

TeleWell
TW-EA510 v3

ADSL2+ Router
WLAN 54 Mbps (802.11b+g)

English User's Manual

CE

Chapter 1	1
1.1 Introducing the TW-EA510 v3 ADSL2+ Router	1
1.2 Features	3
Chapter 2	6
2.1 Important Notes	6
2.2 Package Contents	6
2.3 The Front LEDs	7
2.4 The Rear Ports	8
2.5 Cabling	10
Chapter 3	11
3.1 Before Configuration	11
3.2 Factory Default Settings	16
3.3 Username and Password	16
3.4 LAN and WAN Port Addresses	17
3.4 Information from your ISP	17
3.5 Configuring with your Web Browser	18
Chapter 4	19
4.1 Status	20
4.1.1 ARP Table	23
4.1.2 Wireless Association (only TW-EA510 v3)	24
4.1.3 Routing Table	25
4.1.4 DHCP Table	26
4.1.5 System Log	27
4.1.6 Security Log	28
4.2 Quick Start	29
4.3 Configuration	32
4.3.1 LAN (Local Area Network)	33
4.3.2 WAN (Wide Area Network)	40
4.3.3 System	47
4.3.4 Firewall	52
4.3.5 QoS (Quality of Service)	62
4.3.6 Virtual Server	74
4.3.7 Advanced	78
4.4 Save Configuration to Flash	90
4.5 Restart	91
Chapter 5	92

Chapter 1

Introduction

1.1 Introducing the TW-EA510 v3 ADSL2+ Router

Thank you for purchasing the TW-EA510 v3. Your new router is an all-in-one unit that combines an ADSL modem, ADSL router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

The TW-EA510 v3 complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

The router supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, the router allows multiple users to have high-speed Internet access simultaneously.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

The router provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port forwarding) functions allow the product to provide limited visibility to local machines with specific services for outside users. You can set an ISP (Internet Service Provider) provided IP address on the router and then you can reroute specific services to individual computers on your local network. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Features

● **Express Internet Access – ADSL2/2+ capable**

The router complies with ADSL worldwide standards. Supporting downstream rates of 8Mbps with ADSL, the router is capable of up to 12/24 Mbps with ADSL2/2+, and upstream rates of up to 1 Mbps. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio which are easier and faster than ever. The router is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); and G.dmt.bisplus (ITU G.992.5)

● **Fast Ethernet Switch**

A 4-port 10/100Mbps fast Ethernet switch is built-in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports, with auto detection allowing you to use either straight or cross-over Ethernet cables.

● **Wireless Ethernet 802.11g**

With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP, WPA/WPA2 and WDS for securing your wireless networks.

● **Multi-Protocol to Establish a Connection**

The router supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) and IPoA (RFC1577) to establish a connection with an ISP. The router also supports VC-based and LLC-based multiplexing.

● **Quick Installation Wizard**

A web-based GUI and quick installation wizard help you easily install the router. Enter your ISP's information and begin browsing the Internet immediately.

● **Universal Plug and Play (UPnP) and UPnP NAT Traversal**

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors, and it makes setting up a network simple and affordable. UPnP architecture leverages TCP/IP and the Web to enable proximity networking in addition to control and data transfer among networked devices. With this feature enabled, you can seamlessly connect to Net Meeting or MSN Messenger.

● **Network Address Translation**

Network Address Translation (NAT) allows multiple users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

● **Firewall**

NAT technology supports simple firewalls and provides options for blocking access from the Internet, like Telnet, FTP, TFTP, WEB, SNMP and IGMP.

● **Domain Name System Relay**

Domain Name System (DNS) relay provides an easy way to map a domain name with a user-friendly name such as www.yahoo.com with an IP address. When a local machine sets its DNS server to the router's IP address, every DNS conversion request packet from the PC to this router is forwarded to the real DNS on the outside network.

● **Dynamic Domain Name System (DDNS)**

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. To use the service, you must first apply for an account from a DDNS service such as <http://www.dyndns.org/>.

● **PPP over Ethernet (PPPoE)**

The router provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

● **Quality of Service (QoS)**

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

● **Virtual Server:**

You can specify which services are visible to outside users. The router detects an incoming service request and forwards it to the specific local computer for handling. For example, you can assign a PC in a LAN to act as a Web server inside and expose it to the outside network. Outside users can browse inside the web server directly while it is protected by NAT. A DMZ host setting is also provided for local computers exposed to the outside Internet network.

● **Dynamic Host Configuration Protocol (DHCP) Client and Server**

On a WAN site, the DHCP client obtains an IP address from the Internet Service Provider (ISP) automatically. On a LAN site, the DHCP server allocates a range of client IP addresses, including subnet masks and DNS IP addresses and distributes them to local computers. This provides an easy way to manage the local IP network.

● **Rich Packet Filtering**

This feature filters the packet based on IP addresses as well as Port numbers. Filtering packets to and from the Internet provides a higher level of security control.

● **Static and RIP1/2 Routing**

An easy static routing table or RIP1/2 routing protocol supports routing capability.

● **Simple Network Management Protocol (SNMP)**

SNMP allows convenient remote management of the router.

● **Web-based GUI**

A web-based GUI offers easy configuration and management. User-friendly and with on-line help, it also supports remote management capability for remote users to configure and manage this product.

● **Firmware Upgradeable**

You can upgrade the router with the latest firmware through its web-based GUI.

Chapter 2

Product Overview

2.1 Important Notes



Warning

- ✓ Do not use the router in high humidity or high temperatures.
- ✓ Do not use the same power source for the router as other equipment.
- ✓ Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.



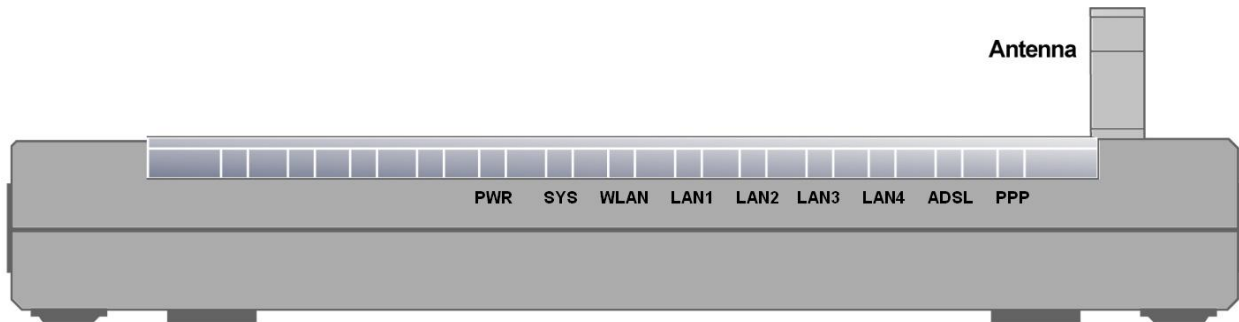
Attention

- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.2 Package Contents

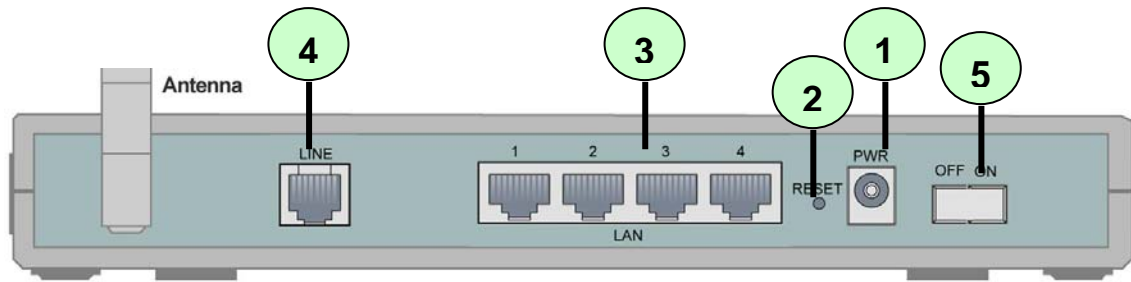
- TW-EA510 v3 ADSL2+ Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable (1.8M)
- Ethernet (CAT-5 LAN) Cable (2M Straight)
- AC-DC power adapter (12V DC, 1A)

2.3 The Front LEDs



LED		Description
1	PPP :	● Steady glow when there is a PPPoA / PPPoE connection.
2	ADSL:	● Lights when successfully connected to an ADSL DSLAM (linesync).
3	LAN Port 1-4:	<ul style="list-style-type: none"> ● Steady glow when connected to an Ethernet device. ● Glows green for 100Mbps; Orange for 10Mbps. ● Blinking light when data is Transmitted / Received.
4	WLAN	<ul style="list-style-type: none"> ● Lit green when the wireless connection is established. ● Flashes when sending/receiving data.
5	SYS :	● Lights when the system is ready.
6	PWR :	● Lights when the power is ON.

2.4 The Rear Ports



Port		Description
1	PWR	Connect the supplied power adapter to this jack.
2	RESET	<p>After the router is powered on, press this recessed button using the end of paper clip or other small pointed object to reset the router or to restore it to factory default settings.</p> <p>1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):</p> <p>Hold the <i>Emergency/Failure Recovery Button</i> on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the <i>Emergency/Failure Recovery Button</i>. The modem's emergency-reflash web interface will then be accessible via http://192.168.0.254/ where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.</p> <p>2. Recovery procedures for a lost web interface password:</p> <p>After turning the router on press the <i>Emergency/Failure Recovery Button</i> on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. The login will be reset to <i>admin</i> and the password will be reset to <i>admin</i>, and the modem will be accessible via its default IP address at http://192.168.0.254/</p>
3	LAN	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
4	LINE	Connect the supplied RJ-11 (telephone) cable to this port when connecting to the ADSL/telephone network.
5	Power Switch	Power ON/OFF switch.

● The detail instruction in Emergency/Failure Recovery Button

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):
Hold the *Emergency/Failure Recovery Button* on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the *Emergency/Failure Recovery Button*. The modem's emergency-reflash web interface will then be accessible via <http://192.168.0.254/> where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

2. Recovery procedures for a lost web interface password:

After turning the router on press the *Emergency/Failure Recovery Button* on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. The login will be reset to *admin* and the password will be reset to *admin*, and the modem will be accessible via its default IP address at <http://192.168.0.254/>



Before powered on the router to enter the recovery process. please configure the IP address of the PC as 192.168.0.1 and process step by step.

1. Power the router off.
2. Hold the " Emergency/Failure Recovery Button".
3. Power on the router. Then Router's IP will reset to Default (Say 192.168.0.254)
4. Download the firmware.

2.5 Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analog modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including frequent disconnections.

Chapter 3

Installation

You can configure the router through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux, MAC, and Windows 98/NT/2000/XP/Me include a web browser as a standard application.

3.1 Before Configuration

PCs must have a properly installed Ethernet interface and connect to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.0.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.0.1 to 192.168.0.253). The easiest way is to configure the PC to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.0.254 IP address of the router.

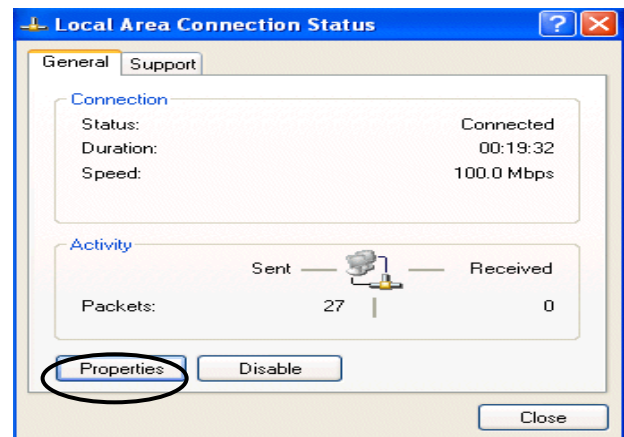
Please follow the steps below for installation on your PC's network environment. First of all, check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

Configuring a PC in Windows XP

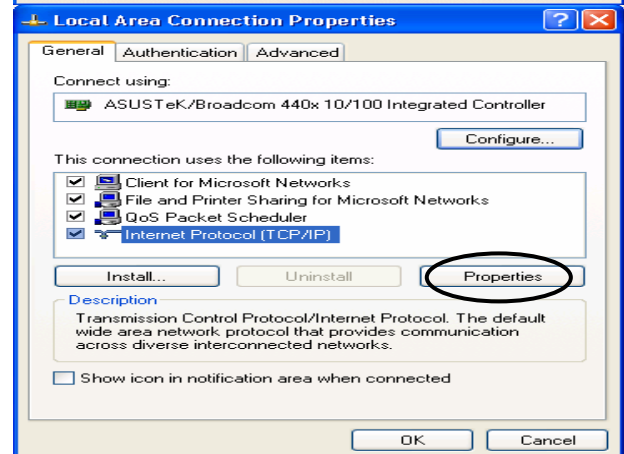
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

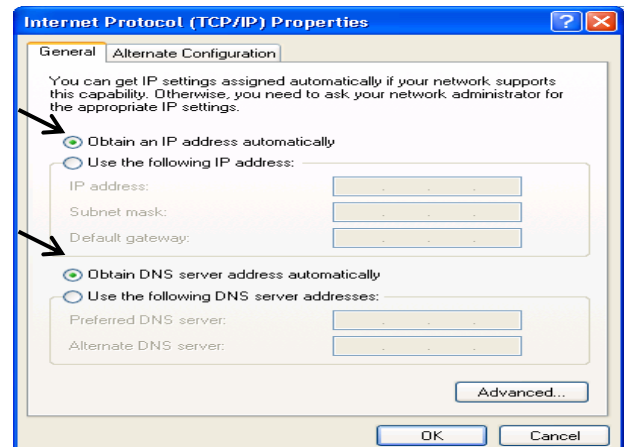


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



Configuring a PC in Windows 2000

1. Go to **Start / Settings / Control Panel**.
In the Control Panel, double-click on **Network and Dial-up Connections**.

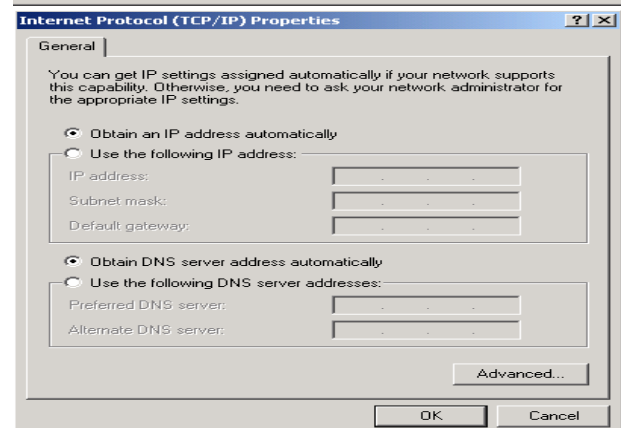
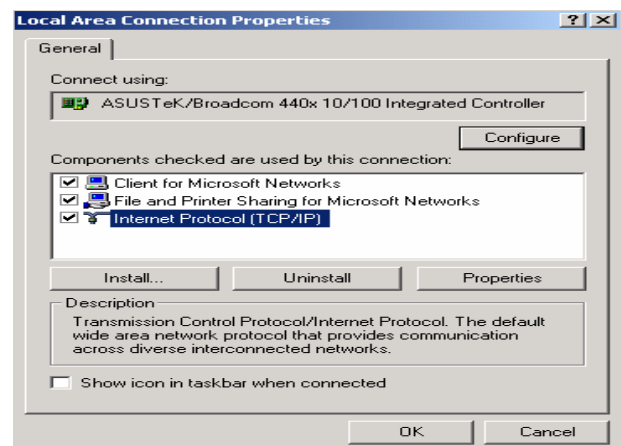
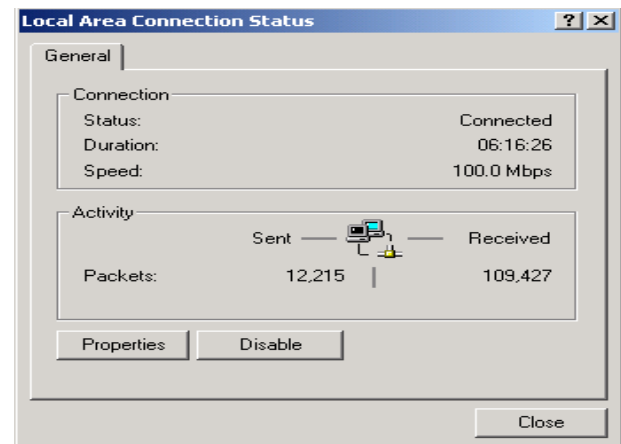
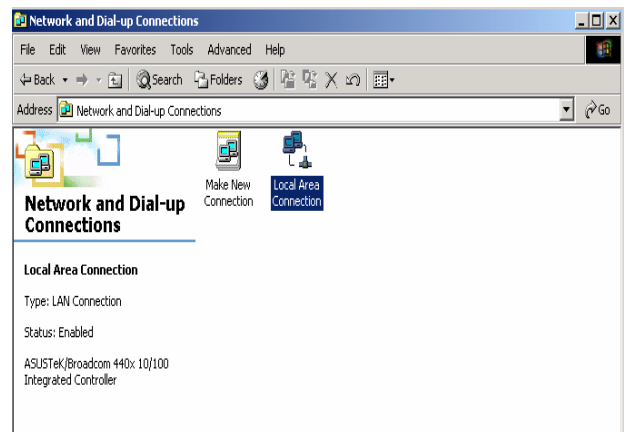
2. Double-click **Local Area Connection**.

3. In the **Local Area Connection Status** window click **Properties**.

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



Configuring PC in Windows 98/Me

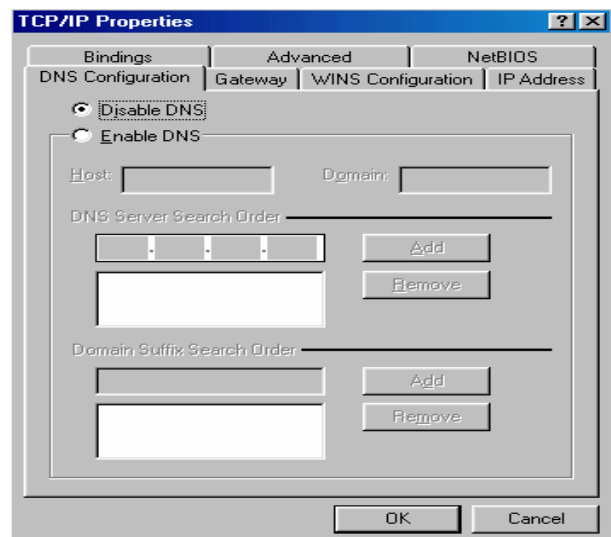
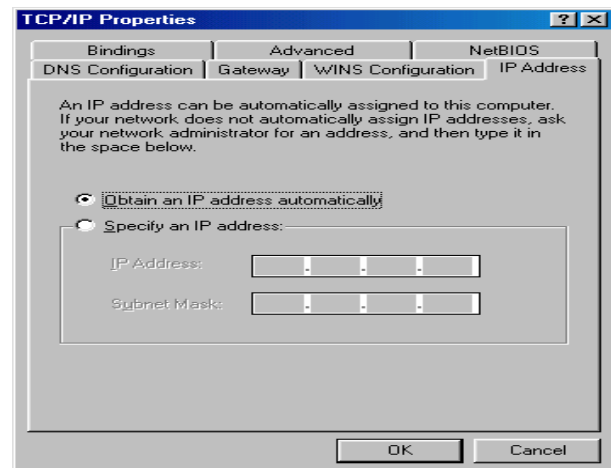
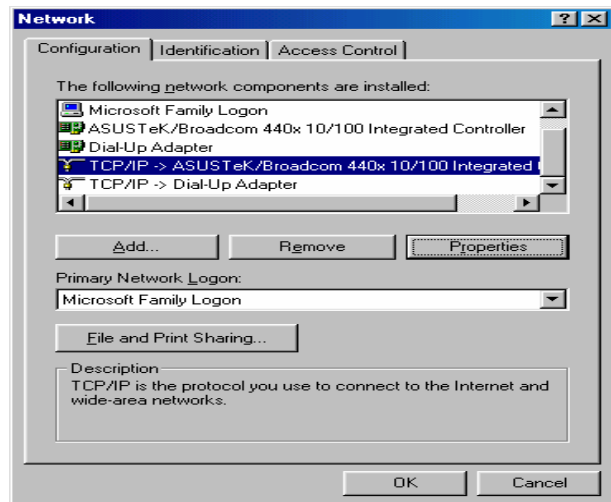
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP/IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.

3. Select the **Obtain an IP address automatically** radio button.

4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

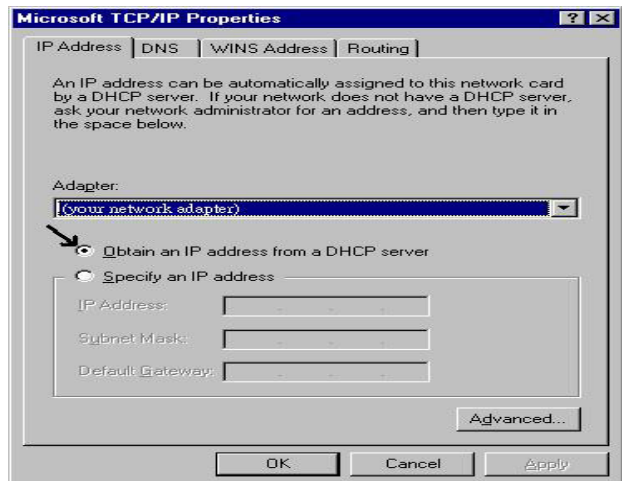
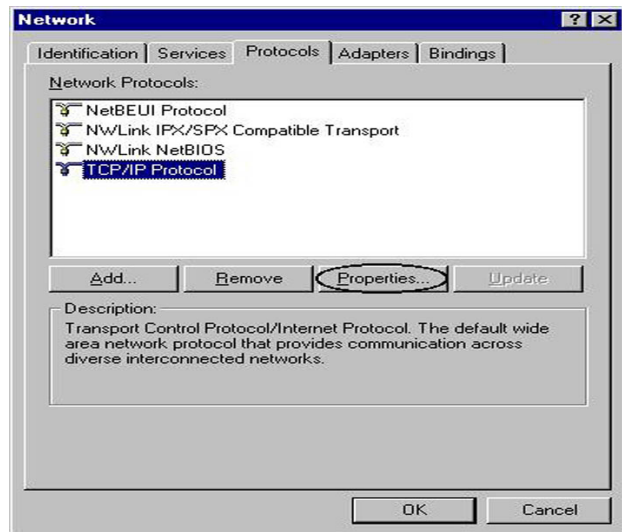


Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



3.2 Factory Default Settings

Before configuring the router, you need to know the following default settings.

● Web Interface:

- ✘ Username: admin
- ✘ Password: admin

● LAN Device IP Settings:

- ✘ IP Address: 192.168.0.254
- ✘ Subnet Mask: 255.255.255.0

● ISP setting in WAN site:

- ✘ RFC 1483 LLC Bridge
- ✘ Auto support for VPI=0,14 and VCI=24,33,50,100 if auto-scan fails!
During the 1st connection IP – traffic may take 2-4 minutes after boot.
Device will auto-scan correct parameters for ISP line on this period.
- ✘ NAT enabled

● DHCP Server:

- ✘ DHCP server is enabled.
- ✘ Start IP Address: 192.168.0.100
- ✘ IP pool counts: 100

3.3 Username and Password

The default username and password are “**admin**” and “**admin**” respectively.



Attention

To reset the router or to restore it to factory default settings press the Reset button using the end of paper clip or other small pointed object.

1. To perform Failure recovery for a dead router:

Simply hold the Reset button when powering on the router and download an application if necessary.

2. To perform recovery in case of a misplaced Password:

Hold the Reset button until the LEDs all turn Off, turn On and then turn Off. The router performs configuration factory reset and the router reboots. You can then access the router from the web GUI.

3.4 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are preset at the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.0.254	Bridge is automatic setting in WAN port.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.0.100 through 192.168.0.199	

3.4 Information from your ISP

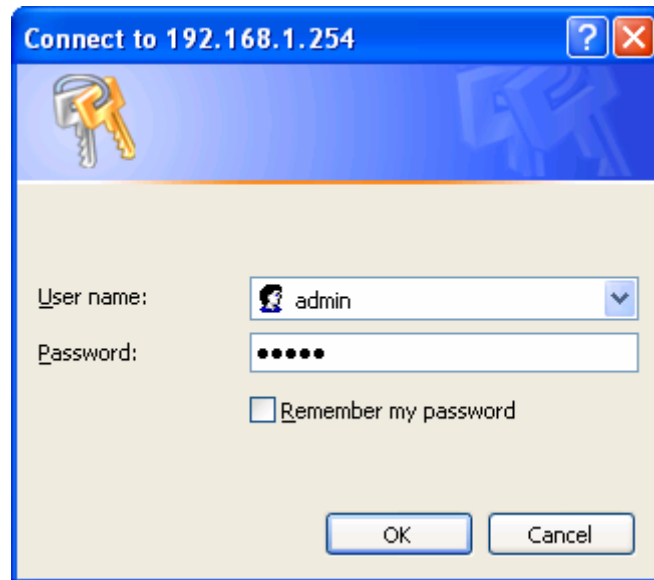
Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, or IPoA.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

3.5 Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **192.168.0.254**, and click **“Go”**, a user name and password window prompt appears. **The default username and password are “admin” and “admin”.**



Congratulations! You have successfully logged on to your 802.11g ADSL2+ Router!

Chapter 4

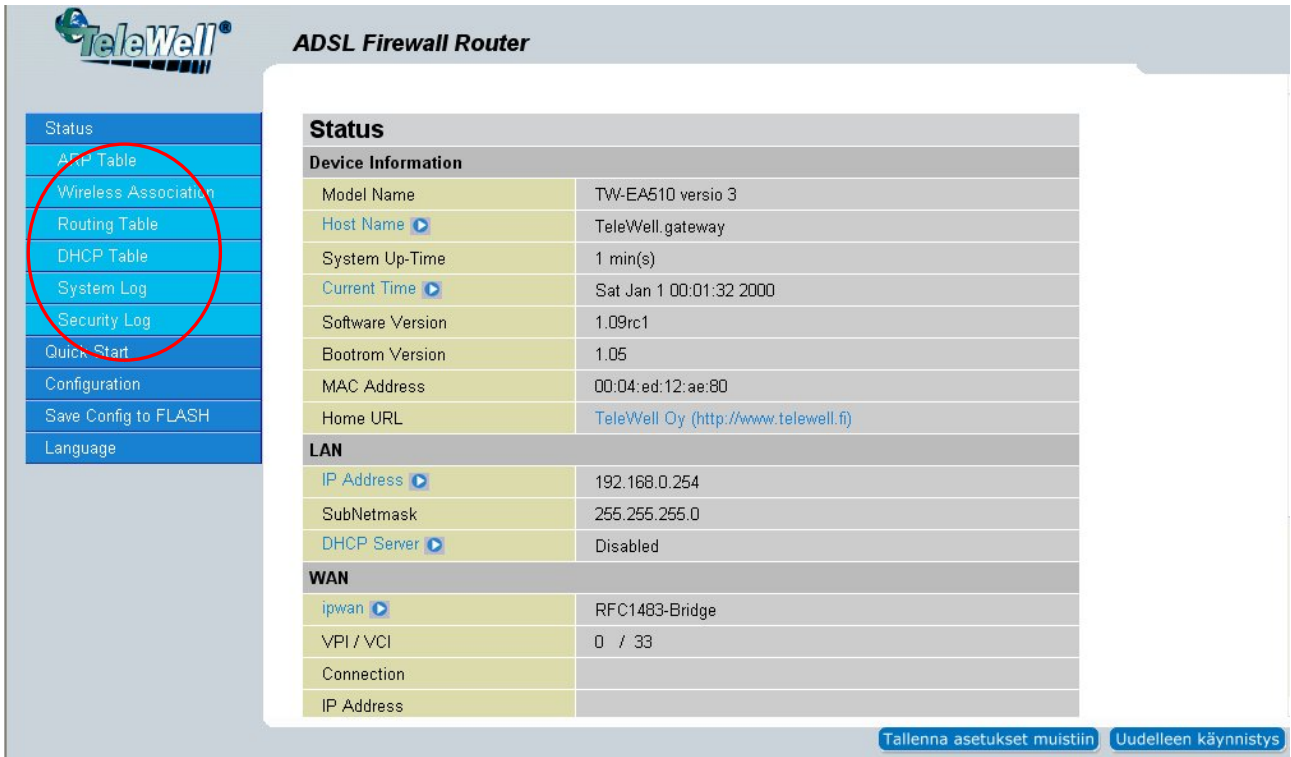
Configuration

Once you have logged on to your ADSL Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Status** (ARP Table, Wireless Association, Routing Table, DHCP Table, System Log, Security Log)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, QoS, Virtual Server and Advanced)
- **Save Config to FLASH**

The following sections provide an overview of the settings available for configuring your TW-EA 510 v3 router.

4.1 Status



TeleWell® ADSL Firewall Router

Status

Device Information

Model Name	TW-EA510 versio 3
Host Name ▶	TeleWell.gateway
System Up-Time	1 min(s)
Current Time ▶	Sat Jan 1 00:01:32 2000
Software Version	1.09rc1
Bootrom Version	1.05
MAC Address	00:04:ed:12:ae:80
Home URL	TeleWell Oy (http://www.telewell.fi)







LAN

IP Address ▶	192.168.0.254
SubNetmask	255.255.255.0
DHCP Server ▶	Disabled

WAN

ipwan ▶	RFC1483-Bridge
VPI / VCI	0 / 33
Connection	
IP Address	

Tallenna asetukset muistiin Uudelleen käynnistys

Status	
Device Information	
Model Name	TW-EA510 versio 3
Host Name 	TeleWell.gateway
System Up-Time	2 min(s)
Current Time 	Sat Jan 1 00:02:31 2000
Software Version	1.09rc1
Bootrom Version	1.05
MAC Address	00:04:ed:12:ae:80
Home URL	TeleWell Oy (http://www.telewell.fi)
LAN	
IP Address 	192.168.0.254
SubNetmask	255.255.255.0
DHCP Server 	Disabled
WAN	
ipwan 	RFC1483-Bridge
VPI / VCI	0 / 33
Connection	
IP Address	
Netmask	
Gateway	
Primary DNS 	

Device Information

- **Host Name:** Provide a name for the router for identification purposes. Host Name lets you change the router name.

Host Name	
Device Host Name	
Host Name	<input type="text" value="home.gateway"/>
<input type="button" value="Apply"/>	

- **System Up-Time:** Records system up-time.
- **Current time:** Set the current time. See the Time Zone section for more information.
- **Hardware Version:** Chipset version
- **Software Version:** Firmware version

- **LAN MAC Address:** The LAN MAC address
- **WAN MAC Address:** The WAN MAC address
- **Home URL:** Connects to the Home Website.

LAN

- **IP Address:** LAN port IP address.
- **Sub Net Mask:** LAN port IP subnet mask.
- **DHCP Server:** LAN port DHCP role - Server, Relay or None.

WAN

- **IP WAN:** Name of the WAN connection.
- **VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Connection:** Selects “Disconnected” or “Connected”
- **IP Address:** WAN port IP address.
- **Net mask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.

Port Status			
Port	Ethernet 	ADSL 	Wireless 
Connected			

- **Port Status** User can look up for your connected condition

4.1.1 ARP Table

The router's ARP (Address Resolution Protocol) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information.

ARP Table			
IP <> MAC List			
IP Address	MAC Address	Interface	Static
192.168.0.111	00:0D:88:18:7D:F7	br0	no

- **IP Address:** A list of IP addresses of devices on your LAN (Local Area Network).
- **MAC Address:** MAC (Media Access Control) address for each device on your LAN.
- **Interface:** The interface name (on the router) that this IP Address connects to.
- **Static:** Static status of the ARP table entry:
 - “no” for dynamically-generated ARP table entries
 - “yes” for static ARP table entries added by the user

4.1.2 Wireless Association

Wireless Association Table

Wireless client's MAC address and the corresponding IP address

IP Address	MAC
------------	-----

- **IP Address:** It is IP Address of wireless client that join this network.
- **MAC:** The MAC address of wireless client.

4.1.3 Routing Table

Routing Table						
Routing Table						
#	Destination	Netmask	Gateway/Interface	Cost		
1	192.168.0.0	255.255.255.0	0.0.0.0/br0	0	Edit	Delete
Create						

Static Route				
Add Rule2				
Destination	<input type="text"/>			
Netmask	<input type="text"/>			
Gateway	<input type="text"/>	Interface	Please Select <input type="button" value="v"/>	
Cost	<input type="text" value="0"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

Routing Table:

- #: Item number
- **Destination:** IP address of the destination network.
- **Netmask:** The destination netmask address.
- **Gateway/Interface:** IP address of the gateway or existing interface that this route uses.
- **Cost:** The cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.
- **Interface:** Select the interface through which packets are forwarded.

4.1.4 DHCP Table

DHCP Table			
Leased Table			
IP Address	MAC Address	Client Host Name	Register Time
192.168.1.100	00:0d:88:18:7d:f7		2000/01/01 00:05:22 - 2000/01/01 02:05:22

- **Leased:** DHCP assigned IP addresses information.
- **IP Address:** IP addresses of devices on your LAN (Local Area Network).
- **MAC Address:** The MAC Address that you want to assign the fixed IP address
- **Client Host Name:** Expired IP addresses information
- **Register Time:** Register time information

4.1.5 System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

System Log

Current Time: Sat Jan 1 00:52:48 2000

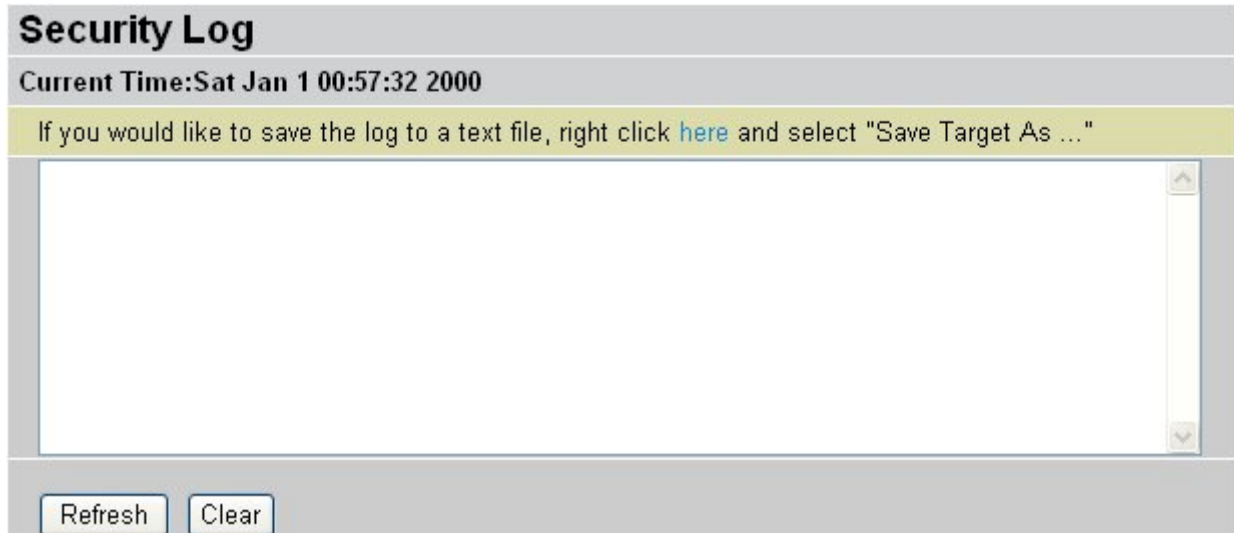
If you would like to save the log to a text file, right click [here](#) and select "Save Target As ..."

```
Jan 1 00:00:21 syslog: bil_CPU revision: 0000cd01
Jan 1 00:00:21 syslog: bil_ld 4kb instruction cache, linesize 16 bytes
Jan 1 00:00:21 syslog: bil_ld 1kb data cache 16kb, linesize 81 bytes
Jan 1 00:00:21 syslog: BINOS (19:34:17, Jan 13 2005)
Jan 1 00:00:21 syslog: memory map:
Jan 1 00:00:21 syslog:  memory: 01000000 @ 00000000 (usable)
Jan 1 00:00:21 syslog: On node 0 totalpages: 4096
Jan 1 00:00:21 syslog: zone(0): 4096 pages.
Jan 1 00:00:21 syslog: zone(1): 0 pages.
```

Refresh Clear

4.1.6 Security Log

This screen displays security log information. If a hacker attacks your server, he is isolated by the firewall function and the router records related information. This helps you know where the hacker comes from.



4.2 Quick Start

The screenshot shows the configuration interface for a TeleWell ADSL Firewall Router. On the left is a navigation menu with options: Status, Quick Start (highlighted with a red circle), Configuration, Save Config to FLASH, and Language. The main content area is titled 'Quick Start' and is divided into several sections:

- Connection**: Encapsulation (Pure Bridged LLC), VPI (0), VCI (33), and an Auto Scan button.
- Optional Settings**: IP Address (0.0.0.0), SubnetNetmask (0.0.0.0), and Default Gateway (0.0.0.0). A note indicates that '0.0.0.0' means 'Obtain an IP address automatically'.
- DNS**: Obtain DNS automatically (checked/Enable), Primary DNS, and Secondary DNS.

At the bottom of the form are 'Apply' and 'Cancel' buttons. At the bottom right of the page are two buttons: 'Tallenna asetukset muistiin' and 'Uudelleen käynnistys'.

For detailed instructions on configuring WAN settings, see the **WAN** section of this manual.

The information you need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password, and the encapsulation type.

Your ISP can supply all the details you need. Alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to determine the Encapsulation types offered by your ISP.

Quick Start	
Connection	
Encapsulation	1483 Bridged IP LLC <input type="button" value="Auto Scan"/>
VPI	0
VCI	33
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Optional Settings	
IP Address	0.0.0.0 (0.0.0.0' means 'Obtain an IP address automatically')
SubnetNetmask	0.0.0.0
Default Gateway	0.0.0.0
DNS	
Obtain DNS automatically	<input checked="" type="checkbox"/> Enable
Primary DNS	
Secondary DNS	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

■ Connection

- **Encapsulation:** Select the encapsulation type your ISP uses or choose “Auto Scan”.

Auto Scan	
Before you scan the PVCs, please DELETE all the WAN interfaces.	
IP Address	<input type="text"/> if provided by ISP
Gateway	<input type="text"/> if provided by ISP
<input type="button" value="Start"/> <input type="button" value="Cancel"/>	

Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful, you are presented with a list of supported options.

- **VCI:** Enter the VCI assigned to you. This field may already be configured.
- **VPI:** Enter the VPI assigned to you. This field may already be configured.
- **NAT:** Select “Enabled” or “Disabled”.

■ Optional Setting

- **IP Address:** Type your ISP assigned IP address in the IP Address text box.
- **Subnet Mask:** Enter a subnet mask in dotted decimal notation.
- **Default Gateway:** You must specify a gateway IP address (supplied by your ISP)

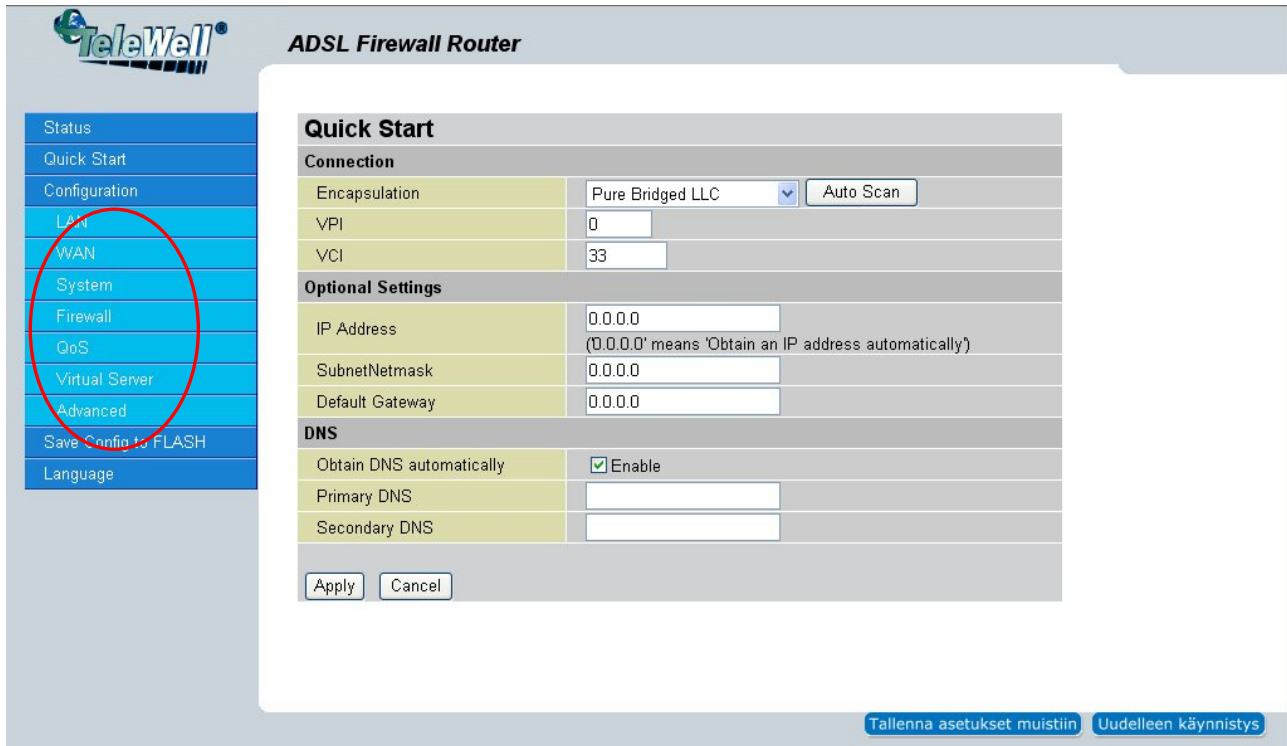
■ DNS

- **Obtain DNS automatically:** Select this check box to use DNS.
- **Primary DNS:** 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:** 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.

4.3 Configuration

Click this item to access the following sub-items that configure the ADSL router: **LAN, WAN, System, Firewall, QoS, Virtual Server** and **Advanced**.

These functions are described in the following sections.



TeleWell
ADSL Firewall Router

Quick Start

Connection

Encapsulation	Pure Bridged LLC	Auto Scan
VPI	0	
VCI	33	

Optional Settings

IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
SubnetNetmask	0.0.0.0
Default Gateway	0.0.0.0

DNS

Obtain DNS automatically	<input checked="" type="checkbox"/> Enable
Primary DNS	
Secondary DNS	

Apply Cancel

Tallenna asetukset muistiin Uudelleen käynnistys

4.3.1 LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

There are four items within the LAN section: **Ethernet, Wireless, Wireless Security** and **DHCP Server**.

■ 4.3.1.1 Ethernet

Ethernet	
Primary IP Address	
IP Address	<input type="text" value="192.168.0.254"/>
SubnetNetmask	<input type="text" value="255.255.255.0"/>
RIP	<input type="text" value="NO RIP"/> ▼
Secondary IP Address	
The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask.	
IP Address	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The router supports two Ethernet IP addresses in the LAN, and two different LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN, so there is no need to configure a Secondary IP address. The default IP address for the router is 192.168.0.254.

RIP: RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.



The Subnet mask of the Secondary IP Address depends on the setting of the Primary IP Address.

4.3.1.2 Wireless

Wireless	
Parameters	
Mode	802.11b+g
ESSID	wlan_ap
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
MAC Address	00:11:09:0d:96:48
AP Version	IPN2220AP Ver:1.45.10.2004
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC Address	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **Mode:** 802.11b + g (Mixed mode), 802.11b and 802.11g. The factory default is 802.11b + g.

● **ESSID:** Enter the unique ID given to the Access Point (AP), which is already built-in to the router's wireless interface. To connect to this device, your wireless clients must have the same ESSID as the device.

● **Regulation Domain:** There are five Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

● **Channel ID:** Select the ID channel that you would like to use.

● **MAC Address:** The AP's MAC Address

● **AP Version:** The Access Point firmware version.

● **WDS Service:**

⊙ **Disable:** Any client that using the "any" setting cannot discover the Access Point (AP) in question.

⊙ **Enable:** Any client that using the "any" setting can discover the Access Point (AP) in question.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply define peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client

device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

● **WDS Service:** The default setting is **Disable**. Check **Enable** radio button to activate this function.

● **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other. **(Note: For MAC Address, Semicolon (:) must be included)**

■ 4.3.1.3 Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network.

The default mode of wireless security is **disabled**.

Wireless Security	
Parameters	
Security Mode	Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● WPA Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA Pre-Shared Key
WPA Algorithm	TKIP
WPA Shared Key	0000000000
Group Key Renewal	3600 Seconds
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **WPA Algorithms:** TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

● **WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

● **Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

● **Hide ESSID:** User can select Enable or Disable to hide ESSID.

● WPA2 Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA2 Pre-Shared Key ▾
WPA2 Algorithm	TKIP ▾
WPA2 Shared Key	0000000000
Group Key Renewal	3600 Seconds

● **WPA2 Algorithms:** TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

● **WPA2 Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

● **Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

● WEP

Wireless Security	
Parameters	
Security Mode	WEP ▾
WEP Encryption	HEX ▾ <input checked="" type="radio"/> WEP64 <input type="radio"/> WEP128
<input checked="" type="radio"/> Key 1	0000000000
<input type="radio"/> Key 2	0000000000
<input type="radio"/> Key 3	0000000000
<input type="radio"/> Key 4	0000000000
Passphrase	<input type="text"/> <input type="button" value="Generate Key"/>
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

**** WDS uses Key 1 for WEP encryption. ****

● **WEP Encryption:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64** and **WEP 128**. WEP 128 will offer increased security over WEP 64.

● **Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled..

● **Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively. For example, using WEP64, 1122334455 is a valid key.

● **Hide ESSID:** User can select Enable or Disable to hide ESSID.

■ 4.3.1.4 DHCP Server

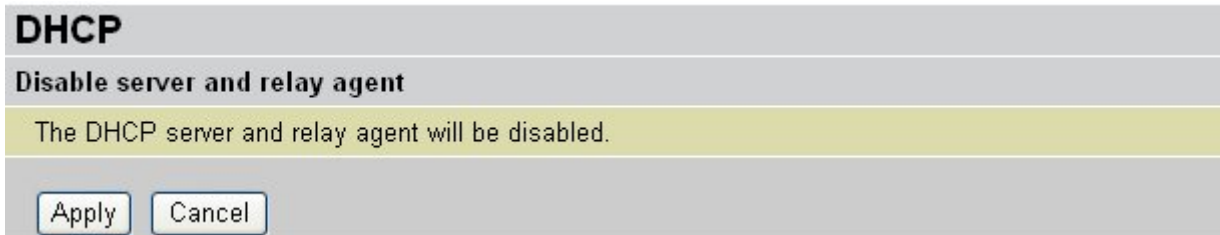
You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server	
Configuration	
DHCP Server Mode	<input type="radio"/> Disable
	<input checked="" type="radio"/> DHCP Server
	<input type="radio"/> DHCP Relay Agent
<input type="button" value="Next"/>	

DHCP Server Status	
Status	DHCP Server Running
Subnet Definitions	
Subnet Value	192.168.0.0
SubnetNetmask	255.255.255.0
Domain Name	home.gateway
DNS Server	192.168.0.254
Maximum/Default Lease Time	86400 / 43200 seconds
IP Range	192.168.0.100 - 192.168.0.199

To disable the router's DHCP Server, check **Disabled** and click **Next** then click **Apply**. When the DHCP Server is disabled you need to manually assign a fixed IP address to each

PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.0.254).



To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).

DHCP SERVER

Parameters

Domain Name	<input type="text" value="home.gateway"/>
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	<input type="text" value="192.168.0.254"/>
Secondary DNS Server Address	<input type="text"/>
Default Lease Time	<input type="text" value="43200"/> seconds
Maximum Lease Time	<input type="text" value="86400"/> seconds
Range Start	<input type="text" value="192.168.0.100"/>
Range End	<input type="text" value="192.168.0.199"/>

Specify fixed Mac Address Mapping to fixed IP Address (optional)

	Host Name	MAC Address	IP Address
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

The MAC address is represented as a string of 2 digit hexadecimal numbers seperated by colons (:) - (eg. 00:11:22:33:44:55)

If you check **DHCP Relay Agent** and click **Next** then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.

DHCP Relay

Parameters

DHCP Relay Server	<input type="text"/>
-------------------	----------------------

4.3.2 WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are three items within the **WAN** section: **ISP**, **DNS** and **ADSL**.

4.3.2.1 ISP

The factory default is 1483_Routed_mode. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use 1483_Routed_mode, you can change the default WAN connection entry by clicking **Change**.

A simpler alternative is to select **Quick Start** from the main menu on the left. See the Quick Start section of the manual for more information.

WAN Connection						
WAN Services Table						
Name	Description	Creator	VPI	VCI		
RFC1483 Routed	1483_Routed_mode	admin	0	33	Edit	Change

RFC 1483 Routed Connections

WAN Connection		
RFC 1483 Routed		
Description	<input type="text" value="1483_Routed_mode"/>	
VPI	<input type="text" value="0"/>	
VCI	<input type="text" value="33"/>	
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Encapsulation Method	<input type="text" value="LLC Bridged"/>	
IP Assignment	<input checked="" type="radio"/> Obtain an IP address automatically via DHCP client	
	<input type="radio"/> Use the following IP address	
	IP Address	<input type="text" value="0.0.0.0"/>
	Netmask	<input type="text" value="0.0.0.0"/>
	Gateway	<input type="text" value="0.0.0.0"/>
RIP	<input type="text" value="No RIP"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Description: Your description of this connection.

VPI and VCI: Enter the information provided by your ISP.

● **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

● **Encapsulation method:** Select the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.

● **DHCP client:** Enable or disable the DHCP client, specify if the router can get an IP address from the Internet Service Provider (ISP) automatically or not.

● **Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

● **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

● **PPPoA Routed Connections**

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.

WAN Connection	
PPPoA Routed	
Description	PPPoA
VPI	0
VCI	0
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
RIP	No RIP
MTU	1492

Apply Cancel

● **Description:** User-definable name for the connection.

● **VPI/VCI:** Enter the information provided by your ISP.

● **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

● **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

● **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

● **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

● **Authentication Protocol Type:** Default is **Chap (Auto)**. Your ISP advises you whether to use **Chap** or **Pap**.

● **Connection:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

● **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

● **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.

Apply

WAN Connection

WAN Services Table

Name	Description	Creator	VPI	VCI		
PPPoA Routed	PPPoA	admin	0	32	Edit ▶	Change ▶

● PPPoE Routed Connections

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

WAN Connection	
PPPoE Routed	
Description	PPPoE
VPI	0
VCI	33
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
Service Name	
IP Address	0.0.0.0 (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
Idle Timeout	10 minutes
RIP	No RIP
MTU	1492
PPPoE Relay	<input type="checkbox"/> Enable

Apply Cancel

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the information provided by your ISP.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **20** alphanumeric characters.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Authentication Protocol:** Default is **Chap**. Your ISP advises on using **Chap** or **Pap**.

● Connection:

Ⓒ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

Ⓒ **Connect to Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

● **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

● **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

● **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Apply

WAN Connection						
WAN Services Table						
Name	Description	Creator	VPI	VCI		
PPPoE Routed	PPPoE	admin	0	32	Edit ▶	Change ▶

● RFC 1483 Bridged Connections

WAN Connection	
RFC 1483 Bridged	
Description	<input type="text" value="1483_Bridged_mode"/>
VPI	<input type="text" value="0"/>
VCI	<input type="text" value="0"/>
Encapsulation Method	<input type="text" value="LLC Bridged"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **Description:** A user-definable name for this connection.

● **VPI/VCI:** Enter the information provided by your ISP.

● **Encapsulation method:** Select the encapsulation format, this is provided by your ISP.

4.3.2.2 DNS

DNS	
Parameters	
Obtain DNS automatically	<input checked="" type="checkbox"/> Enable
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as `www.yahoo.com` and an IP address. An IP address is a 32-bit number in the form of `xxx.xxx.xxx.xxx`, for example `192.168.0.254`. You can think of an IP address as a telephone number for devices on the Internet, and the DNS allows you to find the telephone number for any particular domain name. Since an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP provides the DNS IP address automatically. You may leave the configuration field blank. Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

If you choose one of the other protocols, RFC1483 Routed or Bridged, check with your ISP, as it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS Server address on your PC to the LAN IP address of this router.

4.3.2.3 ADSL

ADSL	
Parameters	
ADSL Mode	Annex A
Modulator	Auto
DSP FirmwareVersion	DMT FwVer: 3.5.6.1_A_TC, HwVer:T14F7_1.0
DMT Status	Down
Operational Mode	-----
Upstream	0 kbps
Downstream	0 kbps

● **ADSL Mode:** There are four modes “Open Annex Type and Follow DSLAM's Setting”, “Annex A Only”, “Annex L Only” and “Annex M Only” that user can select for this connection.

● **Modulator:** There are four modes “**AUTO**”, “**ADSL multimode**”, “**ADSL2**” and “**ADSL2+**” that user can select for this connection.

● **DSP Firmware Version:** DSP code version

● **DMT Status:** DMT Status

● **Operational Mode:** To show the state when user select “AUTO” on connect mode.

● **Annex Type:** To show the router's type, e.g. Annex A, Annex B

● **Upstream:** Upstream rate

● **Downstream:** Downstream rate


4.3.3 System

There are six items within the **System** section: **Time Zone**, **Remote Access**, **Firmware Upgrade**, **Backup/Restore**, **Restart** and **User Management**.

■ 4.3.3.1 Time Zone

Time Zone	
Parameters	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local Time Zone (+GMT Time)	(GMT+02:00)Helsinki, Riga, Tallinn ▼
SNTP Server IP Address	192.43.244.18
	129.6.15.29
	128.138.140.44
	131.107.1.10
Daylight Saving	<input checked="" type="checkbox"/> Automatic
Resync Period	1440 minutes

v

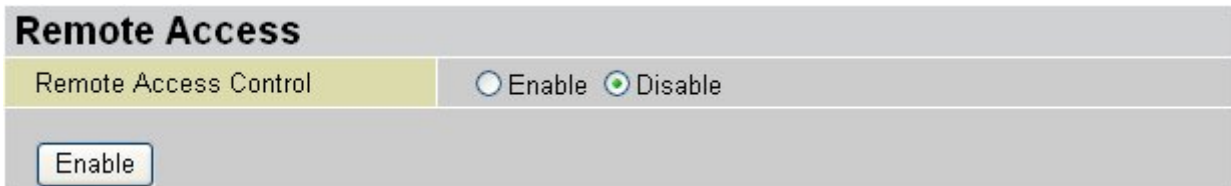


The map shows a world map with landmasses in green and oceans in blue. A small 'v' is centered above the map.

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

4.3.3.2 Remote Access



Remote Access

Remote Access Control Enable Disable

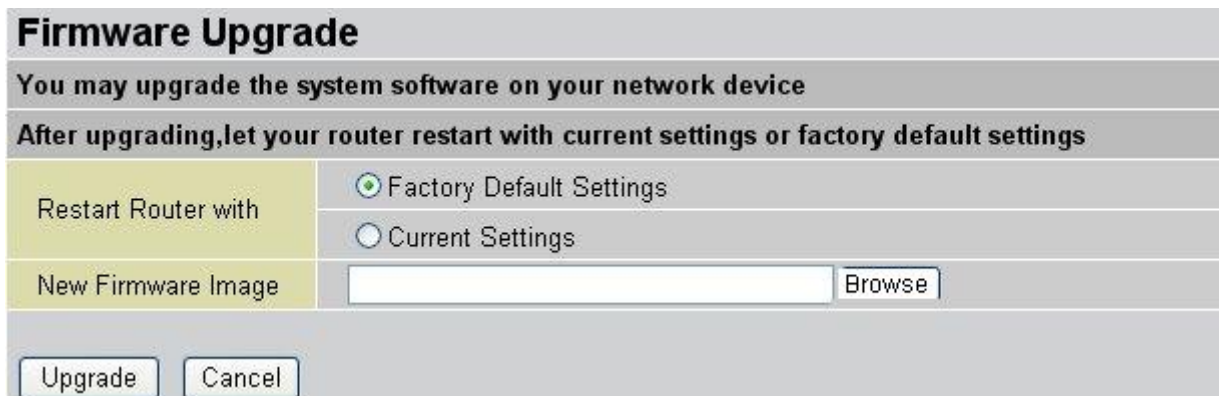
Enable

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router permits remote access for and click **Enable**. You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

4.3.3.3 Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



Firmware Upgrade

You may upgrade the system software on your network device

After upgrading, let your router restart with current settings or factory default settings

Restart Router with Factory Default Settings Current Settings

New Firmware Image Browse

Upgrade Cancel

● **Restart Router with:** To choose "Factory Default Setting" or "Current Settings" that user want.

● **New Firmware Image:** Type in the location of the file you wish to upload in this field or click **Browse ...** to find it.

● **Browse...:** Click **Browse...** to find the afw file you wish to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

● **Upgrade:** Click **upgrade** to begin the upload process. This process may take up to two minutes.



DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. Please see section 2.4 for emergency recovery procedures.

■ 4.3.3.4 Backup / Restore

Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Backup

Restore Configuration

Configuration File

Browse...

"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

■ 4.3.3.5 Restart Router

Click **Restart** with option **Current Settings** to reboot your router and restore your last saved configuration.

Restart

After restarting. Please wait for several seconds to let the system

Restart Router with

Save Config to Flash
 Current Settings
 Factory Default Settings

Restart Cancel

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

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

4.3.3.6 User Management

User Management

Current Defined Users

Valid	User	
true	admin	Edit ▶

Create ▶

To prevent unauthorized access to your router's configuration interface, all users are required to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit**, you are shown the following options:

User Management

Edit

Username	admin
Password	•••••
Valid	true

Apply Cancel

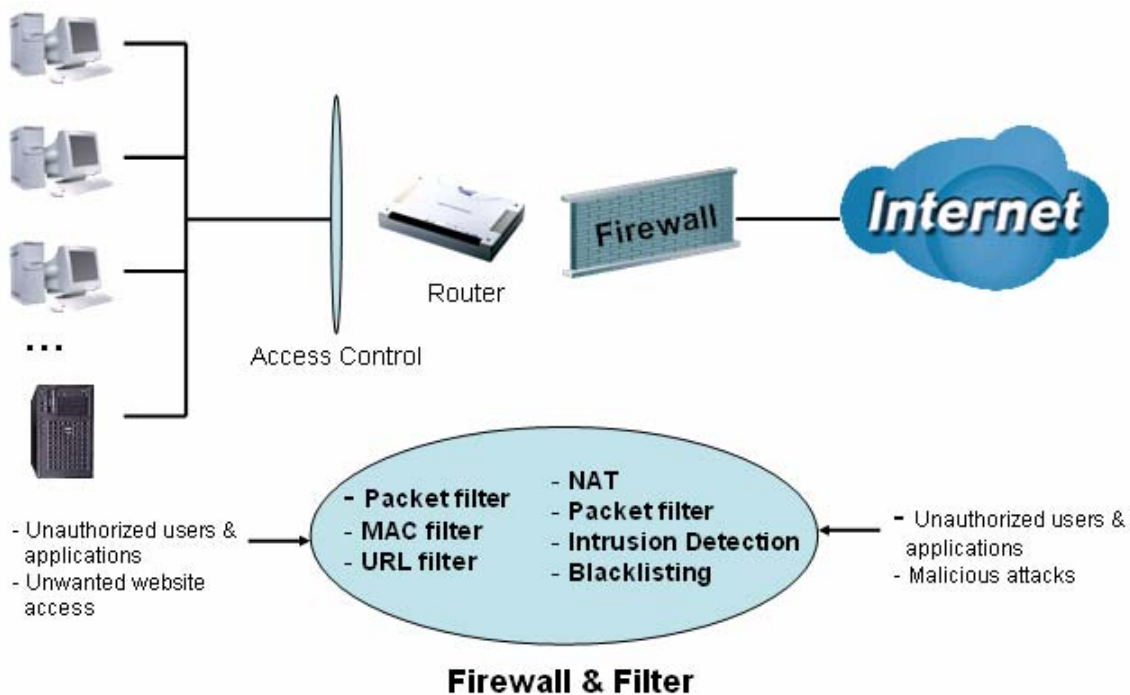
You can change the user's **password**, whether their account is active and **Valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking **Cancel** when editing the user.

You are strongly advised to change the password on the default “**admin**” account when you receive your router, and any time you reset your configuration to Factory Defaults.

4.3.4 Firewall

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.



When using Virtual Servers (port forwarding) your PCs are exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

URL Filter: Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: Packet Filter, Ethernet MAC Filter, Wireless MAC Filter, Intrusion Detection, Block WAN Request and URL Filter..

4.3.4.1 Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action is taken.

Packet Filter														
Default Rules Forward														
Parameters														
Rule No.	Active	Flow	Packet Type	Action	Source IP		Source Port		Destination IP		Dest. Port		Log	Schedule Time
					from	to	from	to	from	to	from	to		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>														
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>														

Add: Click this button to add a new packet filter rule and the next figure appears.

Edit: Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

Firewall - Packet Filter									
Parameters									
Rule 1	<input checked="" type="radio"/> Outgoing <input type="radio"/> Incoming								
Active	Yes		Packet Type	Any					
Log	Yes		Action When Matched	Drop					
Source IP Address				Destination IP Address					
From	<input type="text"/>			From	<input type="text"/>				
To	<input type="text"/>			To	<input type="text"/>				
Source Port				Destination Port					
From	<input type="text"/>			From	<input type="text"/>				
To	<input type="text"/>			To	<input type="text"/>				
<input checked="" type="radio"/> Always									
<input type="radio"/> Schedule from									
				08	:	00	to 18	:	00
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat									
<input type="button" value="Return"/> <input type="button" value="Cancel"/>									

Outgoing **Incoming:** Determine whether the rule is for outgoing packets or for incoming packets.

- **Active:** Choose “Yes” to enable the rule, or choose “No” to disable the rule.
- **Packet Type:** Specify the packet type (TCP, UDP, ICMP or any) that the rule applies to. Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.
- **Log:** Choose “Yes” if you wish to generate logs when the filter rule is applied to a packet.
- **Action When Matched:** If a packet matches this filter rule, **Forward** or **Drop** this packet.
- **Source IP Address:** Enter the incoming or outgoing packet’s source IP address(es).
- **Source Port:** Check the TCP or UDP packet’s source port number(s).
- **Destination IP Address:** Enter the incoming or outgoing packet’s destination IP address(es).
- **Destination Port:** Check the TCP or UDP packet’s destination port number(s).
- **Schedule time:** User can setup the time to use the packet filter.



Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

■ 4.3.4.2 Ethernet MAC Filter

A Ethernet MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network’s interface (i.e. its Network Interface Card or Ethernet card). Using your router’s MAC Address Filter function, you can configure the switch to only accept traffic from specified machines, or else to block specific machines from accessing your LAN. There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.

Ethernet MAC Filter

Default Rules Forward ▾

Parameters

	Rule No.	Active	Action	Log	MAC Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Ethernet MAC Filter

Default Rules Forward ▾

Parameters

	Rule No.	Active	Action	Log	MAC Address
<input checked="" type="radio"/>	1	Yes	Drop	Yes	00:04:ed:ff:f1:23
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

MAC Address Filter

Parameters

Rule 1

Active	Yes ▾
Action When Matched	Drop ▾
Log	Yes ▾
Mac Address	<input type="text"/> Candidates ▶

- **Active:** Select **Yes** from the drop down list box to enable MAC address filtering.
- **Action When Matched:** Select “Drop” or “Forward”.
- **Log:** Choose “Yes” if you wish to generate logs when the filter rule is applied to a packet.
- **MAC Address:** Enter the MAC addresses you wish to manage.
- **Candidates:** it automatically detects devices connected to the router through the Ethernet.

Associated Clients	
MAC	IP Address
<input checked="" type="radio"/> 00:0D:88:18:7D:F7	192.168.1.125
<input type="button" value="Add"/>	

■ 4.3.4.3 Wireless MAC Filter

The MAC Address supports up to 30 wireless network machines and helps you to manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) to access your LAN.

There are no pre-define MAC Address filter rules; you can add the filter rules to meet your requirements

Wireless MAC Filter					
Default Rules		Forward <input type="button" value="v"/>			
Parameters					
	Rule No.	Active	Action	Log	MAC Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Wireless MAC Filter

Default Rules Forward ▾

Parameters

	Rule No.	Active	Action	Log	MAC Address
<input type="radio"/>	1	Yes	Drop	Yes	00:04:ed:ff:f1:26
<input checked="" type="radio"/>	2	Yes	Drop	Yes	00:04:ed:ff:f1:25

Add Edit Delete

Apply Cancel

MAC Address Filter

Parameters

Rule 1

Active	Yes ▾
Action When Matched	Drop ▾
Log	Yes ▾
Mac Address	<input type="text"/> Candidates ▶

Return Cancel

- **Active:** Select **Yes** from the drop down list box to enable MAC address filtering.
- **Action When Matched:** Select “Drop” or “Forward”.
- **Log:** Choose “Yes” if you wish to generate logs when the filter rule is applied to a packet.
- **MAC Address:** Enter the MAC addresses you wish to manage.
- **Candidates:** it automatically detects devices connected to the router through the Ethernet.

■ 4.3.4.4 Intrusion Detection

Check “Enable” if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users are not able to access network resources.

Intrusion Detection	
Parameters	
Intrusion Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Alert Mail	<input type="checkbox"/>
Alert Mail Time	<input type="text" value="30"/> minutes
Your E-mail(Must be xxx@yyy.zzz)	<input type="text"/>
Recipient's E-mail(Must be xxx@yyy.zzz)	<input type="text"/>
SMTP server	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **Intrusion Detection:** Check “Enable” if you wish to detect intruders accessing your computer without permission.

● **Alert Mail:** Select this check box to use Alert Mail.

● **Alert Mail Time:** Set the time for receiving Alert mail.

● **Your E-Mail:** Set your email address.

● **Recipient’s E-mail:** Set the Recipient’s email address to which the E-<mail notification is sent.

● **SMTP server:** Set the SMTP (mail) server address.

■ 4.3.4.5 Block WAN Request

Check “Enable” if you wish to exclude outside PING requests from reaching this router.

Block WAN Request	
Parameters	
Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

■ 4.3.4.6 URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.yahoo.com> or <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

URL Filter								
	Rule No.	Active	PC IPs		Block Mode	Keywords Filtering	Domains Filtering	Restrict URL Features
			from	to				
<input checked="" type="radio"/>	1	Yes	192.172.5.3	192.172.5.223	Always Block	Disabled	Disabled	Block Java Applet, Cookies
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

Url Filter

Parameters

Rule 1 Active

PC IP Address Range

From To

Block Mode

Always Block

Block from : to :

Sun Mon Tue Wed Thu Fri Sat

Keywords Filtering Enable

Domains Filtering Enable

Restrict URL Features

Block Java Applet

Block ActiveX

Block Cookies

Block Proxy

- **Active:** Select **Yes** from the drop down list box to enable or disable the URL Filter feature.
- **Always Block:** Select to always check URL filter rules (i.e. at all hours of the day).
- **Block from:** Specify the time period to check URL filter rules (e.g. during work hours).
- **Keywords Filtering:** Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif"). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL <http://www.abc.com/abcde.html> would be dropped since the keyword "abcde" occurs in the URL.

Keywords Filtering

Create

Keyword

Block WEB URLs which contain these keywords

Name	Keyword
<input type="text"/>	<input type="text"/>

Domains Filtering: Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please note that only the domain is specified, not the full URL. For example to block traffic to www.sex.com, enter "sex" or "sex.com" instead of "www.sex.com". In the example below, the URL request for www.abc.com is sent to the remote web server because it is listed in the trusted list, while the URL request for www.sex or www.sex.com is dropped because sex.com is in the forbidden list.

Domains Filtering

Create

Domain Name

Forbidden Domains

Name	Domain	
item1	sex	<input type="button" value="Delete"/>
item2	alcohol	<input type="button" value="Delete"/>

Restrict URL Features

- ⊙ **Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- ⊙ **Block ActiveX:** Blocks ActiveX
- ⊙ **Block Cookies:** Blocks Cookies
- ⊙ **Block Proxy:** Blocks Proxy

4.3.5 QoS (Quality of Service)

Quality of Service Introduction

If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in routers is such a breakthrough for home users and office users.

QOS: Keeping Your Net Connection Fast and Responsive

Configurable by source IP address, destination IP address, protocol, and port, the Quality of Service (QOS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QOS Setup

Please choose the **QOS** in the **Configuration** item of the left window as depicted below.

The screenshot shows a configuration window titled "QoS". It includes sections for "Maximal ISP Bandwidth" with input fields for "Upstream(LAN->WAN)" (256 Kbps) and "Downstream(WAN->LAN)" (2048 Kbps). Below is a "QoS Rule List" table with columns for Application, Time Schedule, Direction, and Assigned Bandwidth Ratio. A "Non-Assigned Bandwidth Ratio" section shows "LAN to WAN : 100%" and "WAN to LAN : 100%". At the bottom are buttons for "Add", "Edit", "Delete", "Apply", and "Cancel".

QoS Rule List			
Application	Time Schedule	Direction	Assigned Bandwidth Ratio
Non-Assigned Bandwidth Ratio			
LAN to WAN : 100%		WAN to LAN : 100%	

After clicking the QOS item, you can Add/Edit/Delete a QOS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

QOS				
	Application	Time Schedule	Direction	Assigned Bandwidth Ratio
<input type="radio"/>	PPTP	Always On	LAN to WAN	20% (46kbps) Minimum Guaranteed Rate with High priority
<input type="radio"/>	VoIP	Always On	LAN to WAN	20% (46kbps) Minimum Guaranteed Rate with High priority
<input type="radio"/>	FTP Server	Always On	LAN to WAN	20% (46kbps) Fixed Rate
Non-Assigned Bandwidth Ratio			LAN to WAN : 40% , WAN to LAN : 100%	
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- **Application:** A name that identifies an existing policy.
- **Time Schedule:** Scheduling your QOS policy to be applied.
- **Direction:** The traffic flow direction to be controlled by the QOS policy.

There are two settings to be provided in the Router:

⊙ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. E.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QOS policy. So, you need to add a policy with LAN to WAN direction setting.

⊙ **LAN to WAN:** Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

● **Assigned Bandwidth Ratio:** This field shows the assigned bandwidth ratio in percentage for a QOS policy. If WAN connection to internet is established, the estimated transfer rate will be shown in kbps. You may specify a fixed transfer rate or Minimum Guaranteed Rate with priority for non-used bandwidth.

Non-Assigned Bandwidth Ratio: This field shows the available bandwidth ratio, for LAN to WAN and WAN to LAN, that has not yet assigned.

: Press this button to add a new QOS policy.

: Before using these buttons to edit or delete a policy, please select one policy

you want to edit/delete from the radio option VoIP .

: After you have configured the policies, you can press this button to apply the

configuration. If you want to make the change persistent in flash, choose

Save Config to Flash

in the left windows to save it into flash.

When you press **Add** or **Edit** buttons described above, the following page will show up in your browser. You can use it to define a QOS policy.

QOS			
Parameters			
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN		
Application	FTP Server		
Packet Type	TCP		
Assigned Data Rate	Rate Type: Fixed (Maximum)	Data Ratio: 20 %	Priority for Non-used Bandwidth: Normal
DSCP Marking (LAN to WAN only)	Disabled		
Local Machine IPs	From 192.168.0.1	To	
Remote Machine IPs	From	To	
Local Application Ports	From	To	
Remote Application Ports	From	To	
Schedule Time	<input type="radio"/> Always		
	<input checked="" type="radio"/> Schedule from	09 : 00	to 17 : 00
<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat			
Apply		Cancel	

Controlled Traffic Flow: Specify the traffic flow you want to control. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

Packet type: The packet type will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

ANY: No specified protocol type is specified.

TCP

UDP

ICMP

⊙ **GRE:** For PPTP VPN Connections.

● **Assigned Data rate:** Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is $20\% * 256 * 0.9 = 46\text{kbps}$. (For 0.9 is an estimated factor for the effective data transfer rate for a ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

● **Data Ratio:** percentage for the data rate to be controlled by this policy. As above FTP server examples, it is 20.

● **Rate Type:** We provide 2 types here:.

⊙ **Fixed (Maximum):** specify a fixed data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

⊙ **Guaranteed (Minimum):** specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

● **Priority for Non-used Bandwidth:** Specify the priority for the bandwidth that is not used. For examples, you may specify two different QOS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

⊙ **High**

⊙ **Normal:** The default is normal priority.

⊙ **Low**

For the sample priority assignment for different policies, it is saved in a First-In-First-Out way.

● **DSCP Marking:** Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

DSCP Mapping Table	
Disabled	None

Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

● **Local Machine IPs:** The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

● **Remote Machine IPs:** The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

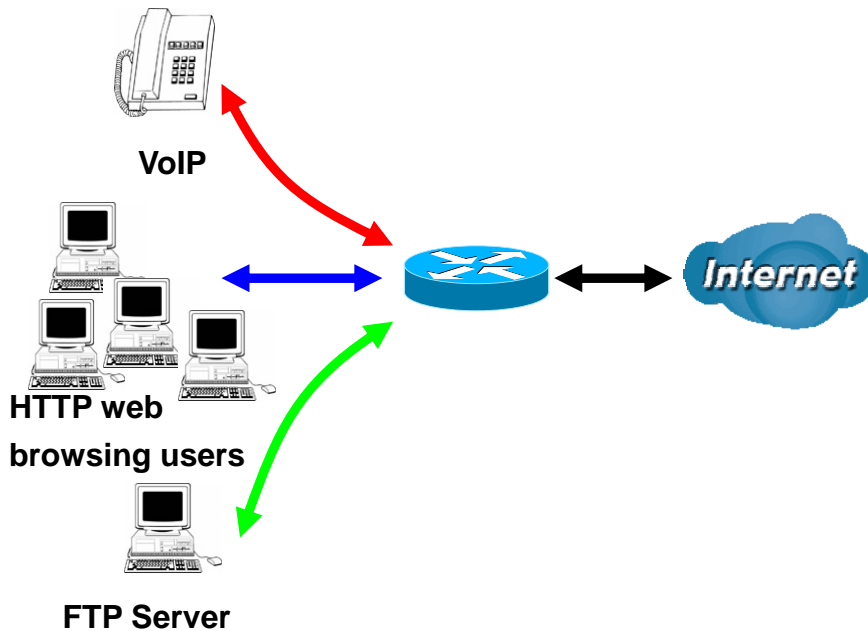
● **Local Application Ports:** The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

● **Remote Application Ports:** The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

● **Schedule Time:** Schedule your QOS policy.

■ QOS example for your Network

Connection Diagram



ADSL Subscription Rate

Upstream: 256 kbps

Downstream: 2048 Mbps

Example QOS Plan

∴

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.0.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with SDCP marking Class 1 Gold Service	Always
FTP Sever	192.168.0.100	Incoming and Going	outgoing :minimal 30%. Data rate. incoming :minimal 30%. Data rate. Both with low priority for non-used bandwidth.	Only Working Hours 9:00 to 17:00 Monday to Friday.
HTTP web browsing users	80	Incoming and Going	outgoing : limited 20%. Data rate. incoming : limited 30%. Data rate.	Always

Example QOS Setup

QOS				
	Application	Time Schedule	Direction	Assigned Bandwidth Ratio
<input type="radio"/>	VoIP	Always On	LAN to WAN	20% (46kbps) Minimum Guaranteed Rate with High priority
<input type="radio"/>	FTP_Server_Out	Day Time	LAN to WAN	30% (69kbps) Minimum Guaranteed Rate with Low priority
<input type="radio"/>	FTP_Server_In	Day Time	WAN to LAN	30% (522kbps) Minimum Guaranteed Rate with Low priority
<input type="radio"/>	HTTP_Browsing_Out	Always On	LAN to WAN	20% (46kbps) Fixed Rate
<input type="radio"/>	HTTP_Browsing_In	Always On	WAN to LAN	30% (522kbps) Fixed Rate
	Non-Assigned Bandwidth Ratio		LAN to WAN : 30% , WAN to LAN : 40%	
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

VoIP application

Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

QoS

Parameters	
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN
Application	<input type="text" value="FTP"/>
Packet Type	<input type="text" value="ANY"/>
Assigned Data Rate	Rate Type: <input type="text" value="Guaranteed (Minimum)"/> Data Ratio: <input type="text" value="20"/> % Priority for Non-used Bandwidth: <input type="text" value="High"/>
DSCP Marking (LAN to WAN only)	<input type="text" value="Gold service(L)"/>
Local Machine IPs	From <input type="text" value="192.168.0.1"/> To <input type="text"/>
Remote Machine IPs	From <input type="text"/> To <input type="text"/>
Local Application Ports	From <input type="text"/> To <input type="text"/>
Remote Application Ports	From <input type="text"/> To <input type="text"/>
Schedule Time	<input checked="" type="radio"/> Always
	<input type="radio"/> Schedule from <input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/> <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Above settings will help to improve quality of your VoIP service when traffic is full loading.

FTP Server Application

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.

LAN to WAN direction:

QOS			
Parameters			
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN		
Application	FTP_Server_Out		
Packet Type	ANY		
Assigned Data Rate	Rate Type: Guaranteed (Minimum)	Data Ratio: 30 %	Priority for Non-used Bandwidth: Low
DSCP Marking (LAN to WAN only)	Disabled		
Local Machine IPs	From 192.168.0.100	To	
Remote Machine IPs	From	To	
Local Application Ports	From	To	
Remote Application Ports	From	To	
Schedule Time	<input type="radio"/> Always		
	<input checked="" type="radio"/> Schedule from		09 : 00 to 17 : 00
	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat		
Apply		Cancel	

WAN to LAN direction:

QOS			
Parameters			
Controlled Traffic Flow	<input type="radio"/> LAN to WAN <input checked="" type="radio"/> WAN to LAN		
Application	<input type="text" value="FTP_Server_In"/>		
Packet Type	<input type="text" value="ANY"/>		
Assigned Data Rate	Rate Type: <input type="text" value="Guaranteed (Minimum)"/>	Data Ratio: <input type="text" value="30"/> %	Priority for Non-used Bandwidth: <input type="text" value="Low"/>
DSCP Marking (LAN to WAN only)	<input type="text" value="Disabled"/>		
Local Machine IPs	From <input type="text" value="192.168.0.100"/>	To <input type="text"/>	
Remote Machine IPs	From <input type="text"/>	To <input type="text"/>	
Local Application Ports	From <input type="text"/>	To <input type="text"/>	
Remote Application Ports	From <input type="text"/>	To <input type="text"/>	
Schedule Time	<input type="radio"/> Always		
	<input checked="" type="radio"/> Schedule from		<input type="text" value="09"/> : <input type="text" value="00"/> to <input type="text" value="17"/> : <input type="text" value="00"/>
	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat		
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at day time.

HTTP Web Browsing

You can control the internet web browsing by specify the HTTP 80 (8080 for some proxy server).

LAN to WAN direction:

QOS			
Parameters			
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN		
Application	<input type="text" value="HTTP_Browsing_Out"/>		
Packet Type	<input type="text" value="ANY"/>		
Assigned Data Rate	Rate Type: <input type="text" value="Fixed (Maximum)"/>	Data Ratio: <input type="text" value="20"/> %	Priority for Non-used Bandwidth: <input type="text" value="Normal"/>
DSCP Marking (LAN to WAN only)	<input type="text" value="Disabled"/>		
Local Machine IPs	From <input type="text"/> To <input type="text"/>		
Remote Machine IPs	From <input type="text"/> To <input type="text"/>		
Local Application Ports	From <input type="text"/> To <input type="text"/>		
Remote Application Ports	From <input type="text" value="80"/> To <input type="text" value="0"/>		
Schedule Time	<input checked="" type="radio"/> Always		
	<input type="radio"/> Schedule from <input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/>		
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

WAN to LAN direction:

QOS			
Parameters			
Controlled Traffic Flow	<input type="radio"/> LAN to WAN <input checked="" type="radio"/> WAN to LAN		
Application	<input type="text" value="HTTP_Browsing_In"/>		
Packet Type	<input type="text" value="ANY"/>		
Assigned Data Rate	Rate Type: <input type="text" value="Fixed (Maximum)"/>	Data Ratio: <input type="text" value="30"/> %	Priority for Non-used Bandwidth: <input type="text" value="Normal"/>
DSCP Marking (LAN to WAN only)	<input type="text" value="Disabled"/>		
Local Machine IPs	From <input type="text"/>	To <input type="text"/>	
Remote Machine IPs	From <input type="text"/>	To <input type="text"/>	
Local Application Ports	From <input type="text"/>	To <input type="text"/>	
Remote Application Ports	From <input type="text" value="80"/>	To <input type="text" value="0"/>	
Schedule Time	<input checked="" type="radio"/> Always		
	<input type="radio"/> Schedule from	<input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/>	
	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat		
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

4.3.6 Virtual Server

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Virtual Server

Parameters

	Item	Type	Port Start	Port End	IP Address
<input type="radio"/>	1	TCP	23	23	192.168.1.2
<input checked="" type="radio"/>	2	UDP	500	500	192.168.1.68

DMZ
 Enable
 DMZ IP Address:

- **Item:** Item number
- **Type:** Select **TCP** if you wish to search for connection-based application services on the remote server using the port number.
- **Port Start & Port End:** Enter the public port number & range you wish to configure.
- **IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.
- **Add:** Click to add a new virtual server rule. Click again and the next figure appears.
- **Edit:** Check the Rule No. you wish to edit and then click "Edit".

● **Delete:** Check the Rule No. you wish to delete, then click “Delete”.

Virtual Server	
Parameters	
Item	1
Service select	User Defined
Protocol	User Defined
Start Port	Telnet (TCP:23)
End Port	SMTP (TCP:25)
IP Address	HTTP (TCP:80)
	POP3 (TCP:110)
	NNTP (TCP:119)
	NTP (TCP:123)
	HTTPS (TCP:443)
	IKE (UDP:550)
	T.120 (TCP:1503)
	H.323 (TCP:1720)
	PPTP (TCP:1723)

Return Cancel

● **Item:** Item number

● **Service select:** Select the service you wish to configure

● **Protocol:** Automatic when you choose Service select

● **Start Port & End Port:** Enter the public port number & range you wish to configure.


● **IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.0.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.0.2. If the port is not listed as a predefined application, you need to add it manually.

Virtual Server

Parameters

	Item	Type	Port Start	Port End	IP Address
	1	TCP	80	80	192.168.1.2

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ: The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.



Using port forwarding does have security implications, since outside users are 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 simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.



If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.

Attention



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 a static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are 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.

Attention

4.3.7 Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are four items within the **Advanced** section: **Static Route**, **Dynamic DNS**, **VLAN Control** and **Device Management**.

■ 4.3.7.1 Static Route

Click on **Routing Table** and then choose **Create Route** to add a routing table.

Static Route			
Add Rule1			
Destination	<input type="text"/>		
Netmask	<input type="text"/>		
Gateway	<input type="text"/>	Interface	Please Select <input type="button" value="v"/>
Cost	<input type="text" value="0"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Destination:** The destination subnet IP address.
- **Netmask:** Subnet mask of the destination IP addresses based on above destination.
- **Gateway:** The gateway IP address to which packets are forwarded.
- **Interface:** Select the interface through which packets are forwarded.
- **Cost:** Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

■ 4.3.7.2 Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still 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 ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

Dynamic DNS	
Parameters	
Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org (custom) ▾
Host	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Period	28 <input type="text"/> Days ▾
Wildcard	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

There are more than 5 DDNS services supported.

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The fields following are activated and required.
- **Dynamic DNS Server:** Select the DDNS service you have established an account with.
- **Host:** Enter one domain name you have registered.
- **Domain Name, Username and Password:** Enter your registered domain name and your username and password for this service.
- **Period:** Set the time period between updates, for the router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router performs an update when your dynamic IP address changes.
- **Wildcard:** Select this check box to enable the DYNDNS Wildcard.

■ 4.3.7.3 Vlan Control

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.

Vlan Control

Parameters

Vlan	<input checked="" type="radio"/> Port Base <input type="radio"/> Disable			
Vlan Port Setting	P1	P2	P3	P4
vlan1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
vlan2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
vlan3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
vlan4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

4.3.7.4 Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.

Device Management

Embedded Web Server

HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)	
-----------	---------------------------------	---------------------------	--

Universal Plug and Play (UPnP)

UPnP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
UPnP Port	<input type="text" value="2800"/>		

SNMP Access Control

SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write		

Apply Cancel

Embedded Web Server:

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses). The default value is the standard HTTP port, 80. You may specify an

alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.0.55**, and sets the logout time to be **100** seconds. The router only allows User A access from the IP address **192.168.0.55** to logon to the Web GUI by typing: <http://192.168.0.254.100> in their web browser. After 100 seconds, the device automatically logs out User A.

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

UPnP Port: The default setting is 2800. It is highly recommended that you use this port value. If the value conflicts with other ports already in use you may wish to change the port.

SNMP Access Control

Simple Network Management Protocol—software on a PC within the LAN is required to use this function.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string is checked against the string entered in the configuration file. Once the string name is matched, you can obtain this IP address and are able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string is checked against the string entered in the configuration file. Once a string name is matched, users from this IP address are able to view and modify data.

Trap Community: Specify a name and an IP address. This community string is checked

against the string entered in the configuration file. Once a string name is matched, users from this IP address are sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication, and define access rights from the identified IP address. Once authentication has succeeded, users from this IP address are able to view and modify data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security" but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

➤ **From RFC 1213 (MIB-II):**

- System group
- Interfaces group
- Address Translation group
- IP group
- ICMP group
- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

➤ **From RFC1650 (EtherLike-MIB):**

- dot3Stats

➤ **From RFC 1493 (Bridge MIB):**

- dot1dBase group
- dot1dTp group
- dot1dStp group (if configured as spanning tree)

- **From RFC 1471 (PPP/LCP MIB):**
 - pppLink group
 - pppLqr group

- **From RFC 1472 (PPP/Security MIB):**
 - PPP Security Group)

- **From RFC 1473 (PPP/IP MIB):**
 - PPP IP Group

- **From RFC 1474 (PPP/Bridge MIB):**
 - PPP Bridge Group

- **From RFC1573 (IfMIB):**
 - ifMIBObjects Group

- **From RFC1695 (atmMIB):**
 - atmMIBObjects

- **From RFC 1907 (SNMPv2):**
 - only snmpSetSerialNo OID

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

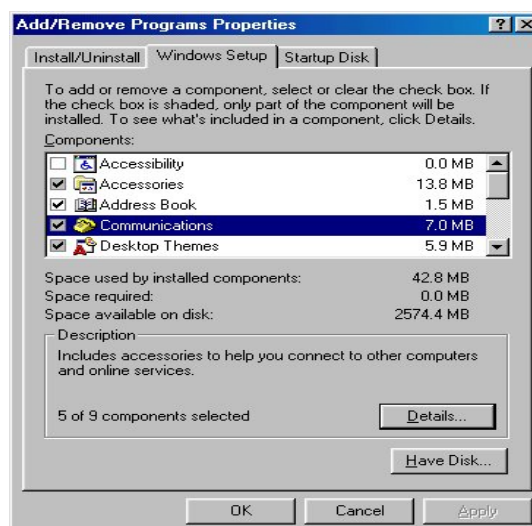
UPnP Port: The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

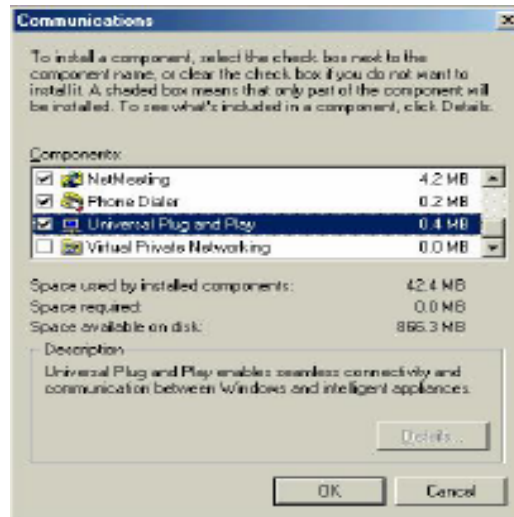
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

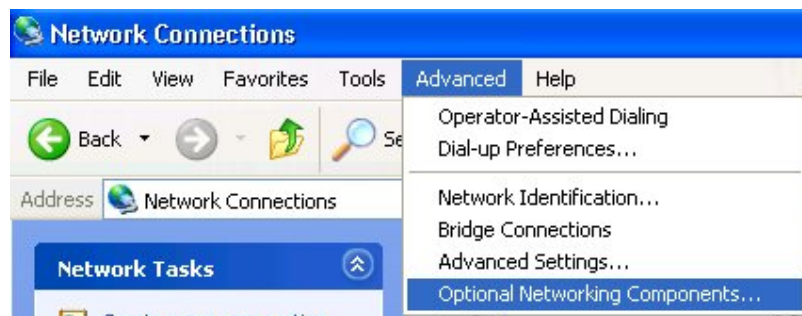
Step 5: Restart the computer when prompted.

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

Step 1: Click Start and Control Panel.

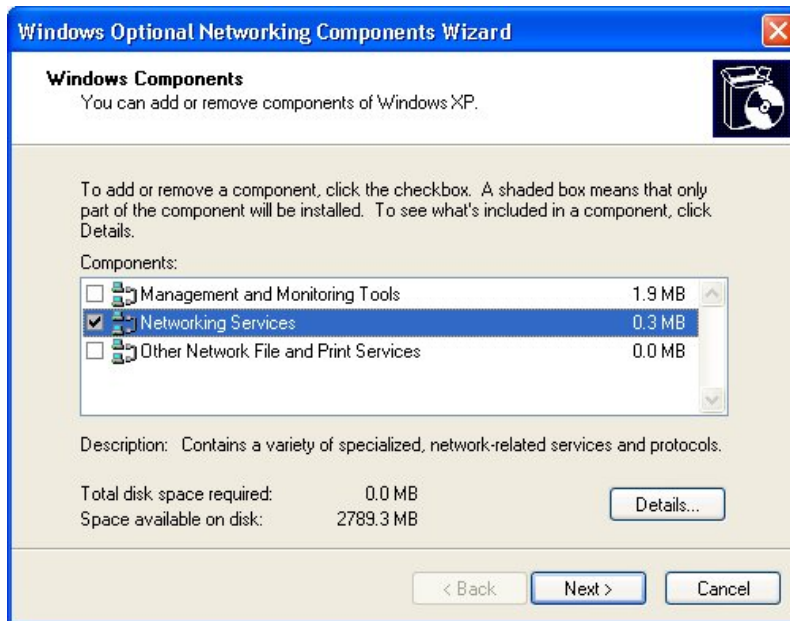
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components



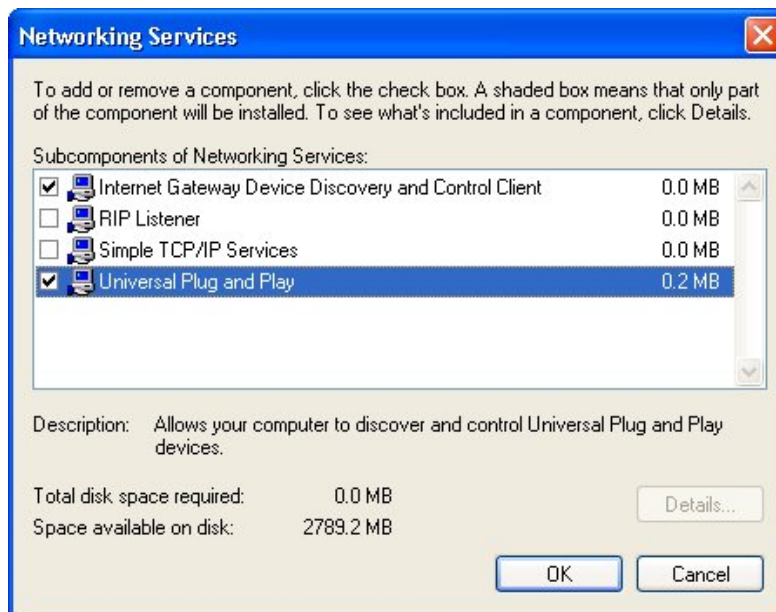
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



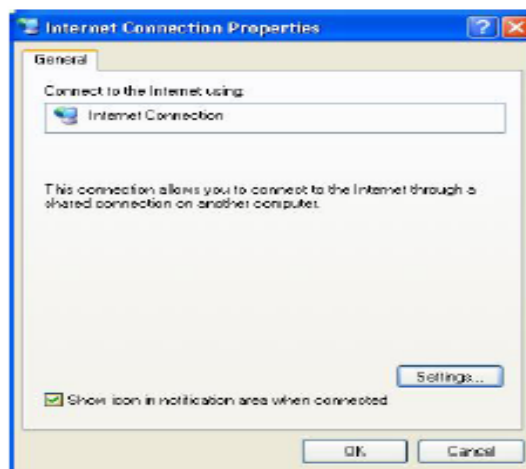
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

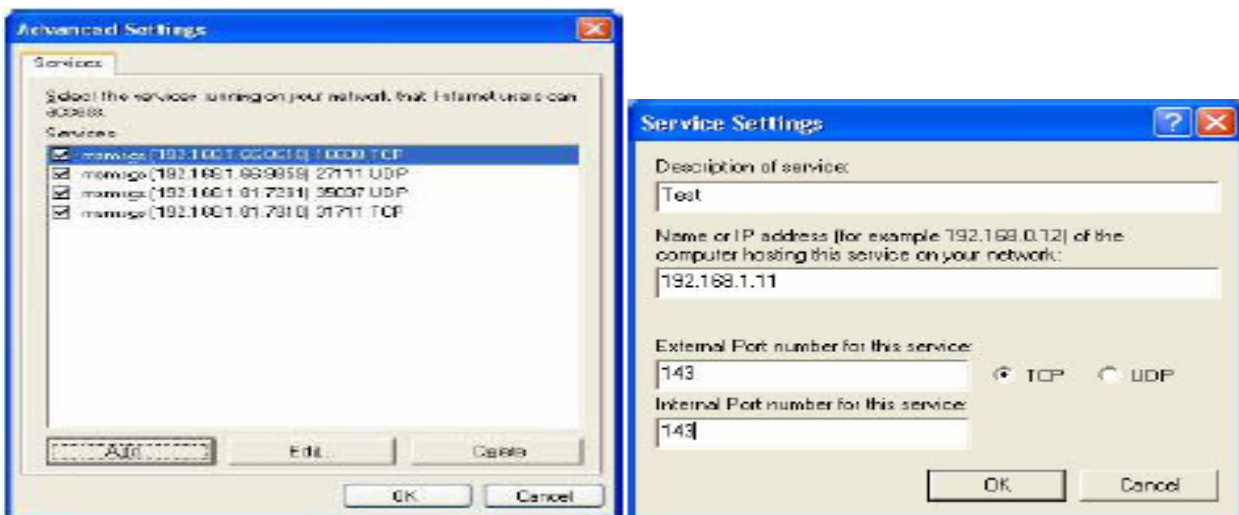
Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



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



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Web Configurator Easy Access

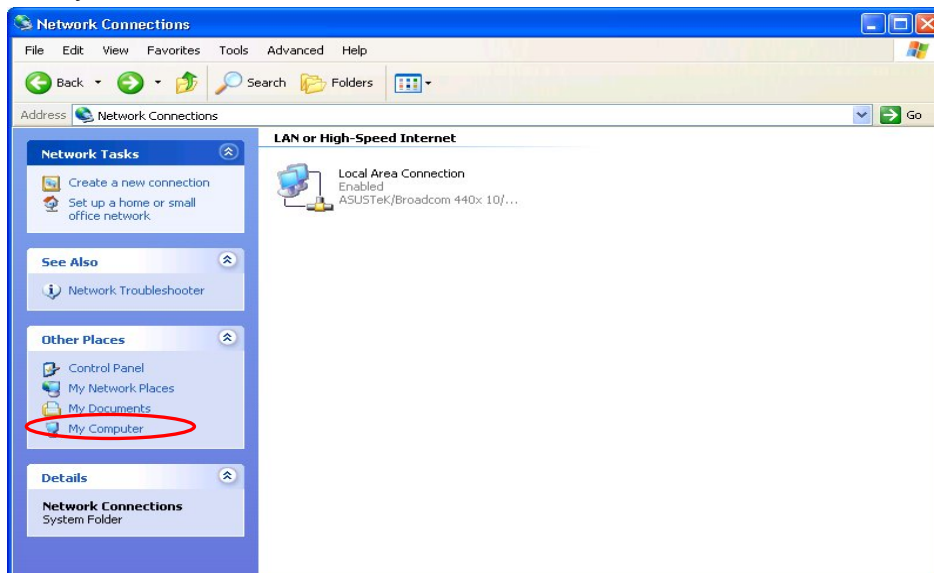
With UPnP, you can access web-based configuration for the router without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your router and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your router and select Properties. A properties window displays basic information about the router.

■ 4.3.7.5 IGMP

IGMP, known as *Internet Group Management Protocol*, is used to management hosts from multicast group.

IGMP	
Parameters	
IGMP Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

● **IGMP Proxy:** Accepting multicast packet. Default is set to **Enable**.

● **IGMP Snooping:** Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to **Enable**

■ 4.3.7.6 WAN IP Change Alert

WAN IP Change Alert	
Parameters	
Send a log via Email When WAN IP is changed	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

● Send a log via Email When WAN IP is changed. Default is set to **Disable**.

4.4 Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.

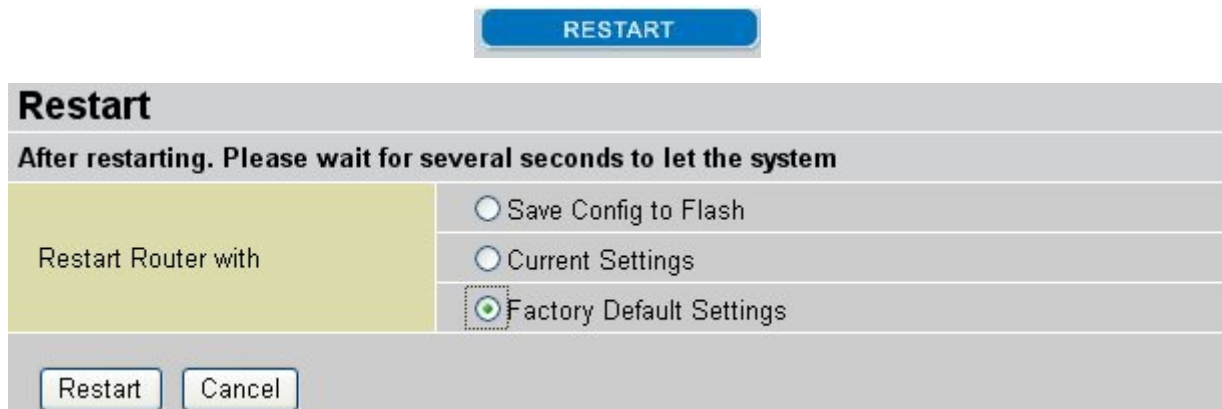
Save Config to Flash

Write settings to flash

Apply

4.5 Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



The screenshot shows a web interface for restarting a router. At the top, there is a blue button labeled "RESTART". Below it is a grey panel titled "Restart" with the instruction "After restarting. Please wait for several seconds to let the system". Underneath, there is a yellow box labeled "Restart Router with" followed by three radio button options: "Save Config to Flash", "Current Settings", and "Factory Default Settings". The "Factory Default Settings" option is selected and highlighted with a dashed box. At the bottom of the panel are two buttons: "Restart" and "Cancel".

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

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

Chapter 5

Troubleshooting

If your ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider or support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, please refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router for 6 seconds or more.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problems, you may need to verify these settings with your ISP.

<p>Frequent loss of ADSL linesync (disconnections).</p>	<p>Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.</p>
--	--

Problems with the LAN Interface

Problem	Corrective Action
<p>Can't ping any PCs on the LAN.</p>	<p>Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.</p> <p>Verify that the IP address and the subnet mask are consistent between the router and the workstations.</p>