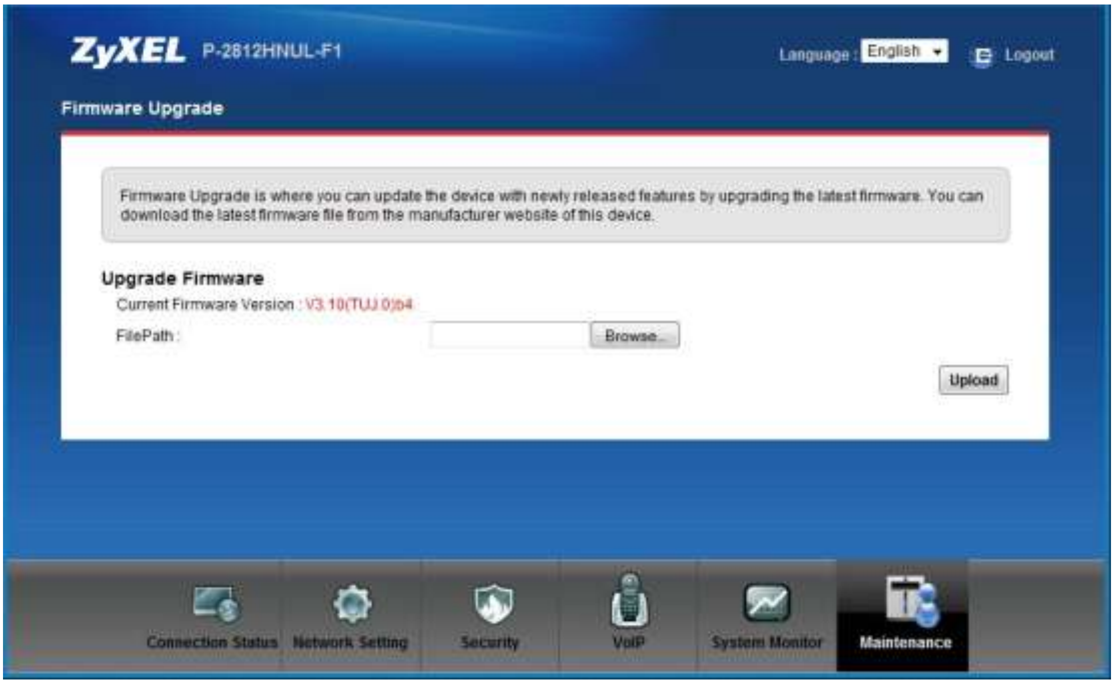
#	Time	Level	Message
1	Sep 27 12:27:07	err	SIP Registration: SIP:ChangeMe: Register Fail, error_cause 43 [last message repeated 1 times in 1 seconds]
2	Sep 27 12:28:57	err	SIP Registration: SIP:ChangeMe: Register Fail, error_cause 43
3	Sep 27 12:31:57	err	SIP Registration: SIP:ChangeMe: Register Fail, error_cause 43
4	Sep 27 12:34:58	err	SIP Registration: SIP:ChangeMe: Register Fail, error_cause 43
5	Sep 27 12:36:59	err	SIP Registration: SIP:ChangeMe: Register Fail, error_cause 43

Maintenance Tools

Maintenance Procedure

a. Upgrading Firmware.

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



Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

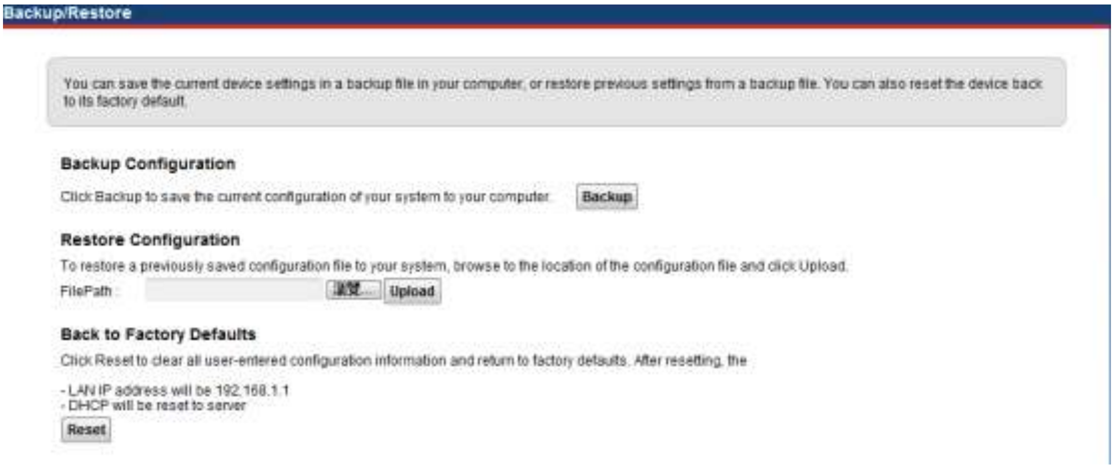
Current Firmware Version : V3.10(TUJ.0)b4

FilePath :

2. Click “**Browse**”.
3. Select the Firmware to upload and click “**Open**”.
4. Click “**Upload**”.

b. Backing-up the Configuration.

1. Go to **Maintenance** > **Backup/Restore**.



Backup/Restore

You can save the current device settings in a backup file in your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default.

Backup Configuration

Click Backup to save the current configuration of your system to your computer. [Backup]

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

FilePath : [Upload]

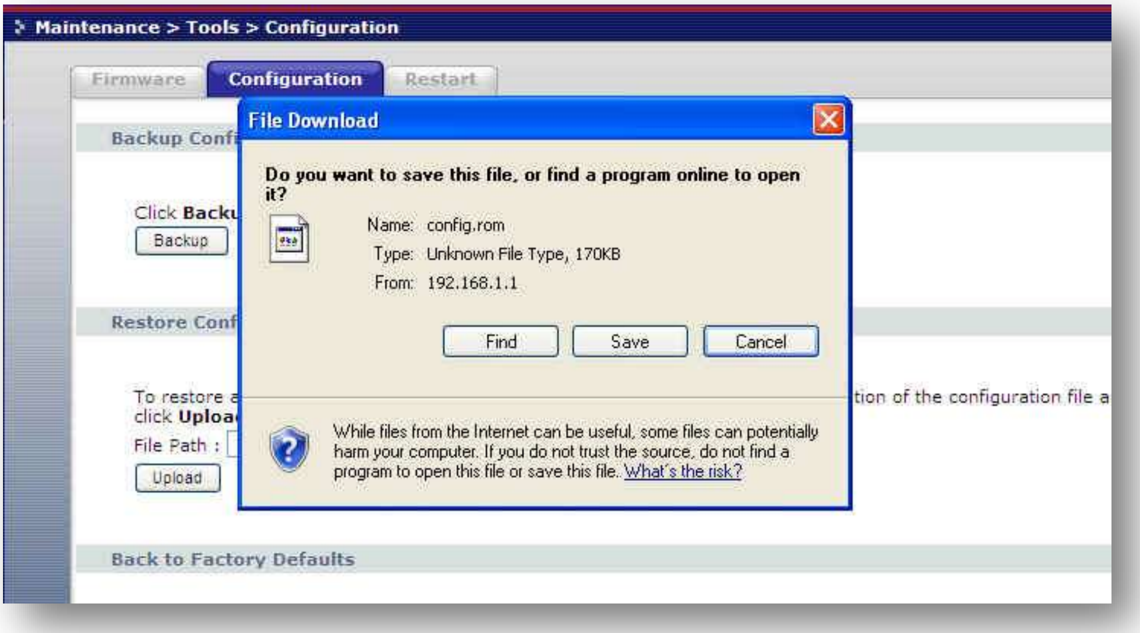
Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

[Reset]

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



Maintenance > Tools > Configuration

File Download

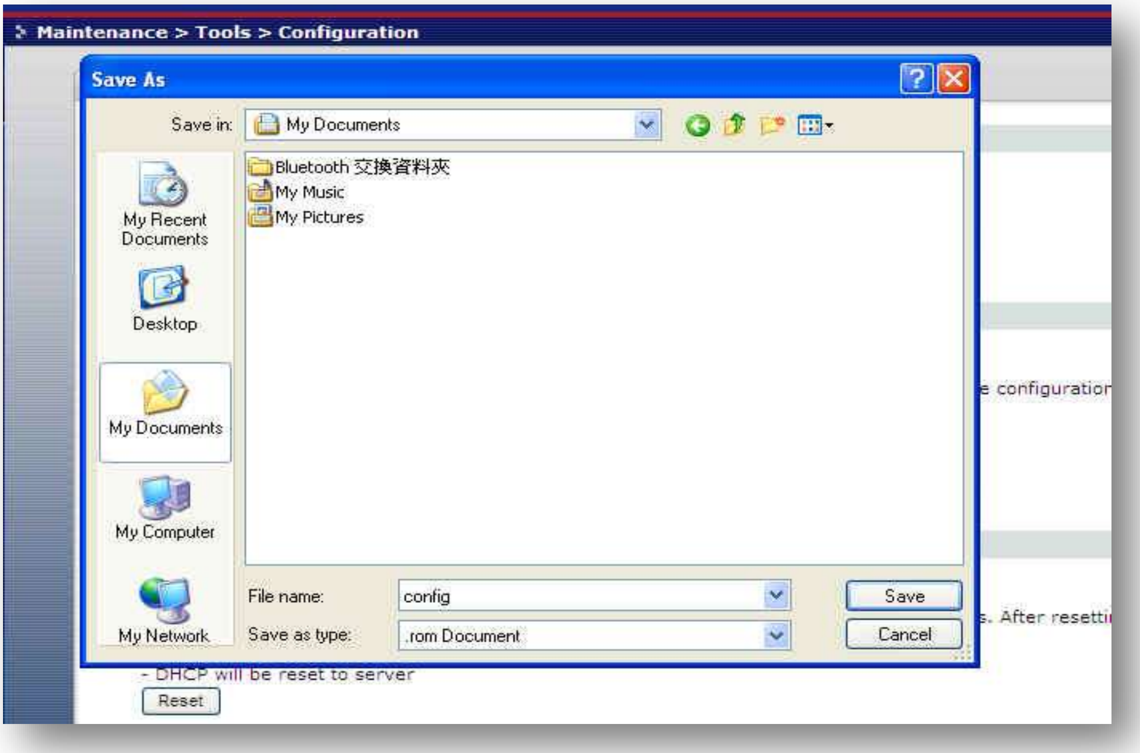
Do you want to save this file, or find a program online to open it?

Name: config.rom
Type: Unknown File Type, 170KB
From: 192.168.1.1

[Find] [Save] [Cancel]

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

4. Select the directory to save and click "**Save**".



Bluetooth 交換資料夾
My Music
My Pictures

File name: config
Save as type: .rom Document

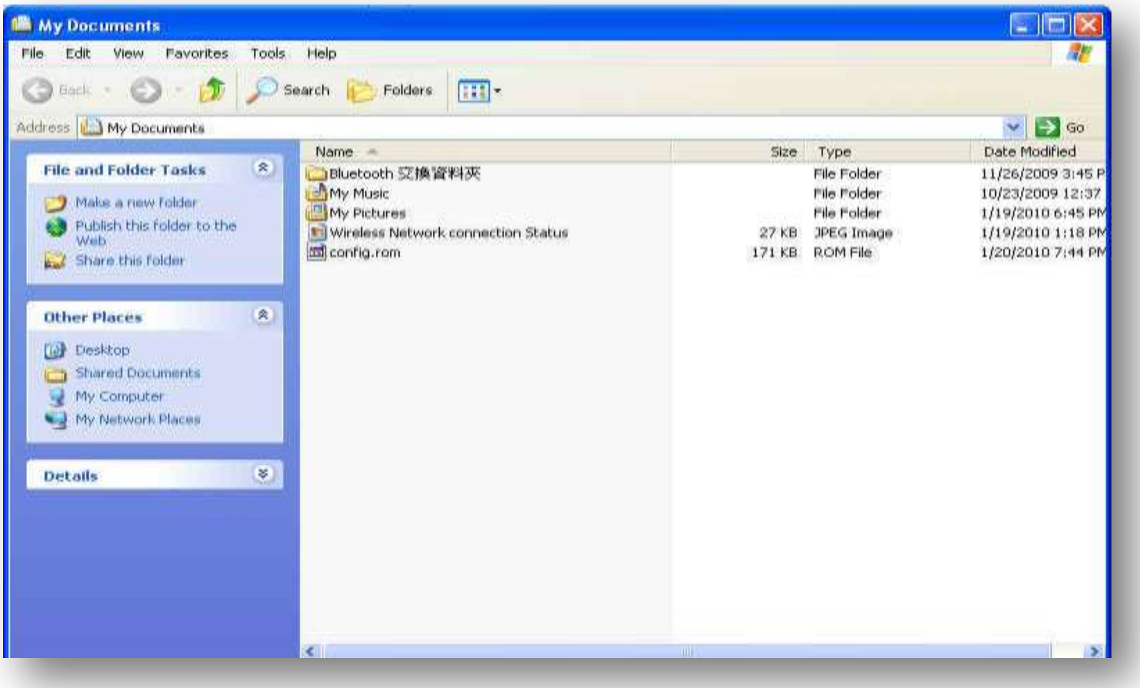
e configuration

s. After resetti

- DHCP will be reset to server

c. Upload Configuration.

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



Name	Size	Type	Date Modified
Bluetooth 交換資料夾		File Folder	11/26/2009 3:45 P
My Music		File Folder	10/23/2009 12:37
My Pictures		File Folder	1/19/2010 6:45 PM
Wireless Network connection Status	27 KB	JPEG Image	1/19/2010 1:18 PM
config.rom	171 KB	ROM File	1/20/2010 7:44 PM

Product FAQ

Will the device work with my Internet connection?

P-2812HNU(L)-Fx is designed to be compatible with major ISPs utilize ADSL as a broadband service. P-2812HNU(L)-Fx 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-2812HNU(L)-Fx?

You need an ADSL modem/router to use with ADSL line, P-2812HNU(L)-Fx is an ideal device for such application. The device has 4 Ethernet ports (LAN ports) and one ADSL WAN port. You should connect the computer to the LAN port and connect the ADSL 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 **over 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 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.

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 uses 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 use a sharp pointed object insert it into the little reset button 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.

When do I need 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.

b. 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 cannot login to the same server simultaneously.

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 P-2812HNU(L)-Fx 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 P-2812HNU(L)-Fx.

When the ISP assigns the device (P-2812HNU(L)-Fx) 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 acts 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 utilize 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.

What is 802.11n?

802.11n supports frequency in both 2.4GHz and 5 GHz and its data rate from 54 Mbit/s up to 600 Mbit/s in theory; in the 802.11n Channel Doubling technology which can double the bandwidth from 20 MHz to 40 MHz and effectively doubles data rates and throughput. It adds MIMO feature, which using multiple transmission and reception antennas to allow higher raw rate, and resolve more information using a single antenna possibility. It also uses the “Alamouti coding” coding schemes to increase transmission range.

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 interfere. 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 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, e.g.: 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 receiver 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.

What is 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.

What is WPA2?

WPA2 (Wi-Fi Protected Access 2) which security is a higher level then WPA, cause it brings AES-base algorithm and CCMP in it and offers stronger encryption then WPA uses (TKIP). WPA2 encryption keys that are used for each client on the network are unique and specific to that client. Eventually, each packet which is sent over the air is encrypted with a unique key. The higher security is enhanced with the use of a new and unique encryption key because there is no key reuse.