USER MANUAL

X96 series

Broadband Residential Gateway

VDSL2 4-port Ethernet Bridge/Router
with optional 802.11b/g WLAN AP,
USB2.0 host or 2 VoIP ports

Table of Contents

1 Introduction

Congratulations on becoming the owner of the **DYX9667R series**, VDSL router. You will now be able to access the Internet using your high-speed DSL connection.

This User Guide will show you how to connect your **DYX9667R series** DSL Modem, and how to customize its configuration to get the most out of your new product.

Features{ XE "Device:Features" }

The list below contains the main features of the device (**DYX9667R**) and may be useful to users with knowledge of networking protocols. The chapters throughout this guide will provide you with enough information to get the most out of your device.

The features include:

- High Speed Data Transmission on Twisted Copper Pair Wire
- Service providers can deploy VDSL rapidly over existing wire infrastructure (POTS line)
- Support mandatory and optional features of VDSL2 (G.993.2) standard
- Support VDSL2 profiles, 8a/8b/8c/8d, 12a/12b, 17a and 30a
- Support the speed of downstream or upstream up to 100Mbps
- Support bridge and router mode
- Interchangeable between Bridge and Router mode
- Network address translation (NAT) functions to provide security for your LAN and multiple PCs surfing Internet simultaneously.
- Network configuration through DHCP Server and DHCP Client
- Services including IP route, QoS and UPnP
- Built-in four-port 10/100BaseTX Ethernet switch for PC or LAN connection
- 802.11b/g WLAN supports up to 54Mbps (for model with wireless interface only)
- Provides Allow/Deny Wireless MAC address list for wireless access control (for model with wireless interface only)
- 64 and 128-bit WEP key lengths are supported (for model with wireless interface only)
- Supports Wi-Fi WPA and WPA2 in PSK mode (for model with wireless interface only)
- Supports 2 FXS ports with SIP protocol for VoIP application including call waiting, call forward, call transfer and so on (for model with VoIP port only)
- Supports USB host interface for connecting USB storage devices (for model with USB host interface only)
- Configuration and management with Telnet through the Ethernet interface, and remote Telnet through VDSL interface
- Firmware upgradeable through HTTP
- User-friendly configuration program accessed via a web browser

Device Requirements{ XE "Device:Requirements" }

In order to use the **DYX9667R series**, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your ISP on what type of Internet access you will be using, and the addresses needed to set up access

- One or more computers, each containing an Ethernet card (10Base-T/100Base-T network interface card (NIC)).
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v4 or later, or Netscape v4 or later. Note that version 4 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v5, or Netscape v6.1

Note

You do not need to use a hub or switch in order to connect more than one Ethernet PC to the device. Instead, you can connect up to four Ethernet PCs directly to the device using the ports labeled LAN1 to LAN4 on the rear panel.

2 Getting to know the device

Parts Check{ XE "Device:Parts check" }

In addition to this document, your package should arrive containing the following:

- ***The device (one of DYX9667R series)***
- ***Ethernet cable***
- ***USB cable (for X9627r-XXX and X9667r-XXX only)***
- ***Standard phone/DSL line cable***
- ***Power adapter***
- ***User Manual CD***

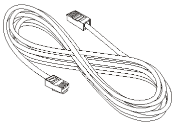
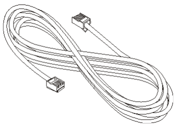
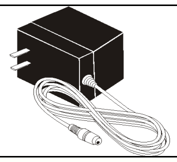
	One of **DYX9667R series** devices (please refer chapter 1 for the mapping between model and interfaces)
	RJ-45 Ethernet Cable
	RJ-11 Phone Cable
	Power adapter
	User's Manual CD

Figure 1: DSL Modem Package Contents

DYX9667R Front Panel

{ XE "Front panel" **}**The front panel of this **DYX9667R** will be described here which cover all front panel definitions of other models. Please refer Chapter 1 for the mapping between model and interfaces.

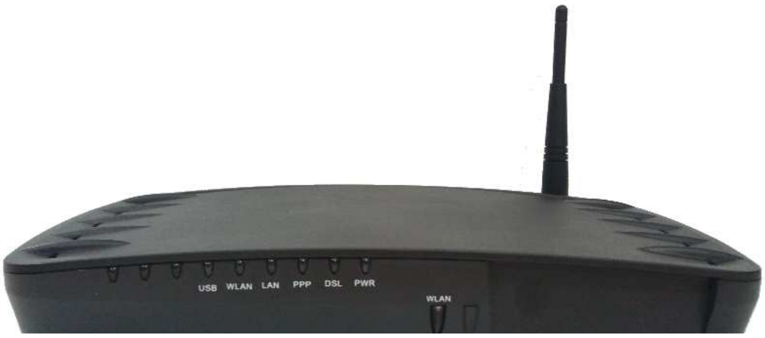


Figure 2: DYX9667R Front Panel and LEDs

Connector and LED definitions from right to left:

Label	Color	Function
WLAN button	N/A	Push this button to start the WiFi Protected Setup for easy configuration of wireless security and connection
PWR	Green/ Red	Red Blink: Only occur when you open the modem, it will become green after 5s. Green On: device is powered on Red On: boot fail
DSL	Green	On: DSL link reaches showtime, which means that your device has successfully connected to your ISP's DSL network. Off: DSL link not in showtime, your device has not successfully connected to your ISP's DSL network. Blink: Try to connect to ISP's DSL network
PPP	Green/ Red	Green On: establish a PPP connection Red On: PPP disconnection
LAN	Green	On: LAN link established and active Off: No LAN link Blink: Data being transmitted
WLAN	Green	On: WLAN service is enabled Off: WLAN service is disabled
USB	Green	On: make or receive a phone call Off: disconnect the phone call Blink: incoming call (ringing)

DYX9667R Rear Panel

{ XE "Front panel" **}**The rear panel of this **DYX9667R** will be described here which cover all rear panel definitions of other models. Please refer Chapter 1 for the mapping between model and interfaces.

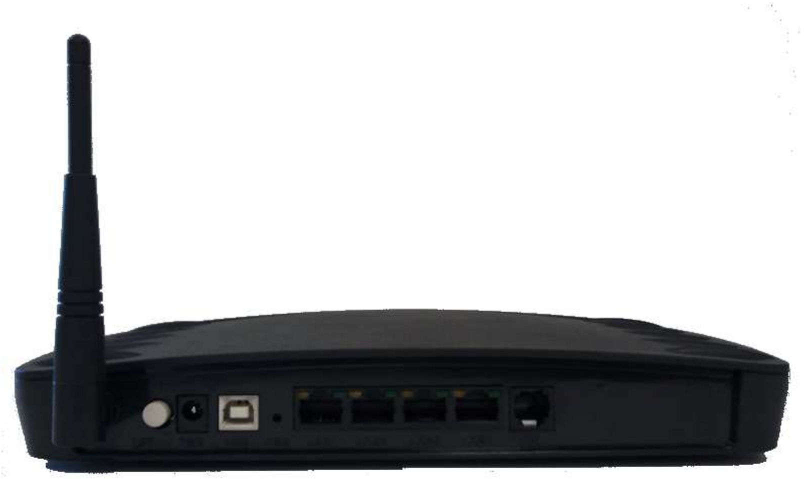


Figure 3: DYX9667R Rear Panel Connections

Connector definition:

Label	**Function**
Antenna	Connects to the 802.11b/11g enabled wireless devices in LAN
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
USB port (slave)	Connects the device via USB cable to your PC
RES	A reset button to reset the device or reset to default settings
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
DSL Jack	Connects to the ISP's DSL network

3 Connecting your device { XE "Device:Connecting" }

This chapter provides basic instructions for connecting the device to a computer or LAN and to the Internet.

In addition to configuring the device, you need to configure the Internet properties of your computer(s). For more details, see the following sections in Appendix A:

Configuring Ethernet PCs section

Configuring Wireless PCs section

Configuring USB PCs section

This chapter assumes that you have already established a DSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Connecting the Hardware{ XE "Hardware connections" }

This section describes how to connect the device to the power outlet and your computer(s) or network.

WARNING

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the device.*

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

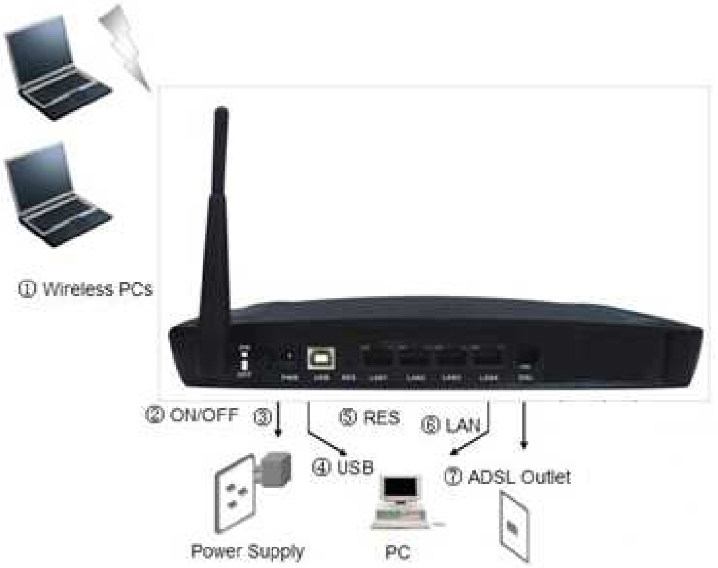


Figure 4: Overview of Hardware Connections for DYX9667R{ XE "Hardware connections" }

Step 1. Connect the DSL cable and optional telephone line

Connect one end of the provided phone cable to the port labeled DSL on the rear panel of the device. Connect the other end to DSL outlet.

Step 2. Connect the Ethernet cable

Connect up to four single Ethernet computers or to a HUB/Switch directly to the device via Ethernet cable(s).

Note that the cables do not need to be crossover cables, the switch provides MDI and MDIX auto-detection.

Step 3. Attach the power connector

Connect the AC power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 4. Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. See Configuring Ethernet PCs section.

Or, step 5. Install a Wireless card and connect Wireless PCs if the VDSL device is with wireless interface

You can attach a Wireless LAN that enables Wireless PCs to access the Internet via the device.

You must configure your Wireless computer(s) in order to access your device. For complete instructions, see Configuring Wireless PCs section.

Next step

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in “Getting Started with the Web pages” on chapter 4. The chapter includes a section called Testing your Setup, which enables you to verify that the device is working properly.

4 Getting Start with the Web pages{ XE "Web pages:Getting started" }

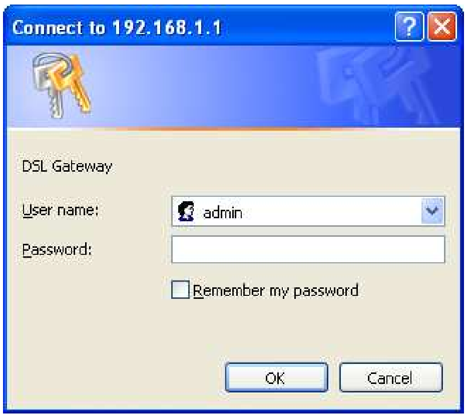
The DSL Modem includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through a web browser on a PC connected to the device.

Accessing the Web pages{ XE "Web pages:Accessing" }

To access the web pages, you need the following:

A laptop or PC connected to the LAN or WLAN port on the device.

A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox from any of the LAN computers, launch your web browser, type the URL, http://192.168.1.1 in the web address (or location) box, and press [Enter]. The default IP address of the device is 192.168.1.1. Then enter the default username and password: admin/admin to access the configuration web page, if you have not changed the username and password.



Connect to 192.168.1.1

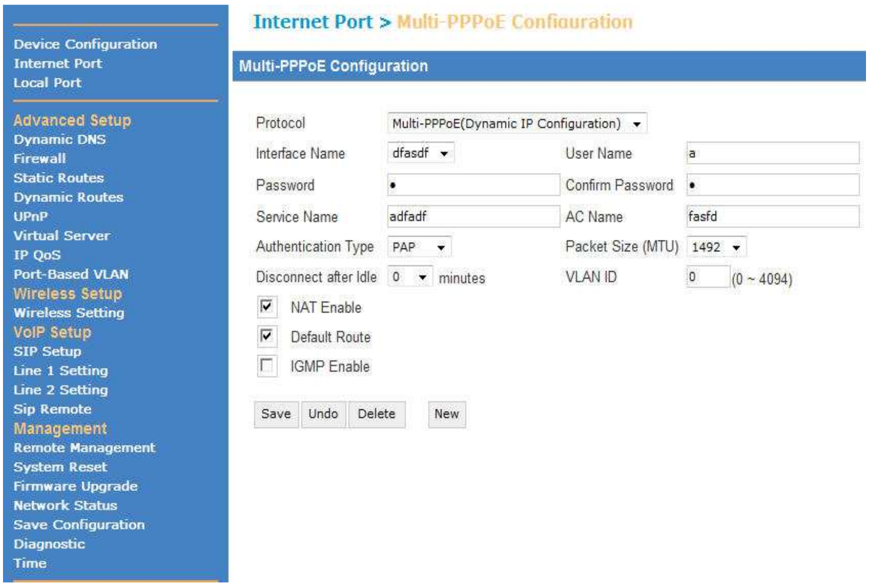
DSL Gateway

User name: admin

Password:

□ Remember my password

The home page opens displaying the Internet Port Configuration page of device:



Internet Port > Multi-PPPoE Configuration

Multi-PPPoE Configuration

Protocol	Multi-PPPoE(Dynamic IP Configuration)		
Interface Name	dfasdf	User Name	a
Password	•	Confirm Password	•
Service Name	adfadf	AC Name	fasfd
Authentication Type	PAP	Packet Size (MTU)	1492
Disconnect after Idle	0 minutes	VLAN ID	0 (0 ~ 4094)

☑ NAT Enable

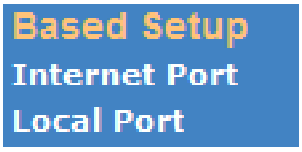
☑ Default Route

☐ IGMP Enable

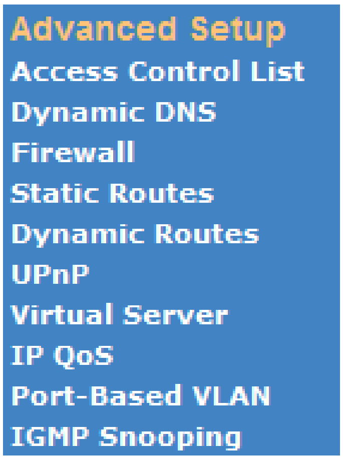
Figure 5: Home – Internet Port Configuration

The Menu comprises:

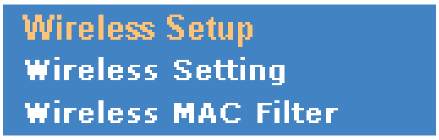
It provides the basic configuration of the system. It includes sub menus, Internet Port, Local Port. By default, the page of Internet Port is displayed after the login.



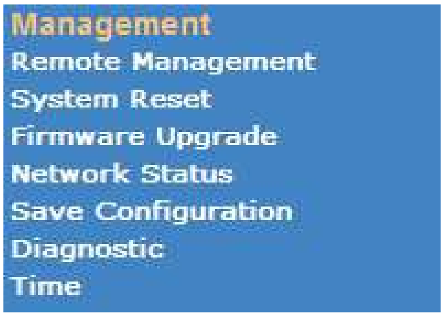
Advanced Setup: provides information about the current configuration of various system features with options to change the configuration. It includes the sub menus Access Control List, Dynamic DNS, Firewall, Static Routes, Dynamic Routes, UPnP, Virtual Server, IP QoS, and Port-Based VLAN and IGMP Snooping.



Wireless Setup: provides wireless SSID, security, key and various options to change the configuration. It includes the sub menu, Wireless Setting and Wireless MAC Filter.

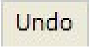
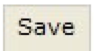


Management: provides the administration utilities such as Remote Management, System Reset, Firmware Upgrade, Network Status, Save Configuration, Diagnostic and Time Zone.



Commonly used buttons{ XE "Web page menu:Commonly used buttons" }

The following buttons are used throughout the web pages:

Button	Function
Refresh	You could click this button to refresh the information on this current page again so that you could get the real time information.
 Undo	This button appears on every configuration page. Click on this button if at any time you decide that you do not want to change the existing settings.
☑ Enable	check button – these appear on many configuration pages. You will be asked to check if you want this feature be selected.
 Save	This button appears on every configuration page. Click on this button once you are through with the changes and decide to save the made changes.
Browse...	You may need to browse to find a file which needs to be uploaded for new configuration.
Upgrade	This button allows you to upgrade to the new configuration file attached using the Browse button.

The following terms are used throughout this guide in association with these buttons:

Click – point the mouse arrow over the button, menu entry or link on the screen and click the left mouse button. This performs an action, such as displaying a new page or performing the action specific to the button on which left mouse button is clicked.

Select – usually is used when describing which radio button to select from a list, or which entry to select from a drop-down list. Point the mouse arrow over the entry and left-click to select it. This does not perform an action – you will also be required to click on a button, menu entry or link in order to proceed.

Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device’s DSL connection to access the Internet.

To test the connection, turn on the device, wait for 30 seconds and then verify that the LEDs are illuminated as follows:

LED	Behavior
Power (PWR)	Red Blinking when you first turn on the modem, it will become green after 5s. If it stays Red, this means there is a fault.
Wireless (WLAN)	Solid green to indicate that the Wireless LAN function is operational. (If Enabled)
LAN	Solid green to indicate that the device can

	communicate with your LAN. (If being used)
DSL	Flashing on/off while trying to SYNC UP with ISP. Solid green to indicate that the device has successfully established a line connection with your ISP.
PPP	Red to indicate there is no internet connection, Solid green to indicate that the device has successfully established a internet account connection with your ISP.

Table 1. LED Indicators

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as http://www.google.com).

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. If the LEDs still do not illuminate as expected or the web page is not displayed, see Troubleshooting section or contact your ISP for assistance.

Default device settings{ XE "Device:Default settings" }

{ XE "Default configuration" **}**In addition to handling the DSL connection to your ISP, the DSL Modem can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

WARNING

We strongly recommend that you contact your ISP prior to changing the default configuration.

Option	Default Setting	Explanation/Instructions
User/Password	admin/admin	User name and password to access the device
LAN Port IP Address **{** XE "Eth-0 interface:defined" **}**	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See *Local Network* section.

Option	Default Setting	Explanation/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.10 through 192.168.1.250 (Please be noted that the default DHCP IP address pool may be different in each firmware version.)	The device maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in *DHCP Server* section.

5 Basic Setup{ XE "Home page:Overview" }

The Basic Setup web page menu includes the following submenus:

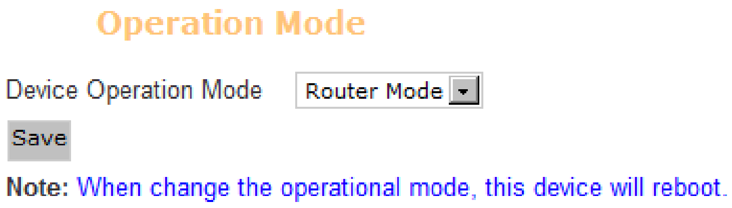
Operation Mode

Internet Port

Local Port

Device Configuration

The Operation Mode Page of the device allows you to configure the device to work as router or bridge.



Operation Mode

Device Operation Mode: Router Mode

Note: When change the operational mode, this device will reboot.

Figure 6: Operation Mode

To configure the *Operation Mode*:

- Select Router Mode or Bridge Mode from the list.

Internet Port

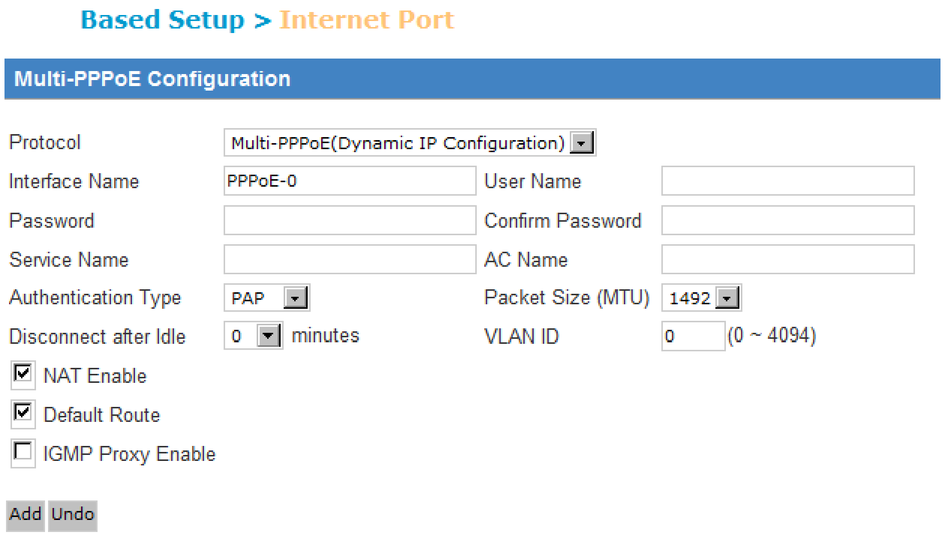
You can configure your internet connection from this page. This page displays the details of the existing internet connection, if any. This page contains all of options that could establish a connection to your Telco or ISP.

Before configuring the device, you should ask for the following information from your ISP:

- Connection Protocol: PPPoE (dynamic IP assignment), DHCP (dynamic IP assignment) or Static IP address from ISP.
- If the connection protocol is “fixed IP address”, need more information about subnet mask, default gateway, and DNS server.
- NAT: Disabled or Enabled
- Default Route: Disabled or Enabled
- IGMP: Disabled or Enabled
- PPP User Name and Password (also known as Broadband User Name and Password)

PPPoE connection

This web page allows you to configure the device to establish a connection through PPPoE protocol.



Based Setup > Internet Port

Multi-PPPoE Configuration

Protocol	Multi-PPPoE(Dynamic IP Configuration)		
Interface Name	PPPoE-0	User Name	
Password		Confirm Password	
Service Name		AC Name	
Authentication Type	PAP	Packet Size (MTU)	1492
Disconnect after Idle	0 minutes	VLAN ID	0 (0 ~ 4094)

☑ NAT Enable

☑ Default Route

☐ IGMP Proxy Enable

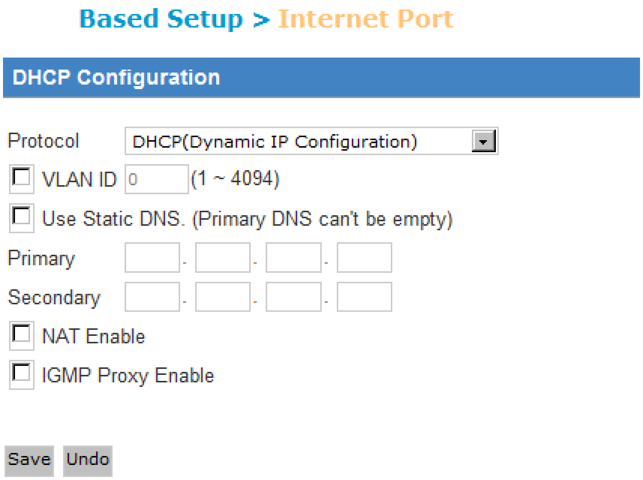
Figure 7: Internet Port – PPPoE (Dynamic IP assignment)

To configure the PPPoE settings:

- Select the Multiple-PPPoE (Dynamic IP Configuration) to be used as *Protocol*.
- Enter name in the *Interface Name*
- Enter the *username* and *password* provided from your Telco or ISP and enter the password again in the *Confirm Password* field again to double check the password.
- Enter name in the *Service Name* and *AC Name*.
- Select the *Authentication Type*, PAP or CHAP
- Select the *Packet Size (MTU)* from the list
- Select the minutes from *Disconnect after Idle minutes* to disconnect the PPPoE connection if there is no traffic for that minutes.
- Enter the *VLAN ID* if the traffic is tagged with VLAN ID.
- Click to *Enable NAT*.
- Click to *Add Default Route*
- Click to *Enable IGMP* if need
- Click *Add* and then click *Save* to save the configuration, otherwise click *New* to configure it again.

DHCP (Dynamic IP Configuration)

This web page allows you to configure the device to establish a connection through DHCP client protocol. The Dynamic IP Configuration means “get an IP address automatically”.



Based Setup > Internet Port

DHCP Configuration

Protocol: DHCP(Dynamic IP Configuration)

□ VLAN ID 0 (1 ~ 4094)

□ Use Static DNS. (Primary DNS can't be empty)

Primary: ___ . ___ . ___ . ___

Secondary: ___ . ___ . ___ . ___

□ NAT Enable

□ IGMP Proxy Enable

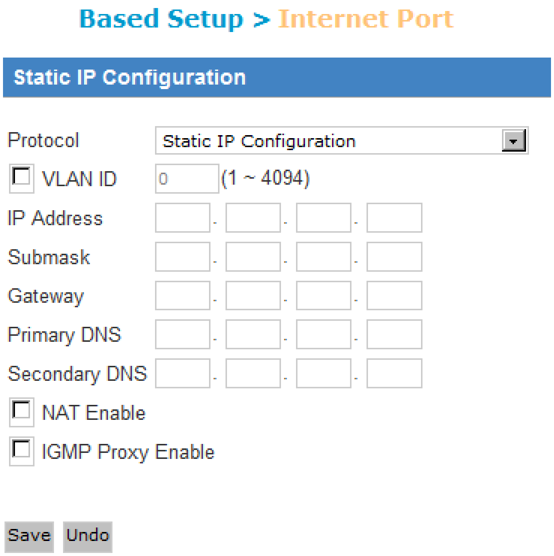
Figure 8: Internet Port - DHCP (Dynamic IP Configuration)

To configure the DHCP (Dynamic IP Configuration) settings:

- Select the DHCP (Dynamic IP Configuration) to be used as *Protocol*.
- Enter the *VLAN ID* if the traffic is tagged with VLAN ID.
- Click to *use Static DNS* (Domain Name Server) and then enter the IP addresses of *Primary DNS* and *Secondary DNS*. Usually, the information of DNS sever will be given from DHCP server in ISP site.
- Click to *enable NAT* if need
- Click to *enable IGMP* if need
- Click *Save* to save the configuration

Static IP Configuration

This web page allows you to set the fixed IP address in the Internet (WAN) port.



Based Setup > Internet Port

Static IP Configuration

Protocol: Static IP Configuration

□ VLAN ID 0 (1 ~ 4094)

IP Address . . .

Submask . . .

Gateway . . .

Primary DNS . . .

Secondary DNS . . .

□ NAT Enable

□ IGMP Proxy Enable

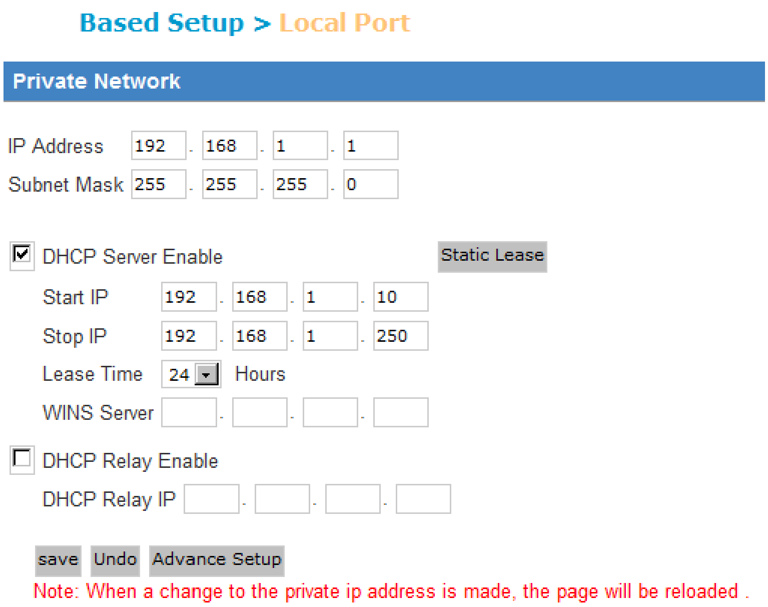
Figure 9: Internet Port – Static IP Configuration

To configure the Static IP settings:

- Select the Static IP Configuration to be used as *Protocol*.
- Enter the *VLAN ID* if the traffic is tagged with VLAN ID.
- Enter the IP address, Submask, Gateway, Primary DNS address and Secondary DNS address.
- Click to *enable NAT* if needed
- Click to *enable IGMP* if needed
- Click *Save* to save the configuration

Local Port

This page allows you to setup the Local Network (LAN) connection.



Based Setup > Local Port

Private Network

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

☑ DHCP Server Enable

Start IP 192 . 168 . 1 . 10

Stop IP 192 . 168 . 1 . 250

Lease Time 24 Hours

WINS Server . . .

□ DHCP Relay Enable

DHCP Relay IP . . .

Note: When a change to the private ip address is made, the page will be reloaded .

Figure 10: Local Port Configuration

To configure the Local Port settings:

- Enter the device *IP address*.
- Enter the *Subnet Mask* : The subnet mask determines the number of computers are allowed in this network. Usually a class (255.255.255.0) is satisfactory for a local network.
- Click to enable *DHCP server* to assign IP addresses to the client.
- Enter the *start of the IP address* for DHCP client users. The default value is 192.168.1.10. Please make sure there is no fixed IP address within the rage of DHCP IP pool, otherwise the DHCP client may not get the IP address correctly.
- Enter the number of IP addresses (users) allowed to use the DHCP service.
- Select the *lease time*. A DHCP client gets the IP address with a lease time. When the lease time is expired, the client must connect to the DHCP server to request the dynamic IP address again.
- Enter the IP address of WINS (Windows Internet Naming Service). The WINS provides a distributed database for registering and querying dynamic computer name-to-IP address in a routed network environment. It means WINS provides easy configuration and administration of Windows-based TCP/IP networks. If you do not use WINS server, leave it as blank.
- Click to enable *DHCP RELAY Enable* to setup the DHCP RELAY function.
- Click *Save* to save the configuration

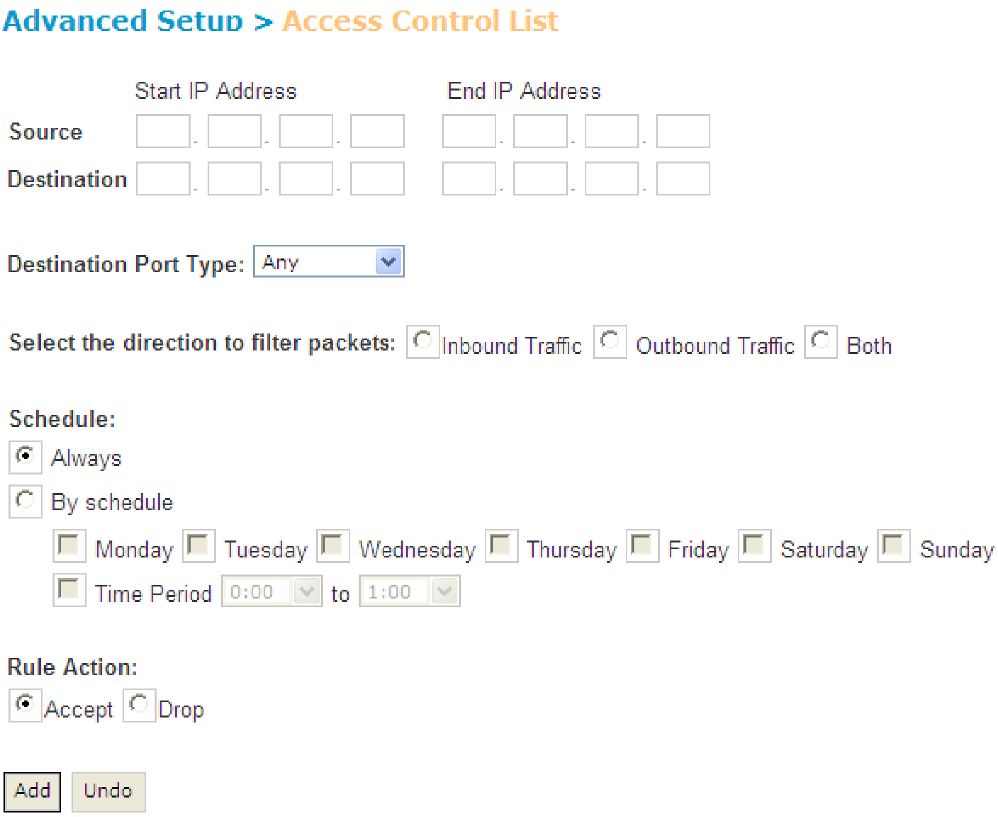
6 Advanced Setup

The Configuration web page menu comprises:

Access Control List
Dynamic DNS
Firewall
Static Routes
Dynamic Routes
UPnP
Virtual Server
IP QoS
Port-Based VLAN
IGMP Snooping

Access Control List{ XE "Configuring:Quick setup" }

This menu provides the Access Control List to control the Date/Time/ IP of the incoming Client.



Advanced Setup > Access Control List

	Start IP Address	End IP Address
Source	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Destination	___ . ___ . ___ . ___	___ . ___ . ___ . ___

Destination Port Type: Any

Select the direction to filter packets: ○ Inbound Traffic ○ Outbound Traffic ○ Both

Schedule:

● Always

○ By schedule

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

□ Time Period 0:00 to 1:00

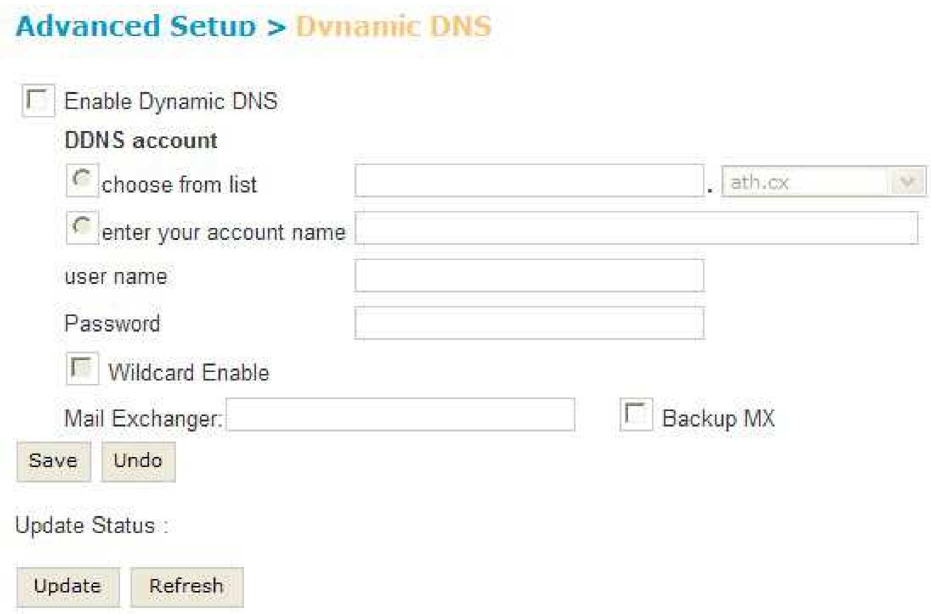
Rule Action:

● Accept ○ Drop

Figure 11: Access Control Configuration

Dynamic DNS{ XE "Configuring:Quick setup" }

The device provides Dynamic Domain Name System (DDNS) feature. The DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server and other server applications behind the device. Before you can use this feature, you need to sign up for DDNS service from the DDNS service provider like dyndns.org (refer to www.dyndns.org).



Advanced Setup > Dynamic DNS

□ Enable Dynamic DNS

DDNS account

○ choose from list . ath.cx

○ enter your account name

user name

Password

□ Wildcard Enable

Mail Exchanger: □ Backup MX

Update Status :

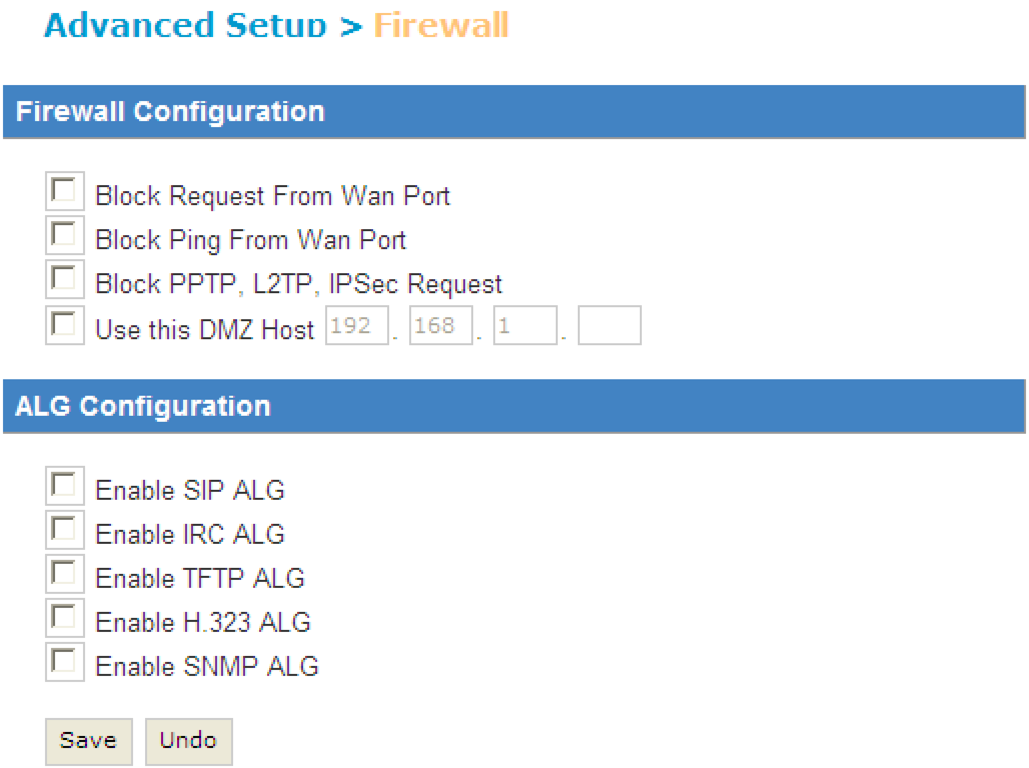
Figure 11: Dynamic DNS Configuration

To configure the Dynamic DNS (DDNS) page:

- Click to enable *Dynamic DNS* feature
- Enter your registered *account name* (host name) and select the *DDNS service provider* from the pull down list if you find your DDNS service provider from the list.
- Enter your *account name* (full registered host name) if your DDNS service provider is not supported in the above pull down list.
- Enter your *username* and *password* for login which you register the account name in the DDNS service provider.
- Click to enable *Wildcard*. If you like to have an unregistered hostname followed by the registered hostname and domain name to work as well.
- Click to *enable the Mail Exchanger*. If you like that others send emails to your DDNS name will be redirected to the mail server you specified in the *Mail Exchanger* field.
- Click to enable *Backup MX* if you need to back up the mail exchanger's address while you login the DDNS service provider every time.
- Click *Save* to save the configuration.
- Click *Update* to update the DDNS service or click *Refresh* to refresh display.

Firewall{ XE "Configuring:Quick setup" }

The device provides firewall feature to protect the device.



Advanced Setup > Firewall

Firewall Configuration

□ Block Request From Wan Port

□ Block Ping From Wan Port

□ Block PPTP, L2TP, IPSec Request

□ Use this DMZ Host 192 . 168 . 1 .

ALG Configuration

□ Enable SIP ALG

□ Enable IRC ALG

□ Enable TFTP ALG

□ Enable H.323 ALG

□ Enable SNMP ALG

Figure 12: Firewall Configuration

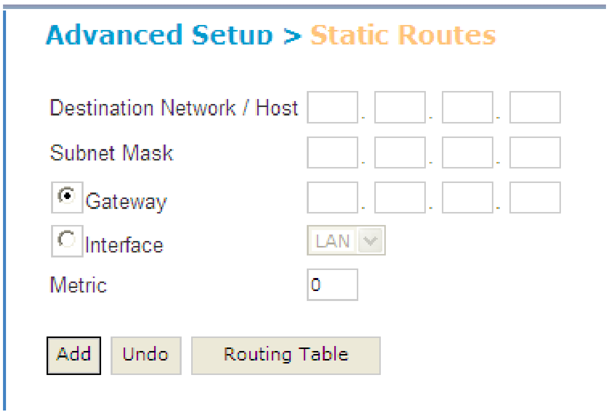
Global Setting

- Check to enable "*Block Request From Wan Port*"
- Check to enable "*Block Ping From Wan Port*"
- Check to enable "*Block PPTP, L2TP, IPSec Request*"
- Check to enable *DMZ* and enter the IP address of DMZ host
- Click *Save* to save the configuration

Besides, A DMZ (DeMilitarized Zone) host is a computer on your network that can be accessed from the Internet regardless of NAT, port forwarding and IP filter settings. A DMZ is often used to host Web servers, FTP servers etc that need to be accessible from the Internet.

Static Routes{ XE "Configuring:Quick setup" }

The device provides to add the routing rules manually.



Advanced Setup > Static Routes

Destination Network / Host

Subnet Mask

● Gateway

○ Interface LAN

Metric 0

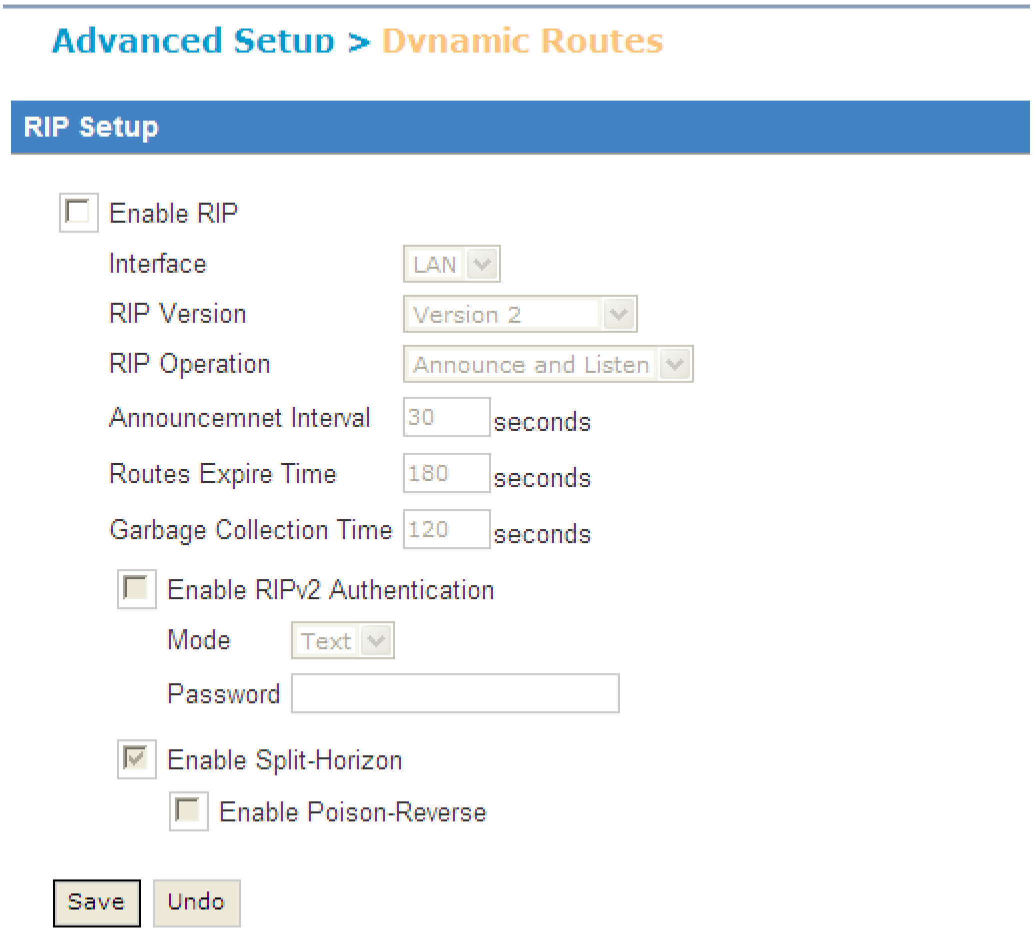
Figure 13: Static Routes Configuration

Global Setting

- Enter the IP address of *Destination Host/Network*
- Enter the *Subnet Mask* related the Destination Host/Network that packets to those IP addresses will be forwarded to the gateway.
- Enter the IP address of *Gateway*
- Enter the number of *Metric*
- Click *Add* to add this routing rule
- The added routing rule will be shown in the table. Click *Delete All* to remove all entries or click *Delete* to remove the specified entry.
- Click *Routing Table* to get the current routing table.

Dynamic Routes{ XE "Configuring:Quick setup" }

The device provides to set RIP, RIPv2 Authentication, Split-Horizon and Poison-Reverse.



Advanced Setup > Dynamic Routes

RIP Setup

□ Enable RIP

Interface: LAN

RIP Version: Version 2

RIP Operation: Announce and Listen

Announcemnet Interval: 30 seconds

Routes Expire Time: 180 seconds

Garbage Collection Time: 120 seconds

□ Enable RIPv2 Authentication

Mode: Text

Password:

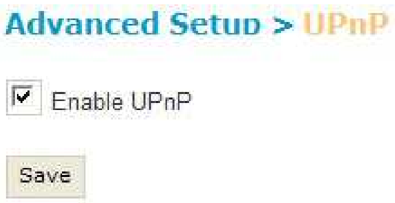
☑ Enable Split-Horizon

□ Enable Poison-Reverse

Figure 14: Dynamic Routes Configuration

UPnP{ XE "Configuring:Quick setup" }

The device provides UPnP feature..



Advanced Setup > UPnP

☑ Enable UPnP

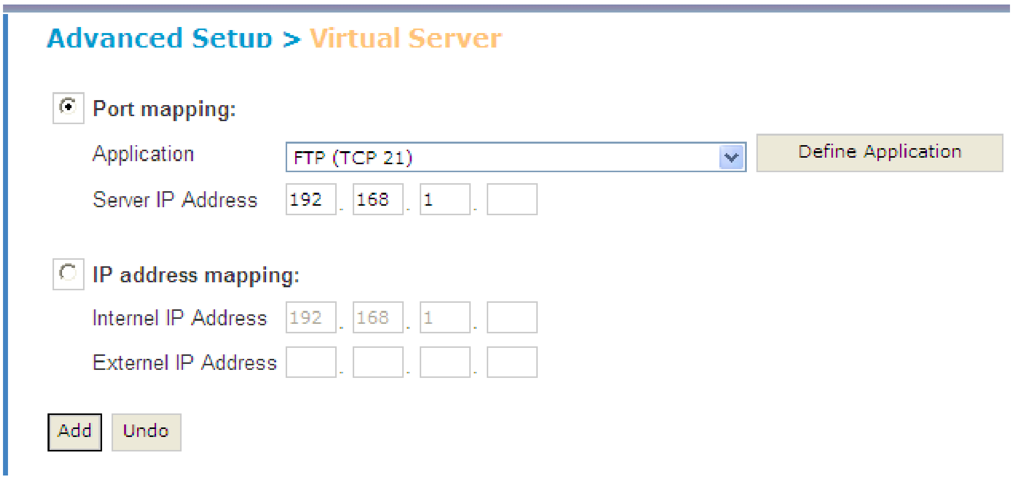
Figure 15: UPnP Configuration

Global Setting

- Check to enable "*UPnP*"
- Click *Save* to save the configuration

Virtual Server{ XE "Configuring:Quick setup" }

The device provides port mapping to local host for incoming packets. Virtual server enables you to run a server on your local network that can be accessed from the Internet. You need to set up port forwarding rule to tell the device on which computer the server is held. When port forwarding is enabled, your router (the device) routes all the inbound traffic on a particular port to the chosen computer on your network.



Advanced Setup > Virtual Server

● Port mapping:

Application: FTP (TCP 21) [Define Application]

Server IP Address: 192 . 168 . 1 .

○ IP address mapping:

Internel IP Address: 192 . 168 . 1 .

Externel IP Address: . . .

[Add] [Undo]

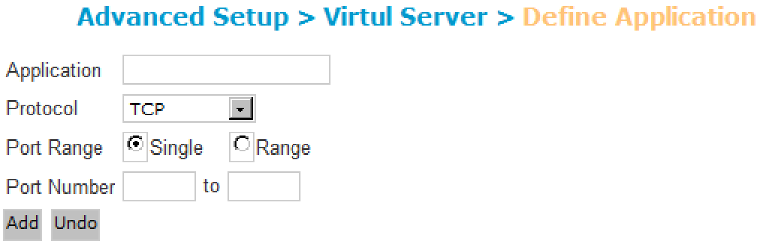
Figure 16: Virtual Server Configuration

Global Setting

- Select the *application (port)*. If it is not listed in default, click *Define Application* to add your own application as below figure.
- Enter the IP address of *Server IP Address* in your local network.
- Click *Add* to add this rule
- The added port forwarding rule will be shown in the table. Click *Delete All* to remove all added entries or click *Delete* to remove the specified entry.

To define the application

- Enter the *Application* name
- Select the *Protocol* (TCP, UDP, or ICMP) used by the application
- Check if you want to forward the *Single* port or a *Range* of ports
- Enter the *Port number (Range)* from start to end
- Click *Add* to add this application into the selection list



Advanced Setup > Virtul Server > Define Application

Application:

Protocol: TCP

Port Range: ● Single ○ Range

Port Number: to

[Add] [Undo]

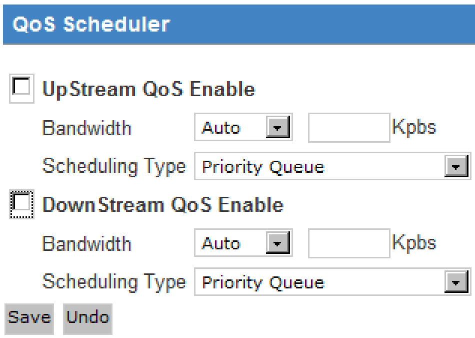
Figure 17: Virtual Server Configuration – Define Application

IP QoS{ XE "Configuring:Quick setup" }

The page provides to configure the four different priority queues (High, Middle, Low and Default) and provide bandwidths to them separately. Besides, setup the checking rules to determine the packets to each queue. That will help to provide better bandwidth efficiently and serve important packets like voice, email, FTP and so on in higher priority with more bandwidth.

QoS Scheduler

The page provides to enable upstream and/or downstream QoS and configure the four different priority queues (High, Middle, Low and Default) and provide bandwidths to them separately.



QoS Scheduler

□ UpStream QoS Enable

Bandwidth: Auto, Kpbs

Scheduling Type: Priority Queue

□ DownStream QoS Enable

Bandwidth: Auto, Kpbs

Scheduling Type: Priority Queue

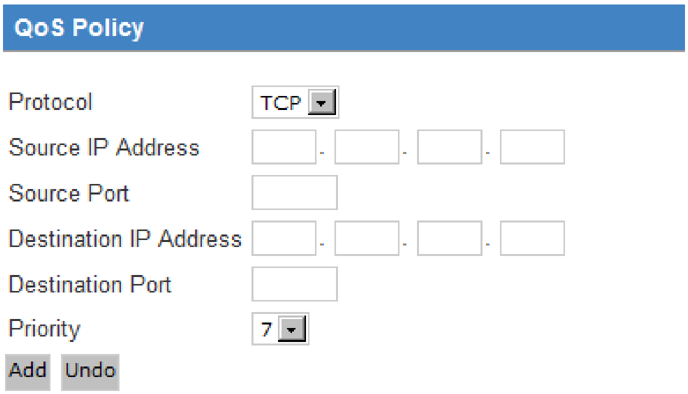
Figure 18: IP QoS – QoS Scheduler

Global Setting

- Check to *Enable Upstream* (packets from LAN to Internet) QoS.
- Select *Auto* in *Bandwidth* that the device will get the sync up upstream bandwidth and determine the bandwidth used for QoS. Select the *Manual* in the *Bandwidth* and then enter the bandwidth in Kbps used for QoS.
- Enter the *Priority Percentage* for *High*, *Medium*, and *Low* queues. The rest of percentage will be assigned to *Default* queue automatically.
- Check to *Enable Downstream* (packets from LAN to Internet) QoS.
- Select *Auto* in *Bandwidth* that the device will get the sync up downstream bandwidth and determine the bandwidth used for QoS. Select the *Manual* in the *Bandwidth* and then enter the bandwidth in Kbps used for QoS.
- Enter the *Priority Percentage* for *High*, *Medium*, and *Low* queues. The rest of percentage will be assigned to *Default* queue automatically.
- Click *Save* to save the configuration

QoS Policy

This page provides to setup the rule to check the packet and put it into the right priority queue.



QoS Policy

Protocol TCP

Source IP Address . . .

Source Port

Destination IP Address . . .

Destination Port

Priority 7

Figure 19: IP QoS – QoS Policy

Global Setting

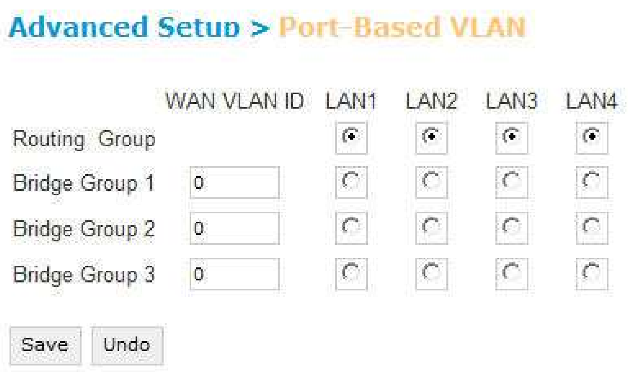
- Select the *Packet Type* (TCP or UDP).
- Enter the *Source IP Address* and/or *Port Number* if any.
- Enter the *Destination IP Address* and/or *Port Number* if any.
- Select the *Priority Queue* for this packet.
- Click *Add* to create this rule.

In the above figure, it shows the any packet with destination IP address, 192.168.1.100 and port number, 20 will be put into medium queue.

- Select the specified entry in the QoS policy table and click *Delete* to remove the rule.

Port-Based VLAN{ XE "Configuring:Quick setup" }

The page provides port-based VLAN configuration. In default, the LAN1 to LAN4 are grouped together as a single Ethernet environment. But you could enable VLAN feature and get up to 4 separated Ethernet environments. Besides, each VLAN can associate with VLAN ID in the Internet (WAN) port. Those packets does not match the VLAN ID in below figure will be sent to default group (Routing Group).



Advanced Setup > Port-Based VLAN

	WAN VLAN ID	LAN1	LAN2	LAN3	LAN4
Routing Group		●	●	●	●
Bridge Group 1	0	○	○	○	○
Bridge Group 2	0	○	○	○	○
Bridge Group 3	0	○	○	○	○

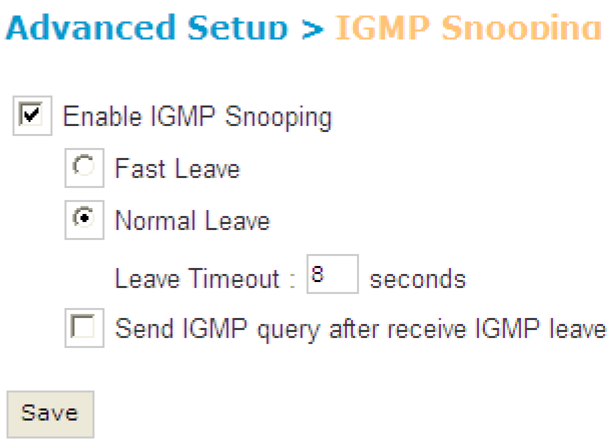
Figure 20: Port-Based VLAN Configuration

Global Setting

- Enter the value of *WAN VLAN ID* in Bridge Group 1, 2 and 3
- Select the *LAN ports* from LAN1 to LAN4 for each Bridge Group.
- Click *Save* to save the configuration.

IGMP SNOOPING { XE "Configuring:Quick setup" }

The device provide the IGMP SNOOPING function to Prevent the multicast packets flood to other port.



Advanced Setup > IGMP Snooping

☑ Enable IGMP Snooping

○ Fast Leave

● Normal Leave

Leave Timeout : 8 seconds

□ Send IGMP query after receive IGMP leave

7 Wireless Setup

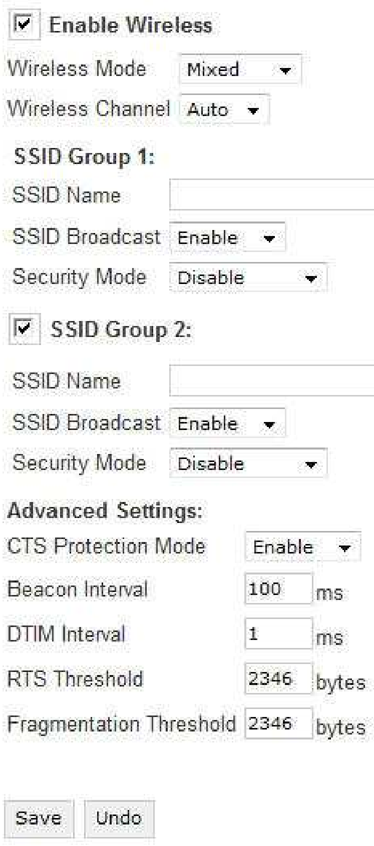
The Wireless Setup web page menu comprises:

Wireless Setting
Wireless MAC Filter

Wireless Setting{ XE "Configuring:Quick setup" }

The device provides wireless connection to wireless clients. This page allows you to enable the wireless service, SSID, and security mode to protect transmitted data in the air. This device provides the Virtual AP (VAP) feature that could provide two virtual APs in the physical AP. You could setup different SSID for each virtual AP and different security code too. There are five wireless security modes supported in the wireless security mode, Disable (no security), WEP, WPA, WPA2, and WPA+WPA2.

Wireless Setting – Security Mode: Disable



☑ Enable Wireless
Wireless Mode: Mixed
Wireless Channel: Auto

SSID Group 1:
SSID Name:
SSID Broadcast: Enable
Security Mode: Disable

☑ SSID Group 2:
SSID Name:
SSID Broadcast: Enable
Security Mode: Disable

Advanced Settings:
CTS Protection Mode: Enable
Beacon Interval: 100 ms
DTIM Interval: 1 ms
RTS Threshold: 2346 bytes
Fragmentation Threshold: 2346 bytes

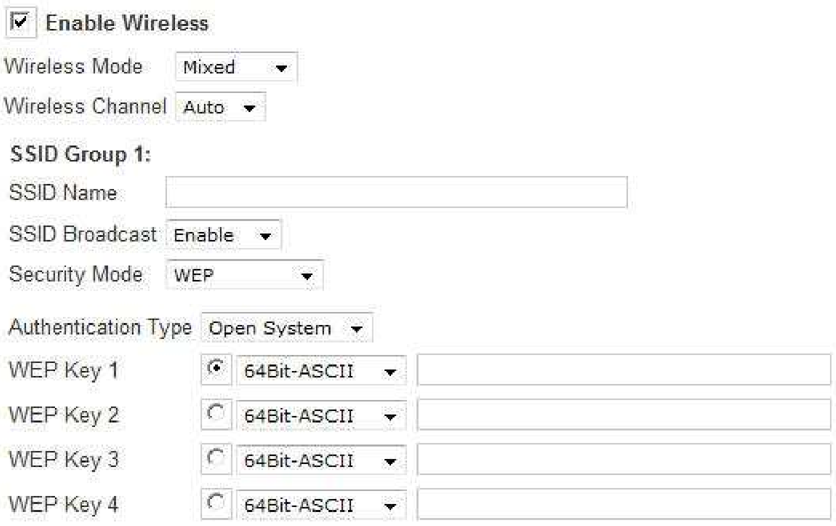
Figure 21: Wireless Setting – Security Mode: Disable (no security)

Global Setting

- Check to enable *Wireless*
- Select the *wireless channel manually* or *automatically*
- Specify the *Network Name (SSID)* used among the device and the wireless clients.

- Select to enable/disable *SSID Broadcast*
- Select Disable as *Security Mode*
- Check *SSID Group 2* if you want to have secondary SSID in the same Wireless Access Point (AP) and enter the other SSID name, SSID Broadcast and Security Mode.
- Enter the Advanced Parameters of wireless module. Leave them as default value for best compatibility and performance with most of wireless clients.
- Click *Save* to save the configuration

Wireless Setting – Security Mode: WEP



☑ Enable Wireless

Wireless Mode: Mixed

Wireless Channel: Auto

SSID Group 1:

SSID Name:

SSID Broadcast: Enable

Security Mode: WEP

Authentication Type: Open System

WEP Key 1 ● 64Bit-ASCII

WEP Key 2 ○ 64Bit-ASCII

WEP Key 3 ○ 64Bit-ASCII

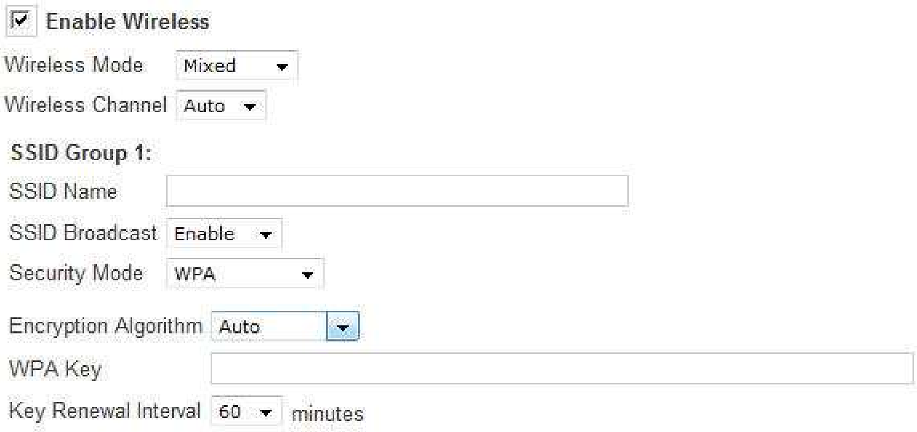
WEP Key 4 ○ 64Bit-ASCII

Figure 22: Wireless Setting – Security Mode: WEP

Global Setting

- Check to enable *Wireless*
- Select the *wireless channel manually* or *automatically*
- Specify the *Network Name (SSID)* used among the device and the wireless clients.
- Select to enable/disable *SSID Broadcast*
- Select WEP as *Security Mode*
- Select *Authentication Type* : Open System or Shared-Key
- There are four *WEP keys*, but only one of them is used by clicking the radio button. The format of WEP key can be 64-bits ASCII, 64-bits HEX, 128-bits ASCII or 128-bits HEX. Enter the value for WEP key. Please be noted that WEP key should be the same among the device and the wireless clients.
- Check *SSID Group 2* if you want to have secondary SSID in the same Wireless Access Point (AP) and enter the other SSID name, SSID Broadcast and Security Mode.
- Click *Save* to save the configuration

Wireless Setting – Security Mode: WPA



☑ Enable Wireless

Wireless Mode Mixed

Wireless Channel Auto

SSID Group 1:

SSID Name

SSID Broadcast Enable

Security Mode WPA

Encryption Algorithm Auto

WPA Key

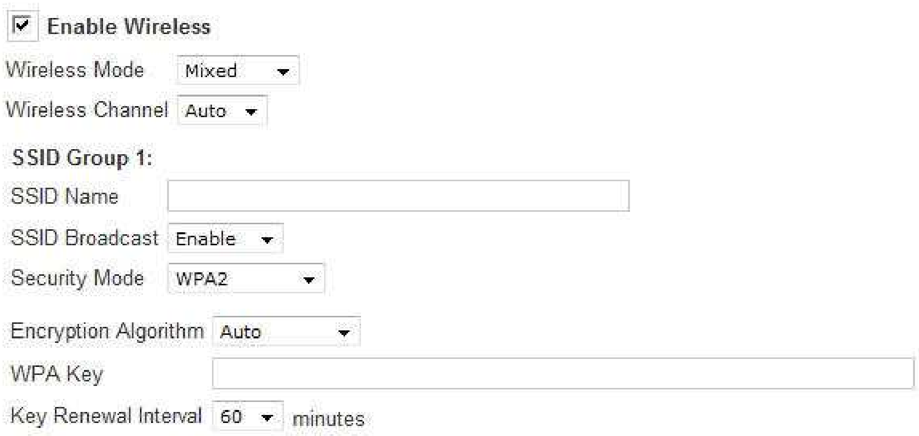
Key Renewal Interval 60 minutes

Figure 23: Wireless Setting – Security Mode: WPA

Global Setting

- Check to enable *Wireless*
- Select the *wireless channel manually* or *automatically*
- Specify the *Network Name (SSID)* used among the device and the wireless clients.
- Select to enable/disable *SSID Broadcast*
- Select WPA as *Security Mode*
- Select *Encryption Algorithm* : AUTO, TKIP, or AES-CCMP
- Enter the value as *WPA key*.
- Enter the value as *Key Renewal Interval minutes*. The key will be renewed automatically after this interval minutes.
- Check *SSID Group 2* if you want to have secondary SSID in the same Wireless Access Point (AP) enter the other SSID name, SSID Broadcast and Security Mode.
- Click *Save* to save the configuration

Wireless Setting – Security Mode: WPA2



☑ Enable Wireless

Wireless Mode: Mixed

Wireless Channel: Auto

SSID Group 1:

SSID Name:

SSID Broadcast: Enable

Security Mode: WPA2

Encryption Algorithm: Auto

WPA Key:

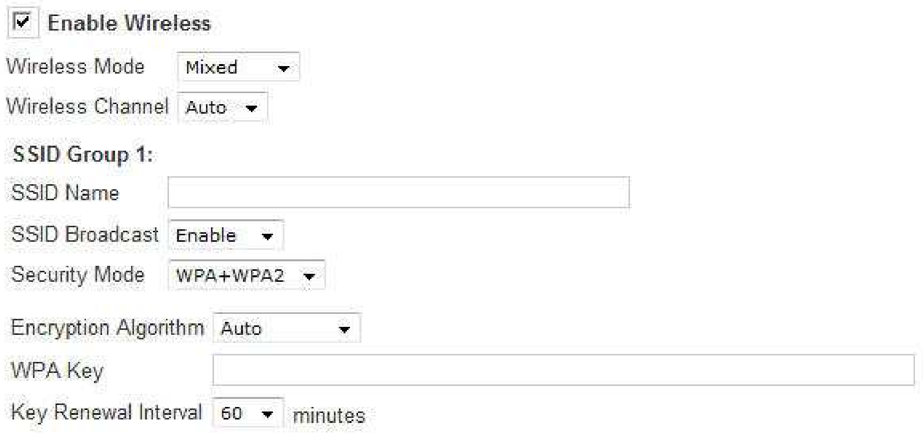
Key Renewal Interval: 60 minutes

Figure 24: Wireless Setting – Security Mode: WPA2

Global Setting

- Check to enable *Wireless*
- Select the *wireless channel manually* or *automatically*
- Specify the *Network Name (SSID)* used among the device and the wireless clients.
- Select to enable/disable *SSID Broadcast*
- Select WPA2 as *Security Mode*
- Select *Encryption Algorithm* : AUTO, TKIP, or AES-CCMP
- Enter the value as *WPA key*.
- Enter the value as *Key Renewal Interval minutes*. The key will be renewed automatically after this interval minutes.
- Check *SSID Group 2* if you want to have secondary SSID in the same Wireless Access Point (AP), then enter the other SSID name, SSID Broadcast and Security Mode.
- Click *Save* to save the configuration

Wireless Setting – Security Mode: WPA+WPA2



☑ Enable Wireless

Wireless Mode: Mixed

Wireless Channel: Auto

SSID Group 1:

SSID Name:

SSID Broadcast: Enable

Security Mode: WPA+WPA2

Encryption Algorithm: Auto

WPA Key:

Key Renewal Interval: 60 minutes

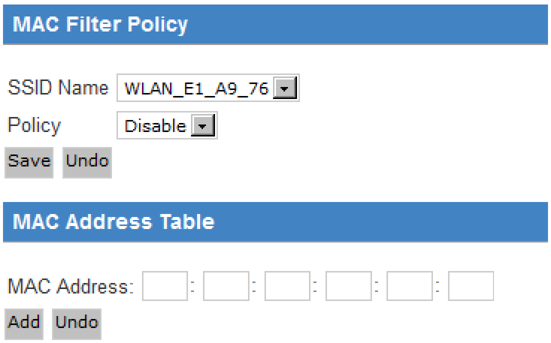
Figure 25: Wireless Setting – Security Mode: WPA+ WPA2

Global Setting

- Check to enable *Wireless*
- Select the *wireless channel manually* or *automatically*
- Specify the *Network Name (SSID)* used among the device and the wireless clients.
- Select to enable/disable *SSID Broadcast*
- Select WPA+WPA2 as *Security Mode*
- Select *Encryption Algorithm* : AUTO, TKIP, or AES-CCMP
- Enter the value as *WPA key*.
- Enter the value as *Key Renewal Interval minutes*. The key will be renewed automatically after this interval minutes.
- Check *SSID Group 2* if you want to have secondary SSID in the same Wireless Access Point (AP), then enter the other SSID name, SSID Broadcast and Security Mode.
- Click *Save* to save the configuration

Wireless MAC Filtering{ XE "Configuring:Quick setup" }

The page provides you to configure the access control of wireless clients.



MAC Filter Policy

SSID Name WLAN_E1_A9_76

Policy Disable

MAC Address Table

MAC Address: __ : __ : __ : __ : __ : __

Figure 26: Wireless MAC Filter Configuration

Global Setting

- Select the *SSID Name* from the list
- Select the *Policy* from the list
- Enter the *MAC Address* of packets to be filtered and *Add* to the table

8 Management

The Management web page menu comprises:

Remote Management

System Reset

Firmware Upgrade

Network Status

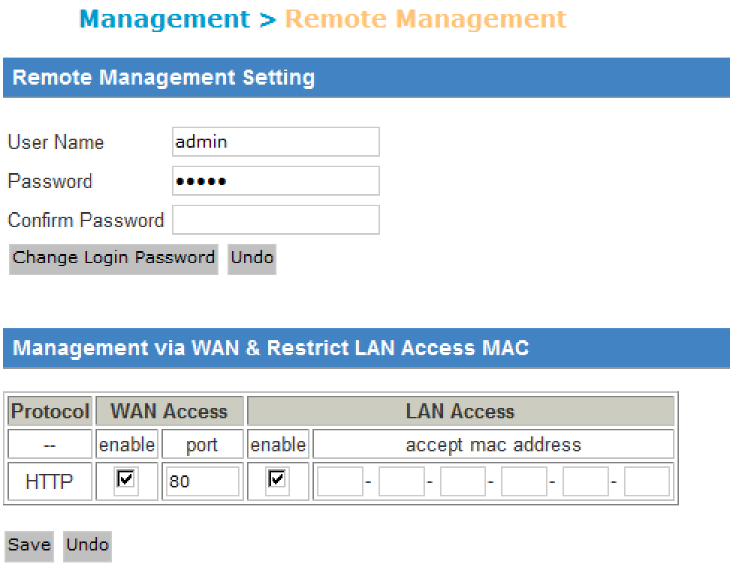
Save Configuration

Diagnostic

Time

Remote Management{ XE "Configuring:Quick setup" }

This page allows you to setup the remote management capability which is useful to check and configure the device from remote site.



Management > Remote Management

Remote Management Setting

User Name	admin
Password	•••••
Confirm Password	

Management via WAN & Restrict LAN Access MAC

Protocol	WAN Access		LAN Access	
--	enable	port	enable	accept mac address
HTTP	☑	80	☑	_ - _ - _ - _ - _ - _

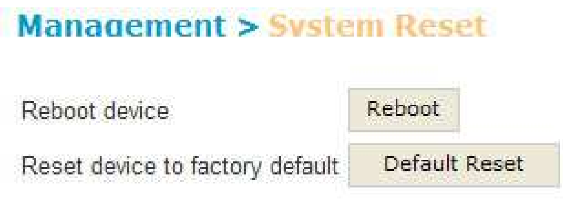
Figure 31: Management Configuration – Remote Management

Global Setting

- The default username/password is admin/admin. You could enter the new username, password in the *Password* and *Confirm Password* fields and then click *Change Login Password* to change it.
- Check and enter the port number of WEB to allow login request from remote site by WEB browser.
- Check to enable *Restrict Management from LAN*, the default is disabled. Enter the *MAC addresses* that you allow them to access the device if this feature is enabled.
- Click *Save* to save the configuration

System Reset{ XE "Configuring:Quick setup" }

This page allows you to reboot the device with current settings or factory default settings.



Management > System Reset

Reboot device

Reset device to factory default

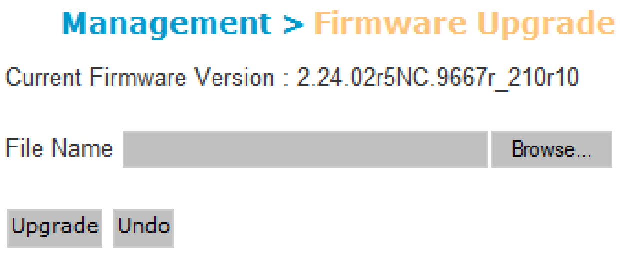
Figure 32: Management Configuration – System Reset

Global Setting

- Click *Reboot* to reboot the device with current settings
- Click *Default Reset* to reboot the device with factory default settings

Firmware Upgrade{ XE "Configuring:Quick setup" }

This page allows you to upgrade the firmware of the device to get more features and improvements.



Management > Firmware Upgrade

Current Firmware Version : 2.24.02r5NC.9667r_210r10

File Name

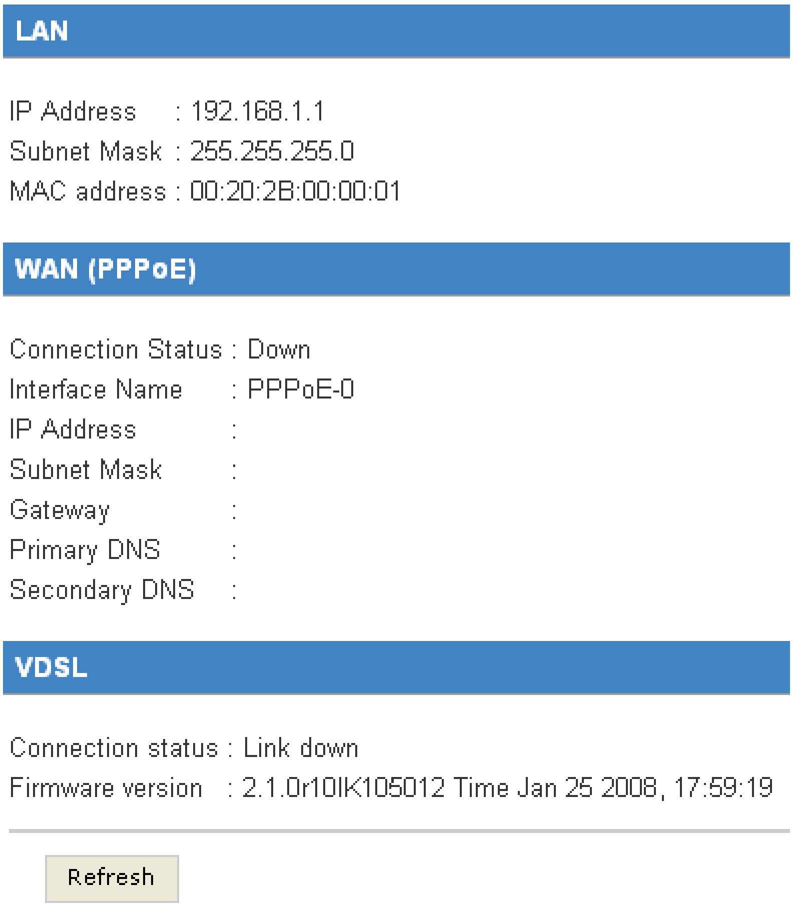
Figure 33: Management Configuration – Firmware Upgrade

Global Setting

- Click *Browse* to specify the location of firmware
- Click *Upgrade* to start the upgrade procedure. The device will reboot automatically when the firmware is loaded completely.

Network Status{ XE "Configuring:Quick setup" }

This page shows the network status and most important information about LAN, WAN protocol, and VDSL.



LAN

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
MAC address : 00:20:2B:00:00:01

WAN (PPPoE)

Connection Status : Down
Interface Name : PPPoE-0
IP Address :
Subnet Mask :
Gateway :
Primary DNS :
Secondary DNS :

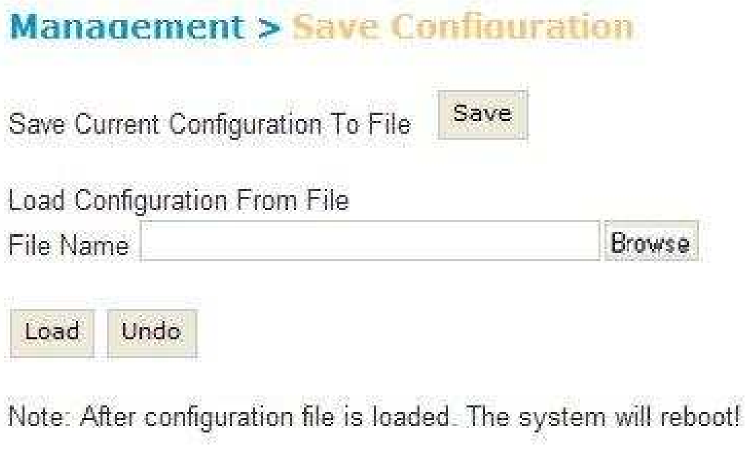
VDSL

Connection status : Link down
Firmware version : 2.1.0r10IK105012 Time Jan 25 2008, 17:59:19

Figure 34: Management Configuration – Network Status

Save Configuration{ XE "Configuring:Quick setup" }

This page allows you to save current configuration into file in your PC or load the configuration from PC.



Management > Save Configuration

Save Current Configuration To File

Load Configuration From File

File Name

Note: After configuration file is loaded. The system will reboot!

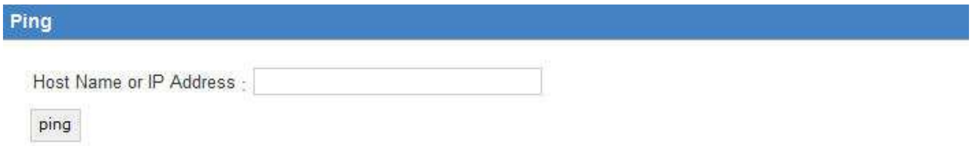
Figure 35: Management Configuration – Save Configuration

Global Setting

- Click *Save* and follow the system instructions to save configuration profile into file
- To load the configuration profile from file, click *Browse* to specify the location of file and click *Load* to load the configuration profile into the device. The device will reboot automatically when the configuration is loaded.

Diagnostic{ XE "Configuring:Quick setup" }

This page allows you to ping a remote IP or domain name to test the Internet connection working fine or not.


Ping

Host Name or IP Address :

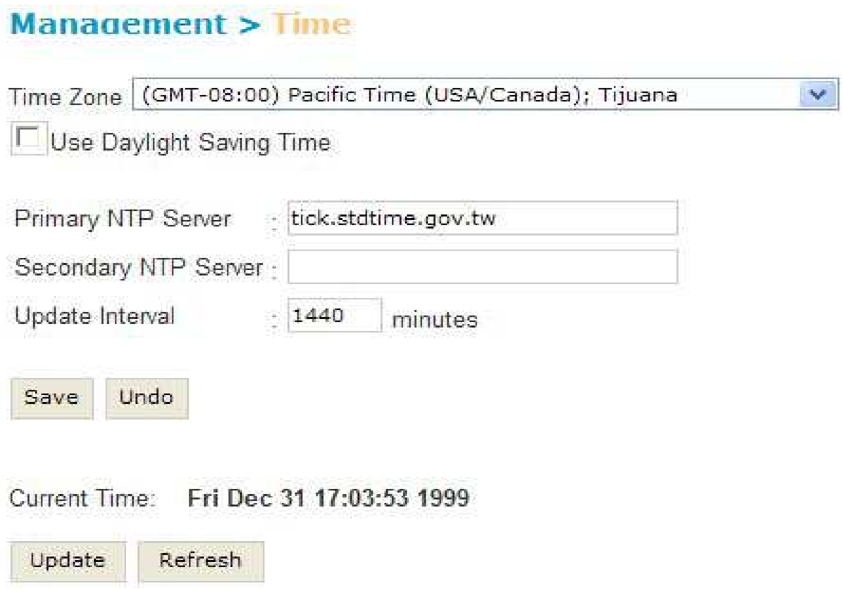
Figure 36: Management Configuration – Diagnostic

Global Setting

- Enter the *IP address* or *Host name* (domain name)
- Click *ping* to start the diagnostic process.

Time{ XE "Configuring:Quick setup" }

This page allows you to setup the time zone and get the real time clock from Internet. .


Management > Time

Time Zone (GMT-08:00) Pacific Time (USA/Canada); Tijuana

□ Use Daylight Saving Time

Primary NTP Server : tick.stdtime.gov.tw

Secondary NTP Server :

Update Interval : 1440 minutes

Current Time: Fri Dec 31 17:03:53 1999

Figure 37: Management Configuration – Time Zone Configuration

Global Setting

- Select the your local *Time Zone* from the list
- Check to use the *Daylight Saving Time*
- Enter the NTP server domain name in the *Primary NTP Server* and *Secondary NTP Server* fields which provide the real time network clock
- Enter the value of *Update Interval* to sync up the clock with NTP server
- Click *Save* to save your settings
- Click *Update* to get the real time clock now

Appendix A - Configuring the Internet Settings

This appendix provides instructions for configuring the Internet settings on your computers to work with the device.

Configuring Ethernet PCs

Before you begin

By default, the device automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.

Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the device to do so. See

Assigning static Internet information to your PCs section.

- If you have connected your LAN PCs via Ethernet to the device, follow the instructions that correspond to the operating system installed on your PC:
- Windows® XP PCs
- Windows 2000 PCs
- Windows Me PCs
- Windows\ 95, 98 PCs
- Windows NT 4.0 workstations
- If you want to allow Wireless PCs to access your device, follow the instructions in Configuring Wireless PCs below..

Windows® XP PCs

In the Windows task bar, click the *Start* button, and then click *Control Panel*.

Double-click the Network Connections icon.

In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labelled *Local Area Connection*).The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Ensure that the check box to the left of the item labelled *Internet Protocol TCP/IP* is checked and click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.

Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*. The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

If Internet Protocol (TCP/IP) does not display as an installed component, click *Install.*

In the *Select Network Component* Type dialog box, select *Protocol*, and then click *Add.*

Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

If prompted, click *OK* to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the *Control Panel*, double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.

In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP),* and then click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.

Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

Double-click the Network and Dial-up Connections icon.

In the Network and Dial-up Connections window, right-click the Network icon, and then select Properties. The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.

If Internet Protocol (TCP/IP) does not display as an installed component, click Add.

In the Select Network Component Type dialog box, select Protocol, and then click Add.

Select Microsoft in the Manufacturers box.

Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

If prompted, click OK to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the Control Panel, double-click the Network and Dial-up Connections icon.

In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.

In the Network Properties dialog box, select TCP/IP, and then click Properties.

In the TCP/IP Settings dialog box, click the radio button labelled Server assigned IP address. Also click the radio button labelled Server assigned name server address.

Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows\ 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network icon. The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

If TCP/IP does not display as an installed component, click *Add.* The Select Network Component Type dialog box displays.

Select *Protocol*, and then click *Add…*The Select Network Protocol dialog box displays.

Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.

Click *OK* to return to the Network dialog box, and then click *OK* again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

Click *OK* to restart the PC and complete the TCP/IP installation. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then click the Network icon.

Select the network component labelled TCP/IP, and then click *Properties*. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

In the TCP/IP Properties dialog box, click the IP Address tab.

Click the radio button labelled Obtain an IP address automatically.

Click the DNS Configuration tab, and then click the radio button labelled *Obtain an IP address automatically*.

Click *OK* twice to confirm and save your changes. You will be prompted to restart Windows.

Click *Yes*.

Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

In the Control Panel window, double click the Network icon.

In the *Network dialog* box, click the *Protocols* tab. The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.

If TCP/IP does not display as an installed component, click *Add.*

In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

Click *Yes* to continue, and then click *OK* if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then double-click the Network icon.

In the *Network* dialog box, click the *Protocols* tab.

In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.

In the Microsoft TCP/IP Properties dialog box, click the radio button labelled Obtain an IP address from a DHCP server.

Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

{ XE "IP configuration: static IP addresses" **}{** XE "PC Configuration:static IP addresses" **}{** XE "Static IP addresses" **}**In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the device to assign it. This option may be desirable (but not required) if:

You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

You maintain different subnets on your LAN (subnets are described in Appendix B).

Before you begin, you must have the following information available:

The IP address and subnet mask of each PC

The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the device. By default, the LAN port{ XE "LAN port:default IP information" } is assigned the IP address 192.168.1.1. (You can change this number or another number can be assigned by your ISP.)

The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the device*'s LAN port.*

Configuring Wireless PCs

You need to configure the operating system installed on your Wireless PCs using the same procedure described for Configuring Ethernet PCs section.

Positioning the wireless PCs

The wireless network cards used determine the maximum distance between your wireless PCs and your device. Guidelines on positioning the hardware components of your wireless network should be provided by your network card provider.

Wireless PC cards and drivers

Each PC on your wireless LAN must be fitted with a wireless access card. You must also install the corresponding driver files for your particular wireless card on your PC. You should receive driver files and instructions on how to install them together with your wireless card.

Configuring PC access to your Wireless device

Before you start configuring your Wireless PC, you must ensure that you have:

A Wireless access card for each of the PCs

Corresponding wireless access card driver software files

The configuration steps below will vary depending on both the operating system and wireless card installed on the PC. These steps provide a basic outline, however you should refer to the documentation provided with your wireless access card for specific instructions.

To configure Wireless PCs:

Install the wireless access card.

Install the wireless driver software files.

Configure the following wireless parameters on each of the wireless PCs:

Set the adapter to use infrastructure mode. This configures the PCs to access each other and the Internet via the device.

Configure the SSID and channel to match the SSID and channel previously configured on the device.

Your wireless network can now communicate with the Internet via the device.

Appendix B - Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the device, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Troubleshooting Suggestions

Problem	**Troubleshooting Suggestion**
LEDs	
Power LED does not illuminate after product is turned on.	**{** XE "LEDs:troubleshooting" **}**Verify that you are using the power cable provided with the device and that it is securely connected to the device and a wall socket/power strip.
Internet LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port. Allow about 30 seconds for the device to negotiate a connection with your ISP.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the device. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Run a health check on your device. Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: Check that the gateway IP address on the computer is your public IP address (see Current Status on page 1 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
My LAN PCs cannot display web pages on the Internet.	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the device is correct, and then you can use the ping utility, discussed on page 44, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
I forgot/lost my user ID or password{ XE "Password:recovering" }.	If you have not changed the password from the default, try using “admin” as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing three times the Reset Default button on the front panel of the device. Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
I cannot access the web pages from my browser.	Use the ping utility, discussed in the following section, to check whether the PC can communicate with the device’s LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC’s IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the device**.**
My changes to the web pages are not being retained.	Be sure to use the *Confirm Changes* function after any changes.

Diagnosing Problem using IP Utilities

Ping

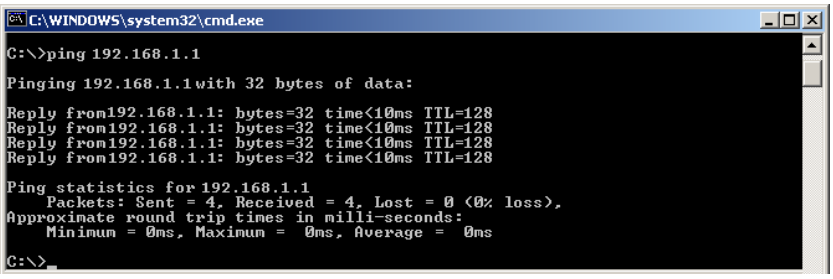
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

ping 192.168.1.1

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window is displayed:



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

If the target computer cannot be located, you will receive the message Request timed out.

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

Nslookup

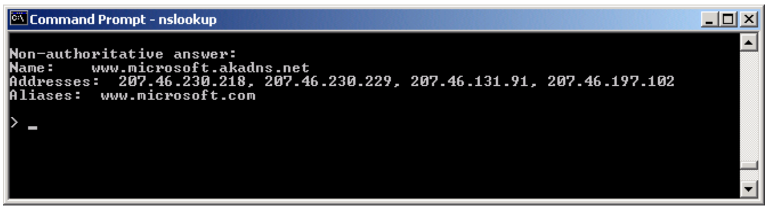
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

Nslookup

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown below:



```
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses:  207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases:  www.microsoft.com

> _
```

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **[Enter]** at the command prompt.

Appendix C – Glossary

Term	Description
802.11	A family of specifications for wireless LANs developed by a working group of the IEEE. This wireless Ethernet protocol, often called Wi-Fi.
10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See data rate, Ethernet.
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See data rate, Ethernet.
ADSL	Asymmetric Digital Subscriber Line The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
Analog	An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See digital.
ATM	Asynchronous Transfer Mode A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See data rate.
Authenticate	To verify a user's identity, such as by prompting for a password.
Binary	The "base two" system of numbers that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See bit, IP address, network mask.
Bit	Short for "binary digit," a bit is a number that can have two values, 0 or 1. See binary.
Bps	bits per second
Bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing which can add more intelligence to data transfers by using network addresses instead. The device can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other

	types of data. See routing.
Broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device’s interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
Digital	Of data, having a form based on discrete values expressed as binary numbers (0’s and 1’s). The data component in DSL is a digital signal. See analog.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See domain name.
Domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See DNS.
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Encryption keys	See network keys
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.

FTP	File Transfer Protocol A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See web browser, web site.
Hub	A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.
Internet	The global collection of interconnected networks used for both private and business communications.
Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.
IP address	Internet Protocol address The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See domain name, network mask.
ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network. A network limited to a small geographic area, such as a home or small office.

LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the device are LEDs.
MAC address	Media Access Control address The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; NN:NN:NN:NN:NN:NN.
Mask	See network mask.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
NAT	Network Address Translation A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
Network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.
Network keys	(Also known as encryption keys.) 64-bit and 128-bit encryption keys used in WEP wireless security schemes. The keys encrypt data over the WLAN, and only wireless PCs configured with WEP keys that correspond to the keys configured on the device can send/receive encrypted data.
Network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See binary, IP address, subnet.
NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See Ethernet, RJ-45.
Packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
Ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
Port	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the device uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.

PPPoA	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
PPPoE	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
Protocol	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
Remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
Routing	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See DNS.
Subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See network mask.
Subnet mask	A mask that defines a subnet. See network mask.
TCP	See TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
Telnet	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TKIP	Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.
Triggers	Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them. Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.
Twisted pair	The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.
Unnumbered interfaces	An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.1). The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.
Upstream	The direction of data transmission from the user to the Internet.
VC	Virtual Circuit A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See VC.
VDSL	Very High Speed Digital Subscriber Line It provides faster transmission rate and is capable of supporting high bandwidth applications like IPTV and bandwidth consumed applications.
VPI	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See VC.

WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See HTTP, web site, WWW.
Web page	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See hyperlink, web site.
Web site	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See hyperlink, web page.
WEP	Wired Equivalent Privacy (WEP) encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.
Wireless	Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. See wireless LAN.
Wireless LAN	A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.
WPA	Wi-Fi Protected Access WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device. It provides improved data encryption and stronger user authentication. The mode of WPA supported on your device is called Pre-Shared Key (PSK), which allows you to manually enter a type of key called a pass phrase.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

Appendix D - Specification

A1. Hardware Specifications for DYX9667R

- ■ LAN Interface
- Four port 10/100BaseT Ethernet Switch (4 * RJ-45 connectors), IEEE 802.3u with MDI/MDIX auto-detection
- Integrated 802.11b/g WLAN Access Point
- Integrated USB slave and host ports

- ■ WAN VDSL2 Line Interface
- Comply with VDSL2 and support 8a/8b/8c/8d, 12a/12b, 17a and 30a
- Connection Loops: One (pair wire)
- Connector: RJ-11

- ■ Analog Voice Interface
- 2 FXS ports (2 * RJ-11 connectors) for analog phone sets

- ■ Indicators
- PWR – Red Blink: Only occur when you open the modem, it will become green after 5s.Red On: boot fail
  Green On: device is powered on
- DSL – Green LED indicates VDSL2 connection
- PPP – Green On: establish a PPP connection
  Red On: PPP disconnection
- LAN – Green LED indicates LAN connection
- WLAN – Green LED indicates wireless AP enabled
- USB – GREEN LED indicates USB connection

- ■ OAM&P
- Local: Web management
- Remote: Web Management

- ■ Environment
- Operation Temperature: 0°C ~ 40°C
- Operation Humidity: 5% ~ 95%
- Storage Temperature: -20 ~ +85°C
- Storage Humidity: 5%~95%

- ■ Power
- AC/DC Switching Input =100~240V 50/60Hz Output=12VDC 1.5Amp

- ■ Certificates
- CE, CB

A2. Software Specifications

- VDSL
  - Support VDSL2 profiles, 8a/8b/8c/8d, 17a
  - Plug-and-play multi-mode (VDSL2, VDSL) operation
- Bridging
  - Transparent Bridging and spanning(IEEE 802.1D)
- Routing
  - IP routing and PPP supported
  - PAP and CHAP for user authentication in PPP connection
  - RFC2684 (RFC1483) Routed
  - NAT/PAT with extensive ALG support
  - IP QoS Supported
- Wireless LAN
  - WEP: 64 or 128 bits key length
  - WPA (Wi-Fi Protected Access) and WPA2 in PSK mode
  - Multiple SSIDs supported
- Configuration and Network Management Features
  - DHCP client and server for IP management
  - UPnP Internet Gateway Device (IGD v1)
  - System Log capability
  - WEB for local or remote management
  - HTTP for firmware upgrade and configuration

Note: The hardware and software specifications are subjected to change without notices.

Appendix E - Warranties

B1. Product Warranty

Dynalink Modems warrants that the xDSL unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.

Dynalink Modems shall incur no liability under this warranty if

- The allegedly defective goods are not returned prepaid to Dynalink Modems within thirty (30) days of the discovery of the alleged defect and in accordance with Dynalink Modems' repair procedures; or

- Dynalink Modems' tests disclose that the alleged defect is not due to defects in material or workmanship.

Dynalink Modems' liability shall be limited to either repair or replacement of the defective goods, at Dynalink Modems' option.

DYNALINK MODEMS MARKS NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE USER'S DOCUMETATION. DYNALINK SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

B2. Warranty Repair

1. During the first three (3) months of ownership, Dynalink Modems will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Dynalink Modems will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced products shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Dynalink Modems will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to Dynalink Modems within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Dynalink Modems will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

Dynalink Modems will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Appendix F - Regulation

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless Dynalink expressly approves the changes or modifications.

FCC Part 15 Notice with Wireless

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Warning: Operation is subject to the following two conditions:
1) This device may not cause harmful interference.
2) This device must accept any interference received including interference that may cause undesired operation.

FCC Part 68 Notice

This equipment complies with Part 68 of FCC Rules. On the base unit of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. IF REQUESTED, THIS INFORMATION MUST BE GIVEN TO THE TELEPHONE COMPANY.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

NOTICE: The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or an electronic device to send any message via a telephone fax machine, unless such a message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission the following information:

- ✓ The date and time of transmission
- ✓ Identification of either business, business entity or individual sending message
- ✓ Telephone number of either the sending machine, business entity or individual

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate.
Do not use any other power adapter except the one that accompanies the unit. Use of other adapter could result in damage to the unit. To prevent electronic shock, please do not open the cover.

UL Safety Regulations

- ✓ Disconnect TNV circuit connector or before removing cover or equivalent.
- ✓ Disconnect TNV circuit connector(s) before disconnecting power.
- ✓ Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- ✓ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- ✓ Do not use the telephone to report a gas leak in the vicinity of the leak.
- ✓ Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

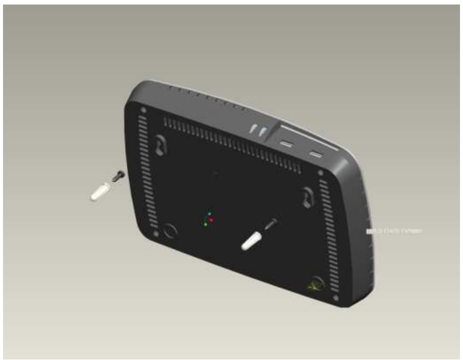
No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Wall Mounting

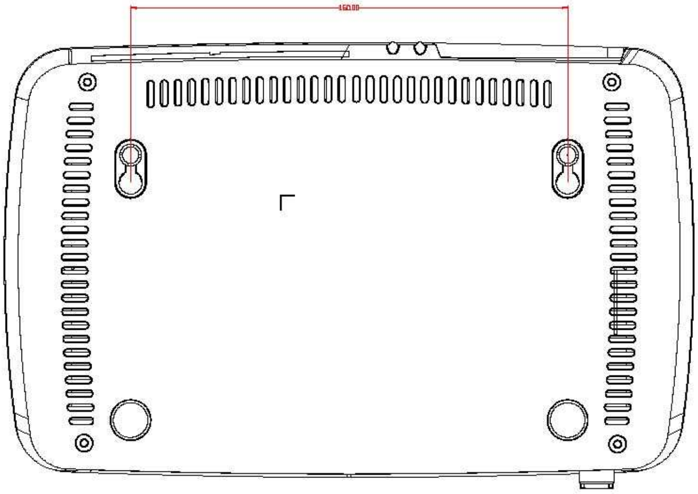
There are two slots on the underside of the VDSL Broadband Gateway that can be used for Wall Mounting.

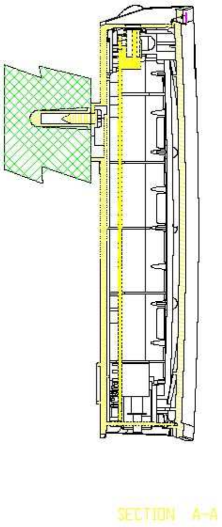
When wall mounting the unit, ensure that it is within reach of the power outlet.



You will need two suitable screws (suggest pan head screw) to wall mount the unit. To do this:

- ✓ Ensure that the wall you use is smooth, flat, dry and sturdy and use the two screw holes which both are 177.8mm apart
- ✓ Fix the screws into the wall, leaving their heads above 2.54mm (0.1 in.) clear of the wall surface.
- ✓ Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.





Appendix G - Contact information

You can help us serve you better by sending us your comments and feedback. Listed below are the addresses, telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.dynalink.co.nz for more information. We look forward to hearing from you!

Filename: Manual_X96 series_Eng
Directory: C:\Documents and Settings\Mace\My Documents\Technical Writing\PDF Converts
Template: C:\Documents and Settings\Mace\Application Data\Microsoft\Templates\Normal.dotm
Title: User Manual
Subject:
Author: xavi
Keywords:
Comments:
Creation Date: 7/2/2012 12:16:00 PM
Change Number: 2
Last Saved On: 7/2/2012 12:16:00 PM
Last Saved By: Netomm Wireless Limited
Total Editing Time: 1 Minute
Last Printed On: 7/2/2012 12:16:00 PM
As of Last Complete Printing
Number of Pages: 64
Number of Words: 14,727 (approx.)
Number of Characters: 75,847 (approx.)