



Wireless ADSL2⁺ Router
802.11n 150 Mbit



User Manual
HRDSL150W

www.hamletcom.com

INDEX

1. Introduction	4
1.1 System Requirements	4
1.2 Package Contents	4
2. Specification	5
2.1 LED Meaning	6
2.2 Connectors	7
2.3 Factory Default Settings	8
3. Installation & Setup	9
3.1 Connection of Wireless ADSL2+ Router	9
4. Configuration Procedures	10
4.1 Windows 98SE/ME/2000/XP	10
4.2 Windows Vista 32/64	12
4.3 Windows 7 32/64	15
5. Router Configuration	17
6. Connect Wirelessly	20
7. Web Configuration	22
7.1 Accessing the Web Interface	22
7.2 Quick Start	23
7.3 Interface Setup	26
7.4 Advanced Setup	35
7.5 Access Management	43
7.6 Maintenance	50
7.7 Status	53
7.8 Help	57
8. Universal Plug-and-Play (UPnP)	58
8.1 Universal Plug and Play Overview	58
8.2 How do I know if I'm using UPnP?	58
8.3 NAT Traversal	58
8.4 Cautions with UPnP	58
8.5 Configuring UPnP	59
8.6 Installing UPnP in Windows XP	60
8.7 Using UPnP in Windows XP	62
9. Web Configuration Easy Access	64
10. Troubleshooting	65
11. Technology Glossary	69

Dear Customer,
thanks for choosing an Hamlet product. Please carefully follow the instructions for its use and maintenance and, once this item has run its life span, we kindly ask You to dispose of it in an environmentally friendly way, by putting it in the separate bins for electrical/electronic waste, or to bring it back to your retailer who will collect it for free.

Responsibility Statement

The European importer declares that this product is compliant with CE standards. Importer references and contact details available on www.hamletcom.com in the "About Us" section.

The importer for Italy is:
Careca Italia S.p.A.
VAT number 02078660350
www.careca.com

In order to reduce paper consumption we only printed a concise version of CE declaration of conformity and Quick installation guide.

Full compliance declaration and product documentation will be available contacting us at info@hamletcom.com specifying product code and documentation required.

We inform You this product is manufactured with materials and components in compliance with RoHS directives: 2002/95/CE; with RAEE Directives: 2003/96/CE, Italian Legislative Decree 2005/151 and below EEC Directives: IEC 60950-1: 2005 (2nd Edition), EN 60950-1: 2006+A11: 2009, ETSI EN 300 328 V1.7.1 (2006-10), ETSI EN 300 386 V1.4.1 (2008-04), EN 61000-3-2: 2006, EN 61000-3-3: 1995+A1: 2001+A2: 2005, IEC 61000-4-2 Edition 1.2: 2001-04, IEC 61000-4-3 Edition 3.0: 2006, IEC 61000-4-4: 2004, IEC 61000-4-5 Edition 2.0: 2005, IEC 61000-4-6 Edition 2.2: 2006, IEC 61000-4-8 Edition 1.1: 2001-03, IEC 61000-4-11 2nd Edition: 2004-03, ETSI EN 301-489-17: V1.3.2 (2008-04), ETSI EN 301-489-1: V1.8.1 (2008-04).

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.



Trademarks

All trademarks and company names mentioned in this manual are used for description purpose only and remain property of their respective owners.

Changes

The material in this document is for information only and subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Hamlet assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. Hamlet reserves the right to make changes or revisions in the product design or the product manual without reservation and without obligation to notify any person of such revisions and changes.

1. Introduction

The Hamlet Wireless ADSL2+ Router is a low cost, high performance and high-speed device based on 802.11n wireless technology that provides a full rate ADSL2+ Router with the superb reliability and a complete solution for home and office router. Hamlet HRDSL150W can have a maximum downstream data rate of up to 24Mbps and an upstream of up to 1Mbps. When configured as a DHCP server, it will assign IP address to every connected PC and acts as the only externally recognized Internet device on your local area network. With build-in NAT, the Hamlet Wireless ADSL2+ Router serves as an Internet firewall, protecting your network from being accessed by outside users.

1.1 System Requirements

- A computer with pre-installed ethernet adapter
- Pentium 200MHz processor or above
- Windows 98SE / Windows Me / Windows 2000 / Windows XP / Windows Vista and Windows 7
- 64MB of RAM or above
- 25MB free disk space

1.2 Package Contents

- 802.11n Wireless ADSL2+ Router
- CD-ROM (Software & Manual)
- Quick Installation Guide
- 1 x Telephone Cable (RJ-11)
- Ethernet Cable (RJ-45)
- Power Adaptor

2. Specification

ADSL Standards supported

- Compliant to ITU-T G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3 (ADSL2), G.992.4 (splitterless ADSL2), G.992.5 (ADSL2+) for Annex A, B
- G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream
- Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1 and G.996.1(for ISDN only); G.991.1;G.lite (G992.2))
- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells
- ATM Forum UNI 3.1/4.0 PVC
- Supports up to 8 PVCs (UBR, CBR, VBR)
- Multiple Protocols over AAL5 (RFC 1483)
- PPP over AAL5 (RFC 2364)
- PPP over Ethernet (RFC 2516)

Wireless Ethernet 802.11n

With built-in 802.11n access point for extending the communication media to WLAN while providing the WEP, WPA and WPS for securing your wireless networks.

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Hamlet Wireless ADSL2+ Router and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

10/100M Auto-negotiation Ethernet / Fast Ethernet Interface

This auto-negotiation feature allows the Router to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address.

Multiple PVC (Permanent Virtual Circuits) Support

Your Wireless ADSL2+ Router supports up to 8 PVC's.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows individual clients (computers) to obtain TCP/IP configuration at start-up from a centralized DHCP server. The 802.11n Wireless ADSL2+ Router has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The 802.11n Wireless ADSL2+ Router can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

2.1 LED Meaning

The Wireless ADSL2+ Router has indicator lights on the front side. Please see below for an explanation of the function of each indicator light.

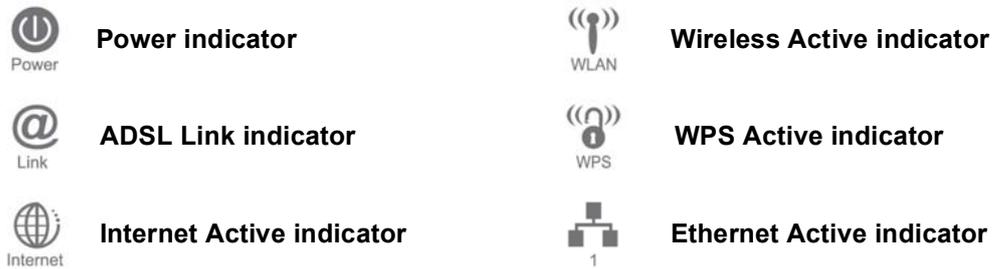


Table 1. LED function

Label	Color	On	Flash	Off
 Power	Green	Ready	Waiting for device ready	Power Off
 Link	Green	Connect to DSLAM	Disconnect to DSLAM	N/A
 Internet	Green	The device has a WAN IP address from ISP	Transmit / Receive Data	N/A
 WLAN	Green	WLAN Ready	Transmit / Receive Data	WLAN Off
 WPS	Green	N/A	Start WPS peer within 2 minutes	WPS Idle
 1	Green	Ethernet Connected	Transmit / Receive Data	Ethernet Disconnected

2.2 Connectors

The below table shows the function of each connector and switch of the device.

CONNECTOR	DESCRIPTION
POWER	Input connector for the 12V power adaptor
SWITCH	ON/OFF Power Switch
LAN1~4	Four Ethernet ports (RJ-45)
LINE	Connects to your ADSL2+ line – for ADSL2+ Line input
RESET	Reset button. Reset the router to its default settings. Press this button for at least 6 seconds to reset it to its default settings.
WPS	Press this button for at least one second and the WPS LED will flash to start WPS.
WLAN	Press this button for at least one full second to turn off/on wireless signals

Figure1. Rear View of the Wireless ADSL2+ Router

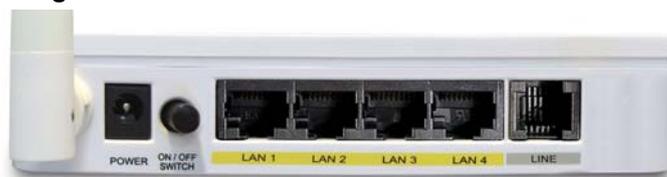


Figure2. WPS and WLAN button



Figure3. RESET button



2.3 Factory Default Settings

Before configuration, please refer to following default settings.

Web interface

Username: admin
Password: hamlet

LAN IP Settings

IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

DHCP

DHCP Server: Enable

3. Installation & Setup

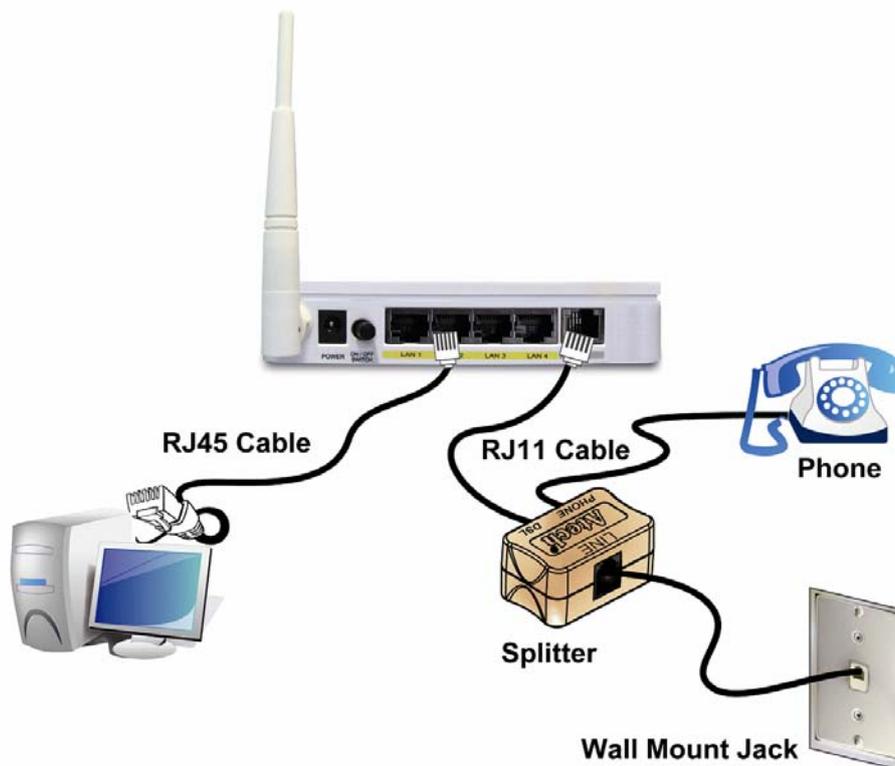
Follow each step carefully and only go to the next step once you have complete the previous one.

Note! Be sure that you are well insulated from any power source to avoid electricity shock.

Note! Use only the manufacturer-approved power supply that shipped with the Router.

1. Connect the power to the Wireless ADSL2+ Router by plugging the power supply into an appropriate electrical outlet.
2. If the Power LED is off, refer to “Troubleshooting” for information.

3.1 Connection of Wireless ADSL2+ Router



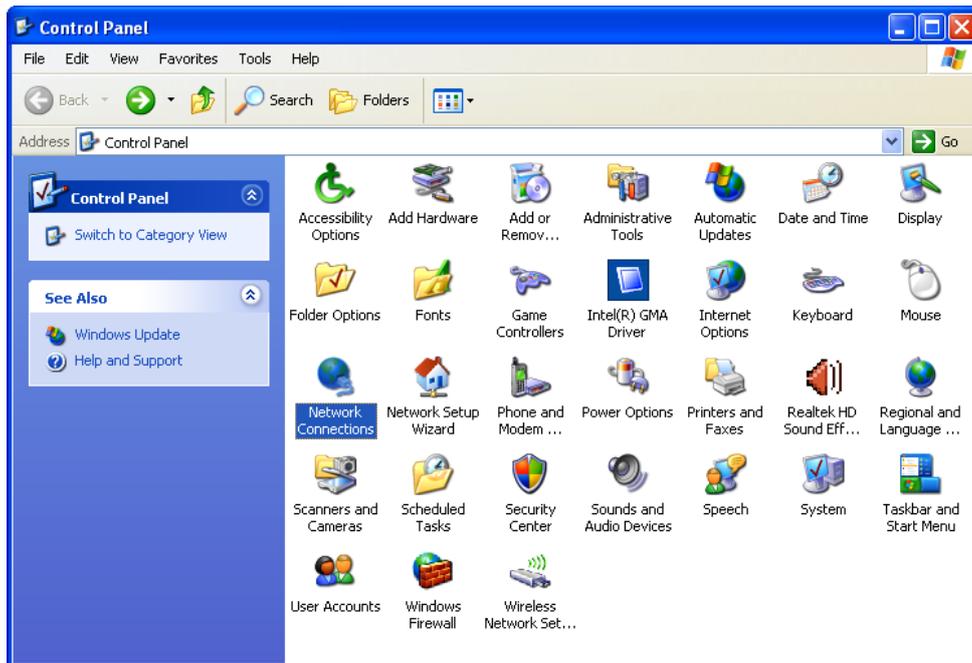
1. Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to any of the 4 Wireless ADSL2+ Router's LAN Ports.
2. Connect the supplied RJ11 telephone cable from your home's telephone jack to the “**LINE**” port of the supplied splitter. Connect the other supplied RJ11 telephone cable to the “**DSL**” port of the splitter and connect the other end of this cable to the “**LINE**” port of your Wireless ADSL2+ Router. (If there is no option Splitter, please connect the supplied RJ11 telephone cable from your home's telephone jack to the “**LINE**” port of your Wireless ADSL2+ Router).
3. Connect a RJ11 telephone cable to the “**PHONE**” port of the splitter and connect the other end to your telephone.
4. Connect the power adapter to the power inlet “**POWER**” of the Wireless ADSL2+ Router and turn the “**ON/OFF SWITCH**” switch of your Wireless ADSL2+ Router on.

4. Configuration Procedures

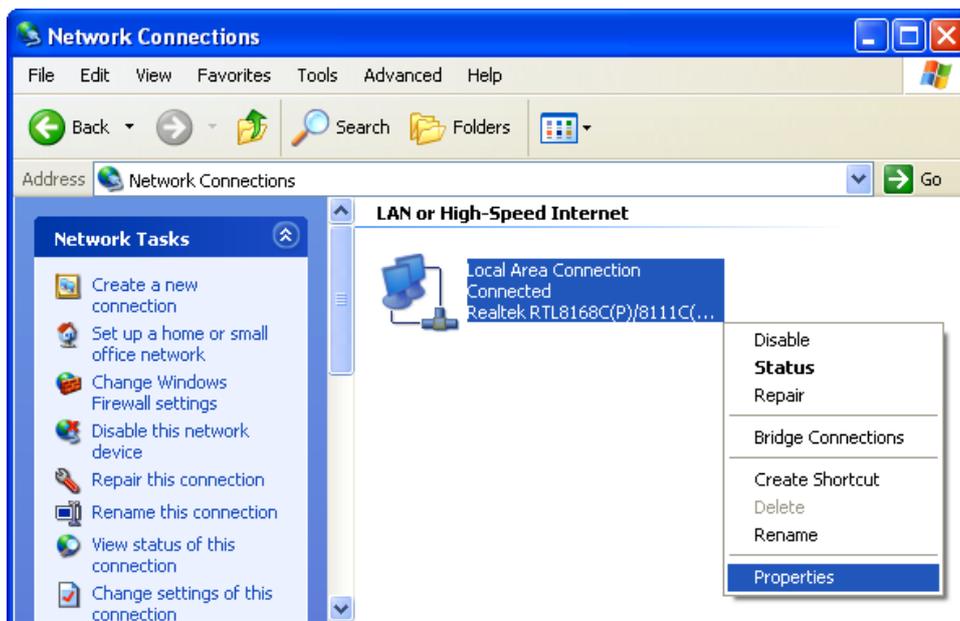
Before starting the Wireless ADSL2+ Router configuration, please kindly configure the PC computer as below, to have automatic IP address / DNS Server.

4.1 Windows 98SE/ME/2000/XP

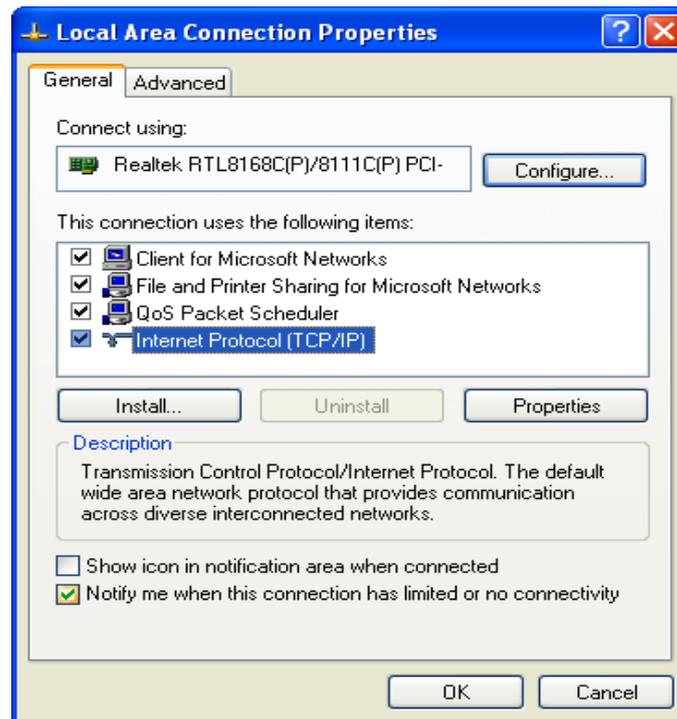
1. Click on **“Start” > “Control Panel” (in Classic View)**. In the Control Panel; double click on **“Network Connections”** to continue.



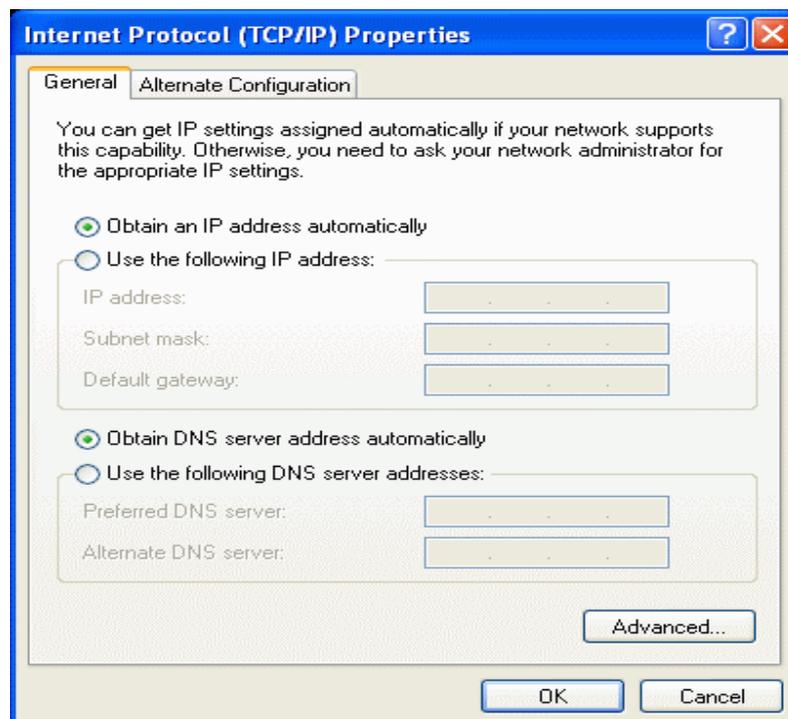
2. Single right click on **“Local Area connection”**, then click **“Properties”**.



3. Double click on “**Internet Protocol (TCP/IP)**”.



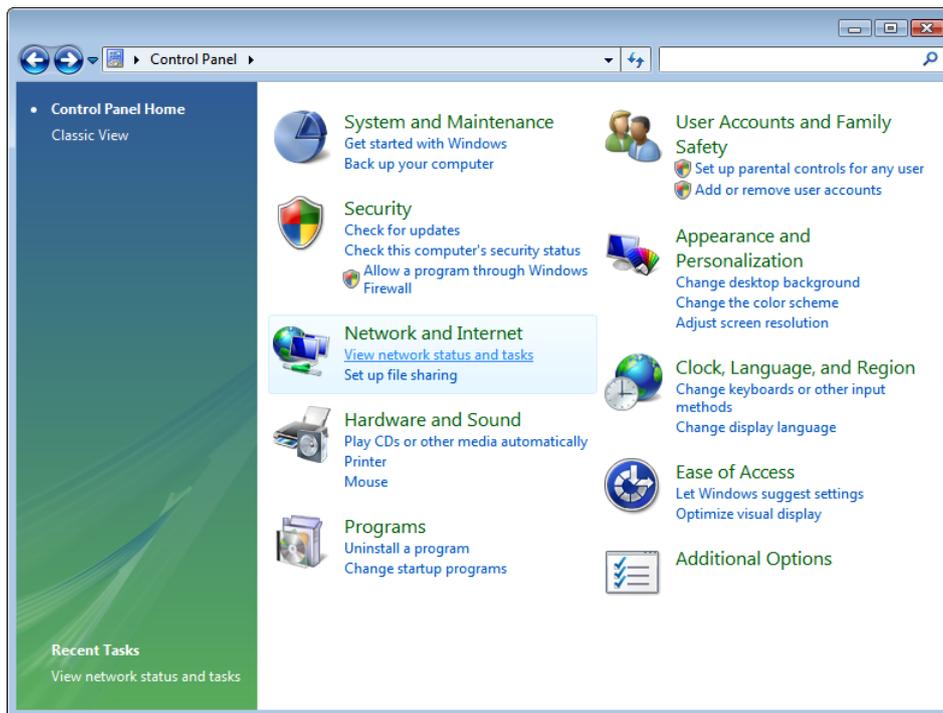
4. Check “**Obtain an IP address automatically**” and “**Obtain DNS server address automatically**” then click on “**OK**” to continue.



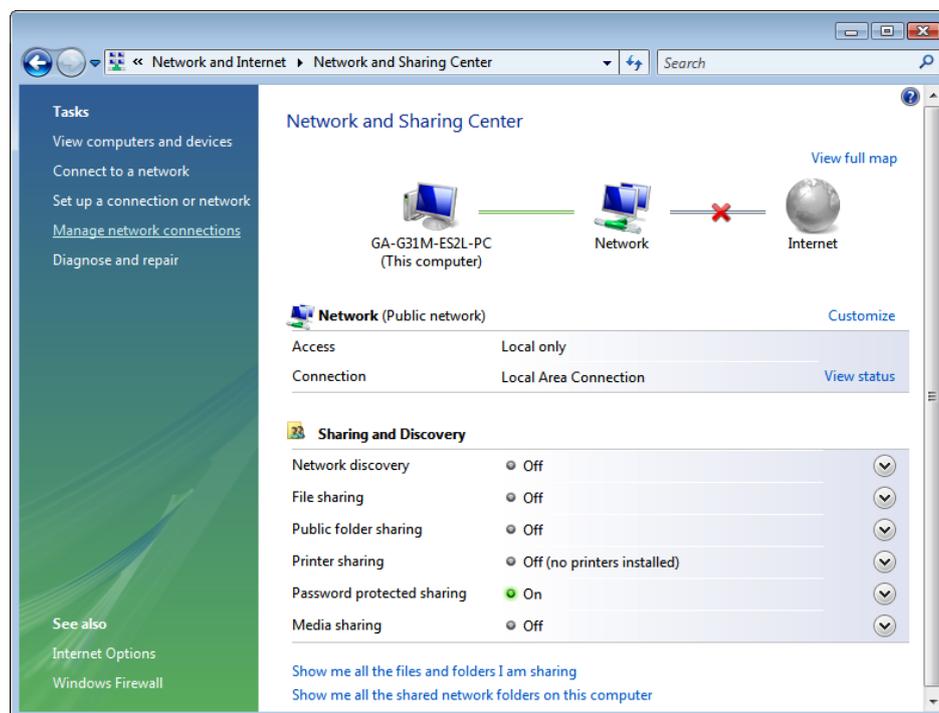
5. Click “**Show icon in notification area when connected**” (see screen image in 3. above) then click on “**OK**” to complete the setup procedures.

4.2 Windows Vista 32/64

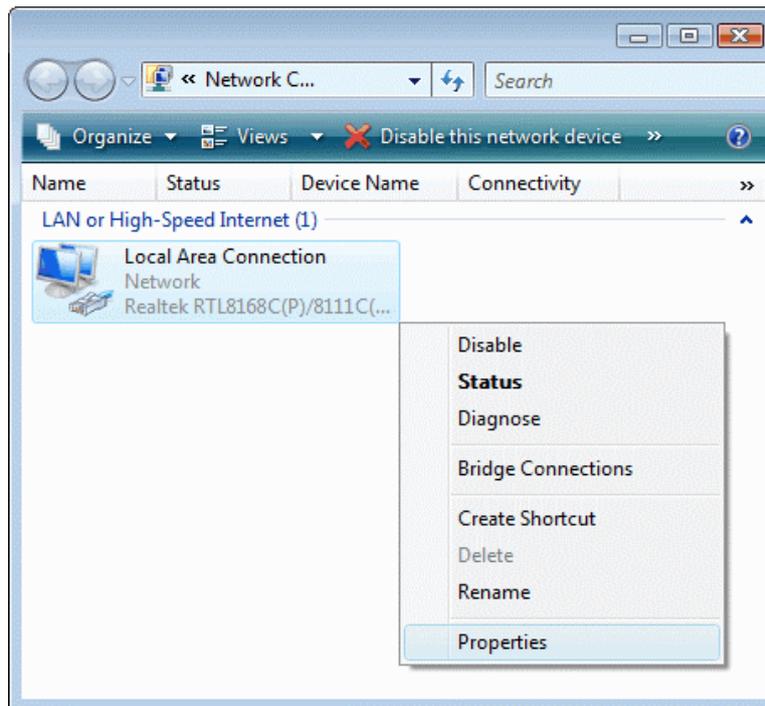
1. Click on “**Start**” > “**Control Panel**” > “**Network and Sharing Center**”.



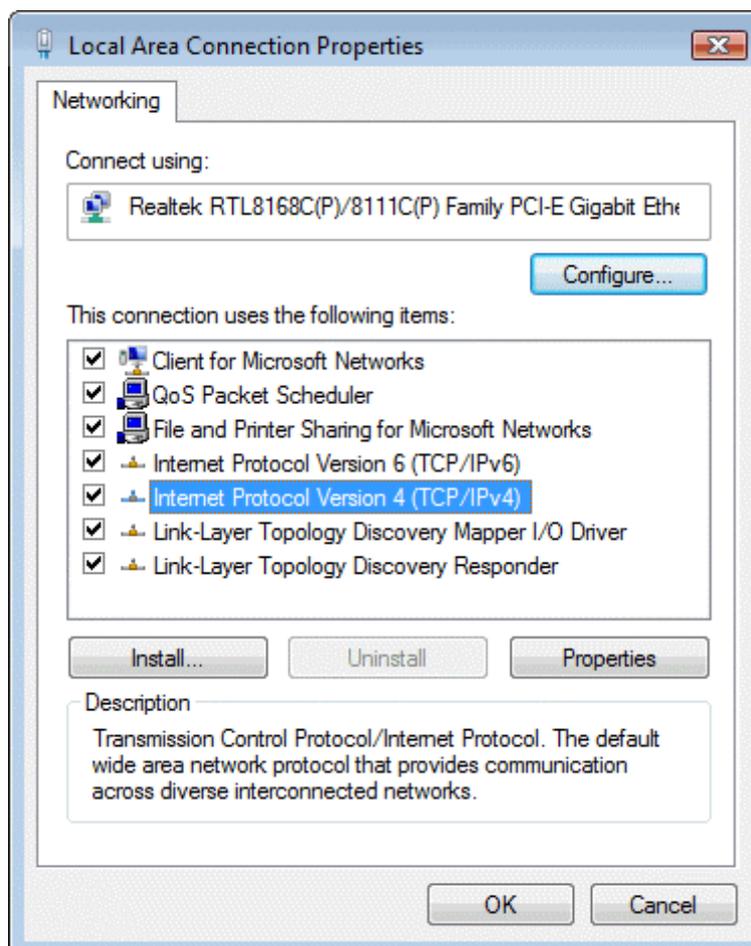
2. In the Manage network connections, click on “**Manage network connections**” to continue.



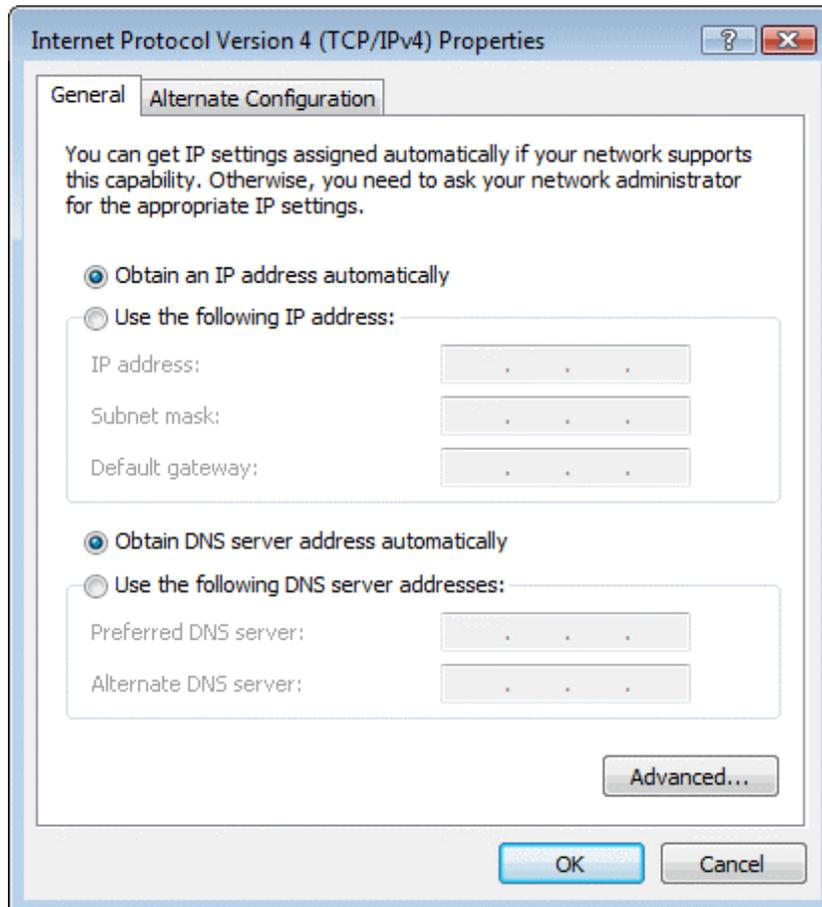
3. Single right click on “**Local Area connection**”, then click “**Properties**”.



4. The screen will display the information “**User Account Control**” and click “**Continue**” to continue.
5. Double click on “**Internet Protocol Version 4 (TCP/IPv4)**”.



6. Check **“Obtain an IP address automatically”** and **“Obtain DNS server address automatically”** then click on **“OK”** to continue.

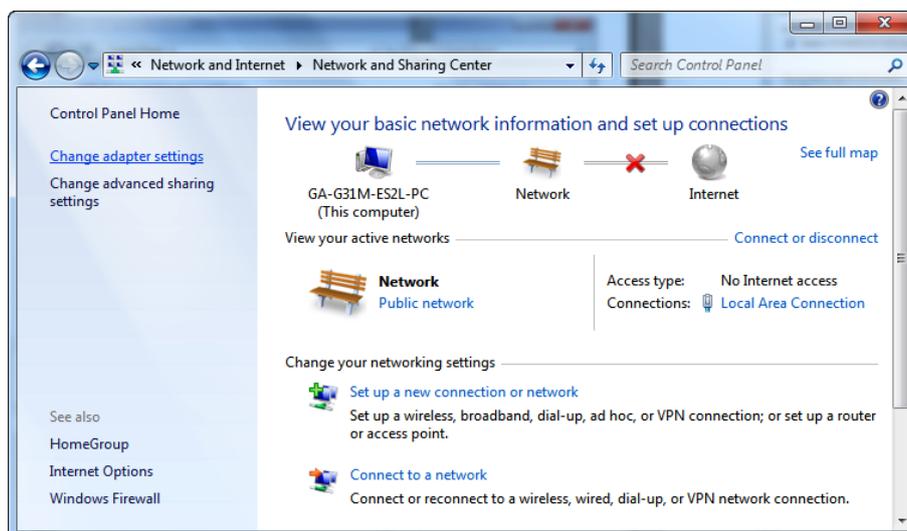


4.3 Windows 7 32/64

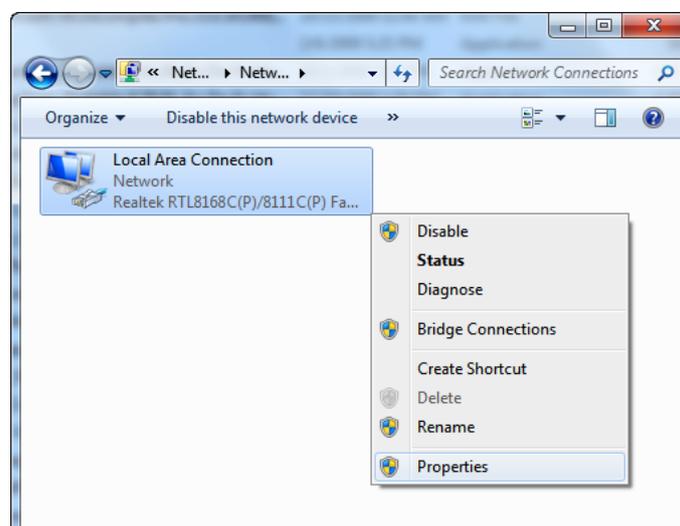
1. Click on “**Start**” > “**Control Panel**” (in **Category View**) > “**View network status and tasks**”.



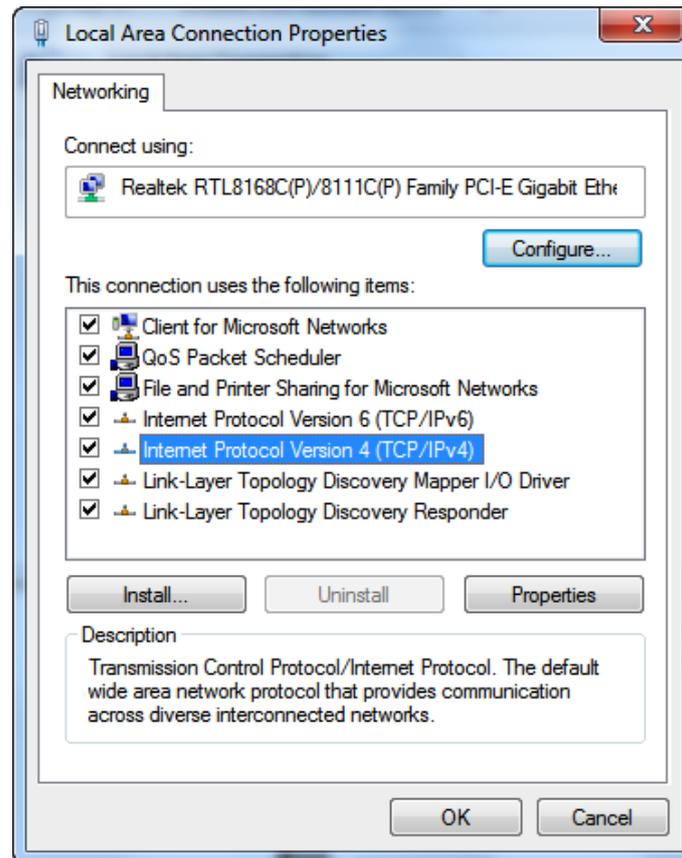
2. In the **Control Panel Home**, click on “**Change adapter settings**” to continue.



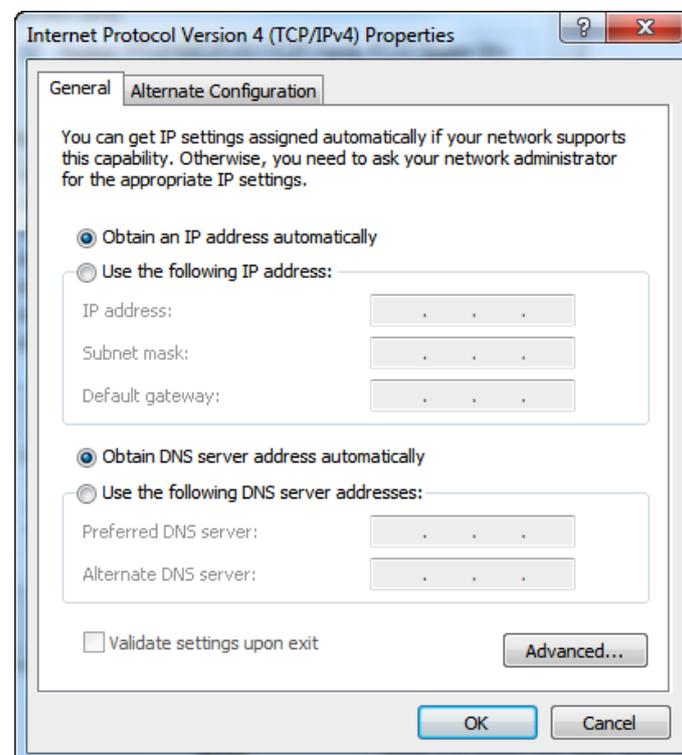
3. Single right click on “**Local Area Connection**”, then click “**Properties**”.



4. Double click on **“Internet Protocol Version 4 (TCP/IPv4)”**.



5. Check **“Obtain an IP address automatically”** and **“Obtain DNS server address automatically”** then click on **“OK”** to continue.



5. Router Configuration

1. Please insert the supplied CD into your CD-ROM drive.
2. The CD should auto-start, displaying the window shown in 3 below. If your CD does not start automatically, go to Windows Explorer, Select your CD drive and double click "autorun.exe".
3. The screen below will appear. To configure the device, please click "Easy Configuration" button and follow the steps illustrated in the following pages.



4. Enter the VPI, VCI, Username and Password your ISP (Internet Services Provider) provided, and Protocol mode. Then press "Next".

5. Please enter the “**ESSID**” and Wireless “**Default Channel**” if you want to change (the default settings **Network= Enable, ESSID = Hamlet, Default Channel=6**).
6. Choose the Encryption type if necessary, as **Off – No Encryption (Default)** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (TKIP) / Wi-Fi Protected Access2 (AES-CCMP) and WPA Mixed Mode. For example, you choose the WPA Mixed Mode type and configure Passphrase.
7. Please click “**Setup**” button, when the procedure is completed, it will start to configure the device for a while.

EASY SETUP 1.0 STANDARD

Hamlet NETWORKING WIRELESS N ADSL ROUTER

Wireless Configuration

Select the Wireless Network enable or disable.

Wireless Network :

Select the Default Channel from your Internet Service Provider (ISP), or allow to automatically select the best channel.

Default Channel :

Select the shared name that with all of Wireless PCs in your Wireless Network.

ESSID :

Select the protective encryption.

Encryption :

Select the key for Wireless Network authentication.

Passphrase :

(Passphrase should be at least 8 characters.)

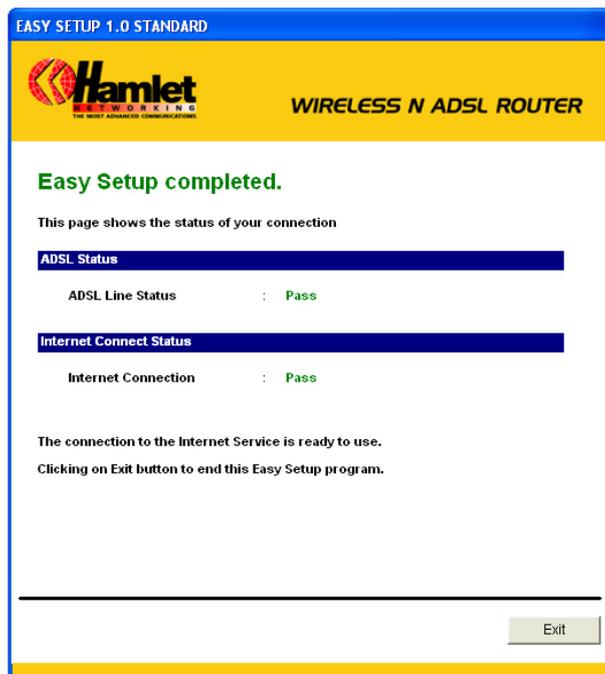
Show characters of Passphrase

8. Now, checking WLAN ADSL 2+ Router hardware connection, ADSL2+ settings, WLAN settings, and ADSL2+ Line connection status.

Setting

Checking Device connect ...

9. Easy setup configuration completed. Click on **"Exit"** to exit this program.



10. Click on **"Exit"** to exit this program.



Now, the Wireless ADSL2+ Router has been configured completely, and suitable for Wireless and Internet Connections.

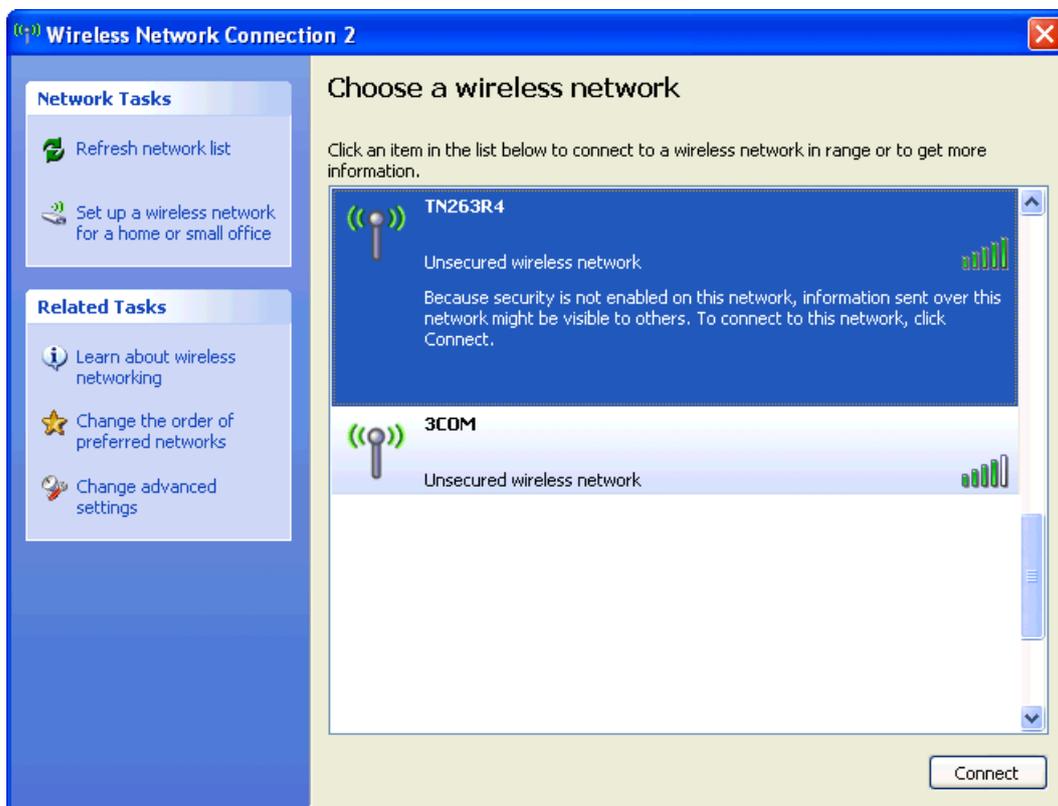
6. Connect Wirelessly

Now that the Easy configuration setup is completed, you can connect wirelessly to your Wireless ADSL2+ Router. Follow the steps below to create a new wireless connection to the Router.

1. Double click on the wireless icon on your computer and search for the wireless network that you enter **ESSID** name.



2. Click on the wireless network that you enter **ESSID** name to connect.



3. If the wireless network isn't encrypted, click on "**Connect Anyway**" to connect.



4. If the wireless network is encrypted, enter the network key that belongs to your Encryption type and Passphrase. You can later change this network key via the wireless configuration menu.



Wireless Network Connection

The network 'TN263R4' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

5. Click on "**Connect**" or "**Apply**".



Wireless Network Connection

The network 'TN263R4' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

Now, your wireless connection to the Wireless ADSL2+ Router has been configured and you are able to connect to Internet.

7. Web Configuration

The embedded web configuration allows you to manage the Router from anywhere through a common web browser such as Internet Explorer or Firefox. Please note that JavaScript must be enabled.

7.1 Accessing the Web Interface

1. Make sure your Wireless ADSL2+ Router is properly connected.
2. Prepare your computer/computer network to connect to the Router.
3. Launch your web browser and type “**192.168.1.254**” in the address bar.
4. An Enter Network Password window displays. Enter the user name (“**admin**” is the default), password (“**hamlet**” is the default) and click **OK**.



5. You should now see the **Status** page of the Router.

Hamlet Wireless N ADSL2+ Broadband Router

Status Quick Start Interface Setup Advanced Setup Access Management Maintenance Status Help

Device Info System Log Statistics

Device Information

Firmware Version : Hamlet(LEM_86_N)_A02_(211980_31261)_2M16
MAC Address : 00:13:33:8d:47:a6

LAN

IP Address : 192.168.1.254
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN

Virtual Circuit : PVC0
Status : Not Connected
Connection Type : PPPoE
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS : 0.0.0.0
Secondary DNS : 0.0.0.0
NAT : Enabled

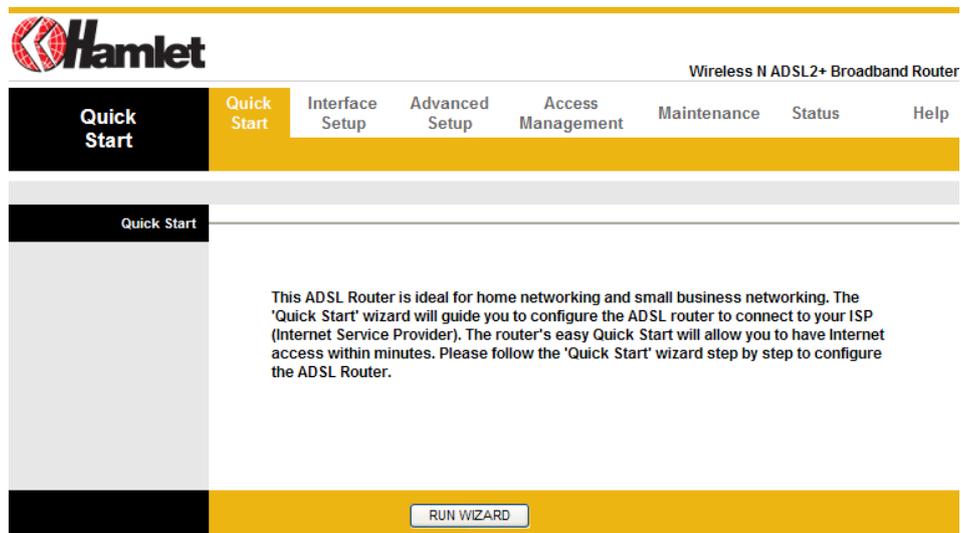
ADSL

ADSL Firmware Version : FwVer:3.12.6.1_TC3086 HwVer:T14.F7_6.0
Line State : Down
Modulation : N/A
Annex Mode : N/A

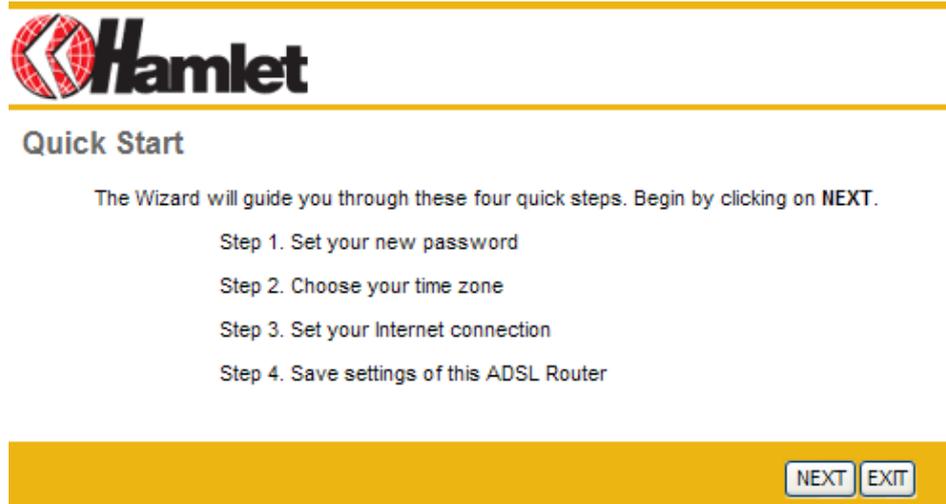
	Downstream	Upstream	
SNR Margin :	N/A	N/A	db
Line Attenuation :	N/A	N/A	db
Data Rate :	N/A	N/A	kbps

7.2 Quick Start

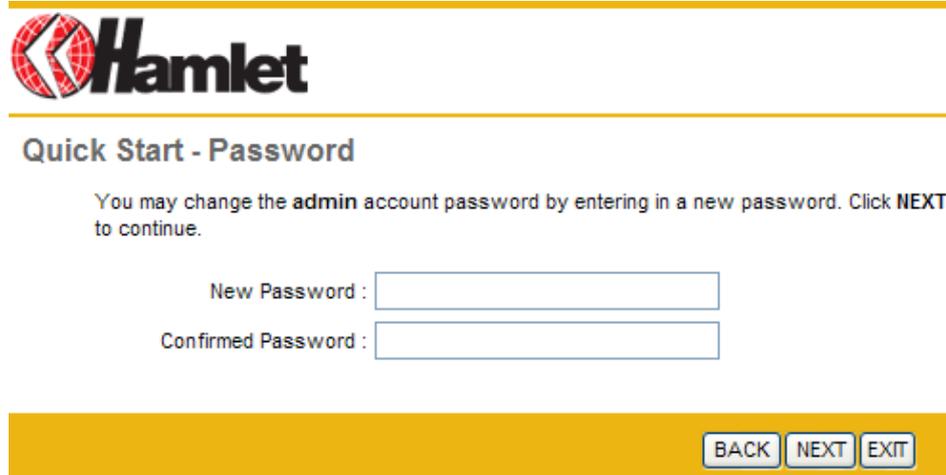
You can use “**Quick Start**” to setup the router as follows, and the router will connect to the Internet via ADSL line.



1. Click “**RUN WIZARD**” to start up this procedure.



2. Please click “**NEXT**” to setup your new administrator's password.



3. Please click **"NEXT"** to setup your time zone.



Quick Start - Time Zone

Select the appropriate time zone for your location and click **NEXT** to continue.

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▼

4. Please click **"NEXT"** to setup your Internet connection type. You can have this information from your Internet Service Provider.



Quick Start - ISP Connection Type

Select the Internet connection type to connect to your ISP. Click **NEXT** to continue.

<input type="radio"/> Dynamic IP Address	Choose this option to obtain a IP address automatically from your ISP.
<input type="radio"/> Static IP Address	Choose this option to set static IP information provided to you by your ISP.
<input checked="" type="radio"/> PPPoE/PPPoA	Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)
<input type="radio"/> Bridge Mode	Choose this option if your ISP uses Bridge Mode.

5. Enter the connection information provided by your ISP and click **"NEXT"**.



Quick Start - PPPoE/PPPoA

Enter the PPPoE/PPPoA information provided to you by your ISP. Click **NEXT** to continue.

Username:

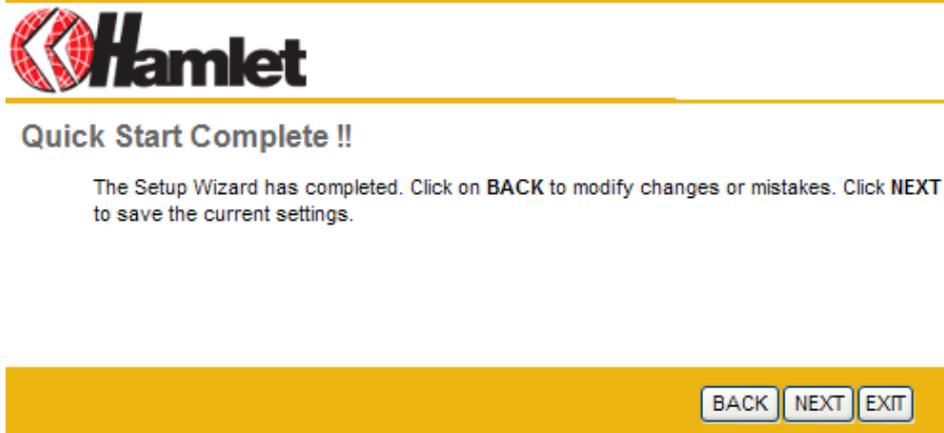
Password:

VPI: (0~255)

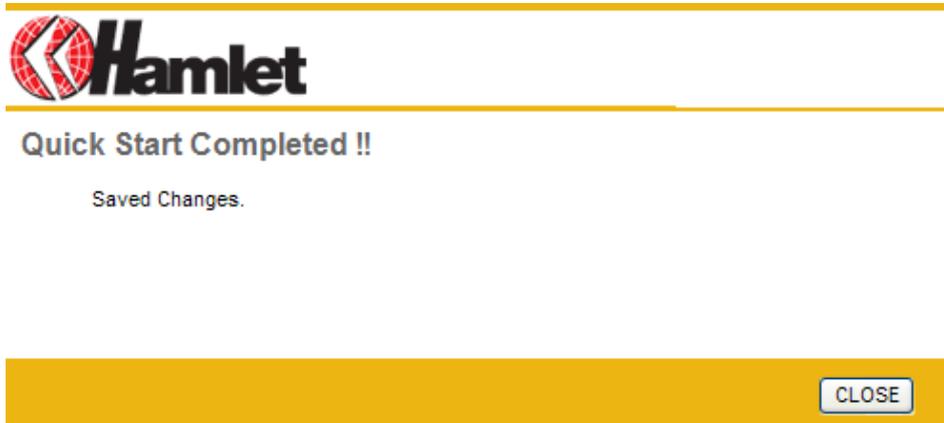
VCI: (1~65535)

Connection Type: ▼

- Click "**NEXT**" to save the current settings.



- Please click "**CLOSE**" to finish Quick Start.



7.3 Interface Setup

Internet (VC Configuration)

Go to **Interface Setup > Internet** to add or delete ADSL VC configuration. These information are provided by your ISP.

ATM VC

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI settings to you. In this Device, you can totally setup 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

- **VCI:** The valid range for the VCI is 1 to 65535. Enter the VCI assigned to you. This field may already be configured.
- **VPI:** The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.
- **Virtual Circuit:** VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
- **PVC Summary:**

Service Information Summary

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	Yes	8	35	PPPoE	LLC	Dynamic	Idle
PVC1	No	0	34	RFC 1483	LLC	-	N/A
PVC2	No	0	35	RFC 1483	LLC	-	N/A
PVC3	No	0	36	RFC 1483	LLC	-	N/A
PVC4	No	0	37	RFC 1483	LLC	-	N/A
PVC5	No	0	38	RFC 1483	LLC	-	N/A
PVC6	No	0	39	RFC 1483	LLC	-	N/A
PVC7	No	0	40	RFC 1483	LLC	-	N/A

- **ATM QoS:** Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR (Constant Bit Rate), VBR (Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS. Select CBR to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Select VBR for burst traffic and bandwidth sharing with other applications.
- **PCR:** Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.
- **SCR:** The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.
- **MBS:** Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535

The screenshot shows the configuration interface for the router, divided into four main sections:

- Encapsulation:** Contains radio buttons for 'ISP' selection: Dynamic IP Address, Static IP Address, PPPoA/PPPoE (selected), and Bridge Mode.
- PPPoE/PPPoA:** Includes input fields for 'Servicename', 'Username' (admin), and 'Password' (masked with dots). It also has a dropdown for 'Encapsulation' (PPPoE LLC) and radio buttons for 'Bridge Interface' (Activated/Deactivated).
- Connection Setting:** Features radio buttons for 'Connection' type: Always On (Recommended) (selected), Connect On-Demand (with a 'minutes' field), and Connect Manually. It also has a 'TCP MSS Option' field set to 0 bytes.
- IP Address:** Contains radio buttons for 'Get IP Address' (Static/Dynamic). It has input fields for 'Static IP Address', 'IP Subnet Mask', and 'Gateway', all set to 0.0.0.0. It also includes a 'NAT' dropdown (Enable), 'Default Route' radio buttons (Yes/No), 'TCP MTU Option' field (0 bytes), 'Dynamic Route' dropdown (RIP1), 'Direction' dropdown (Both), 'Multicast' dropdown (Disabled), and 'MAC Spoofing' radio buttons (Enabled/Disabled) with a MAC address field (00:00:00:00:00:00).

A yellow bar at the bottom contains a 'SAVE' button.

Encapsulation

- **ISP:** Select the encapsulation type your ISP uses from the Encapsulation list. Choices vary depending on what you select in the Mode field.

Dynamic IP: Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

Static IP: Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

PPPoE/PPPoA: Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

Bridge Mode: Bridge mode is a common connection method used for xDSL modem.

PPPoE/PPPoA

- **User Name:** Enter the user name exactly as your ISP assigned.
- **Password:** Enter the password associated with the user name above.
- **Encapsulation:** select Bridge in the Mode field, select either PPPoA or RFC 1483. select Routing in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE. Multiplex: Select the method of multiplexing used by your ISP. Choices are VC or LLC.
- **Bridge interface:** The Bridge mode can only be used when a single IP address has been assigned by the ISP. It is used when the use of NAT is not desired and there is a single computer attached to the router.
- **Connection:** The schedule rule(s) have priority over your Connection settings.
- Always on:** Select Always on Connection when you want your connection up all the time.
- Connect on Demand:** Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
- **TCP MSS Option:** Enter the TCP Maximum Segment Size (MSS)
- **Get IP Address:** Choose Static or Dynamic
- **Static IP Address:** Enter the IP address of ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).
- **IP Subnet Mask:** The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the

subnet mask assigned to you by your ISP (if given).

- **Gateway:** You must specify a gateway IP address (supplied by your ISP) when you use 1483 Bridged IP in the Encapsulation field in the previous screen.

- **NAT:** Select this option to Activate/Deactivated the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis

- **Default Route:** if enable this function, the current PVC will be the default gateway to internet from this device

- **TCP MTU Option:** Enter the TCP maximum transmission unit (MTU)

- **Dynamic Route:** The dynamic routing feature of the router can be used to allow the router to automatically adjust to physical changes in the network's layout. The router uses the dynamic RIP protocol. It determines the route that the network packets take based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2M and RIP-2B. RIP-2M and RIP-2B are both sent in RIP-2 format; the difference is that RIP-2M using Multicast and RIP-2 using Broadcast format

- **RIP Direction:** Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. IN only means the ADLS router will only accept but will not send RIP packet. OUT only means the ADLS router will only send but will not accept RIP packet.

- **Multicast:** IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. The Hamlet HRDSL150W supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it.

LAN (DHCP and DNS)

Go to **Interface > LAN** to enable DHCP server. Then you can set DNS server for the router. A Domain Name system (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, a DNS server will find that name in its index and find the matching IP address.

Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP addresses are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address below.

Router Local IP

- **IP Address:** Enter the IP address of ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).
- **IP Subnet Mask:** The default is 255.255.255.0. User can change it to other such as 255.255.255.128.
- **Dynamic Route:** Select the RIP version from RIP-1, RIP-2B and RIP-2M.
- **RIP Direction:** Select the RIP direction from None, Both, In Only and Out Only.
- **Multicast:** IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. The Hamlet HRDSL150W supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it
- **IGMP Snoop:** Choose Disable or Enable IGMP Snoop function.

DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server.

- **DHCP:** If set to **Enable**, your Hamlet HRDSL150W can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **disabled**, the DHCP server will be disabled.

If set to **Relay**, the Hamlet HRDSL150W acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.

When DHCP is used, the following items need to be set.

- **Starting IP Address:** This field specifies the first of the contiguous addresses in the IP address pool.

- **IP Pool Count:** This field specifies the size or count of the IP address pool.
- **Lease Time:** The current lease time of client.
- **Primary DNS Server:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
- **Secondary DNS Server:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Wireless Settings

This section introduces the Wireless LAN and some basic configurations. Go to **Interface > Wireless** to setup the wireless parameters.

Hamlet Wireless N ADSL2+ Broadband Router

Interface | Quick Start | **Interface Setup** | Advanced Setup | Access Management | Maintenance | Status | Help

Internet | LAN | **Wireless**

Access Point Settings

Access Point : Activated Deactivated

Channel : 09 Current Channel: 9

Beacon Interval(ms) : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold (bytes) : 2346 (range: 256~2346, even numbers only)

DTIM(ms) : 1 (range: 1~255)

Wireless Mode : 802.11b+g+n

11n Settings

Channel Bandwidth : 20/40 MHz

Extension Channel : below the control channel

Guard Interval : AUTO

MCS : AUTO

Multiple SSIDs Settings

SSID Index : 1

Broadcast SSID : Yes No

Use WPS : Yes No

WPS Settings

WPS state : Unconfigured

WPS mode : PIN code PBC

WPS progress : Idle

SSID : TN263R4

Authentication Type : Disabled

WDS Settings

WDS Mode : On Off

Mac Address #1 : 00:00:00:00:00:00

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

Mac Address #4 : 00:00:00:00:00:00

Wireless MAC Address Filter

Active : Activated Deactivated

Action : Deny Association the follow Wireless LAN station(s) association.

Mac Address #1 : 00:00:00:00:00:00

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

Mac Address #4 : 00:00:00:00:00:00

Mac Address #5 : 00:00:00:00:00:00

Mac Address #6 : 00:00:00:00:00:00

Mac Address #7 : 00:00:00:00:00:00

Mac Address #8 : 00:00:00:00:00:00

Access Point Settings

The screenshot shows the configuration interface for the router. It is divided into two main sections: 'Access Point Settings' and '11n Settings'. The 'Access Point Settings' section includes:

- Access Point: Activated Deactivated
- Channel: 09 (Current Channel: 9)
- Beacon Interval(ms): 100 (range: 20~1000)
- RTS/CTS Threshold: 2347 (range: 1500~2347)
- Fragmentation Threshold (bytes): 2346 (range: 256~2346, even numbers only)
- DTIM(ms): 1 (range: 1~255)
- Wireless Mode: 802.11b+g+n

 The '11n Settings' section includes:

- Channel Bandwidth: 20/40 MHz
- Extension Channel: below the control channel
- Guard Interval: AUTO
- MCS: AUTO

- **Access Point:** Default setting is set to **Activated**. If you do not have any wireless, both 802.11g, 802.11b and 802.11n, device in your network, select **Deactivated**.
- **Channel ID:** The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select a channel from the drop-down list box.
- **Beacon interval:** The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.
- **RTS/CTS Threshold:** The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake Enter a value between 1500 and 2347..
- **Fragmentation Threshold:** The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
- **DTM:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).
- **Wireless Mode:** The default setting is **802.11b+g+n** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b and if you only have 802.11n then select 802.11n.

11n Settings

- **Channel Bandwidth:** Select either 20 MHz or 20/40 MHz for the channel bandwidth. The higher the bandwidth the better the performance will be.
- **Guard Interval:** Select either 400nsec or 800nsec for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other, it also prevents propagation delays, echoing and reflections.
- **MCS:** There are options 0~15 and AUTO to select for the **Modulation and Coding Scheme**. We recommend users selecting AUTO.

SSIDs Settings

Multiple SSIDs Settings

SSID Index : 1

Broadcast SSID : Yes No

Use WPS : Yes No

- **SSID Index:** Default SSID index is “1”.
- **SSID:** The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default **wlan-ap** to a unique ID name to the AP which is already built-in to the router’s wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.
- **Broadcast SSID:** Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning. Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning.
- **Use WPS:** Select **Yes** to use WPS function.

WPS Settings

WPS (Wi-Fi Protected Setup) provides a convenient way to establish the connection between this broadband router and wireless clients. Any WPS-compatible wireless clients can establish secure connection with this router with simple push-button type configuration or Pin Code type configuration.

WPS Settings

Wireless MAC Address Filter

WPS state : Configured

WPS mode : PIN code PBC

Start WPS

WPS progress : Idle

Reset to OOB

SSID : TN263R4

Authentication Type : Disabled

Active : WEP-64Bits

Action : WPA-PSK

Mac Address #1 : WPA-PSK/WPA2-PSK

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

- **WPS State:** Displays whether the WPS is **configured** or **unconfigured**.
- **WPS Mode:** Select the mode which to start WPS, choose between **PIN Code** or **PBC** (Push Button). Selecting **Pin Code** mode will require you to know the enrollee PIN code.
- **WPS Progress:** Shows the current progress status of WPS.
- **SSID:** Type in the Service Set Identifier name, it is the unique name of a wireless access point (AP) to be distinguished from another.
- **Authentication Type:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP.&WPA. If you require high security for transmissions, there are four alternatives to select from: **WEP-64Bits**, **WEP-128Bits**, **WPA-PSK**, **WPA2-PSK** and **WPA-PSK/WPA2-PSK**. WEP 128 offers increased security over WEP 64. You can disable or enable with WPA or WEP for protecting wireless network. The default type of wireless is **disabled** and to allow all wireless computers to communicate with the access points without any data encryption.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

WDS Settings	
WDS Mode :	<input type="radio"/> On <input checked="" type="radio"/> Off
Mac Address #1 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #2 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #3 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #4 :	<input type="text" value="00:00:00:00:00:00"/>

- **WDS Mode:** Check this box to enable WDS function, uncheck it to disable WDS.
- **Mac Address #1-4:** Configure up to four MAC Address of peer Access point to do WDS.

Wireless MAC Address Filter

For security reason, using MAC Wireless MAC Address Filter creates another level of difficulty to hacking a network. A Wireless MAC Address Filter is created and distributed to AP so that only authorized NIC's can connect to the network. While MAC address spoofing is a proven means to hacking a network this can be used in conjunction with additional security measures to increase the level of complexity of the network security decreasing the chance of a breach.

MAC addresses can be add/delete/edit from the Wireless MAC Address Filter list depending on the MAC Access Policy.

If you choose 'Allow Association', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Association' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless MAC Address Filter	
Active :	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Action :	Deny Association <input type="button" value="v"/> the follow Wireless LAN station(s) association.
Mac Address #1 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #2 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #3 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #4 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #5 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #6 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #7 :	<input type="text" value="00:00:00:00:00:00"/>
Mac Address #8 :	<input type="text" value="00:00:00:00:00:00"/>

- **Active:** Check this box to enable Wireless MAC Address Filter, uncheck it to disable Wireless MAC Address Filter.
- **Action:** To Allow or Deny Association
- **Mac Address #1-8:** Configure up to 8 MAC Address of Wireless Client.

7.4 Advanced Setup

Firewall

Go to **Advanced Setup > Firewall** to setup Firewall features. Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

Wireless N ADSL2+ Broadband Router

Advanced Setup

Firewall

Firewall: Enabled Disabled

SPI: Enabled Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

SAVE CANCEL

- **Firewall:**
 - ⊙ **Enabled:** As set in default setting, it activates your firewall function.
 - ⊙ **Disabled:** It disables the firewall function.
- **SPI:**
 - ⊙ **Enabled:** As set in default setting, it activates your SPI function.
 - ⊙ **Disabled:** It disables the SPI function.

Routing

Go to **Advanced Setup > Routing** to see the Routing Table. The Routing table allows you to see how many routings on your routing table and interface information.

Wireless N ADSL2+ Broadband Router

Advanced Setup

Routing Table List

#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.254	1	enet0	2441		
2	default	0	Node1	2	Idle	53		

ADD ROUTE

Routing Table List

- **#:** Item number
- **Dest IP:** IP address of the destination network
- **Mask:** The destination mask address.
- **Gateway IP:** IP address of the gateway or existing interface that this route uses.
- **Metric:** It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.
- **Device:** Media/channel selected to append the route.
- **Use:** Counter for access times.
- **Edit:** Edit the route; this icon is not shown for system default route.
- **Drop:** Drop the route; this icon is not shown for system default route.

Static Route

To add a new static route, press the **ADD ROUTE** button.

The static routing function determines the path that router follows over your network before and after it passes through your router. You can use static routing to allow different IP domain users to access the Internet through this device.

The screenshot shows the 'Static Route' configuration page. The navigation menu includes 'Advanced' (selected), 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Advanced Setup', there are sub-menus for 'Firewall', 'Routing', 'NAT', 'QoS', 'VLAN', and 'ADSL'. The 'Static Route' section contains the following fields:

- Destination IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
- Gateway IP Address: 0.0.0.0 (with a dropdown menu set to PVC0)
- Metric: 0
- Announced in RIP: Yes

At the bottom, there are buttons for 'SAVE', 'DELETE', 'BACK', and 'CANCEL'.

- **Destination IP Address:** This is the destination subnet IP address.
- **IP Subnet Mask:** It is the destination IP addresses based on above destination subnet IP.
- **Gateway IP Address:** This is the gateway IP address to which packets are to be forwarded.
- **Metric:** It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.
- **Announced in RIP:** This parameter determines if the Prestige will include the route to the remote node in its RIP broadcasts. Set "No", it is kept private and is not included in RIP broadcasts. Set "Yes", the remote node will be propagated to other hosts through RIP broadcasts.

NAT

Go to **Advanced Setup>NAT** to setup the NAT features. Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

The screenshot shows the 'NAT' configuration page. The navigation menu is the same as in the Static Route page. The 'NAT' section contains the following fields and options:

- Virtual Circuit: PVC0 (dropdown menu)
- NAT Status: Activated
- Number of IPs: Single (radio button), Multiple (radio button, selected)
- DMZ (with a right-pointing arrow)
- Virtual Server (with a right-pointing arrow)
- IP Address Mapping (for Multiple IP Service) (with a right-pointing arrow)

- **Virtual Circuit:** VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. There are eight groups of PVC can be defined and used.
- **NAT Status:** Show the NAT status, Activated or Deactivated.
- **Number of IPs:** User can select Single or Multiple.

DMZ

Go to **Advanced Setup > NAT > DMZ** to set DMZ parameters. If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a virtual DMZ Host.

- **DMZ setting for:** Show the PVC that DMZ will be applied for.
- **DMZ:** Select **Enabled/Disabled** radio button to enable or disable DMZ function.
- **DMZ Host IP Address:** Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet. Select the **SAVE** button to apply your changes.

Virtual Server (Port Mapping)

Go to **Advanced Setup > NAT > Virtual Server** to set virtual server as you need. You can configure the router as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port numbers), the router redirects the external service request to the appropriate server (located at another internal IP address). For some applications, you need to assign a set or a range of ports (example 4000-5000) to a specified local machine to route the packets. The router allows the user to configure the needed port mappings to suit such applications.

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

- **Rule Index:** Choose the rule number.
- **Application:** Choose the predefined rule from Application drop-down menu or enter a custom name.
- **Protocol:** Choose the Protocol Type, ALL, TCP or UDP.
- **Local IP Address:** Enter your server IP address in this field.
- **Start Port Number:** Enter a port number in this field.
- **End Port Number:** Enter a port number in this field.

IP Address Mapping (for Multiple IPs)

IP Address Mapping

Address Mapping Rule : PVC0

Rule Index :

Rule Type :

Local Start IP :

Local End IP :

Public Start IP : (0.0.0.0 for modem's WAN IP)

Public End IP :

Address Mapping List

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

- **Address Mapping Rule:** Shows the PVC where the rule will be applied to
- **Rule Index:** Choose the rule number.
- **Rule Type:**
 - ⊙ One-to-one: This is the mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.
 - ⊙ Many-to-One: This is the mode maps multiple local IP addresses to one global IP address. This is equivalent to Many to One (i.e., PAT, port address translation).
 - ⊙ Many-to-Many Overload: This mode maps multiple local IP addresses to shared global IP addresses.
 - ⊙ Many-to-Many No Overload: This mode maps each local IP address to an unique global IP addresses.
 - ⊙ Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
- **Local Start IP:** This is the starting range for Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.
- **Local End IP:** This is the end range for Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.
- **Public Start IP:** This is the start range for Inside Public IP Address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
- **Public End IP:** This is the end range for Inside Public IP Address. This field is N/A for One-to-one, Many-to-One and Server mapping types.

NOTE: Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention: If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid. If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

QoS

Go to **Advanced Setup > QoS** to setup QoS features.

Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.

The main goal of QoS is prioritizing incoming data, preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on **Add** to save your changes.

Click on **QoS Settings Summary** to view the list of QoS rules that have been added.

Rule

- **Rule Index:** Select 16 different rules, each rule's detail can be set and saved.
- **Active:** Select QoS is activated or deactivated.
- **Application:** Select 11 different applications: IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP, RTP.
- **Physical Ports:** Once you select the application, the associated ports will be displayed.
- **Destination MAC:** Set the Ethernet MAC value that you want to filter in destination side.
- **Destination IP:** Set the IP address value that you want to filter in destination side.
- **Destination Mask:** Set the subnet mask value that you want to filter in destination side.
- **Destination Port Range:** Set the port range value that you want to filter in destination side.
- **Source MAC:** Set the Ethernet MAC value that you want to filter in source side.
- **Source IP:** Set the IP address value that you want to filter in source side.
- **Source Mask:** Set the subnet mask value that you want to filter in source side.
- **Source Port Range:** Set the port range value that you want to filter in source side.
- **Protocol ID:** Set the protocol ID type that you want to filter.
- **Vlan ID Range:** Set the Vlan value that you want to filter.
- **IPP/DS Field:** Select IP QoS format.
- **IP Precedence Range:** Select the IP precedence range.
- **Type of Service:** Select 5 different type of service.
- **DSCP Range:** Set the DSCP value that you want to filter.
- **802.1p:** Set the remarked new 802.1p priority value on the packet that fulfill every detail setting condition of each rule.

Action

After finishing all rules detail condition setting, select the rule you want to execute and action here.

- **IPP/DS Field:** Select IP QoS format.
- **IP Precedence Remarking:** Select the remarking value of IP precedence.
- **Type of service Remarking:** Select the remarking value of type of service.
- **DSCP Remarking:** Select the remarking value of DSCP.
- **802.1p Remarking:** Select the remarking value of 802.1p.
- **Queue #:** Select four types of Queue: Low, Medium, High, Highest.

VLAN

Go to **Advanced Setup > VLAN** to enable VLAN features. Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

VLAN PVID Assign

Go to **Advanced Setup > VLAN > Assign VLAN PVID for each interface** to setup VLAN PVID features. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

VLAN Group Setting

Go to **Advanced Setup > VLAN > Define VLAN Group** to setup VLAN group features.

VLAN Group Setting

VLAN Index :

Active : Yes No

VLAN ID : (Decimal)

Tagged

ATM VCs :

Port #

0 1 2 3 4 5 6 7

Ethernet :

Port #

1 2 3 4

Wireless LAN :

Port #

0

VLAN Group Summary

Group	Active	ID	VLAN Group Ports	VLAN Tagged Ports
1	Yes	1	e1,e2,e3,e4,w,p0,p1,p2,p3,p4,p5,p6,p7	

p:pvc, e:ethernet, and w:wlan

ADSL

Go to **Advanced Setup > ADSL** to configure ADSL.

Wireless N ADSL2+ Broadband Router

Advanced

Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help

Firewall
Routing
NAT
QoS
VLAN
ADSL

ADSL

ADSL Mode:

ADSL Type:

- **ADSL Mode:** The default setting is **Auto Sync-UP**. This mode will automatically detect your ADSL, ADSL2, ADSL2+, G.dmt, G.lite, and T1.413. But in some area, multimode cannot detect the ADSL line code well. If it is the case, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.
- **ADSL Type:** There are five modes "Open Annex Type and Follow DSLAM's Setting", "Annex A", "Annex I", "Annex A/L", "Annex M" and "Annex A/I/L/M" that user can select for this connection.

7.5 Access Management

ACL

Go to **Access Management > ACL** to setup Access Control Listing. ACL allows you to determine which services/protocols can access Hamlet HRDSL150W interface from which computers.

Wireless N ADSL2+ Broadband Router

Access Management | Quick Start | Interface Setup | Advanced Setup | **Access Management** | Maintenance | Status | Help

ACL | Filter | SNMP | UPlP | DDNS | CWMP

Access Control Setup

ACL : Activated Deactivated

Access Control Editing

ACL Rule Index : 1

Active : Yes No

Secure IP Address : 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application : Web

Interface : Both

Access Control Listing

Index	Active	Secure IP Address	Application	Interface

SAVE DELETE CANCEL

- **ACL Rule Index:** This is item number.
- **Secure IP Address:** The default 0.0.0.0 allows any client to use this service to remotely manage the Router. Type an IP address to restrict access to a client with a matching IP address.
- **Application:** Choose a service that you may use to remotely manage the Hamlet HRDSL150W.
- **Interface:** Select the access interface. Choices are **LAN**, **WAN** and **Both**.

IP Filtering

Go to **Access Management > Filter** to block some packets from WAN. The router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. The user can set different IP filter rules of a given protocol (TCP, UDP or ICMP) and a specific direction (incoming, outgoing, or both) to filter the packets.

Hamlet Wireless N ADSL2+ Broadband Router

Access Management | Quick Start | Interface Setup | Advanced Setup | **Access Management** | Maintenance | Status | Help

ACL | Filter | SNMP | UPnP | DDNS | CWMP

Filter

Filter Type

Filter Type Selection: IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index: 1
Interface: PVC0
Direction: Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index: 1
Rule Type: IP
Active: Yes No

Source IP Address: (0.0.0.0 means Don't care)
Subnet Mask:
Port Number: 0 (0 means Don't care)

Destination IP Address: (0.0.0.0 means Don't care)
Subnet Mask:
Port Number: 0 (0 means Don't care)

Protocol: TCP
Rule Unmatched: Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index: 1

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE DELETE CANCEL

Filter Type

- **Filter Type Selection:** There are three types of filter "IP/MAC Filter", "Application Filter", and "URL Filter" that user can select for this connection.

IP/MAC Filter Set Editing

- **IP/MAC filter Set Index:** This is item number.
- **Interface:** Select which channel (PVC) to configure.
- **Direction:** Select the access to the Internet ("Outgoing") or from the Internet ("Incoming") or **Both**.

IP/MAC Filter Rule Editing

- **IP/MAC Filter Rule Index:** This is item number.
- **Rule Type:** Choose "IP" or "MAC" rules.
- **Active:** Select **Yes** from the drop down list box to enable IP filter rule.
- **Source IP Address:** The source IP address or range of packets to be monitored.

- **Subnet Mask:** It is the source IP addresses based on above source subnet IP.
- **Source Port Number:** This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.
- **Destination IP Address:** This is the destination subnet IP address.
- **Subnet Mask:** It is the destination IP addresses based on above destination subnet IP.
- **Destination Port Number:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**
- **Rule Unmatched:** Select action for the traffic unmatching current rule; Forward to leave it pass through, and NEXT to check it by the next rule.

IP/MAC Filter Listing

- #: Item number.
- **Active:** Whether the connection is currently active.
- **Src IP Mask:** The source IP address or range of packets to be monitored.
- **Dest IP Mask:** This is the destination subnet IP address.
- **Src port:** This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.
- **Dest Port:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**
- **Unmatched:** It show this profile's setting :Forward or NEXT

Application Filter

Application Filtering is a technique used to filter or block certain network traffic by the application types.

The screenshot shows the Hamlet router's web interface. The main navigation bar includes 'Access Management', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-menus for 'ACL', 'Filter', 'SNMP', 'UPnP', 'DDNS', and 'CWMP'. The 'Filter' sub-menu is selected. The 'Filter Type' section shows 'Filter Type Selection' set to 'Application Filter'. The 'Application Filter Editing' section has 'Application Filter' set to 'Deactivated' (radio button selected). Below this, there are four rows of radio buttons for 'ICQ', 'MSN', 'YMSG', and 'Real Audio/Video', each with 'Allow' and 'Deny' options. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

- **Application Filter:** Select this option to Activated/Deactivated the Application filter.
- **ICQ:** Select this option to Allow/Deny ICQ.
- **MSN:** Select this option to Allow/Deny MSN.
- **YMSG:** Select this option to Allow/Deny Yahoo messenger.
- **Real Audio/Video:** Select this option to Allow/Deny Real Audio/Video.

URL Filter

URL filtering is a feature that prevents users from accessing Websites based on information contained in a URL list. You can maintain a local URL list on the router.

Wireless N ADSL2+ Broadband Router

Access Management | Quick Start | Interface Setup | Advanced Setup | Access Management | Maintenance | Status | Help

ACL | Filter | SNMP | UPnP | DDNS | CWMP

Filter

Filter Type

Filter Type Selection : URL Filter

URL Filter Editing

Active : Yes No

URL Index : 1

URL :

URL Filter Listing

Index	URL
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

SAVE DELETE CANCEL

- **Active:** Select **Yes** to enable URL Filter.
- **URL Index:** This is item number.
- **URL:** Allow you to prevent users on your network from accessing particular websites by their URL.

SNMP

Go to **Access Management > SNMP** to setup SNMP feature Simple Network Management Protocol is used for exchanging management information between network devices.

- **Get Community:** Select to set the password for the incoming Get and GetNext requests from the management station.
- **Set Community:** Select to set the password for incoming Set requests from the management station.

UPnP

Go to **Access Management > UPnP** to setup Universal Plug-and-Play feature. Please refer to chapter 8 of this manual to setup and configure this function.

- **UPnP:** Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering Router's IP address (although you must still enter the password to access the web configuration).
- **Auto configured:** Select this check box to allow UPnP-enabled applications to automatically configure the Router so that they can communicate through the Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Click **SAVE** button to save your settings.

DDNS

Go to **Access Management > DDNS** to setup your Dynamic DNS parameters.

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your Internet Service Provider.

The screenshot shows the Hamlet router's web interface. At the top left is the Hamlet logo. The page title is "Wireless N ADSL2+ Broadband Router". A navigation menu includes "Access Management", "Quick Start", "Interface Setup", "Advanced Setup", "Access Management", "Maintenance", "Status", and "Help". Under "Access Management", there are sub-menus for "ACL", "Filter", "SNMP", "UPnP", "DDNS", and "CWMP". The "DDNS" sub-menu is active, showing the "Dynamic DNS" configuration page. The page has a left sidebar with "Dynamic DNS" selected. The main content area contains the following settings:

- Dynamic DNS : Activated Deactivated
- Service Provider : www.dyndns.org
- My Host Name :
- E-mail Address :
- Username :
- Password :
- Wildcard support : Yes No

A "SAVE" button is located at the bottom of the configuration area.

- **Dynamic DNS:** Select this check box to use Dynamic DNS.
- **Service Provider:** www.dyndns.org
- **My Host Name:** Type the domain name assigned to your Hamlet HRDSL150W by your Dynamic DNS provider.
- **E-mail Address:** Type your e-mail address.
- **Username:** Type your user name.
- **Password:** Type the password assigned to you.
- **Wildcard support:** Select this check box to enable DDNS Wildcard.

CWMP (TR-069 function)

Go to **Access Management > CWMP** to setup CWMP parameters.

TR-069 (short for Technical Report 069) is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

The screenshot shows the Hamlet router's web interface. The top navigation bar includes 'Access Management' (selected), 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-menus for 'ACL', 'Filter', 'SNMP', 'UPnP', 'DDNS', and 'CWMP'. The 'CWMP Setup' page is displayed, featuring a sidebar with 'CWMP Setup', 'Login ACS', 'Connection Request', and 'Periodic Inform'. The main content area contains the following configuration options:

- CWMP:** Activated Deactivated
- Login ACS:**
 - URL:
 - User Name:
 - Password:
- Connection Request:**
 - Path:
 - Port:
 - UserName:
 - Password:
- Periodic Inform:**
 - Periodic Inform: Activated Deactivated
 - Interval(s):

At the bottom of the page, there are 'SAVE' and 'CANCEL' buttons.

- **CWMP:** Enable or Disable TR069 function.
- **URL:** Type ACS server's URL.
- **User Name:** Type ACS server login username
- **Password:** Type ACS server login password
- **Path:** Type the path for Connection request
- **Port:** Type the port for Connection request
- **Username:** Type username for ACS server to make connection request
- **Password:** Type password for ACS server to make connection request
- **Periodic inform:** Enable or Disable Periodic inform
- **Interval:** interval time of Periodic inform (unit second).

7.6 Maintenance

Administration

Go to **Maintenance > Administration** to set a new username and password to restrict management access to the router. The default for Username and Password are **admin** and **hamlet**.

- **New Password:** Type the new password in this field
- **Confirm Password:** Type the new password again in this field.

Time Zone

Go to **Maintenance > Time Zone** and select system time as you wish.

Connecting to a Simple Network Time Protocol (SNTP) server allows the router to synchronize the system clock to the global Internet. The synchronized clock in the router is used to record the security log and control client filtering.

- **Synchronize time with:** Select the time service protocol that your time server sends when you turn on the Router.
- **Time Zone:** Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
- **Daylight Saving:** Select this option if you use daylight savings time
- **NTP Server Address:** Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Firmware

Go to **Maintenance > Firmware** to upgrade the firmware. The new firmware for your router can improve functionality and performance.

Enter the path and name of the upgrade file then click the **UPGRADE** button below. You will be prompted to confirm the upgrade.

When the upgrade process is completed, go to **Maintenance > SysRestart**, select the "Factory Default Settings" radio button and click **RESTART** to reboot the router with the new firmware settings.

Hamlet Wireless N ADSL2+ Broadband Router

Maintenance | Quick Start | Interface Setup | Advanced Setup | Access Management | **Maintenance** | Status | Help

Administration | Time Zone | Firmware | SysRestart | Diagnostics

Firmware/Romfile Upgrade

Current Firmware Version : Hamlet(LEM_86_N)_A02_(211980_31261)_2M16

New Firmware Location :

New Romfile Location :

Romfile Backup :

Status :

! It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

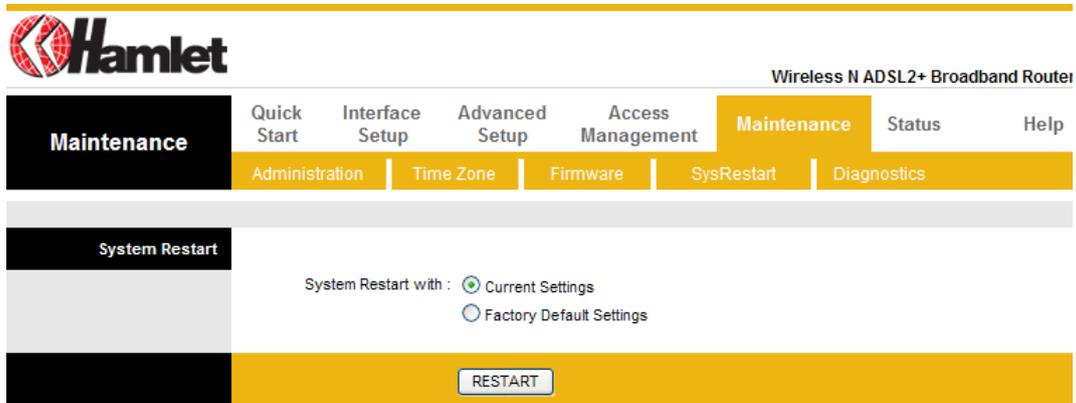
- **New Firmware Location:** Type in the location of the file you want to upload in this field or click **Browse** to find it.
- **New Romfile Location:** Romfile means the configuration file. Type in the location of the file you want to upload in this field or click **Browse** to find it.
- **Browse:** Click **Browse...** to find the .ras file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
- **Romfile Backup:** Click **ROMFILE SAVE** button to save current configuration file to your PC.
- **UPGRADE:** Click **UPGRADE** to begin the upload process. This process may take up to two minutes. After two minutes, log in again and check your new firmware version in the System Status screen.

Attention

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

SysRestart

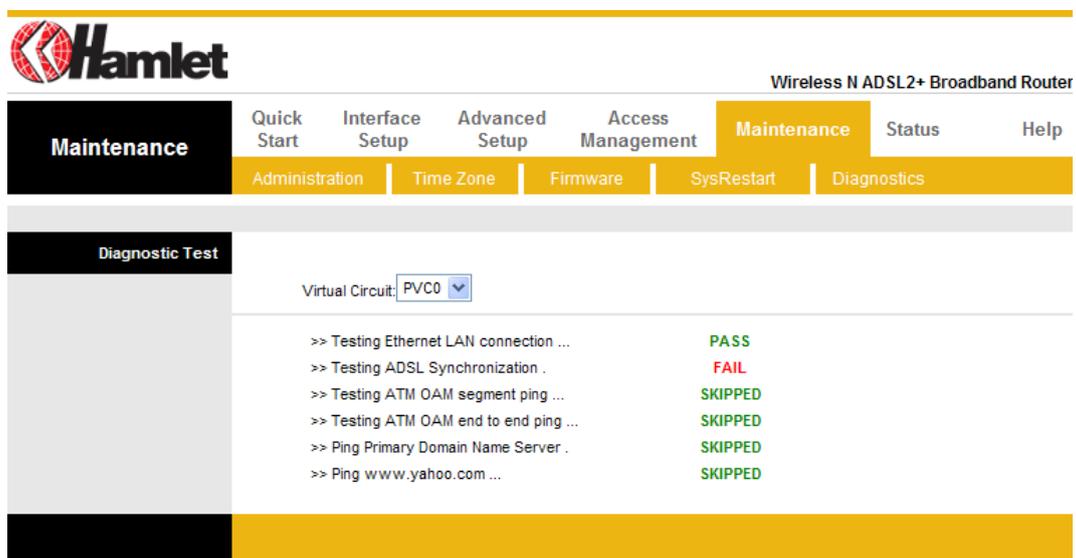
Go to **Maintenance > SysRestart** to restart your system. In the event that the router stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, select "**Current Setting**" and click on the "**RESTART**" button below. The router will reboot with current setting. Select "**Factory Default Setting**" and click on the "**RESTART**" button, the router will reboot with factory default setting.



You may also reset your router to factory settings by holding the small Reset pinhole button on the back of your router in for 10-12 seconds whilst the router is turned on.

Diagnostics

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.



7.7 Status

System Status

Go to **Status > Device Info** to see the router's information. The System Status page shows the WAN, LAN and the router's firmware version.

Hamlet Wireless N ADSL2+ Broadband Router

Status Quick Start Interface Setup Advanced Setup Access Management Maintenance **Status** Help

Device Info System Log Statistics

Device Information

Firmware Version : Hamlet(LEM_86_N)_A02_(211980_31261)_2M16
MAC Address : 00:13:33:8d:47:a6

LAN

IP Address : 192.168.1.254
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN

Virtual Circuit :
Status : Not Connected
Connection Type : PPPoE
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS : 0.0.0.0
Secondary DNS : 0.0.0.0
NAT : Enabled

ADSL

ADSL Firmware Version : FwVer:3.12.6.1_TC3086 HwVer:T14.F7_6.0
Line State : Down
Modulation : N/A
Annex Mode : N/A

	Downstream	Upstream	
SNR Margin :	N/A	N/A	db
Line Attenuation :	N/A	N/A	db
Data Rate :	N/A	N/A	kbps

Device Information

- **Firmware version:** This is the Firmware version.
- **MAC Address:** This is the MAC Address.

LAN

- **IP Address:** LAN port IP address.
- **Sub Net Mask:** LAN port IP subnet mask.
- **DHCP Server:** LAN port DHCP role - Enabled, Relay or disabled.

WAN

- **Virtual Circuit:** There are eight groups of PVC can be defined.
- **Status:** "Not connected" or "Connected".
- **Connection Type:** Name of the WAN connection.
- **IP Address:** WAN port IP address.
- **Subnet mask:** WAN port IP subnet mask.
- **Default Gateway:** The IP address of the default gateway.
- **DNS Server:** WAN port DHCP role - Enabled, Relay or disabled.
- **NAT:** Enabled or Disabled NAT function.

ADSL

- **ADSL firmware version:** This is the DSL firmware version associated with your router
- **Line State:** This is the status of your ADSL link.
- **Modulation:** This field displays the ADSL modulation status for G.dmt or T1.413.
- **Annex Mode:** To show the router's type, e.g. Annex A, Annex B
- **SNR Margin:** To show the router's SNR margin for Downstream/Upstream
- **Line Attenuation :** To show the router's for Downstream/Upstream
- **Data Rate:** To show the router's data rate for Downstream/Upstream

System Log

Go to **Status > System Log** to see the system log file. Click "**Save Log**" to save system log file.

Hamlet Wireless N ADSL2+ Broadband Route

Quick Start | Interface Setup | Advanced Setup | Access Management | Maintenance | **Status** | Help

Device Info | System Log | Statistics

System Log

```

4/6/2010 17:51:19> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 17:51:43> Last errorlog repeat 10 Times
4/6/2010 17:51:43> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 17:51:43> Last errorlog repeat 1 Times
4/6/2010 17:51:50> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 17:53:36> Last errorlog repeat 9 Times
4/6/2010 17:56:18> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 17:56:21> Last errorlog repeat 2 Times
4/6/2010 17:56:22> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 17:56:35> Last errorlog repeat 10 Times
4/6/2010 16:42:25> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 16:42:30> Last errorlog repeat 4 Times
4/6/2010 16:42:33> netMakeChannDial: err=-3001
rn_p=804ffc38
4/6/2010 16:42:34> Last errorlog repeat 1 Times

```

CLEAR LOG | SAVE LOG

Statistics

Go to **Status > Statistics**. In this page you can see the traffic statistics of Ethernet, ADSL and WLAN interface.

Ethernet

The screenshot shows the Hamlet router's web interface. The top navigation bar includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Status' menu is expanded to show 'Device Info', 'System Log', and 'Statistics'. The 'Statistics' page is titled 'Traffic Statistics' and shows the selected interface as 'Ethernet'. Below this, there are two tables: 'Transmit Statistics' and 'Receive Statistics'.

Transmit Statistics		Receive Statistics	
Transmit Frames	3886	Receive Frames	9929
Transmit Multicast Frames	792	Receive Multicast Frames	992
Transmit total Bytes	3188532	Receive total Bytes	1646927
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

A 'REFRESH' button is located at the bottom of the statistics section.

- **Interface:** This field displays the type of port
- **Transmit Frames:** This field displays the number of frames transmitted in the last second.
- **Transmit Multicast Frames:** This field displays the number of multicast frames transmitted in the last second.
- **Transmit total Bytes:** This field displays the number of bytes transmitted in the last second.
- **Transmit Collision:** This is the number of collisions on this port.
- **Transmit Error Frames:** This field displays the number of error packets on this port.
- **Receive Frames:** This field displays the number of frames received in the last second.
- **Receive Multicast Frames:** This field displays the number of multicast frames received in the last second.
- **Receive total Bytes:** This field displays the number of bytes received in the last second.
- **Receive CRC Errors:** This field displays the number of error packets on this port.
- **Receive Under-size Frames:** This field displays the number of under-size frames received in the last second.

ADSL

The screenshot shows the Hamlet router's web interface. The top navigation bar is the same as in the Ethernet screenshot. The 'Statistics' page is titled 'Traffic Statistics' and shows the selected interface as 'ADSL'. Below this, there are two tables: 'Transmit Statistics' and 'Receive Statistics'.

Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

A 'REFRESH' button is located at the bottom of the statistics section.

- **Transmit total PDUs:** This field displays the number of total PDU transmitted in the last second.
- **Transmit total Error Counts:** This field displays the number of total error transmitted in the last second.
- **Receive total PDUs:** This field displays the number of total PDU received in the last second.
- **Receive total Error Counts:** This field displays the number of total error received in the last second.

WLAN

The screenshot shows the Hamlet router's web interface. At the top left is the Hamlet logo. To the right, it says "Wireless N ADSL2+ Broadband Router". Below this is a navigation menu with tabs: "Status" (selected), "Quick Start", "Interface Setup", "Advanced Setup", "Access Management", "Maintenance", and "Help". Under the "Status" tab, there are sub-tabs: "Device Info", "System Log", and "Statistics". The "Statistics" sub-tab is active, showing "Traffic Statistics". Under "Traffic Statistics", there are radio buttons for "Interface": Ethernet, ADSL, and WLAN (selected). Below this is a table with two columns: "Transmit Statistics" and "Receive Statistics".

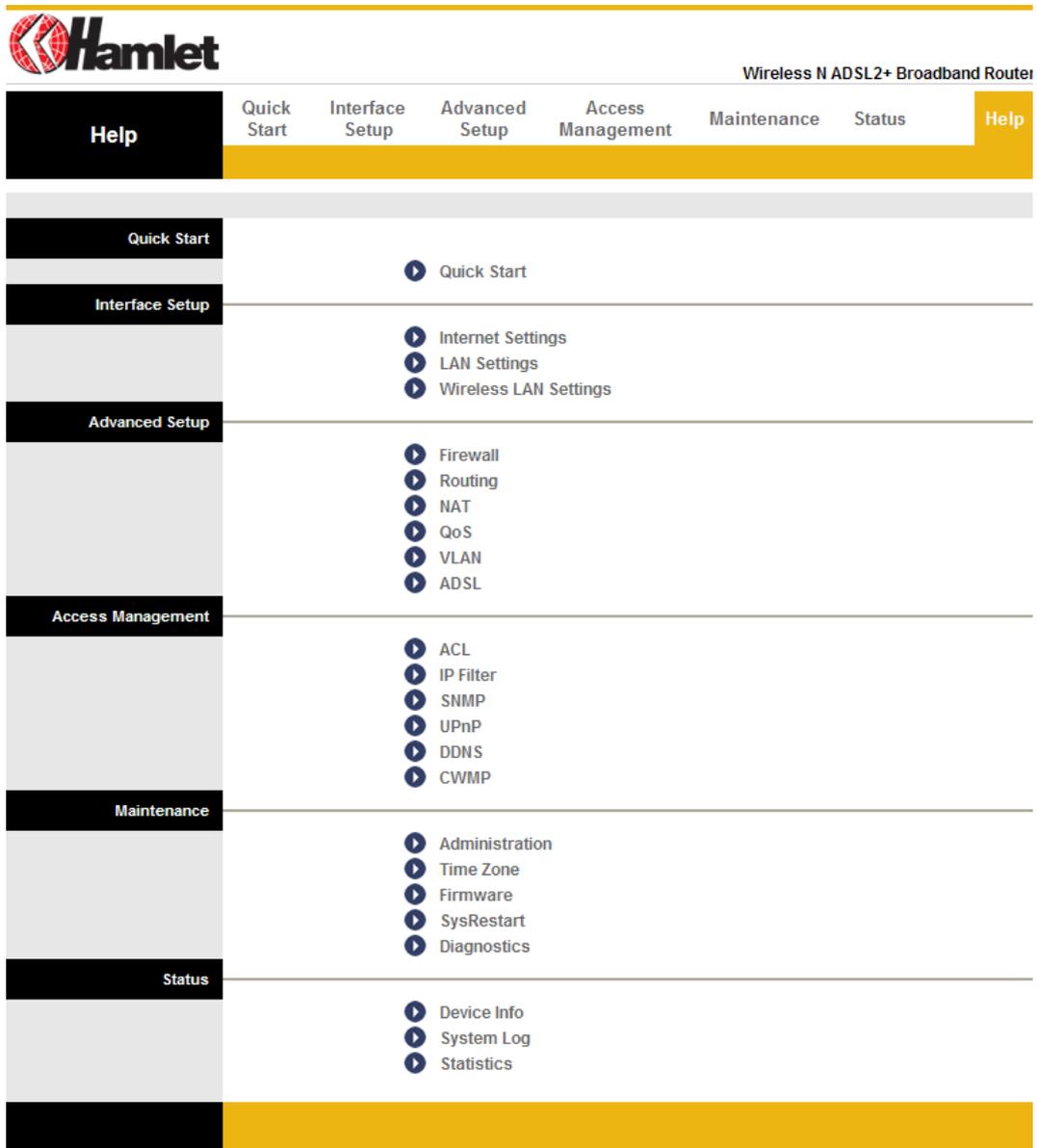
Transmit Statistics		Receive Statistics	
Tx Frames Count	0	Rx Frames Count	1
Tx Errors Count	0	Rx Errors Count	0
Tx Drops Count	0	Rx Drops Count	0

At the bottom of the statistics section is a "REFRESH" button.

- **Tx Frames Count:** This field displays the number of frames transmitted in the last second.
- **Tx Errors Count:** This field displays the number of errors frames transmitted in the last second.
- **Tx Drops Count:** This field displays the number of drops frames transmitted in the last second.
- **Rx Frames Count:** This field displays the number of frames received in the last second.
- **Rx Errors Count:** This field displays the number of errors frames received in the last second.
- **Rx Drops Count:** This field displays the number of drops frames received in the last second.

7.8 Help

This help page provides you some useful messages such as the introductions of some concepts and some guidance. When some problems are encountered, you can turn to this page for help.



Hamlet Wireless N ADSL2+ Broadband Router

Help	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Quick Start			<ul style="list-style-type: none"> ▶ Quick Start 				
Interface Setup			<ul style="list-style-type: none"> ▶ Internet Settings ▶ LAN Settings ▶ Wireless LAN Settings 				
Advanced Setup				<ul style="list-style-type: none"> ▶ Firewall ▶ Routing ▶ NAT ▶ QoS ▶ VLAN ▶ ADSL 			
Access Management					<ul style="list-style-type: none"> ▶ ACL ▶ IP Filter ▶ SNMP ▶ UPnP ▶ DDNS ▶ CWMP 		
Maintenance						<ul style="list-style-type: none"> ▶ Administration ▶ Time Zone ▶ Firmware ▶ SysRestart ▶ Diagnostics 	
Status							<ul style="list-style-type: none"> ▶ Device Info ▶ System Log ▶ Statistics

8. Universal Plug-and-Play (UPnP)

8.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

8.2 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

8.3 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP. See the *Network Address Translation (NAT)* chapter for further information about NAT.

8.4 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

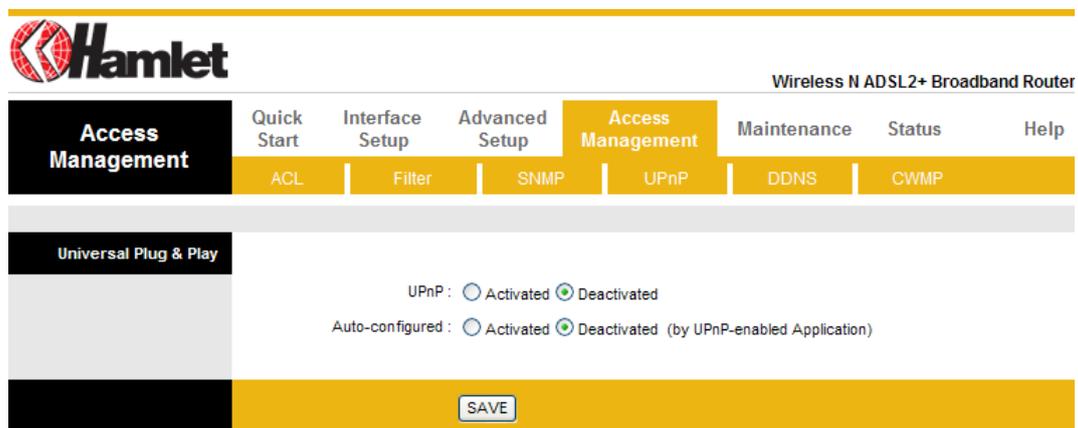
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP broadcasts are only allowed on the LAN.

See later sections for examples of installing UPnP in Windows XP as well as an example of using UPnP in Windows.

8.5 Configuring UPnP

From the Site Map in the main menu, click UPnP under Access Management to display the screen shown next.



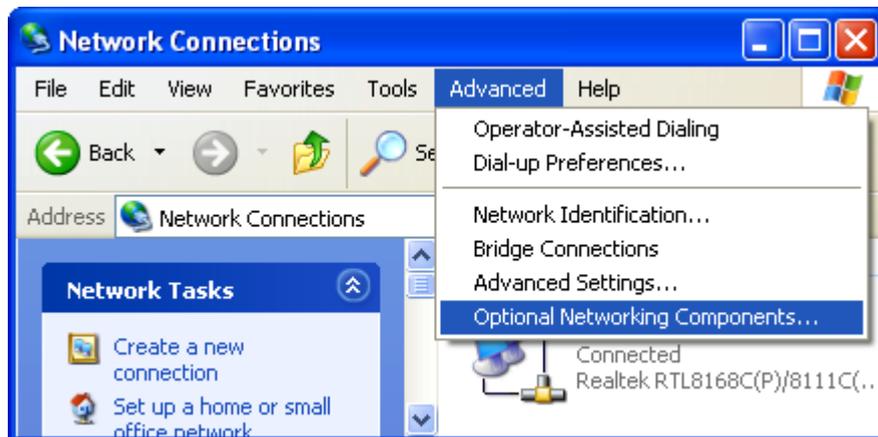
- **UPnP:** Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering Router's IP address (although you must still enter the password to access the web configuration).
- **Auto configured:** Select this check box to allow UPnP-enabled applications to automatically configure the Router so that they can communicate through the Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Click **SAVE** button to save your settings.

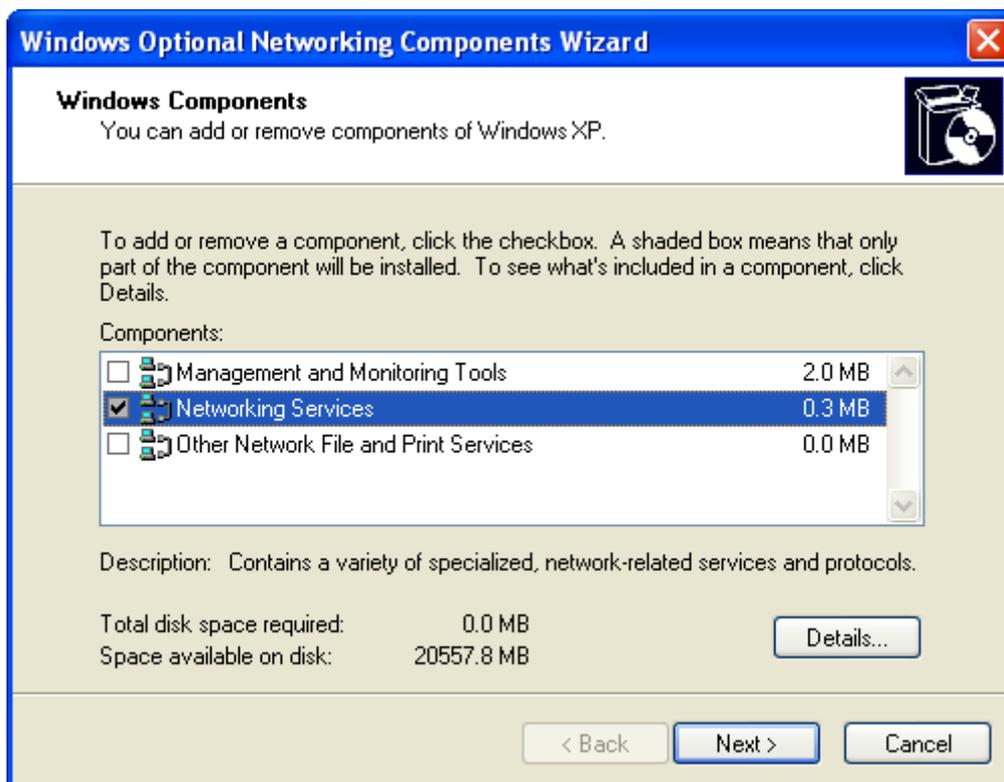
8.6 Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

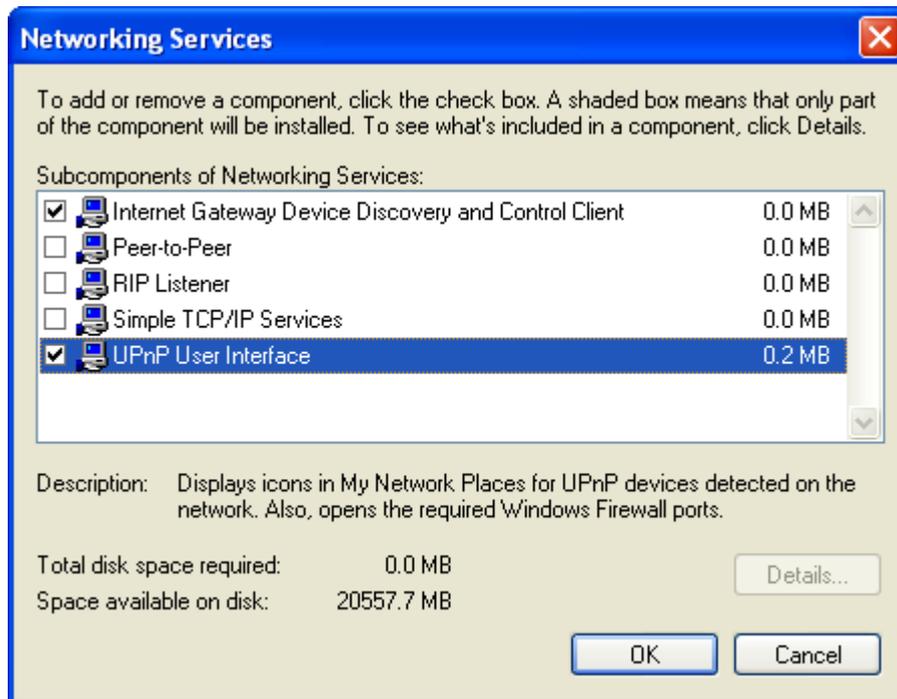
1. Click **Start** and **Control Panel**.
2. Double-click **Network Connections**.
3. In the Network Connections window, click **Advanced** in the main menu and select **Optional Networking Components**.



4. The “Windows Optional Networking Components Wizard” window displays.
5. Select **Networking Service** in the Components selection box and click **Details**.



6. In the “Networking Services” window, select the “UPnP User Interface” check box.
7. Click **OK** to go back to the “Windows Optional Networking Component Wizard” window and click **Next**.



Windows will complete the installation of the “UPnP User Interface” on your computer. Go to the next chapter to see an example of use of Universal Plug-and-Play feature.

8.7 Using UPnP in Windows XP

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Wireless ADSL2+ Router.

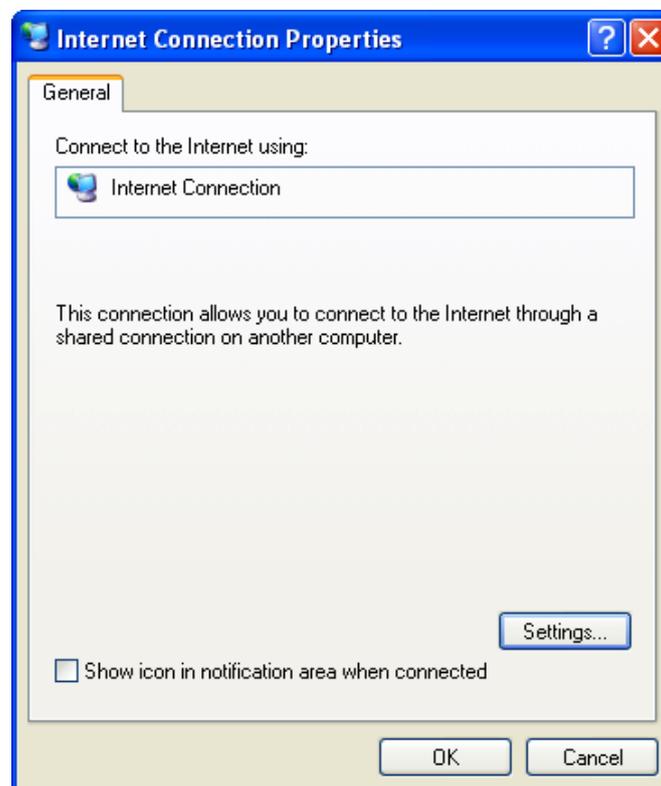
Make sure the computer is connected to a LAN port of the Router. Turn on your computer and Router.

The following steps show how to auto-discover your UPnP-enabled network device.

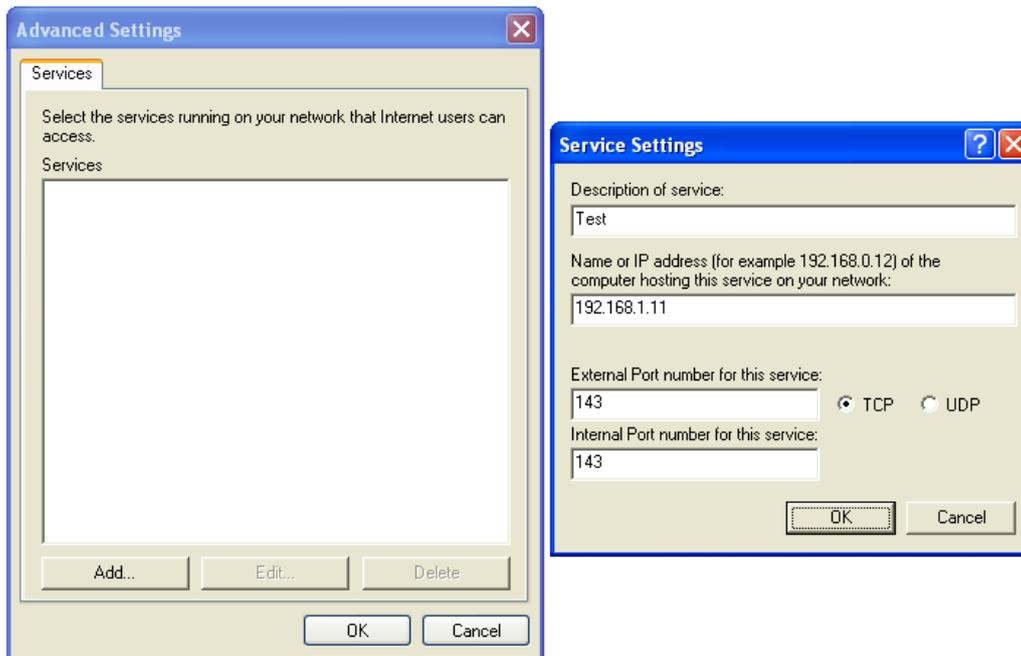
1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.



3. In the "Internet Connection Properties" window, click **Settings** to see the port mappings there were automatically created.



4. You may edit or delete the port mappings or click **Add** to manually add port mappings.



5. Once back in the “Internet Connection Properties” window, select “Show icon in notification area when connected” option and click **OK** to display the status icon in the system tray.



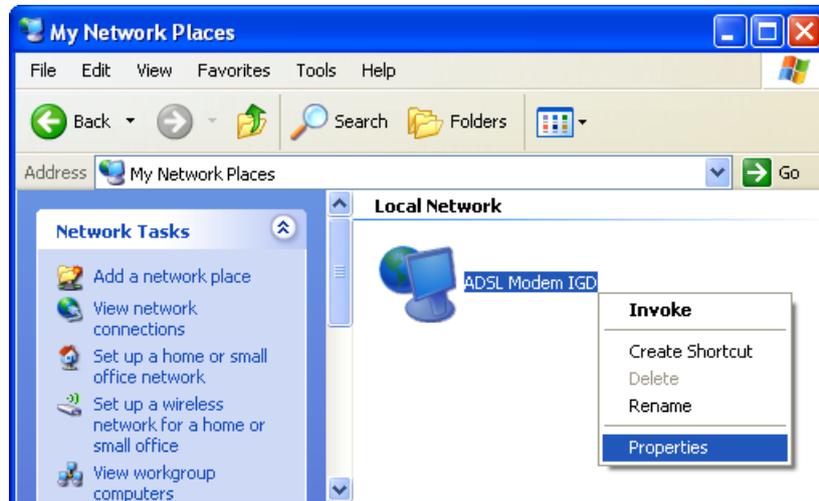
6. Double-clicking on the icon will display the “Internet connection status” window.



9. Web Configuration Easy Access

With UPnP, you can access the web-based configuration on Wireless ADSL2+ Router without finding out the IP address of Router first. This comes helpful if you do not know the IP address of the Router. Follow the steps below to access the web configuration.

1. Click **Start** and then **My Network Places** to open the “My Network Places” window.



2. An icon with the description for each UPnP-enabled device displays under Local Network.
3. Right-click on the icon for your Wireless ADSL2+ Router and select **Invoke**. The web configuration login screen displays.
4. If on the contrary select **Properties**. A properties window displays with basic information about Wireless ADSL2+ Router.



10. Troubleshooting

Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The PWR LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Make sure that Wireless ADSL2+ Router's power adaptor is connected to Wireless ADSL2+ Router and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that Wireless ADSL2+ Router and the power source are both turned on and Wireless ADSL2+ Router is receiving sufficient power.
3	Turn the Wireless ADSL2+ Router off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

LAN LED

The LAN LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your Wireless ADSL2+ Router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

DSL LED (ACT & LINK)

The DSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between ADSL2+ Router DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

Telnet

I cannot telnet into Wireless ADSL2+ Router.

STEPS	CORRECTIVE ACTION
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of Wireless ADSL2+ Router. Check the IP address of Wireless ADSL2+ Router.
3	Ping Wireless ADSL2+ Router from your computer. If you cannot ping Wireless

	ADSL2+ Router, check the IP addresses of Wireless ADSL2+ Router and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as Wireless ADSL2+ Router.
4	Make sure you entered the correct password. The default password is "hamlet".
5	If these steps fail to correct the problem, contact the distributor.

Web Configuration

I cannot access the web configuration.

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of Wireless ADSL2+ Router. Check the IP address of Wireless ADSL2+ Router.
2	Make sure that there is not a console session running.
3	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it.
4	For WAN access, you must configure remote management to allow server access from the Wan (or all).
5	Your computer's and Wireless ADSL2+ Router's IP addresses must be on the same subnet for LAN access.
6	If you changed Wireless ADSL2+ Router's LAN IP address, then enter the new one as the URL.
7	Remove any filters in LAN or WAN that block web service.

The web configuration does not display properly.

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK . (Steps may vary depending on the version of your Internet browser.)

Login Username and Password

I forgot my login username and/or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the Reset button for five seconds, and then release it. When the LINK LED begins to blink, the defaults have been restored and Wireless ADSL2+ Router restarts.
3	The default username is "admin". The default password is "hamlet". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password.

LAN Interface

I cannot access Wireless ADSL2+ Router from the LAN or ping any computer on the LAN.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the LAN LEDs on the front panel are off, refer to <i>Section A.1.2</i> .
2	Make sure that the IP address and the subnet mask of Wireless ADSL2+ Router and your computer(s) are on the same subnet.

WAN Interface

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The DSL LEDs on the front panel of Wireless ADSL2+ Router should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart Wireless ADSL2+ Router. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPOA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct casing).

Internet Access

I cannot access the Internet.

STEPS	CORRECTIVE ACTION
1	Make sure Wireless ADSL2+ Router is turned on and connected to the network.
2	If the DSL LEDs are off, refer to <i>Section A.1.3</i> .
3	Verify your WAN settings.
4	Make sure you entered the correct user name and password.

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

Remote Node Connection

I cannot connect to a remote node or ISP.

STEPS	CORRECTIVE ACTION
1	Check WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If these steps fail, you may need to verify your login and password with your ISP.

11. Technology Glossary

10Base-T

An adaptation of the Ethernet standard for Local Area Network (LAN). 10Base-T uses a twisted pair cable with maximum length of 100 meters.

AAL

ATM Adaptation Layer that defines the rules governing segmentation and reassembly of data into cells. Different AAL types are suited to different traffic classes.

Address mask

A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

ADSL

Asymmetric Digital Subscriber Line, as its name showing, is an asymmetrical data transmission technology with high traffic rate downstream and low traffic rate upstream. ADSL technology satisfies the bandwidth requirement of applications, which demand "asymmetric" traffic, such as web surfing, file download and Video-on-demand (VOD).

ATM

Asynchronous Transfer Mode is a layer 2 protocol supporting high-speed asynchronous data with advanced traffic management and quality of service features.

bps

Bits per second. A standard measurement of digital transmission speeds.

Bridge

A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other, and full-fledged routers which make routing decisions based on several criteria.

CPE

Customer Premises Equipment, such as ADSL router, USB modem.

DHCP

Dynamic Host Configuration Protocol. Used for assigning dynamic IP address to devices on a network. Used by ISPs for dialup users.

DNS

Domain Name Server, translates domain names into IP addresses to help user recognize and remember. However, the Internet actually runs on numbered IP addresses, DNS servers needs to translate domain names back to their respective IP addresses.

DSL

Digital Line Subscriber (DSL) technology provides high-speed access over twisted copper pair for connection to the Internet, LAN interfaces, and to broadband services such as video-on-demand, distance learning, and video conferencing.

FTP

File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

IPoA (RFC 1577)

Classical IP and ARP over ATM. Considers ATM configured as a Logic IP Sub-network(LIS) to replace Ethernet local LAN segments.

ISP

Internet service provider. A company that allows home and corporate users to connect to the Internet.

LAN

Local area network. A limited distance (typically under a few kilometers or a couple of miles) high-speed network (typically 4 to 100 Mbps) that supports many computers.

MAC

Media Access Control Layer. A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MTU

Maximum Transmission Unit

NAT

Network Address Translator as defined by RFC 1631. Enables a LAN to use one set of IP address for internal traffic. A NAT box located where the LAN meets the Internet provides the necessary IP address translation. This helps provide a sort of firewall and allow for a wider address range to be used internally without danger of conflict.

PPP

Point-to-Point-Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoA (RFC 2364)

The Point-to-Point Protocol(PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. This document describes the use of ATM Adaptation Layer 5 (AAL5) for framing PPP encapsulated packets.

PPPoE (RFC 2516)

This document describes how to build PPP sessions and encapsulate PPP packets over Ethernet. PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator.

PVC

Permanent Virtual Circuit. Connection-oriented permanent leased line circuit between end-stations on a network over a separate ATM circuit.

RFC

Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs

RFC 1483

Multi-protocol encapsulation over AAL-5. Two encapsulation methods for carrying network interconnect traffic over ATM AAL-5. The first method allows multiplexing of multiple protocols over a single ATM virtual circuit. The protocol of a carried PDU is identified by prefixing the PDU by an IEEE 802.2 Logical Link Control (LLC) header. This method is in the following called "LLC Encapsulation". The second method does higher-layer protocol multiplexing implicitly by ATM Virtual Circuits (VCs). It is in the following called "VC Based Multiplexing".

Router

A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics."

Spanning Tree

Spanning-Tree Bridge Protocol (STP). Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When bridges connect three or more LAN segments, a loop can occur. Because a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

TELNET

The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

VCI

Virtual Circuit Identifier. Part of the ATM cell header, a VCI is a tag indicating the channel over which a cell will travel. The VCI of a cell can be changed as it moves between switches via Signaling.

VPI

Virtual Path Identifier. Part of the ATM cell header, a VPI is a pipe for a number of Virtual Circuits.

WAN

Wide area network. A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider)

