



# **BEC 8800N**

## **802.11n VDSL2/ ADSL2+ Broadband Firewall Router**

### **User Manual**

# Table of Contents

<b>Chapter 1: Introduction .....</b>	<b>1</b>
Introduction to your Router.....	1
Features .....	4
Hardware Specifications .....	5
Physical Interface .....	5
Physical Specifications.....	5
Operating Environment .....	5
<b>Chapter 2: Installing the Router .....</b>	<b>6</b>
Package Contents.....	6
Important note for using this router .....	6
Device Description .....	7
The Front LEDs.....	7
The Rear Ports .....	8
Cabling.....	9
<b>Chapter 3: Basic Installation .....</b>	<b>10</b>
Hardware Connection .....	11
Network Configuration.....	12
Factory Default Settings.....	18
Information from your ISP .....	19
Internet Access Configuration .....	20
Configuring with your Web Browser .....	20
<b>Chapter 4: Configuration .....</b>	<b>21</b>
Status.....	22
WAN Info.....	23
Statistics.....	24
LAN .....	24
WAN Service .....	25
xTM .....	26
xDSL.....	27

Route Table.....	29
ARP Table .....	30
DHCP Table .....	31
System Log.....	32
<b>Configuration.....</b>	<b>33</b>
LAN - Local Area Network.....	34
LAN .....	34
WAN - Wide Area Network.....	36
Layer2 Interface.....	36
WAN Service .....	40
DSL.....	48
<b>System .....</b>	<b>49</b>
Time Zone .....	49
Firmware Upgrade.....	50
Backup / Restore .....	51
Restart.....	52
User Management .....	53
<b>Firewall.....</b>	<b>54</b>
IP Filtering .....	54
MAC Filtering.....	58
<b>QoS - Quality of Service.....</b>	<b>60</b>
Queue Config .....	61
QoS Classification .....	63
<b>Virtual Server .....</b>	<b>65</b>
Port Mapping .....	66
DMZ Host .....	68
<b>Advanced .....</b>	<b>69</b>
Routing.....	69
DNS.....	72
Interface Grouping.....	74
System Log Server .....	82
TR-069 Client .....	83

Diagnostics .....	84
Diagnostics .....	84
Fault Management .....	85
<b>Chapter 5: Troubleshooting .....</b>	<b>86</b>
<b>Appendix: Product Support &amp; Contact .....</b>	<b>87</b>

# Chapter 1: Introduction

## Introduction to your Router

Thank you for purchasing 8800N Wireless Broadband Firewall Router. Your new router is an all-in-one unit that combines an VDSL2/ADSL2+/Broadband router and Ethernet network to offer users the flexibility of multiple Internet connections. All this is offered while maintaining high-speed broadband access via VDSL2/ADSL2+.

The BEC 8800N automatically adopts the optimal connection to deliver smooth, constant signal reception even if obstacles are present. By using this device, you can easily enjoy high bandwidth applications such as High Definition IPTV services without changing their home network. A robust Firewall is also built in to provide protection against hacker attacks while the Quality of Service feature prioritizes queues and traffic for applications such as music downloads, online gaming, video streaming and file sharing.

## **Express Internet Access**

The BEC 8800N series is compliant with worldwide VDSL/ ADSL standards, and supports download rates of up to 100Mbps using VDSL2, 12 / 24Mbps using ADSL2 / 2+, 8Mbps using ADSL and an upload rate of up to 50Mbps using VDSL2, 1Mbps using ADSL / ADSL2 / ADSL2+. The integrated Annex M standard supports ADSL2 / 2+ for higher uploads by doubling the upload data rate. The 4-port 10/ 100 Mbps Fast Ethernet Switch incorporated into the BEC 8800N enables users to connect to multiple computers or wired-Ethernet devices easily and enjoy blistering LAN transmission for multimedia applications such as interactive gaming, IPTV video streaming and real-time audio.

## **Multi Network Protocol Support**

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

## **PPP over Ethernet (PPPoE)**

This device 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.

## **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. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

## **Network Address Translation (NAT)**

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

## **Domain Name System (DNS) Relay**

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in 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. For example, to use the service, you must first apply for an account from a DDNS service like <http://www.dyndns.org/>. More than 5 DDNS servers are supported.

## **Virtual Server**

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside

network, Internet.

### **Rich Packet Filtering**

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from the Internet and vice versa, in addition to providing a higher level of security control.

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

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

### **Web based GUI**

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

### **Firmware Upgradeable**

Device can be upgraded to the latest firmware through the WEB based GUI.

# Features

- 4-port 10/ 100 Ethernet Switch
- Very High-speed Internet Access via VDSL2; Backward Compatible with ADSL2/+ ADSL2/ ADSL
- VDSL2 Profiles: 8a/b/c/d, 12a/b, 17a
- Quality of Service Control for Traffic Prioritization and Bandwidth Management
- SOHO Firewall Security with DoS Prevention and Packet Filtering
- Universal Plug and Play (UPnP) Compliance
- Dynamic Domain Name System (DDNS)
- Available Syslog
- Ease of Use with Quick Installation Wizard and Auto-scan ADSL settings (Future release)



# Hardware Specifications

## Physical Interface

- DSL: VDSL/ ADSL port
- WAN: Gigabit Ethernet for FTTH and broadband connection
- Ethernet: 4-port 10 / 100 auto-crossover (MDI / MDI-X) Switch
- Factory default reset button
- USB
- Power jack
- Power switch

## Physical Specifications

- Power Requirements: Input: 12V DC, 1.5A

## Operating Environment

- Operating temperature: 0 – 40°C
- Storage temperature: -20 – 70°C
- Humidity: 20 – 95% non-condensing

# Chapter 2: Installing the Router

## Package Contents

**BEC 8800N Router**

**RJ-11 ADSL/telephone cable**

**Ethernet (RJ-45) cable**

**Power adapter**

**Splitter / Microfilter (Optional)**

## Important note for using this router



**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**

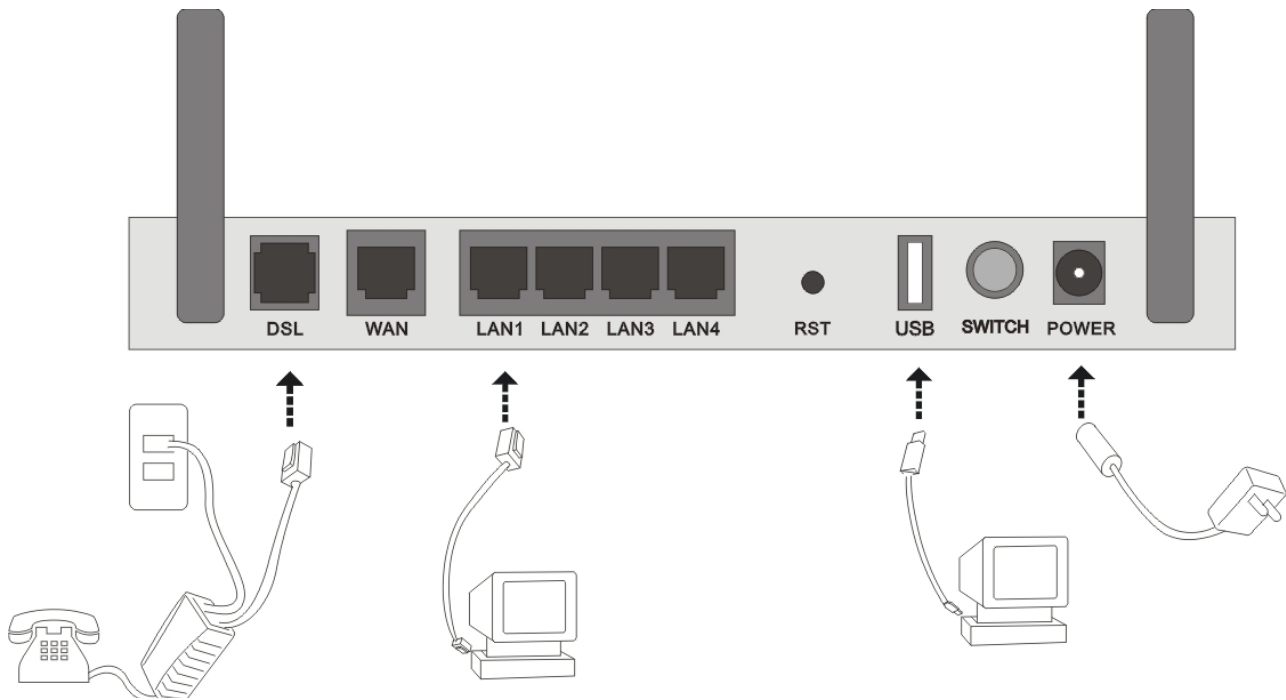
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

# Device Description

## The Front LEDs

LED		Meaning
1	Power	Flash orange when the device is booting Lit green when the system is ready. Lit orange when the device fails to boot or when the device is in emergency mode.
2	WAN	Lit green when WAN port is being connected to a FTTH or broadband device.
3	DSL	Lit green when the device is successfully connected to a DSL DSLAM. ("line sync").
4	Internet	Lit orange when WAN port fails to get IP address. Lit green when WAN port gets IP address. Lit off when device in bridged mode or ADSL connection not present.
5	Ethernet port 1X — 4X (RJ-45 connector)	Lit green when one of LAN ports is connected to an Ethernet device. Blinking when data is being Transmitted / Received.
6	WLAN	Lit green when wireless is being turn on or connection is established .
7	USB	Lit green when there is a USB line connection. Flashing when data is being transmitted or received.

# The Rear Ports



Port		Meaning
1	Power	Connect it with the supplied power adapter.
2	Power Switch	Power ON/OFF switch.
3	USB	Connect the USB cable to this port (BEC 8800N only).
4	Reset	Press this button for 3~5 seconds to restore the device to its default mode. <b>Note: Be sure that the device is being turned on when press Reset button.</b> (If you cannot login to the router or forget your Username/ Password, press this button for 3~5 seconds).
5	Ethernet 1X - 4X (RJ-45 connector)	Connect to a PC or an office/home network of 10Mbps or 100Mbps using the provided RJ-45 Ethernet cables.
6	WAN (RJ-45 connector)	WAN Gigabit Ethernet port. Connect to a Cable modem, VDSL, FTTH, etc using a RJ-45 cable.
7	DSL	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the VDSL/ADSL telephone network.

## Cabling

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

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your DSL connection or may result in frequent disconnections.

# Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC 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.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs 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 192.168.1.254 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 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.



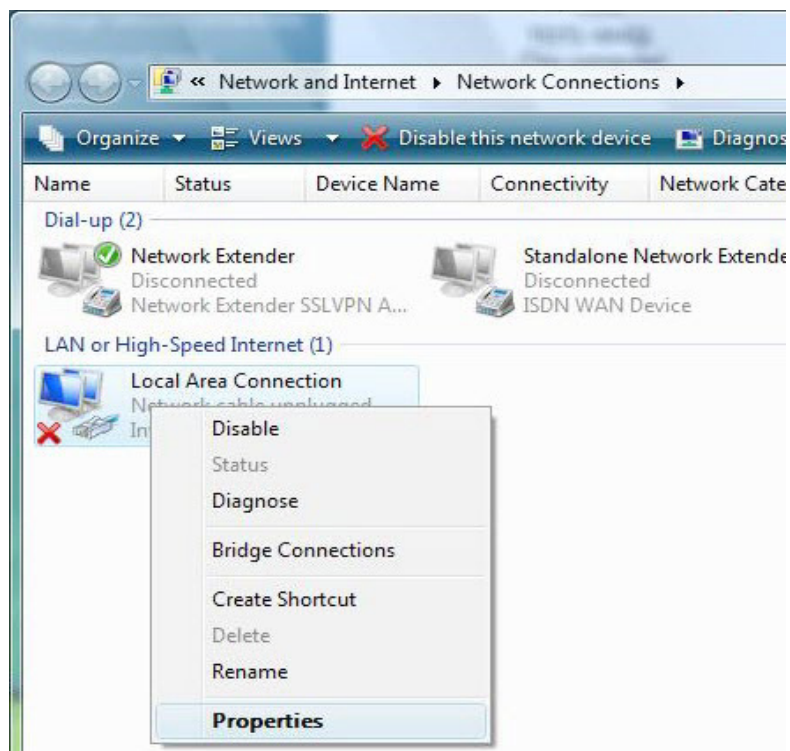
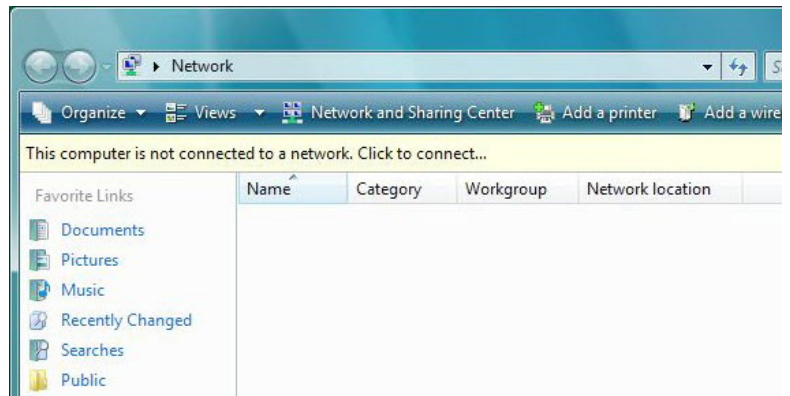
Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

# Hardware Connection

# Network Configuration

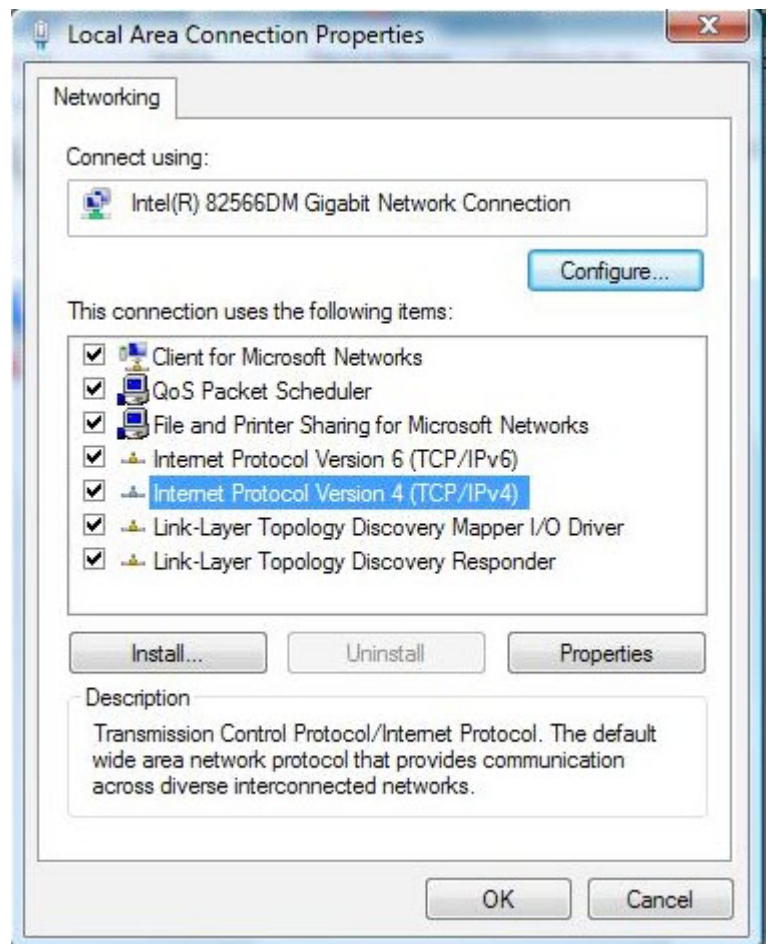
## Configuring PC in Windows Vista

1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.
4. Select the Local Area Connection, and right click the icon to select Properties.

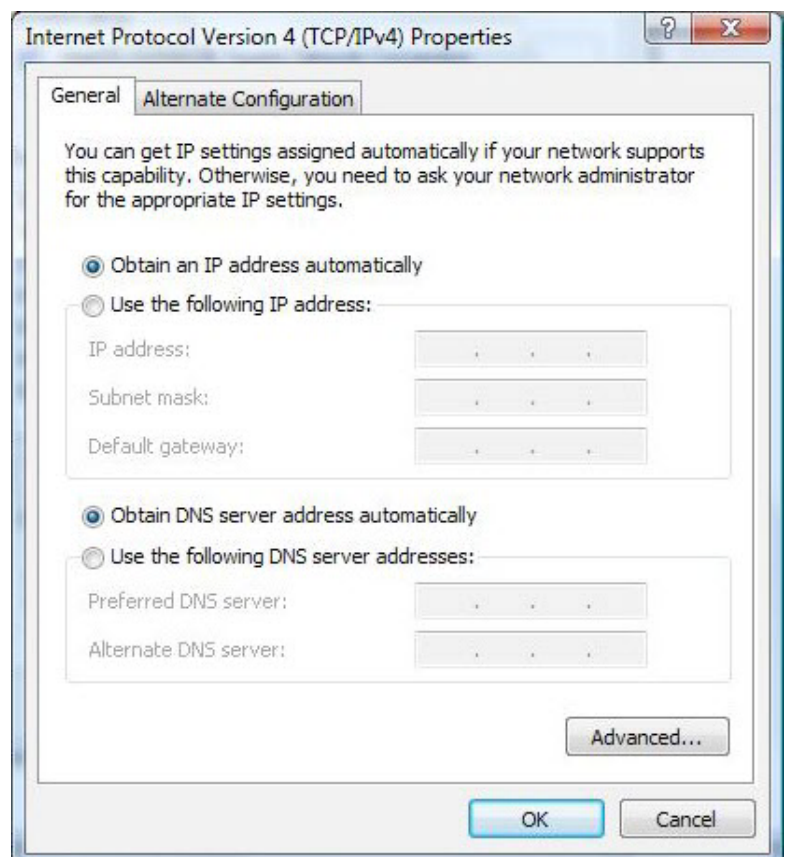




5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.

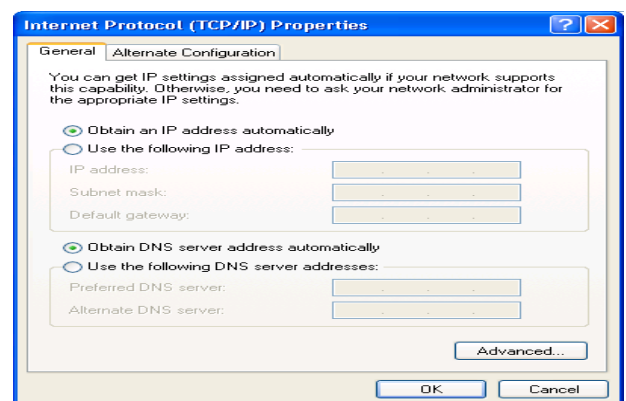
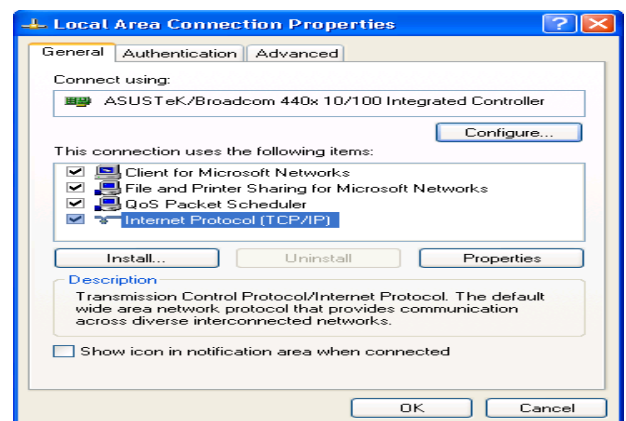
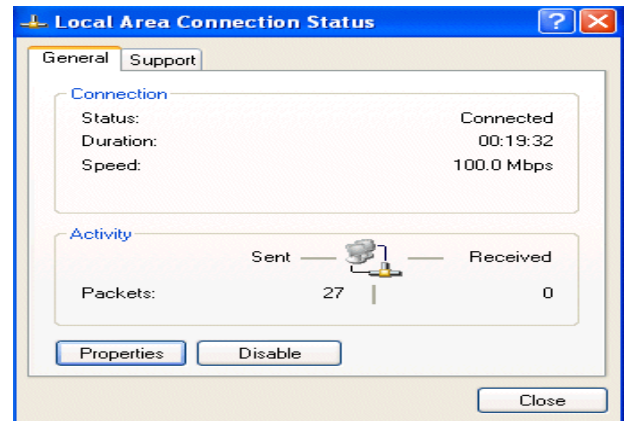
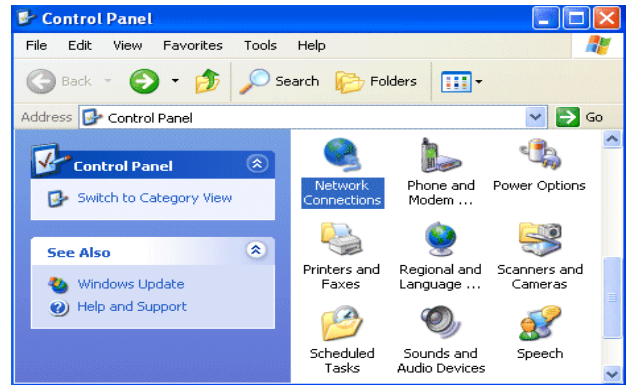


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



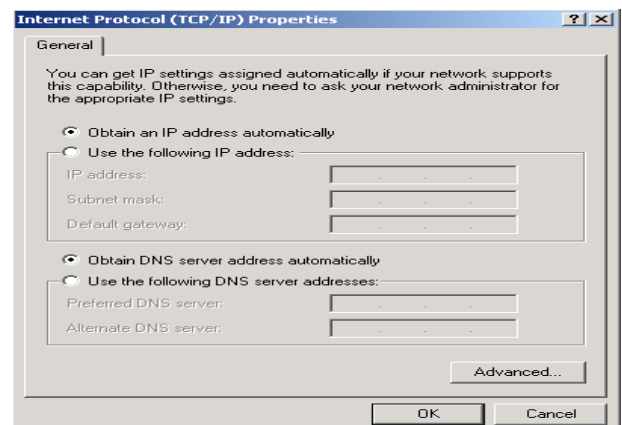
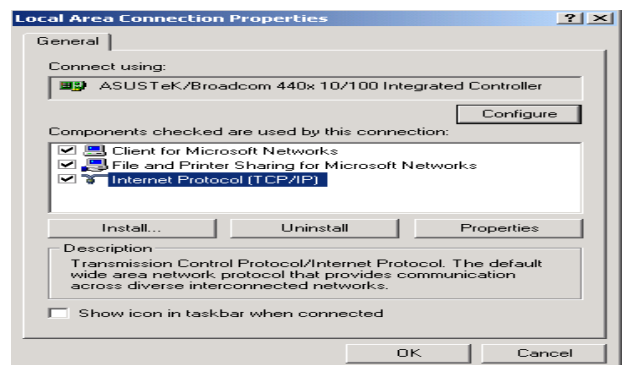
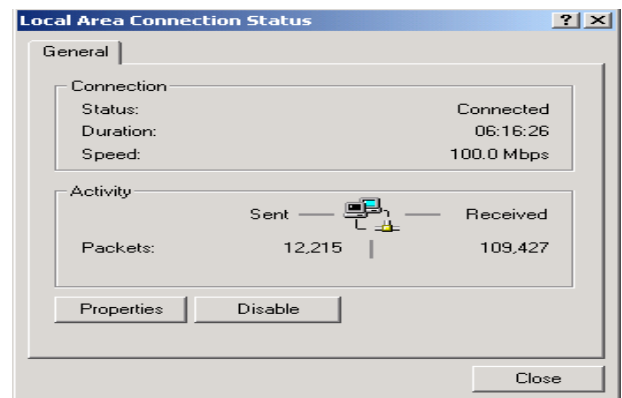
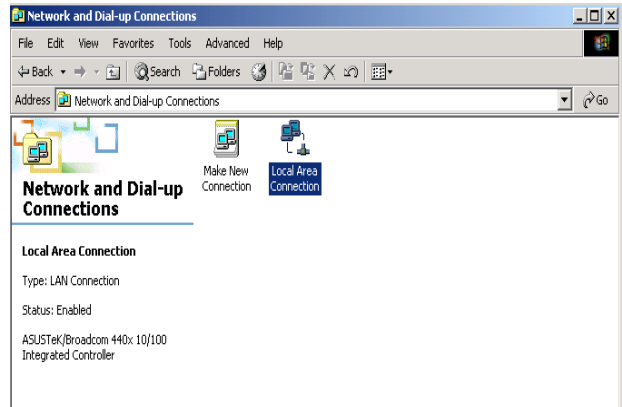
# Configuring PC in Windows XP

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.



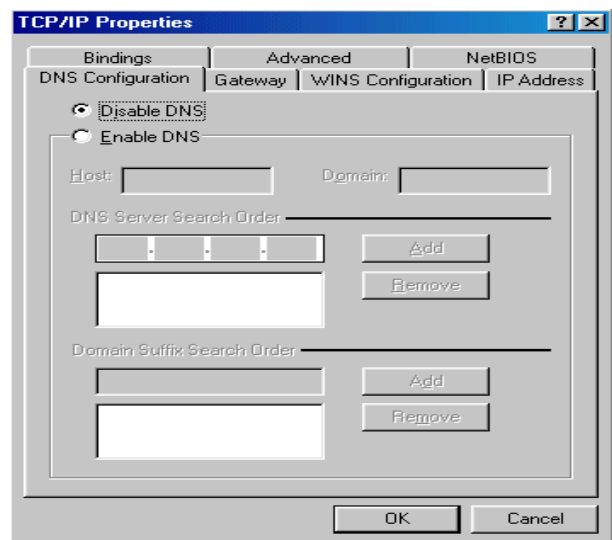
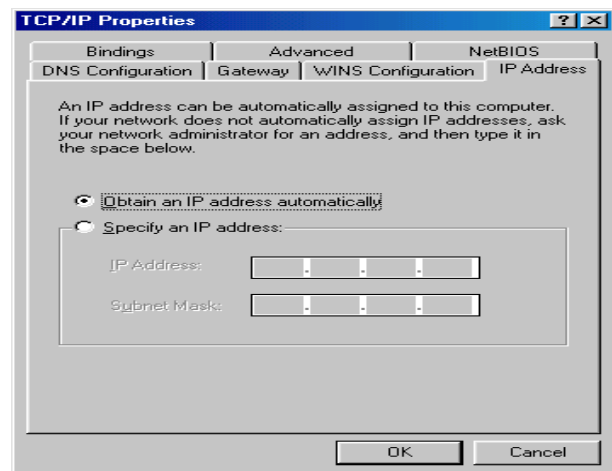
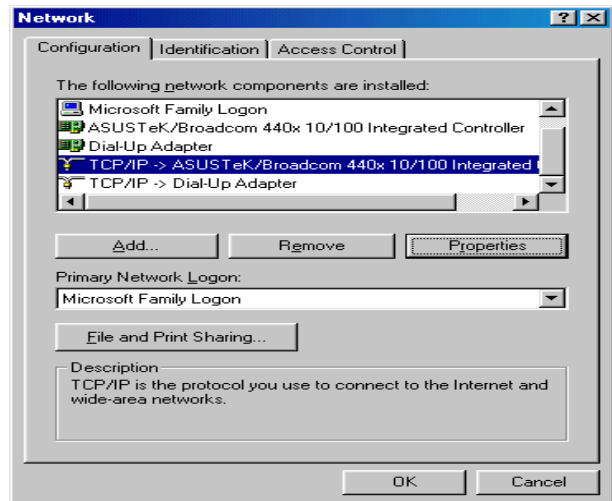
# Configuring PC in Windows 2000

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.



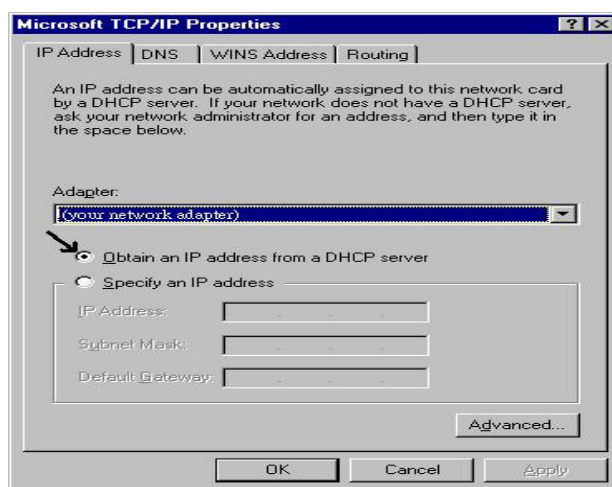
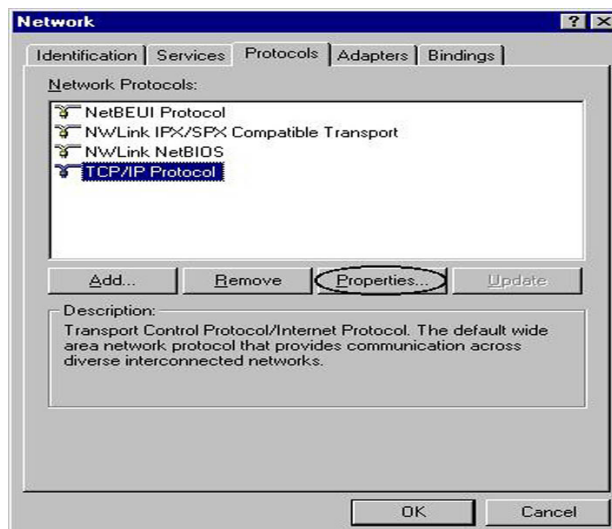
# Configuring PC in Windows 95/98/Me

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.



# Factory Default Settings

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

## Web Interface (Username and Password)

- ▶ Username: admin
- ▶ Password: admin

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



### Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

## Device LAN IP settings

- ▶ IP Address: 192.168.1.254
- ▶ Subnet Mask: 255.255.255.0

## ISP setting in WAN site

- ▶ PPPoE

## DHCP server

- ▶ DHCP server is enabled.
- ▶ Start IP Address: 192.168.1.100
- ▶ IP pool counts: 100

## LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

	LAN Port	WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

## Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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

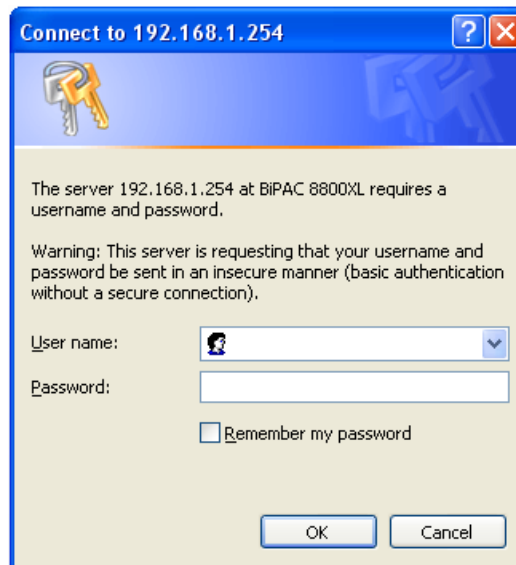
PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

# Internet Access Configuration

To configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There is basically one way to configure your device before you are able to connect to the internet: **Web Interface**. Configuration of this method will be discussed in detail in the following section.

## Configuring with your Web Browser

Open your web browser, enter the IP address of your Ethernet Adapter which by default is 192.168.1.254, and click "Go". A user name and password window prompt will appear. The default username and password are "admin" and "admin".



**Congratulations! You are now successfully logon to the Firewall Router!**

If the authentication succeeds, the homepage Status will appear on the screen.

Status	
▼ Device Information	
Model Name	BEC 8800N
Host Name ▶	gateway
System Up-Time	8 min(s) 47 seconds
Current Time ▶	Sat Jan 1 00:08:47 2000
Hardware Version	ANNEX A
Software Version	1.00m
MAC Address	00:04:ed:88:00:01
Wireless Driver Version	5.10.85.0.cpe4.402.0
▼ DSL connection information	
Line Rate - Upstream (Kbps)	
Line Rate - Downstream (Kbps)	
LAN IPv4 Address	192.168.1.254
Default Gateway	
Primary DNS Server	
Secondary DNS Server	



# Chapter 4: Configuration

Once you have logged on to your adapter GUI via your web browser, you can begin to configure the device according to your needs. On the configuration homepage, the left navigation pane provides the links to different setup pages.

**Status (WAN Info / Statistics / Route Table / ARP Table / DHCP Table / System Log)**

**Configuration (LAN / WAN / System / Firewall / QoS / Virtual Server / Advanced)**

**Diagnostics (Diagnostics / Fault Management)**

# Status

Status	
▼ Device Information	
Model Name	BEC 8800N
Host Name ▶	gateway
System Up-Time	8 min(s) 47 seconds
Current Time ▶	Sat Jan 1 00:08:47 2000
Hardware Version	ANNEX A
Software Version	1.00m
MAC Address	00:04:ed:88:00:01
Wireless Driver Version	5.10.85.0.cpe4.402.0
▼ DSL connection information	
Line Rate - Upstream (Kbps)	
Line Rate - Downstream (Kbps)	
LAN IPv4 Address	192.168.1.254
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

## Device Information

**Model Name:** Displays the model name.

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

**System Up-Time:** Records system up-time.

**Current time:** Set the current time. See the **Time Zone** section for more information.

**Hardware Version:** Device version.

**Software Version:** Firmware version.

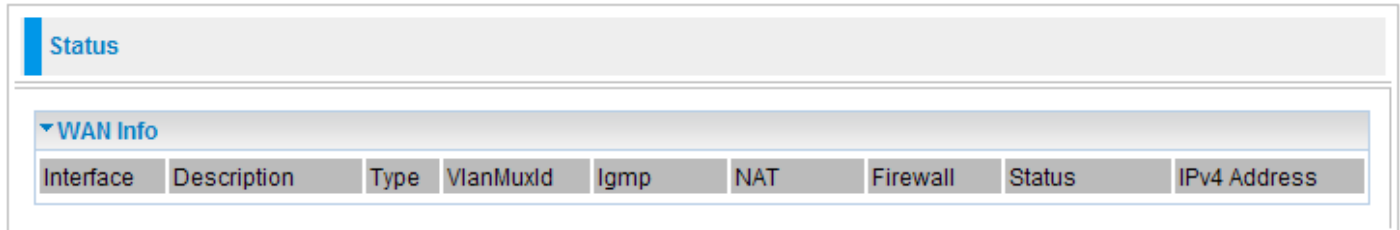
**MAC Address:** The LAN MAC address.

## DSL connection information

**DSL connection information:** User can look up to see all the informaion for DSL connection: Upstream/Downstream Line Rate (Kbps), LAN IPv4 Address, Default Gateway, and Primary/ Secondary DNS Server.

## WAN Info

The WAN Info screen displays the configured PVC(s) and the status.



The screenshot shows a web interface with a 'Status' tab selected. Below it, a 'WAN Info' section is expanded to show a table with the following columns: Interface, Description, Type, VlanMuxId, Igmp, NAT, Firewall, Status, and IPv4 Address.

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
-----------	-------------	------	-----------	------	-----	----------	--------	--------------

**Interface:** Shows connection interfaces.

**Description:** Shows the user defined name of WAN service.

**Type:** Shows the connection type, such as PPPoE, IPoE and so on.

**VlanMuxId:** Shows the status of the VLAN MuxId.

**Igmp:** Shows the status of the IGMP function.

**NAT:** Shows the status of the NAT.

**Firewall:** Shows the status of the firewall.

**Status:** Shows the connection state of the WAN connection.

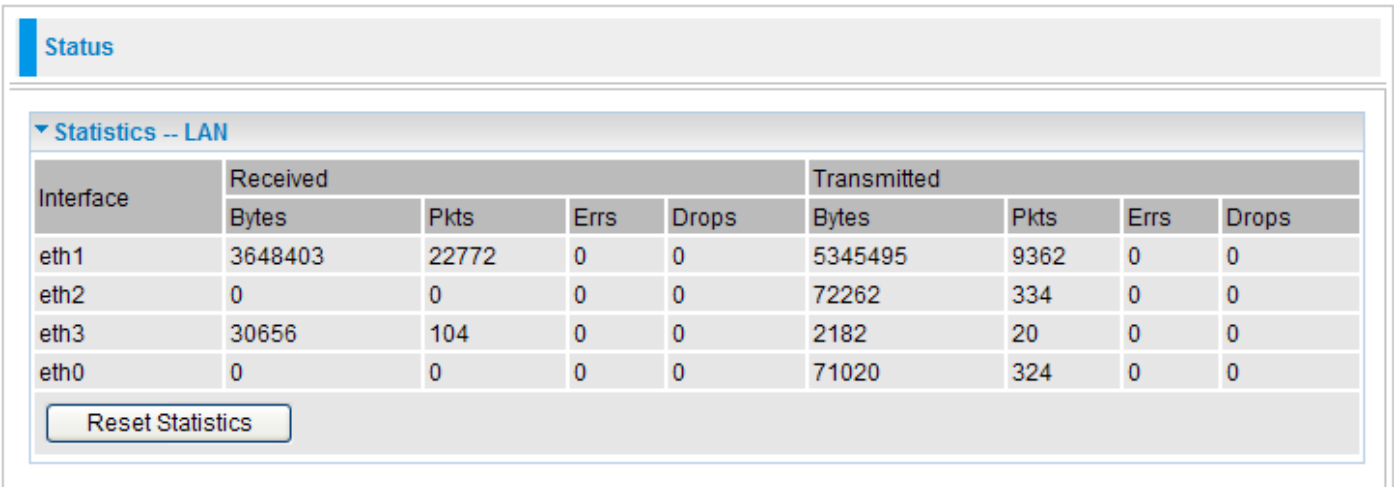
**IPv4 Address:** Shows IP address for WAN interface.

# Statistics

These are the items within the Statistics section: [LAN](#), [WAN Service](#), [xTM](#) and [xDSL](#).

## LAN

This screen shows interface statistics for LAN of Ethernet interfaces.



The screenshot shows a web interface with a 'Status' header and a 'Statistics -- LAN' section. Below this is a table with columns for 'Interface', 'Received' (Bytes, Pkts, Errs, Drops), and 'Transmitted' (Bytes, Pkts, Errs, Drops). The data rows are for interfaces eth1, eth2, eth3, and eth0. A 'Reset Statistics' button is located at the bottom of the table.

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth1	3648403	22772	0	0	5345495	9362	0	0
eth2	0	0	0	0	72262	334	0	0
eth3	30656	104	0	0	2182	20	0	0
eth0	0	0	0	0	71020	324	0	0

Reset Statistics

**Interface:** Lists connection interfaces.

**Received/Transmitted Bytes:** Rx/TX (receive/transmit) packet in Byte.

**Received/Transmitted Pkts:** Rx/TX (receive/transmit) packets.

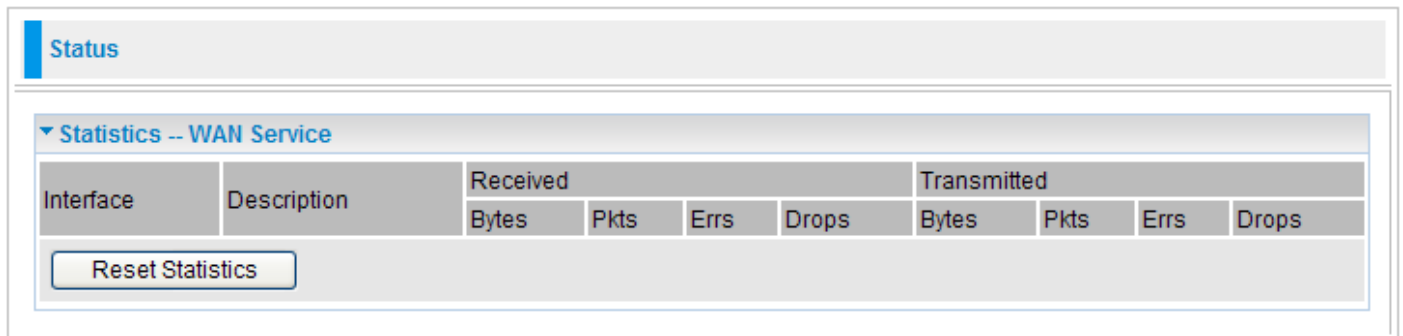
**Received/Transmitted Errs:** Rx/TX (receive/transmit) packets that are errors.

**Received/Transmitted Drops:** Rx/TX (receive/transmit) packets that are dropped.

**Reset statistics:** Click to update the statistics.

## WAN Service

This screen shows the current statistics for WAN.



The screenshot shows a web interface for WAN Service statistics. At the top, there is a 'Status' tab. Below it, a section titled 'Statistics -- WAN Service' contains a table with columns for 'Interface' and 'Description', and sub-columns for 'Received' (Bytes, Pkts, Errs, Drops) and 'Transmitted' (Bytes, Pkts, Errs, Drops). A 'Reset Statistics' button is located below the table.

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
<input type="button" value="Reset Statistics"/>									

**Interface:** Shows connection interfaces.

**Description:** Shows the user defined name of WAN service.

**Received/Transmitted Bytes:** Rx/TX (receive/transmit) packet in Byte.

**Received/Transmitted Pkts:** Rx/TX (receive/transmit) packets.

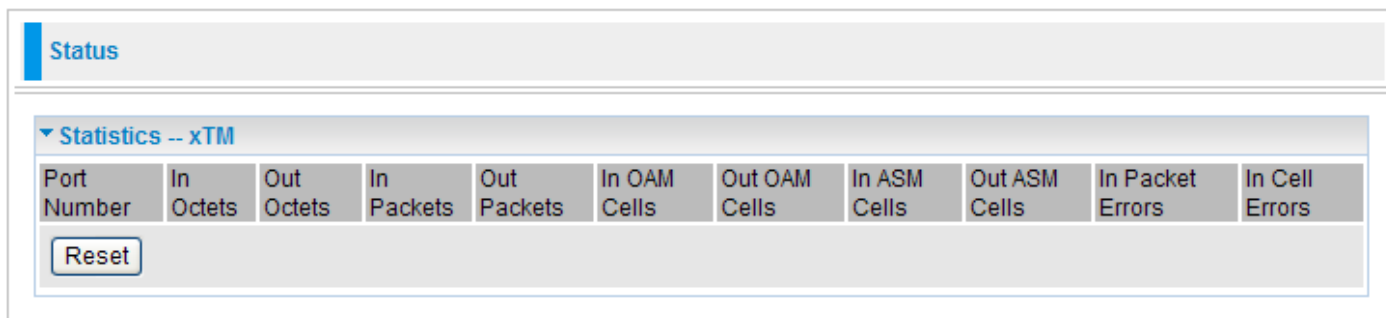
**Received/Transmitted Errs:** Rx/TX (receive/transmit) packets that are errors.

**Received/Transmitted Drops:** Rx/TX (receive/transmit) packets that are dropped.

**Reset statistics:** Click to update the statistics.

## xTM

The Statistics-xTM screen displays all the xTM statistics.



The screenshot shows a web interface for xTM statistics. At the top, there is a 'Status' tab. Below it, a dropdown menu is set to 'Statistics -- xTM'. A table with 12 columns is displayed, and a 'Reset' button is located below the table.

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
-------------	-----------	------------	------------	-------------	--------------	---------------	--------------	---------------	------------------	----------------

**Port Number:** Shows number of the port for xTM.

**In Octets:** Number of received octets over the interface.

**Out Octets:** Number of transmitted octets over the interface.

**In Packets:** Number of received packets over the interface.

**Out Packets:** Number of transmitted packets over the interface.

**In OAM Cells:** Number of OAM cells received.

**Out OAM Cells:** Number of OAM cells transmitted.

**In ASM Cells:** Number of ASM cells received.

**Out ASM Cells:** Number of ASM cells transmitted.

**In Packet Errors:** Number of received packets with errors.

**In Cell Errors:** Number of received cells with errors.

**Reset:** Click to reset the statistics.

# xDSL

The Statistics-xDSL screen displays all the xDSL network statistics.

**Status**

▼ **Statistics -- xDSL**

DSP Firmware Version	A2pvC011d.d21j2	
Mode		
Traffic Type		
Status	Disabled	
Link Power State		
	Downstream	Upstream
Line Coding(Trellis)		
SNR Margin (0.1 dB)		
Attenuation (0.1 dB)		
Output Power (0.1 dBm)		
Attainable Rate (Kbps)		
Rate (Kbps)		
Super Frames		
Super Frame Errors		
RS Words		
RS Correctable Errors		
RS Uncorrectable Errors		
HEC Errors		
OCD Errors		
LCD Errors		
Total Cells		
Data Cells		
Bit Errors		
Total ES		
Total SES		
Total UAS		

**DSP Firmware Version:** DSP code version.

**Mode:** Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, ADSL2+ and VDSL2.

**Traffic Type:** Channel type, including ATM or PTM.

**Status:** Shows the status of the DSL link.

**Link Power State:** Shows link output power state.

**Upstream:** Upstream rate.

**Downstream:** Downstream rate.

**Line Coding(Trellis):** Trellis On/Off.

**SNR Margin (0.1 dB):** This shows the Signal to Noise Ratio (SNR) margin.

**Attenuation (0.1 dB):** This is estimate of average loop attenuation of signal.

**Output Power (0.1 dBm):** Total upstream output power.

**Attainable Rate (Kbps):** The sync rate you would obtain.

**Rate (Kbps):** Current sync rate.

**Super Frames:** Total number of super frames.

**Super Frame Errors:** Number of super frames received with errors.

**RS Words:** Total number of Reed-Solomon code errors.

**RS Correctable Errors:** Total number of RS with correctable errors.

**RS Uncorrectable Errors:** Total number of RS words with uncorrectable errors.

**HEC Errors:** Total number of Header Error Checksum errors.

**OCD Errors:** Total number of out-of-cell Delineation errors.

**LCD Errors:** Total number of Loss of Cell Delineation.

**Total Cells:** Total number of cells.

**Data Cells:** Total number of data cells.

**Bit Errors:** Total number of bit errors.

**Total ES:** Total Number of Errored Seconds.

**Total SES:** Total Number of Severely Errored Seconds.

**Total UAS:** Total Number of Unavailable Seconds.

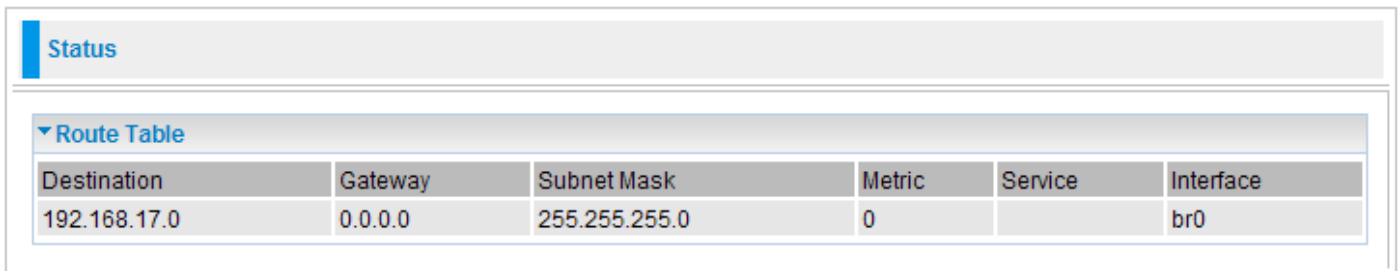
**xDSL BER Test:** Click this button to start a bit Error Rate Test.

**Reset Statistics:** Click this button to reset the statistics.



# Route Table

The Rout Table provides users with a database in the router that contains current network topology such as current paths for transmitted packets. Both static and dynamic routes are displayed.



The screenshot shows a web-based configuration interface. At the top, there is a 'Status' tab. Below it, a 'Route Table' section is expanded, showing a table with the following data:

Destination	Gateway	Subnet Mask	Metric	Service	Interface
192.168.17.0	0.0.0.0	255.255.255.0	0		br0

**Destination:** Displays the IP address of the destination network.

**Gateway:** Displays the IP address of the gateway that this route uses.

**Subnet Mask:** Displays the destination subnet mask address.

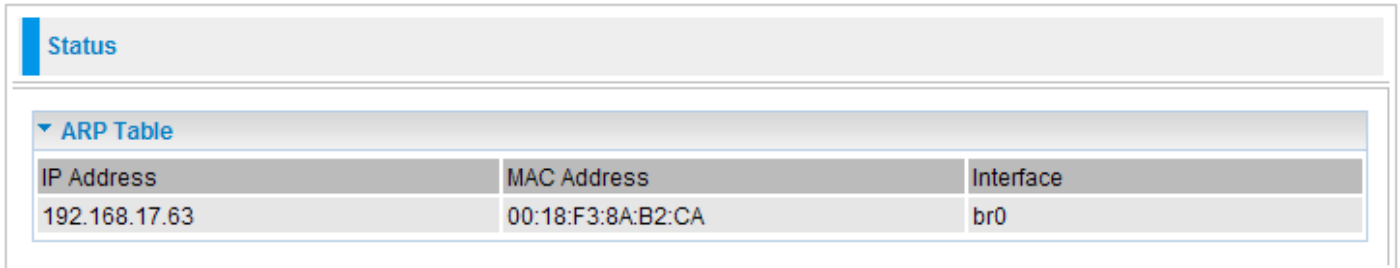
**Metric:** Displays the number of hops counted as the Metric of the route.

**Service:** Displays the current service that this route uses.

**Interface:** Displays the existing interface that this route uses.

# ARP Table

This table stores mapping information that the device uses to find the Layer 2 Media Access Control (MAC) address that corresponds to the Layer 3 IP address of the device via the Address Resolution Protocol (ARP) feature.



Status		
▼ ARP Table		
IP Address	MAC Address	Interface
192.168.17.63	00:18:F3:8A:B2:CA	br0

**IP Address:** Shows the IP Address of the device that the MAC address maps to.

**MAC Address:** Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

**Interface:** The interface name (on the router) that this IP address connects to.

# DHCP Table

This Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Status			
DHCP Table			
Hostname	MAC Address	IP Address	Expires In

**Hostname:** The Hostname of internal dhcp client.

**MAC Address:** The MAC Address of internal dhcp client host.

**IP Address:** This is the IP address that is assigned to the host with this MAC address.

**Expires In:** Shows the information provided during registration.

# System Log

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

Status

System Log

Date/Time	Facility	Message
Jan 1 00:00:03	user	hub 1-0:1.0: over-current change on port 2
Jan 1 00:00:03	user	eth1 Link UP 100 mbps half duplex

Refresh

**Refresh:** Click to update the system log.

# Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your GPON router.

[LAN](#), [WAN](#), [System](#), [Firewall](#), [QoS](#), [Virtual Server](#) and [Advanced](#).

Status
Configuration
LAN
WAN
System
Firewall
QoS
Virtual Server
Advanced
Diagnostics

The function of each configuration sub-item is described in the following sections.

# LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building or just within the same storey of a building.

## LAN

### LAN Setting

---

#### ▼ Ethernet

Parameters	
GroupName	Default ▼
IP Address	192.168.1.254
Subnet Mask	255.255.255.0

#### IGMP

IGMP Snooping	<input type="checkbox"/> Enable IGMP Snooping <input checked="" type="radio"/> Standard Mode <input type="radio"/> Blocking Mode
---------------	--

---

#### ▼ IP Alias

Parameters	
IP Alias	<input type="checkbox"/> Enable
IP Address	
Subnet Mask	

---

#### ▼ DHCP Server/DHCP Relay

Parameters	
DHCP Server Mode	Disable ▼

Apply/Save

## Ethernet

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

## Parameters

**GroupName:** Select the groupname from the listbox. You can add new groups on Interface Grouping screen (Configuration>Advanced>Interface Grouping, please refer to **Interface Grouping** section).

**IP Address:** Enter the default IP on this router.

**Subnet Mask:** Enter the default subnet mask on this router.

## IGMP

**IGMP Snooping:** Allows a layer 2 switch to manage the transmission of any incoming IGMP

multicast packet groups between the host and the router. Default is set to Disable. Check Enable IGMP Snooping check box to activate this function and choose Standard Mode or Blocking Mode.

## IP Alias

This function allows the addition of an IP alias to the network interface. This further allows user flexibility to assign a specific function to use this IP.

**IP Alias:** Check Enable check box to activate this function.

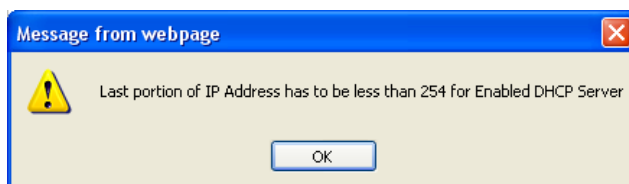
**IP Address:** Enter the IP address to be added to the network.

**Subnet Mask:** Specify a subnet mask for the IP to be added.

## DHCP Server/DHCP Relay

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device.

To configure the router's DHCP Server, select **DHCP Server** from the DHCP Server Mode drop-down menu. A message window will pop up to remind you as below. Click OK to continue.



You can then configure parameters of the DHCP Server including the domain name, IP pool (starting IP address and ending IP address to be allocated to PCs on your network) and lease time for each assigned IP address (the period of time the IP address assigned will be valid). These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click Add to save this entry or Remove to delete an existing entry.

▼ DHCP Server/DHCP Relay		
<b>Parameters</b>		
DHCP Server Mode	DHCP Server ▼	
Domain Name	home	
Start IP Address	192.168.1.100	
End IP Address	192.168.1.199	
Leased Time (hour)	24	
<b>Fixed Host</b>		
MAC Address	IP Address	Remove
Add Remove		

If you select **DHCP Relay** from the DHCP Server Mode drop-down menu, you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

▼ DHCP Server/DHCP Relay	
<b>Parameters</b>	
DHCP Server Mode	DHCP Relay ▼
DHCP Server IP Address	

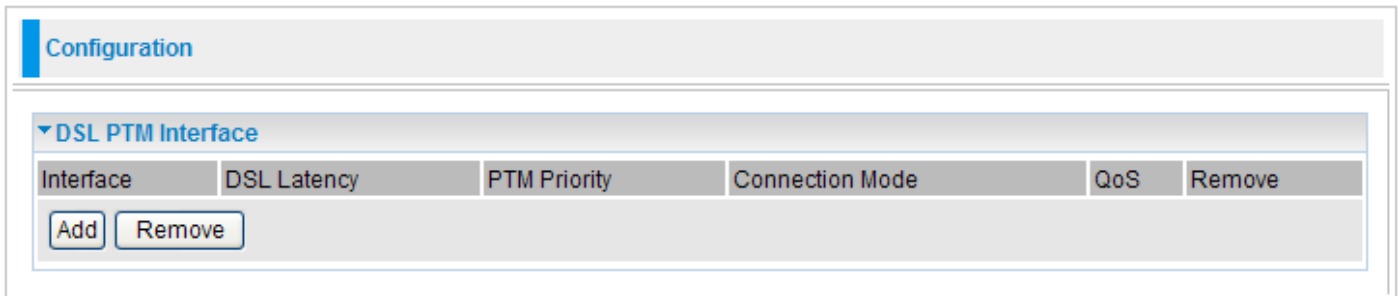
Click Apply/Save to confirm the changes and enable the above functions.

# WAN - Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems. There are the items within the WAN section: [Layer2 Interface](#), [WAN Service](#) and [DSL](#).

## Layer2 Interface

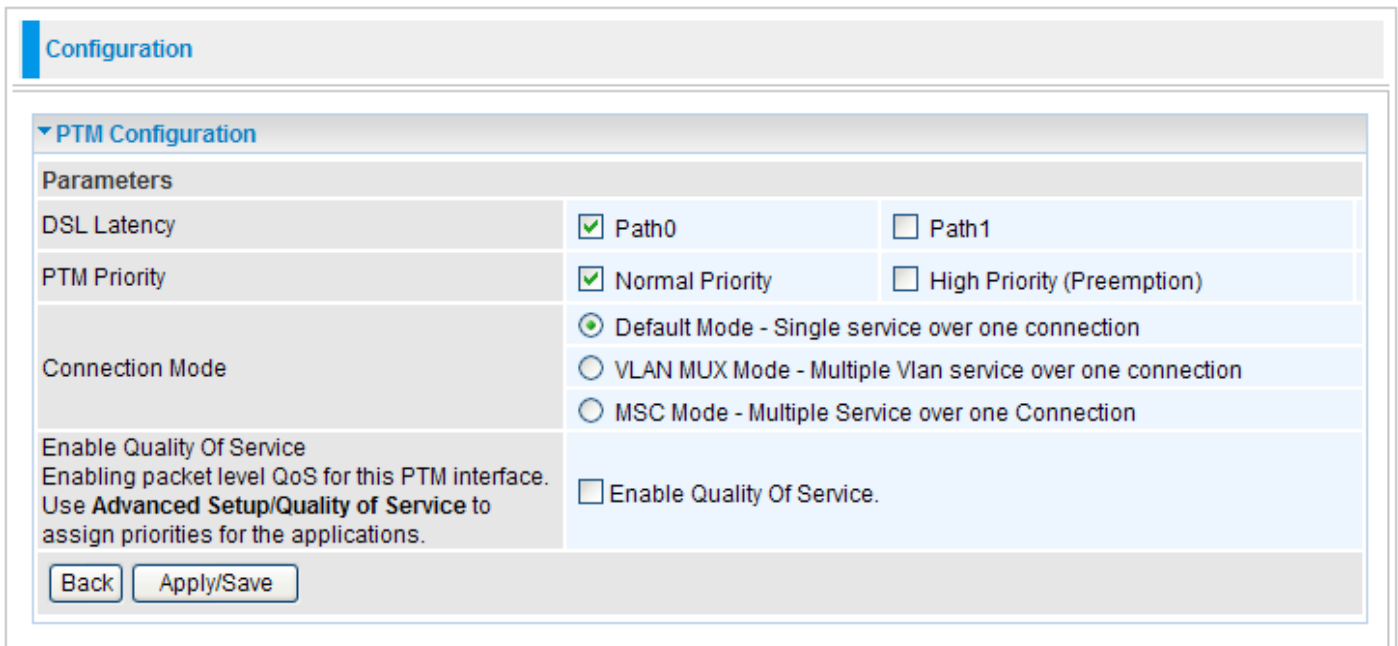
### PTM Interface (VDSL)



The screenshot shows a configuration page with a table for 'DSL PTM Interface'. The table has columns for Interface, DSL Latency, PTM Priority, Connection Mode, QoS, and Remove. Below the table are 'Add' and 'Remove' buttons.

Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove
-----------	-------------	--------------	-----------------	-----	--------

Click Add to go to PTM Configuration screen.



The screenshot shows the 'PTM Configuration' screen with various settings:

- DSL Latency:**  Path0,  Path1
- PTM Priority:**  Normal Priority,  High Priority (Preemption)
- Connection Mode:**  Default Mode - Single service over one connection,  VLAN MUX Mode - Multiple Vlan service over one connection,  MSC Mode - Multiple Service over one Connection
- Enable Quality Of Service:**  Enable Quality Of Service. (Note: Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.)

On this screen, you can configure a PTM connection. Check **DSL Latency**, set **PTM Priority**, and choose the appropriate **Connection Mode**. If you want to activate packet level QoS for this PTM interface, check **Enable Quality Of Service** check box (To assign priorities for the applications, please use Advanced Setup>Quality of Service.).

Click Apply/Save to save the changes or Back to return to DSL PTM Interface table.



## ATM Interface (ADSL)

Configuration

▼ DSL ATM Interface

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								

Click Add to go to ATM PVC Configuration screen.

Configuration

▼ ATM PVC Configuration

Parameters

VPI (0-255)	<input type="text" value="0"/>
VCI (32-65535)	<input type="text" value="35"/>
DSL Latency	<input checked="" type="checkbox"/> Path0 <input type="checkbox"/> Path1
DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)	<input checked="" type="radio"/> EoA <input type="radio"/> PPPoA <input type="radio"/> IPoA
Encapsulation Mode	LLC/SNAP-BRIDGING ▼
Service Category:	UBR Without PCR ▼
Peak Cell Rate (cells/s)	<input type="text"/>
Sustainable Cell Rate (cells/s)	<input type="text"/>
Maximum Burst Size (cells)	<input type="text"/>
Connection Mode	<input checked="" type="radio"/> Default Mode - Single service over one connection <input type="radio"/> VLAN MUX Mode - Multiple Vlan service over one connection <input type="radio"/> MSC Mode - Multiple Service over one Connection
Enable Quality Of Service Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use <b>Advanced Setup/Quality of Service</b> to assign priorities for the applications.	<input type="checkbox"/> Enable Quality Of Service.

**VPI (0~255) / VCI (32~65535):** Enter the VPI/VCI values provided by your ISP.

**DSL Latency:** Check Path0 or Path1 for DSL latency.

**DSL Link Type:** Select EoA (which is for PPPoE, IPoE and Bridge), PPPoA, or IPoA. Select the one provided by your ISP.

**Encapsulation Mode:** Select the encapsulation mode. Different options will be provided for different DSL link types. Select the one provided by your ISP.

**Service Category:** Describes the ATM Quality Of Service (QoS) being used on the VC.

**Peak Cell Rate (cells/s):** Specifies the upstream peak cell rate in cells per second.

**Sustainable Cell Rate (cells/s):** Specifies the upstream sustainable cell rate, in cells per second, used for traffic shaping.

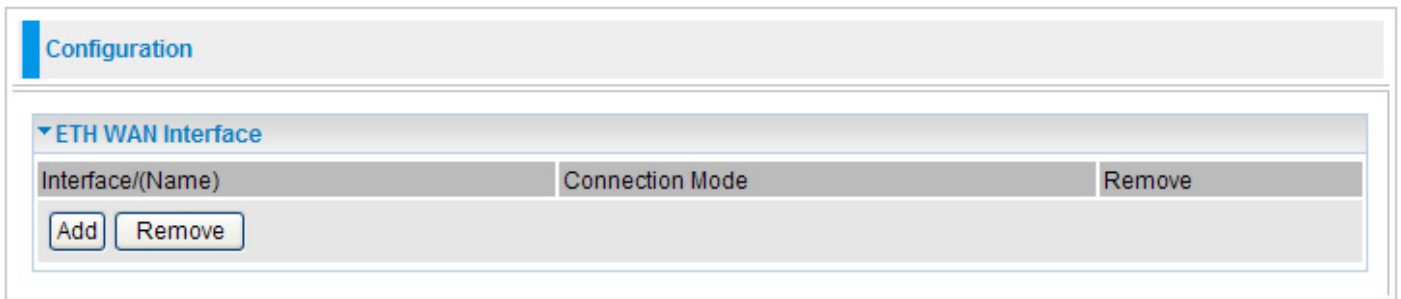
**Maximum Burst Size (cells/s):** Specifies the upstream maximum burst size in cells.

**Connection Mode:** Choose a appropriate connection mode.

**Enable Quality Of Service:** Check to activate packet level QoS for this PTM interface. To assign priorities for the applications, please use Advanced Setup>Quality of Service.

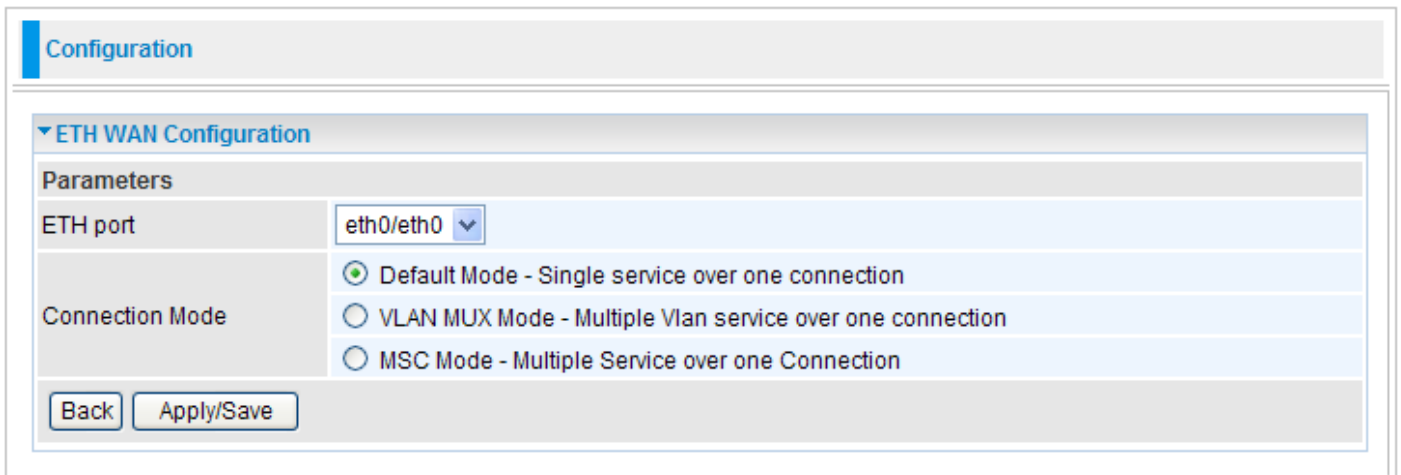
Click Apply/Save to save the changes or Back to return to DSL ATM Interface table.

## ETH Interface (EWAN)



The screenshot shows a web interface with a 'Configuration' header. Below it is a section titled 'ETH WAN Interface' which contains a table with three columns: 'Interface/(Name)', 'Connection Mode', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

Click Add to go to ETH WAN Configuration screen.



The screenshot shows a web interface with a 'Configuration' header. Below it is a section titled 'ETH WAN Configuration' with a 'Parameters' sub-section. It includes a dropdown menu for 'ETH port' set to 'eth0/eth0', and three radio button options for 'Connection Mode': 'Default Mode - Single service over one connection' (selected), 'VLAN MUX Mode - Multiple Vlan service over one connection', and 'MSC Mode - Multiple Service over one Connection'. At the bottom are 'Back' and 'Apply/Save' buttons.

**ETH port:** Select the port for ETH WAN connection from the listbox.

**Connection Mode:** Choose a appropriate connection mode.

Click Apply/Save to save the changes or Back to return to ETH WAN Interface table.

## WAN Service

### WAN Service

▼ WAN Service Interface Table

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
*ETH and PTM/ATM service can not coexist.									

**Note:** You have to set an interface at least previously. (Please refer to PTM Interface, ATM Interface and ETH Interface sections. ETH and PTM/ATM service can not coexist.) If the WAN interface has not set, a page will display as below and you are not allowed to create a WAN connection.

### Error!

**WAN Configuration: No available interfaces.**

Click Add to go to WAN Service Interface screen.

### WAN Setting

▼ WAN Service Interface

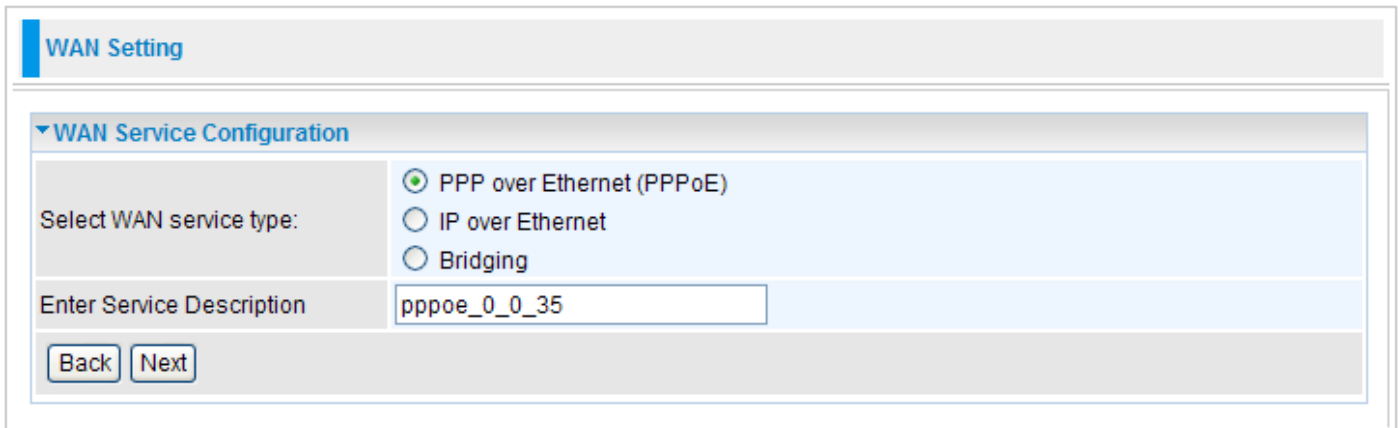
Select a layer 2 interface for this service

Note For ATM interface, the descriptor string is (portId\_vpi\_vci)  
For PTM interface, the descriptor string is (portId\_high\_low)  
Where portId=0 --> DSL Latency PATH0  
portId=1 --> DSL Latency PATH1  
portId=4 --> DSL Latency PATH0&1  
low =0 --> Low PTM Priority not set  
low =1 --> Low PTM Priority set  
high =0 --> High PTM Priority not set  
high =1 --> High PTM Priority set

Select a layer2 interface form the drop-down menu for this service and then click on Next to continue.

## PPP over Ethernet

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

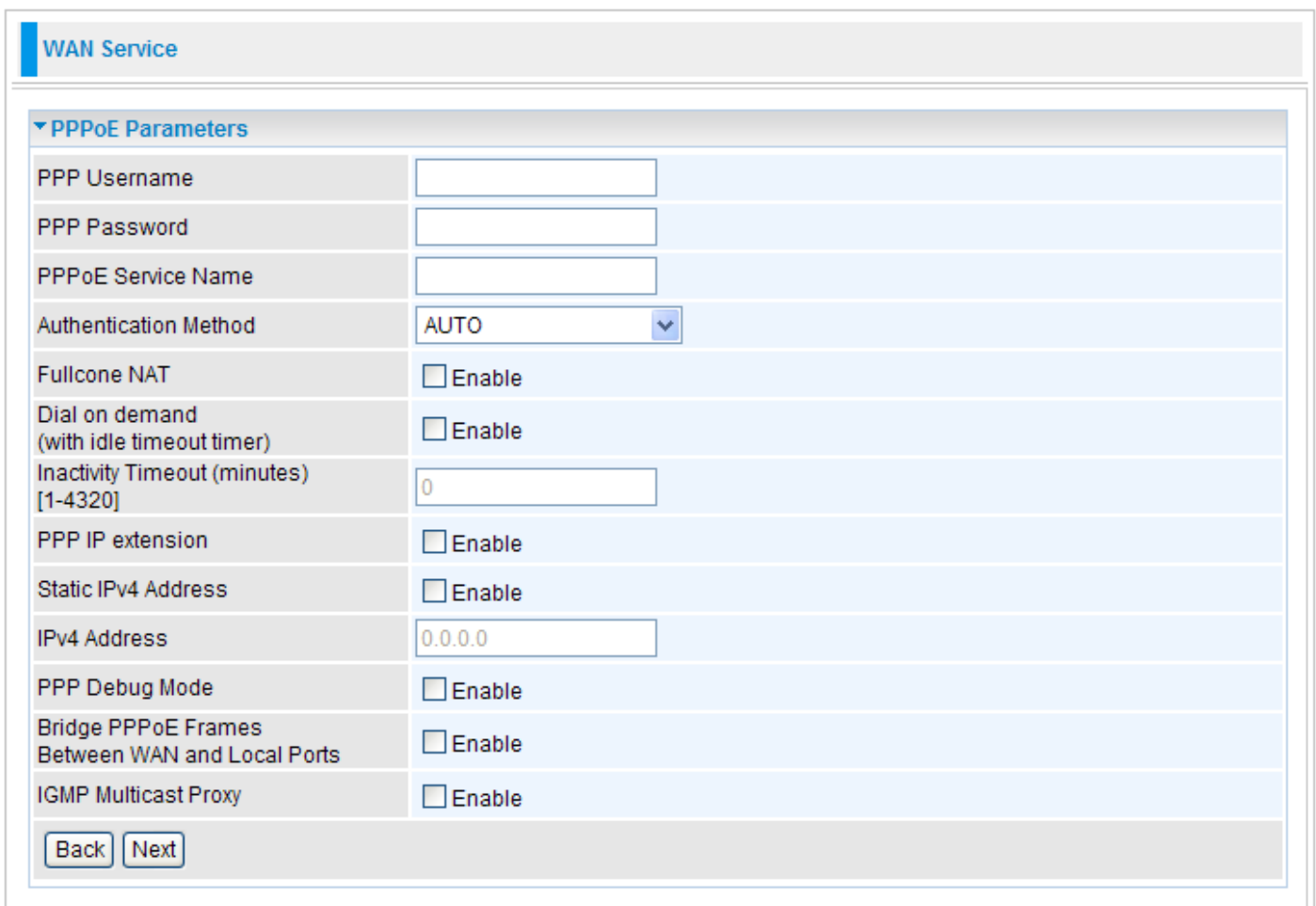


The screenshot shows the 'WAN Setting' configuration page. Under the 'WAN Service Configuration' section, the 'Select WAN service type:' field has three radio buttons: 'PPP over Ethernet (PPPoE)' (selected), 'IP over Ethernet', and 'Bridging'. The 'Enter Service Description' field contains the text 'pppoe\_0\_0\_35'. At the bottom, there are 'Back' and 'Next' buttons.

**Select WAN service type:** Click PPP over Ethernet (PPPoE) radio button.

**Enter Service Description:** You are allowed to enter the user defined name for this service.

Click Next to go to next step.



The screenshot shows the 'WAN Service' configuration page. Under the 'PPPoE Parameters' section, there are several fields and checkboxes: 'PPP Username' (text input), 'PPP Password' (text input), 'PPPoE Service Name' (text input), 'Authentication Method' (dropdown menu set to 'AUTO'), 'Fullcone NAT' (checkbox 'Enable'), 'Dial on demand (with idle timeout timer)' (checkbox 'Enable'), 'Inactivity Timeout (minutes) [1-4320]' (text input set to '0'), 'PPP IP extension' (checkbox 'Enable'), 'Static IPv4 Address' (checkbox 'Enable'), 'IPv4 Address' (text input set to '0.0.0.0'), 'PPP Debug Mode' (checkbox 'Enable'), 'Bridge PPPoE Frames Between WAN and Local Ports' (checkbox 'Enable'), and 'IGMP Multicast Proxy' (checkbox 'Enable'). At the bottom, there are 'Back' and 'Next' buttons.

**PPP Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

**PPP Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

**PPPoE Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

**Authentication Method:** Default is AUTO. Please consult your ISP on whether to use PAP, CHAP or MSCHAP.

**Fullcone NAT:** Check/uncheck this item to activate/inactivate this function.

**Dial on demand (with idle timeout timer) / Inactivity Timeout (minutes) [1-4320]:** Check Enable to activate this function and the following field will be available, so that you can enter the time value to auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

**PPP IP extension:** Check/uncheck this item to enable/disable this function.

**Static IPv4 Address / IPv4 Address:** Check Enable to activate this function and the following field will be available, so that you can enter the IPv4 address (default is 0.0.0.0) to the device.

**PPP Debug Mode:** Check/uncheck this item to enable/disable this function.

**Bridge PPPoE Frames Between WAN and Local Ports:** Check/uncheck this item to enable/disable this function.

**IGMP Multicast Proxy:** Check/uncheck this item to enable/disable this function.

Click Next to go to next step.

The screenshot shows the 'WAN Service' configuration page. Under the 'IP Parameters' section, the 'Selected WAN Interface' is set to 'pppoe\_0\_0\_35/ppp0'. There are 'Back' and 'Next' buttons at the bottom of the section.

**Selected WAN Interface:** Select the WAN interface for the IPv4 Default Gateway.

Click Next to go to next step.

The screenshot shows the 'WAN Service' configuration page. Under the 'Parameters' section, the 'IPv4 DNS Server Configuration' is shown. The 'DNS Type' is set to 'Obtain DNS info from a WAN interface'. The 'WAN Interface selected' is 'pppoe\_0\_0\_35/ppp0'. There are empty text boxes for 'Primary DNS server' and 'Secondary DNS server'. There are 'Back' and 'Next' buttons at the bottom of the section.

**DNS Type:** Select the appropriate DNS type.

**WAN Interface selected:** This field is available when DNS Type is "Obtain DNS info from a WAN interface". Select a WAN interface for this device to obtain the DNS information.

**Primary DNS server/Secondary DNS server:** These fields are available when DNS Type is "Use the following Static DNS IP address". Enter the primary/secondary DNS.

Click Next to go to next step.

WAN Service

▼ Summary

PORT / VPI / VCI	0 / 0 / 35
Connection Type	PPPoE
Service Name	pppoe_0_0_35
Service Category	UBR
IP Address	Automatically Assigned
Service State	Enabled
NAT	Enabled
Full Cone NAT	Disabled
Firewall	Enabled
IGMP Multicast	Disabled
Quality Of Service	Disabled

Back
Apply/Save

This page lists a summary of previous steps. Make sure that the settings are the same as those provided by your ISP and then click Apply/Save to complete the configuration process. Then you will return to WAN Service Interface Table and this new profile will be displayed on this screen.

WAN Service

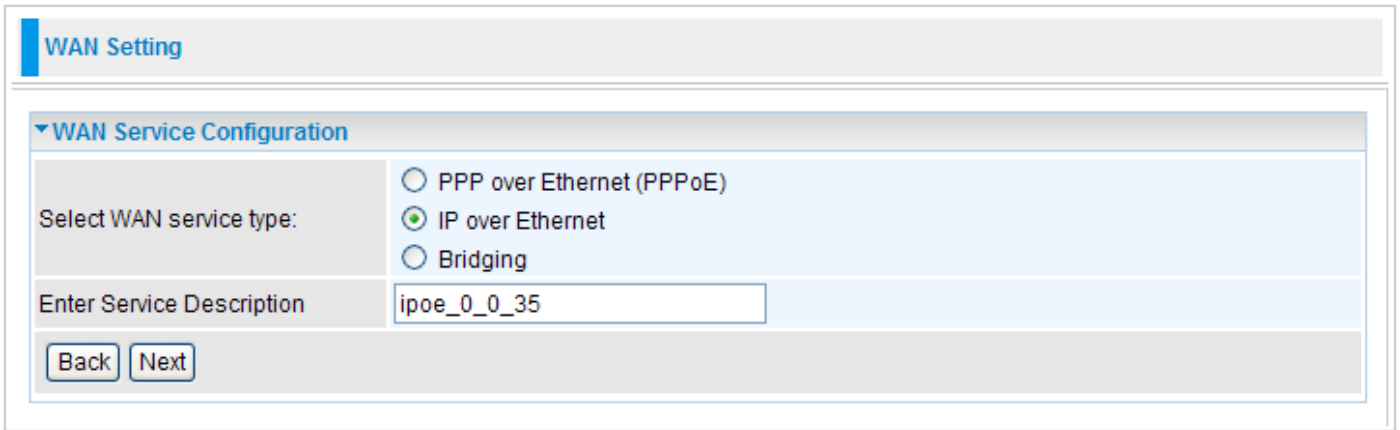
▼ WAN Service Interface Table

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ppp0	pppoe_0_0_1	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>

\*ETH and PTM/ATM service can not coexist.

Add
Remove

## IP over Ethernet

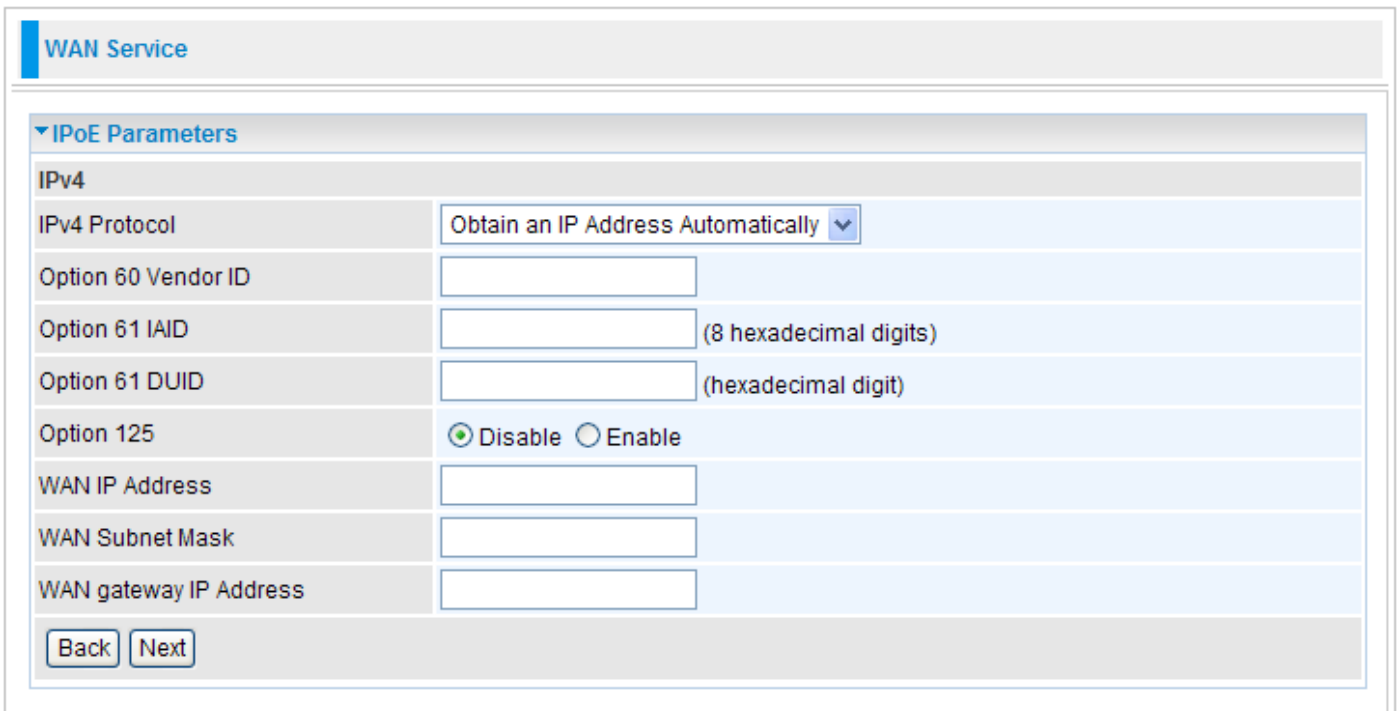


The screenshot shows the 'WAN Setting' configuration page. Under the 'WAN Service Configuration' section, there are three radio buttons for selecting the WAN service type: 'PPP over Ethernet (PPPoE)', 'IP over Ethernet' (which is selected), and 'Bridging'. Below this, there is a text input field for 'Enter Service Description' containing the text 'ipoe\_0\_0\_35'. At the bottom of the configuration area, there are 'Back' and 'Next' buttons.

**Select WAN service type:** Click IP over Ethernet radio button.

**Enter Service Description:** You are allowed to enter the user defined name for this service.

Click Next to go to next step.



The screenshot shows the 'WAN Service' configuration page, specifically the 'IPoE Parameters' section. Under the 'IPv4' sub-section, there are several configuration fields: 'IPv4 Protocol' is set to 'Obtain an IP Address Automatically'; 'Option 60 Vendor ID', 'Option 61 IAID', and 'Option 61 DUID' are empty text input fields with their respective constraints (8 hexadecimal digits, 8 hexadecimal digits, and hexadecimal digit); 'Option 125' has radio buttons for 'Disable' (selected) and 'Enable'; 'WAN IP Address', 'WAN Subnet Mask', and 'WAN gateway IP Address' are empty text input fields. At the bottom, there are 'Back' and 'Next' buttons.

**IPv4 Protocol:** Select the appropriate protocol. There are 2 options: Obtain an IP Address Automatically and Fixed IP Address.

**Option 60 Vendor ID:** Enter the associated information provided by your ISP.

**Option 61 IAID:** Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

**Option 61 DUID:** Enter the associated information provided by your ISP. You should input hexadecimal number(s).

**Option 125:** Check Enable or Disable this function. Default setting is Disable.

**WAN IP Address:** Enter your IP address to the device provided by your ISP. If Fixed IP Address is selected in the IPv4 Protocol field, default value 0.0.0.0 will display in this field.

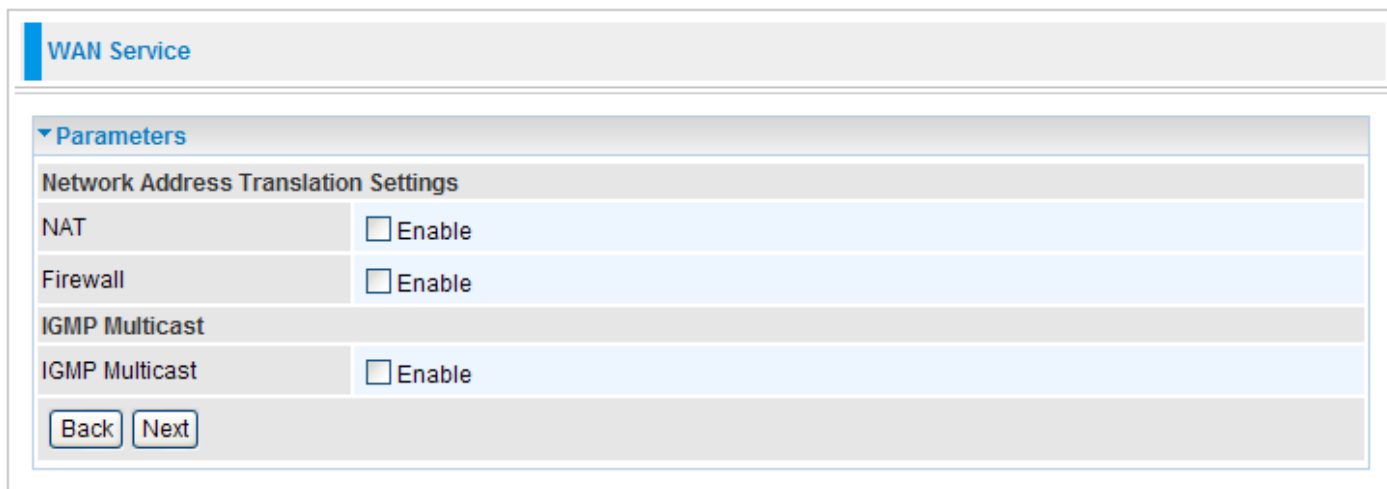
**WAN Subnet Mask:** Enter your submask to the device provided by your ISP. If Fixed IP Address is



selected in the IPv4 Protocol field, default value 0.0.0.0 will display in this field.

**WAN gateway IP Address:** Enter your gateway IP address to the device provided by your ISP. If Fixed IP Address is selected in the IPv4 Protocol field, default value 0.0.0.0 will display in this field.

Click Next to go to next step.



The screenshot shows the 'WAN Service' configuration page. Under the 'Parameters' section, there is a sub-section titled 'Network Address Translation Settings'. It contains three rows: 'NAT' with an unchecked 'Enable' checkbox, 'Firewall' with an unchecked 'Enable' checkbox, and 'IGMP Multicast' with an unchecked 'Enable' checkbox. At the bottom of this section are 'Back' and 'Next' buttons.

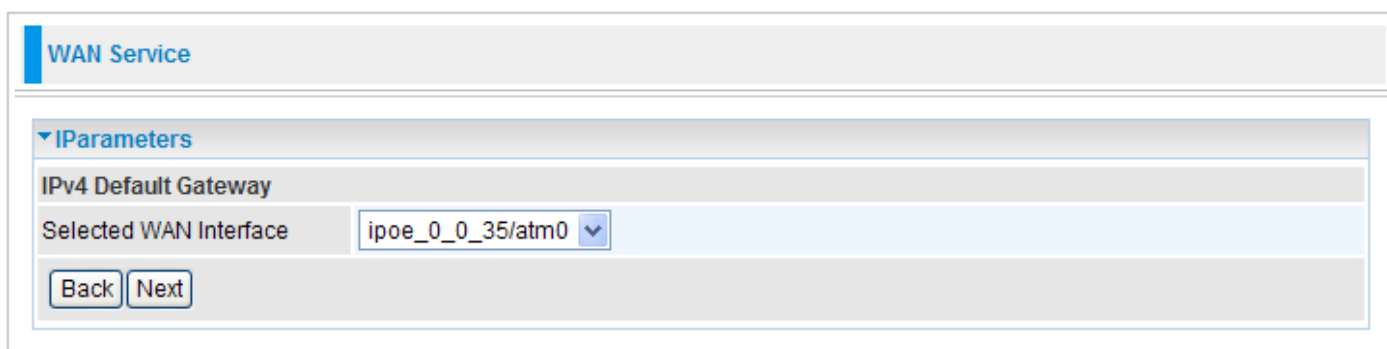
**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**Fullcone NAT:** This field will be displayed when you tick Enable on the NAT field. Check/uncheck this item to activate/inactivate this function.

**Firewall:** Check/uncheck this item to enable/disable firewall function.

**IGMP Multicast:** IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast (proxy) on that wan interface for multicast forwarding.

Click Next to go to next step.



The screenshot shows the 'WAN Service' configuration page. Under the 'IPParameters' section, there is a sub-section titled 'IPv4 Default Gateway'. It contains a 'Selected WAN Interface' dropdown menu with 'ipoe\_0\_0\_35/atm0' selected. At the bottom of this section are 'Back' and 'Next' buttons.

**Selected WAN Interface:** Select the WAN interface for the IPv4 Default Gateway.

Click Next to go to next step.

**WAN Service**

▼ Parameters

**IPv4 DNS Server Configuration**

DNS Type	Obtain DNS info from a WAN interface ▼
WAN Interface selected	ipoe_0_0_35/atm0 ▼
Primary DNS server	<input type="text"/>
Secondary DNS server	<input type="text"/>

**DNS Type:** Select the appropriate DNS type.

**WAN Interface selected:** This field is available when DNS Type is "Obtain DNS info from a WAN interface". Select a WAN interface for this device to obtain the DNS information.

**Primary DNS server/Secondary DNS server:** These fields are available when DNS Type is "Use the following Static DNS IP address". Enter the primary/secondary DNS.

Click Next to go to next step.

**WAN Service**

▼ Summary

PORT / VPI / VCI	0 / 0 / 35
Connection Type	IPoE
Service Name	ipoe_0_0_35
Service Category	UBR
IP Address	Automatically Assigned
Service State	Enabled
NAT	Disabled
Full Cone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Disabled
Quality Of Service	Disabled

This page lists a summary of previous steps. Make sure that the settings are the same as those provided by your ISP and then click Apply/Save to complete the configuration process.

## Bridging

### WAN Setting

▼ WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

**Select WAN service type:** Click Bridging radio button.

**Enter Service Description:** You are allowed to enter the user defined name for this service.

Click Next to go to next step.

### WAN Service

▼ Summary

PORT / VPI / VCI	0 / 0 / 35
Connection Type	Bridge
Service Name	br_0_0_35
Service Category	UBR
IP Address	Not Applicable
Service State	Enabled
NAT	Disabled
Full Cone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Not Applicable
Quality Of Service	Disabled

This page lists a summary of previous steps. Make sure that the settings are the same as those provided by your ISP and then click Apply/Save to complete the configuration process.

# DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.

**Configuration**

▼ **DSL Settings**

**Parameters**

Modulator	<input checked="" type="checkbox"/> G.Dmt Enabled	<input checked="" type="checkbox"/> G.lite Enabled	<input checked="" type="checkbox"/> T1.413 Enabled	<input checked="" type="checkbox"/> ADSL2 Enabled
	<input checked="" type="checkbox"/> AnnexL Enabled	<input checked="" type="checkbox"/> ADSL2+ Enabled	<input type="checkbox"/> AnnexM Enabled	<input checked="" type="checkbox"/> VDSL2 Enabled
VDSL2 profile	<input checked="" type="checkbox"/> 8a Enabled	<input checked="" type="checkbox"/> 8b Enabled	<input checked="" type="checkbox"/> 8c Enabled	<input checked="" type="checkbox"/> 8d Enabled
	<input checked="" type="checkbox"/> 12a Enabled	<input checked="" type="checkbox"/> 12b Enabled	<input checked="" type="checkbox"/> 17a Enabled	
US0	<input checked="" type="checkbox"/> Enabled			
Phone line pair	<input checked="" type="radio"/> Inner pair <input type="radio"/> Outer pair			
Capability	<input checked="" type="checkbox"/> Bitswap Enable <input type="checkbox"/> SRA Enable			

**Modulation:** There are 8 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, “ADSL2+”, “AnnexM”, and “VDSL2” that user can select for this connection.

**G.Dmt/G.lite Enabled:** Tick the G.Dmt/G.lite check box if you want the system to use either G.Dmt or G.lite mode.

**T1.413 Enabled:** Tick the T1.413 check box if you want the system to use only T1.413 mode.

**ADSL2 Enabled:** The device can support the functions of the ADSL2.

**AnnexL Enabled:** The device can support/enhance the long loop test.

**ADSL2+ Enabled:** The device can support the functions of the ADSL2+.

**AnnexM Enabled:** Covers a higher “upstream” data rate version, by making use of some of the downstream channels.

**VDSL2 Enabled:** The device can support the functions of the VDSL2.

**VDSL2 profile:** There are 7 profiles “8a”, “8b”, “8c”, “8d”, “8a”, “12a”, “12b” and “17a” that user can select for this connection.

**US0:** Check/uncheck this item to enable/disable this function.

**Phone line pair:** This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

**Capability:** There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

**Bitswap Enable:** Allows bitswapping function.

**SRA Enable:** Allows seamless rate adaptation.

Click Apply/Save to confirm the changes.

# System

There are 5 items within the System section: [Time Zone](#), [Firmware Upgrade](#), [Backup/Restore](#), [Restart](#) and [User Management](#).

## Time Zone


Enable or disable the time zone function. If you disable time zone, the other blanks are unavailable.

**Configuration**

**Time Zone**

**Parameters**

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local Time Zone (+-GMT Time)	(GMT-08:00) Pacific Time, Tijuana <span>▼</span>
SNTP Server IP Address	time.nist.gov <span>▼</span> <input type="text"/>
	ntp1.tummy.com <span>▼</span> <input type="text"/>

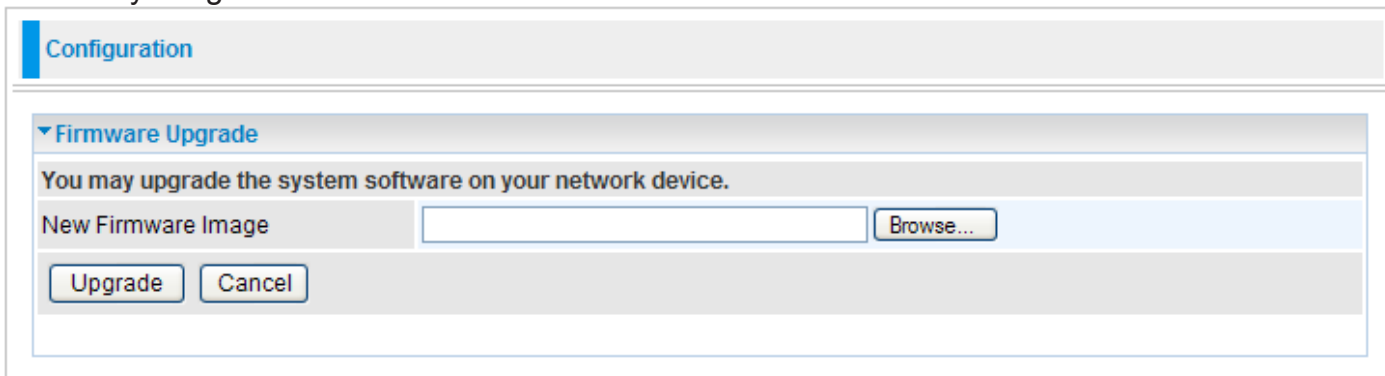


The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve 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 in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Click Apply to confirm the settings.

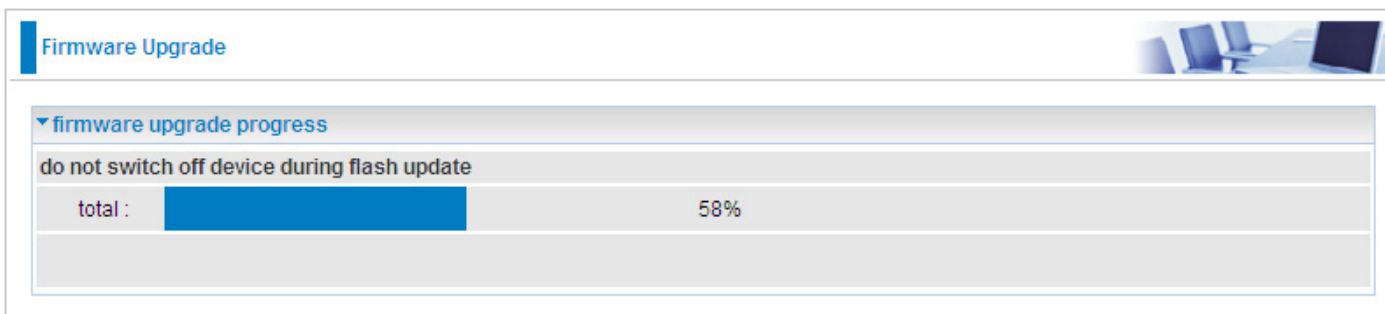
# Firmware Upgrade

Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.



The screenshot shows a web interface for configuring a router. At the top, there is a 'Configuration' tab. Below it, the 'Firmware Upgrade' section is expanded. It contains the instruction: 'You may upgrade the system software on your network device.' There is a text input field labeled 'New Firmware Image' followed by a 'Browse...' button. Below the input field are two buttons: 'Upgrade' and 'Cancel'.

Click on Browse 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 to your router.



The screenshot shows the 'Firmware Upgrade' progress page. It features a progress bar with the text 'firmware upgrade progress' and 'do not switch off device during flash update'. The progress bar is partially filled with blue, and the text 'total : 58%' is displayed next to it. There is a small image of a desk with a laptop and chair in the top right corner.

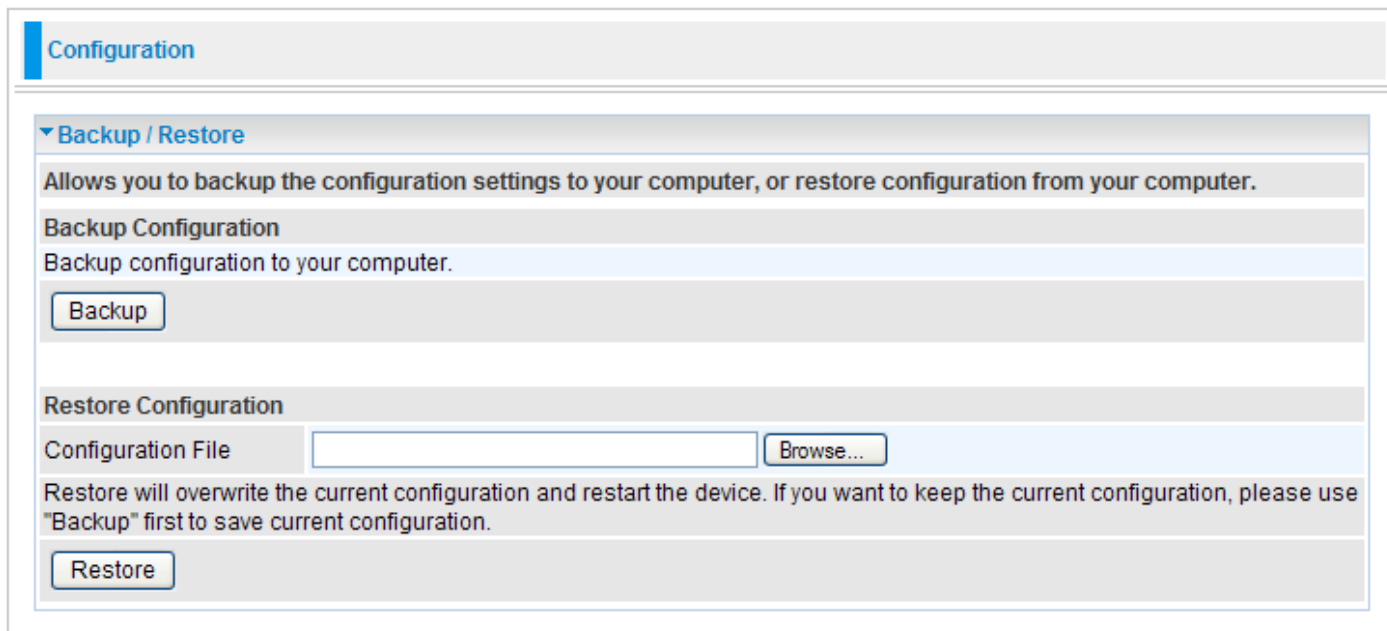


**Warning**

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

## Backup / Restore

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



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a section titled 'Backup / Restore' contains the following elements:

- A descriptive text: "Allows you to backup the configuration settings to your computer, or restore configuration from your computer."
- A sub-section 'Backup Configuration' with the text "Backup configuration to your computer." and a 'Backup' button.
- A sub-section 'Restore Configuration' with a 'Configuration File' input field, a 'Browse...' button, and a 'Restore' button.
- A warning text: "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."

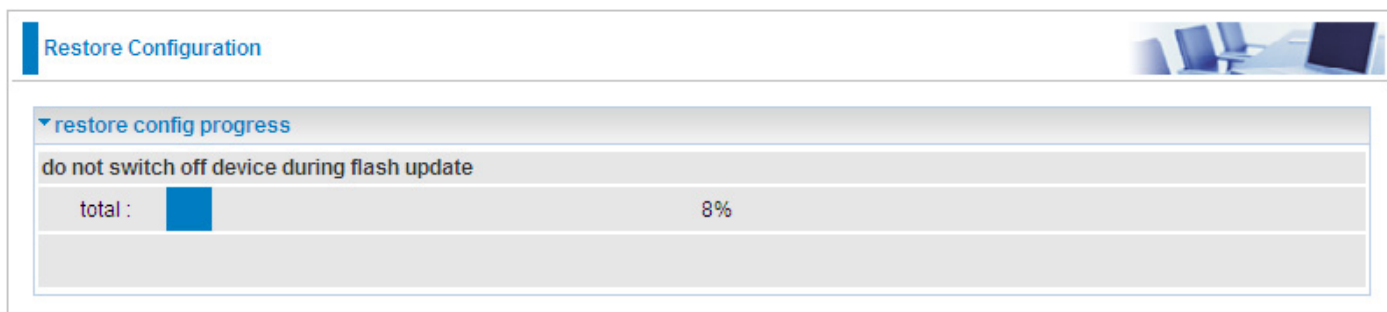
### Backup Configuration

Press Backup Settings to select where on your local PC you want to store your setting file. You may also want to change the name of the file when saving if you wish to keep multiple backups.

### Restore Configuration

Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router 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 the setting into the router. Click Restore to begin restoring the configuration and wait for the router to restart before performing any actions.

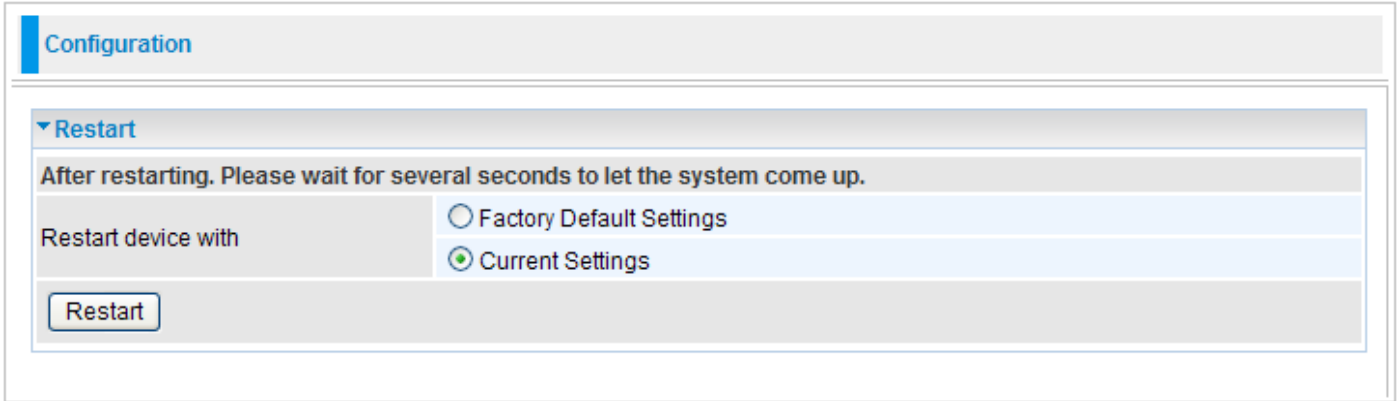


The screenshot shows a web interface for router configuration. At the top, there is a 'Restore Configuration' tab. Below it, a section titled 'restore config progress' contains the following elements:

- A warning text: "do not switch off device during flash update"
- A progress bar showing the restoration progress. The text "total :" is followed by a blue progress bar and the text "8%".

# Restart

There are 2 options for you to choose from before restarting the your device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.

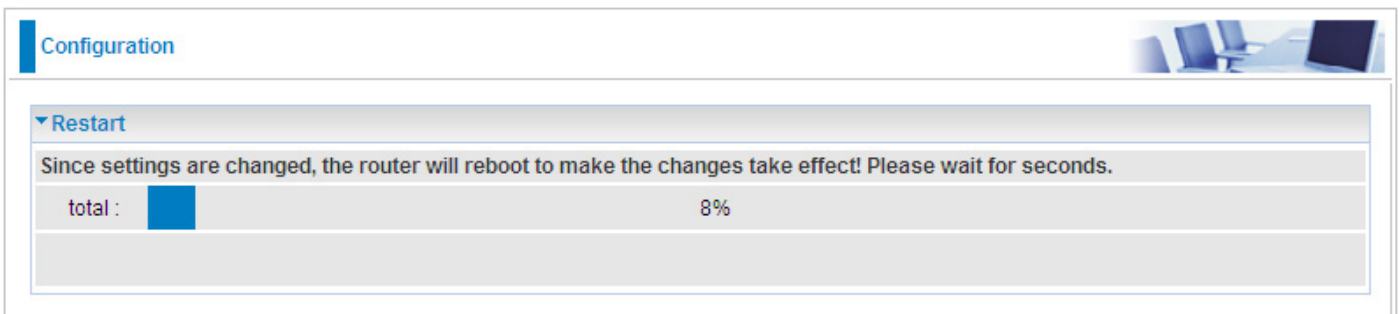


The screenshot shows a web interface with a 'Configuration' header. Below it is a 'Restart' section. A message reads: 'After restarting. Please wait for several seconds to let the system come up.' There are two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. A 'Restart' button is located at the bottom of the section.

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.

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

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.



The screenshot shows the same web interface as before, but now with a progress bar. A message reads: 'Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.' The progress bar is labeled 'total : 8%' and is partially filled with a blue bar.

You may also reset your router to factory settings by holding the small Reset pinhole button more than 1 second on the back of your router.



# User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system. It is highly recommended that you change your password upon receiving your router. The default password is “admin”.

The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a 'User Management' section is expanded. Under 'User Management', there is a 'Parameters' section. This section contains four input fields: 'Username:' with a drop-down menu, 'Old Password' with a text box, 'New Password' with a text box, and 'Confirm Password' with a text box. At the bottom of the 'Parameters' section, there are two buttons: 'Apply' and 'Cancel'.

Select the username you want to configure from the drop-down menu and then set the associated passwords.

To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.

# Firewall

Listed are the items under the Firewall section: [IP Filtering](#), [MAC Filtering](#) and [Parental Control](#).

## IP Filtering

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up 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 will be taken.

### Outgoing

All outgoing IP traffic from LAN is allowed by default, but some IP traffic could be blocked by setting up filters.

The screenshot shows the 'Configuration' page with a sub-section titled 'Outgoing IP Filtering'. It features a table with the following columns: Filter Name, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are two buttons: 'Add' and 'Remove'.

Click Add to enter Add IP Filter -- Outing screen to create a filter to identify the outgoing IP traffic.

The screenshot shows the 'Add IP Filter -- Outgoing' configuration screen. It includes a 'Parameters' section with the following fields: Filter Name (text input), Protocol (dropdown menu), Source IP address (text input), Source Subnet Mask (text input), Source Port (port or port:port) (text input), Destination IP address (text input), Destination Subnet Mask (text input), and Destination Port (port or port:port) (text input). An 'Apply/Save' button is located at the bottom.

**Filter Name:** User defined description for entry identification. The maximum name length is 32 characters.

**Protocol:** Specify the packet type (TCP/UDP, TCP, UDP and ICMP) that the rule applies to from

the listbox. 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.

**Source IP address:** This is an Address-Filter used to allow or block traffic from particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

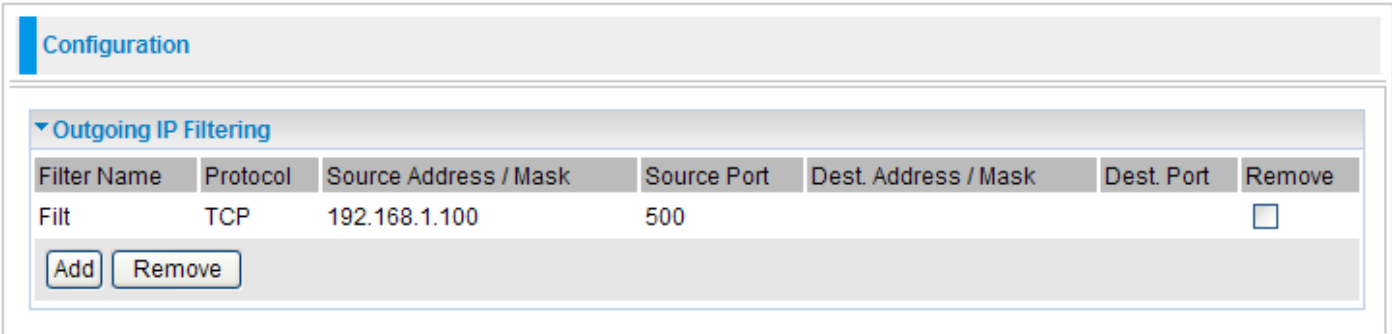
**Source Subnet Mask:** Type the subnet mask associated with the source IP address.

**Source Port (port to port:port):** This is the Port Range that defines the ports allowed by the Remote/WAN to connect to the application. It is recommended that only advance user is to configure this feature.

**Destination IP address:** This is an Address-Filter used to allow or block traffic to particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

**Destination Subnet Mask:** Type the subnet mask associated with the Destination IP address.

**Destination Port (port to port:port):** This is the Port Range that defines the port of the application.



The screenshot shows a web interface for configuration. At the top, there is a 'Configuration' tab. Below it, a section titled 'Outgoing IP Filtering' contains a table with the following data:

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Filt	TCP	192.168.1.100	500			<input type="checkbox"/>

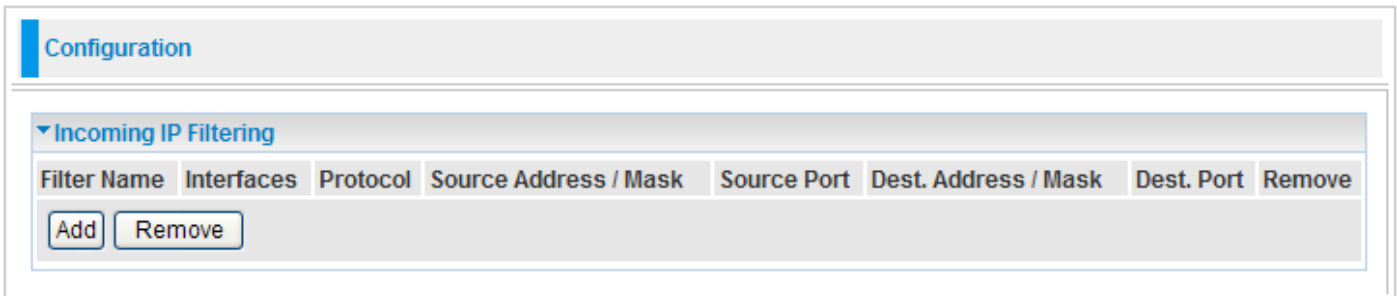
Below the table are two buttons: 'Add' and 'Remove'.

Click Apply/Save to set the new settings and you will be returned to the Outgoing IP Filtering page.

**Remove:** To delete the IP filtering rule from the table, check Remove checkbox then click Remove button to delete the selected item.

## Incoming

All incoming IP traffic from the WAN is blocked by default when the firewall is enabled. However, some IP traffic can be accepted by setting up filters.

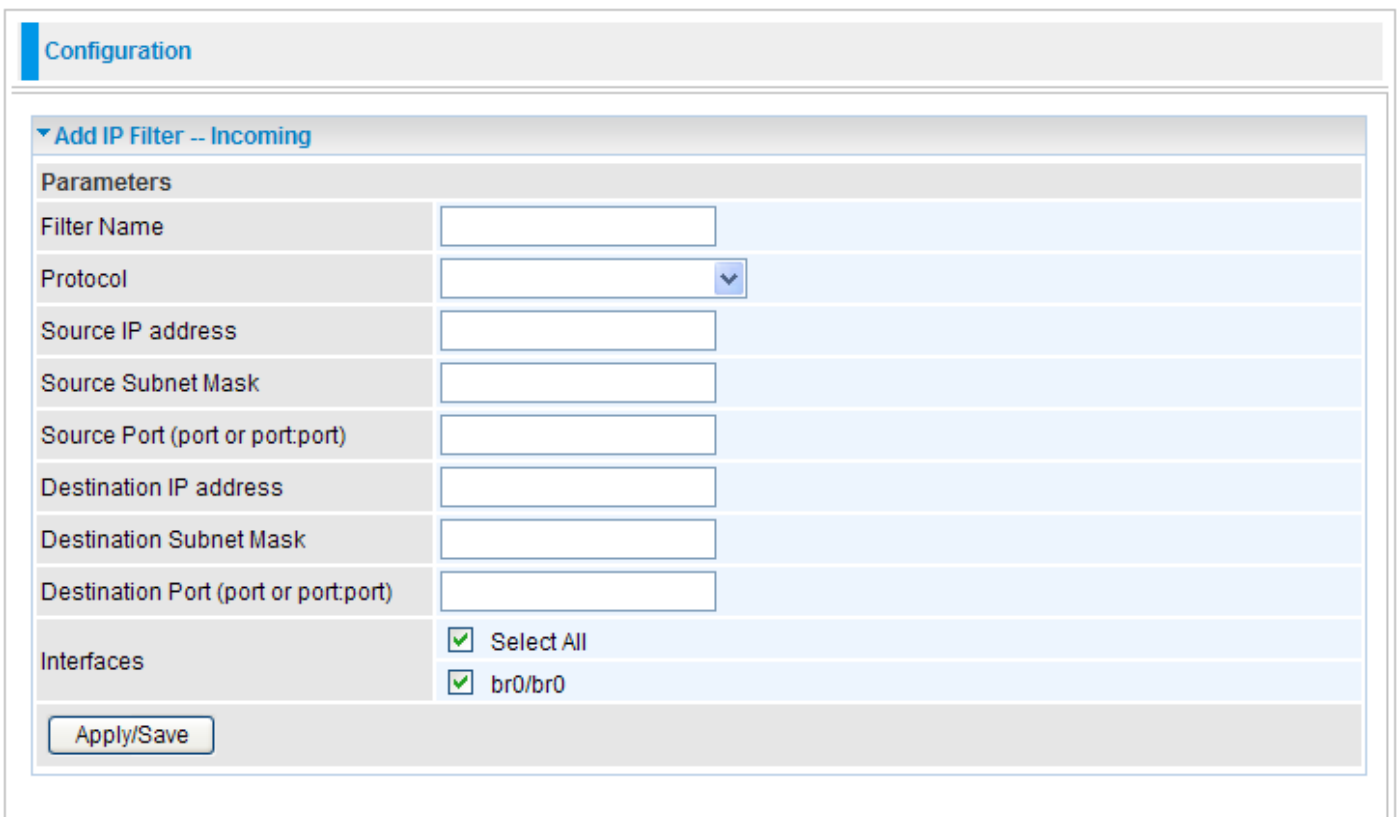


Configuration

▼ Incoming IP Filtering

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	------------	----------	-----------------------	-------------	----------------------	------------	--------

Click Add to enter Add IP Filter -- Incoming screen to add a filter rule for incoming IP traffic.



Configuration

▼ Add IP Filter -- Incoming

Parameters

Filter Name	<input type="text"/>
Protocol	<input type="text" value="Protocol"/> ▼
Source IP address	<input type="text"/>
Source Subnet Mask	<input type="text"/>
Source Port (port or port:port)	<input type="text"/>
Destination IP address	<input type="text"/>
Destination Subnet Mask	<input type="text"/>
Destination Port (port or port:port)	<input type="text"/>
Interfaces	<input checked="" type="checkbox"/> Select All <input checked="" type="checkbox"/> br0/br0

**Filter Name:** User defined description for entry identification. The maximum name length is 32 characters

**Protocol:** Specify the packet type (TCP/UDP, TCP, UDP and ICMP) that the rule applies to from the listbox. 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.

**Source IP address:** This is an Address-Filter used to allow or block traffic from particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

**Source Subnet Mask:** Type the subnet mask associated with the source IP address.

**Source Port (port to port:port):** This is the Port Range that defines the ports allowed by the Remote/WAN to connect to the application. It is recommended that only advance user is to configure this feature.

**Destination IP address:** This is an Address-Filter used to allow or block traffic to particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

**Destination Subnet Mask:** Type the subnet mask associated with the Destination IP address.

**Destination Port (port to port:port):** This is the Port Range that defines the port of the application.

**Interfaces:** Check the check box to select the interface for this rule.

Click Apply/Save to set the new settings and you will be returned to the Incoming IP Filtering page.

**Remove:** To delete the IP filtering rule from the table, check Remove checkbox then click Remove button to delete the selected item.

# MAC Filtering

A 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 network to block specific machines from accessing your LAN.

The screenshot shows the 'Configuration' page for MAC Filtering Setup. It includes a 'MAC Filtering Setup' section with explanatory text and a table for 'MAC Filtering Policy For Each Interface'. Below the table is a 'Change Policy' button. At the bottom, there is a section for 'Configure MAC filtering rules' with a table of columns: Interface, Protocol, Destination MAC, Source MAC, Frame Direction, and Remove. There are 'Add' and 'Remove' buttons below this table.

## MAC Filtering Policy For Each Interface

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARD means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

**Note: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

## Configure MAC Filtering Rules

To create a filter to identify the MAC layer frames, click on Add button.

The screenshot shows the 'Configuration' page for MAC Filter. It includes a 'MAC Filter' section with a 'Parameters' table. The table has the following fields: Protocol Type (dropdown), Destination MAC Address (text input), Source MAC Address (text input), Frame Direction: (dropdown with 'LAN<=>WAN' selected), and WAN Interfaces (Configured in Bridge mode only) (dropdown). There is a 'Save/Apply' button at the bottom.

You should specify at least one condition below to set a MAC filter profile. If multiple conditions are specified, all of them take effect.

**Protocol Type:** Select which protocol this filter will be applied to from the drop-down menu.

**Destination MAC Address:** Enter the destination MAC address this filter will be applied to. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

**Source MAC Address:** Enter the origin MAC address this filter will be applied to. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

**Frame Direction:** Select the frame flow direction from the listbox: LAN to WAN, WAN to LAN, or both directions.

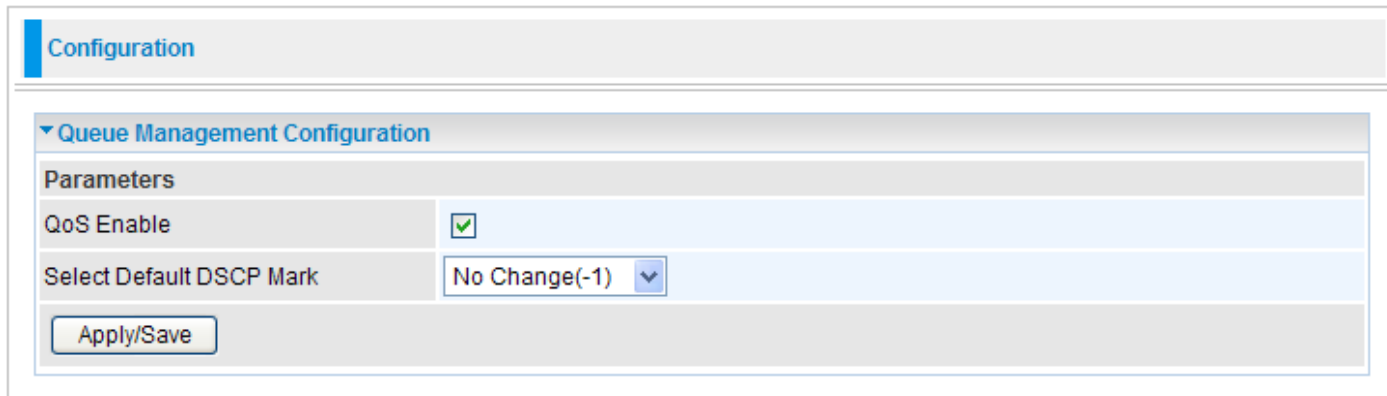
**WAN Interfaces (Configured in Bridge mode only):** Select the WAN interface.

Click Apply/Save to set the new settings and you will be returned to the Incoming IP Filtering page.

**Remove:** To delete the IP filtering rule from the table, check Remove checkbox then click Remove button to delete the selected item.

## QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Queue Management Configuration' is expanded. Under this section, there is a 'Parameters' area. The 'QoS Enable' parameter is checked with a green checkmark. The 'Select Default DSCP Mark' parameter is set to 'No Change(-1)' in a dropdown menu. At the bottom of the configuration area, there is an 'Apply/Save' button.

**QoS Enable:** Check to activate QoS function and the following field will be available.

**Note:** You can enable QoS function in WAN Configuration pages by checking “Enable Quality of Service.” check box (refer to Layer2 Interface section).

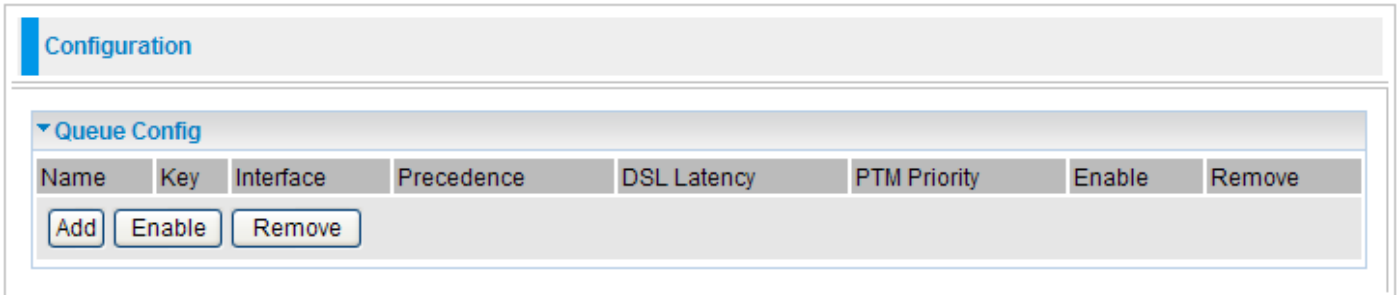
**Select Default DSCP Mark:** Select the default DSCP mark from the listbox. Differentiated Services Code Point (DSCP) is the first 6 bits in the ToS byte. DSCP Mark allows users to classify the traffic of the application to be executed according to the DSCP value.

Click Apply/Save to confirm the settings.



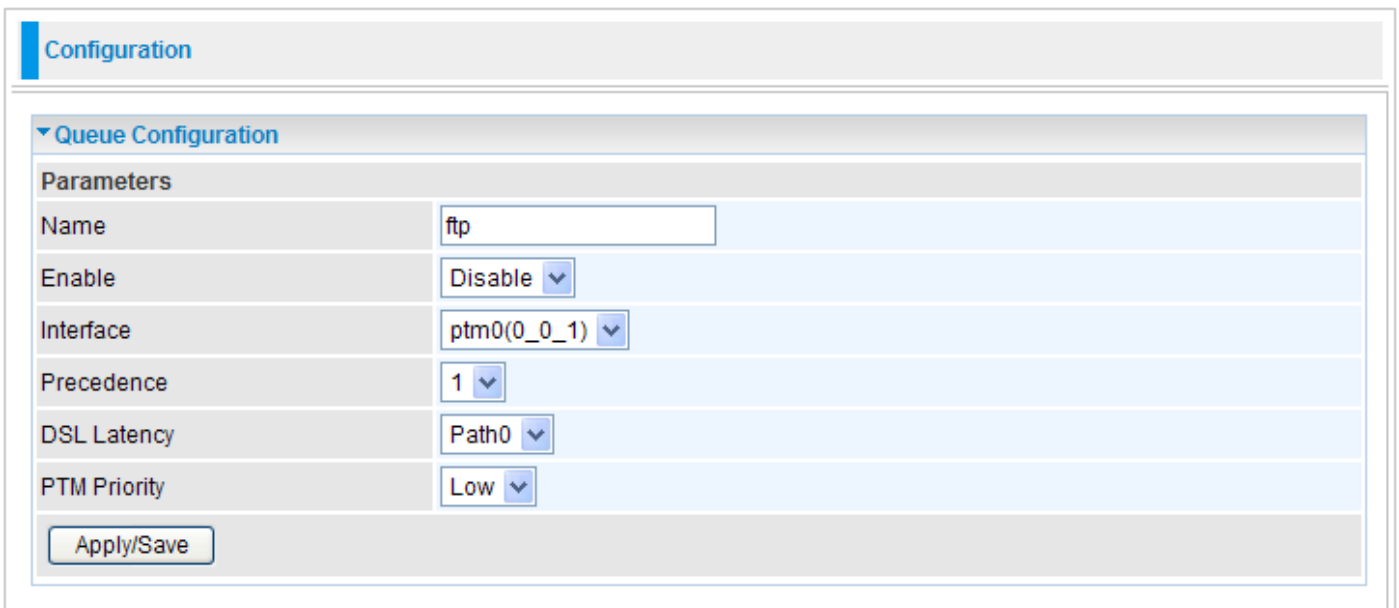
## Queue Config

Queue Config allows you to configure a QoS queue entry and assign it to a specific network interface. Each queue entry set here will be used by the classifier to place ingress packets appropriately.



The screenshot shows a web interface with a 'Configuration' header. Below it is a 'Queue Config' section containing a table with the following columns: Name, Key, Interface, Precedence, DSL Latency, PTM Priority, Enable, and Remove. Below the table are three buttons: 'Add', 'Enable', and 'Remove'.

Click Add to create the queue.



The screenshot shows a 'Queue Configuration' form with the following fields:

- Name: ftp
- Enable: Disable (dropdown)
- Interface: ptm0(0\_0\_1) (dropdown)
- Precedence: 1 (dropdown)
- DSL Latency: Path0 (dropdown)
- PTM Priority: Low (dropdown)

At the bottom of the form is an 'Apply/Save' button.

**Name:** Enter a name for this QoS item.

**Enable:** Select enable or disable this QoS application.

**Interface:** Select the interface you want to assign to this QoS item.

**Precedence:** Select the precedence of this QoS item. The rule is performed by selecting the order of the rules. The highest priority is 1.

**DSL Latency:** Select the DSL latency.

**PTM Priority:** Select the priority given to fit PTM policy/application.

Click Apply/Save to confirm the settings and you will be returned to the Queue Config table.

## Configuration

### Queue Config

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
ftp	1	ptm0	1	Path0	Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>
web	2	ptm0	4	Path0	Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Enable:** To disable the item, please uncheck Enable check box then click Enable button.

**Remove:** To delete the QoS rule from the table, check Remove checkbox then click Remove button to delete the selected item.

# QoS Classification

This screen displays a packet QoS summary table and allows user to add or remove a QoS classification class. This is the main place to configure the classification, marking and queuing rules.

**Configuration**

▼ QoS Classification

CLASSIFICATION CRITERIA													CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove
<div style="display: flex; justify-content: space-between; margin-top: 5px;"> <span>Add</span> <span>Enable</span> <span>Remove</span> </div>																			

Click Add to configure network traffic classes.

**Configuration**

▼ Network Traffic Class Rule

**Parameters**

Traffic Class Name

Rule Order
Last ▼

Rule Status
Disable ▼

**Specify Classification Criteria**

Class Interface
▼

Ether Type
▼

Source MAC Address

Source MAC Mask

Destination MAC Address

Destination MAC Mask

Source IP Address ▼

Source Subnet Mask

Destination IP Address

Destination Subnet Mask

Differentiated Service Code Point (DSCP) Check
▼

Protocol
▼

UDP/TCP Source Port (port or port:port)

UDP/TCP Destination Port (port or port:port)

802.1p Priority Check
▼

**Specify Classification Results**

Assign Classification Queue
▼

Mark Differentiated Service Code Point (DSCP)
▼

Mark 802.1p priority
▼

Tag VLAN ID (0-4094)

Set Rate Control(kbps):

Apply/Save

## **Parameters**

**Traffic Class Name:** Assign a name for this class to uniquely identify the other(s) among multiple classes.

**Rule Order:** Select the priority for this class rule.

**Rule Status:** Select Enable to activate this class rule.

## **Specify Classification Criteria**

Enter or select appropriate parameters on the following fields. A blank criterion indicates it is not used for classification.

## **Specify Classification Results**

Enter or select appropriate parameters in the following fields. You have to choose a classification queue. A blank mark or tag value means no change.

Click Apply/Save to confirm the settings and you will be returned to the QoS Classification page.

**Enable:** To disable the item, please uncheck Enable check box then click Enable button.

**Remove:** To delete the QoS class from the table, check Remove checkbox then click Remove button to delete the selected item.

# Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

In TCP 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.

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	Real Audio

# Port Mapping

Configuration

▼ Port Mapping

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								

Click Add to enter Port Mapping configuration screen.

Configuration

▼ Port Mapping

Parameters

Use Interface:  ▼

Service Name

Select a Service:  ▼

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>

## Parameters

**Use Interface:** Select a interface which you want from the drop-down menu.

## Service Name

Choose the service you need for this server. If you choose Select a Service, select an application from the listbox. If you choose Custom Service, enter a given name for this service.

**Server IP Address:** Enter the IP address.

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

**Protocol:** In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu.

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

Click Apply/Save to confirm the settings and you will be returned to Port Mapping table.

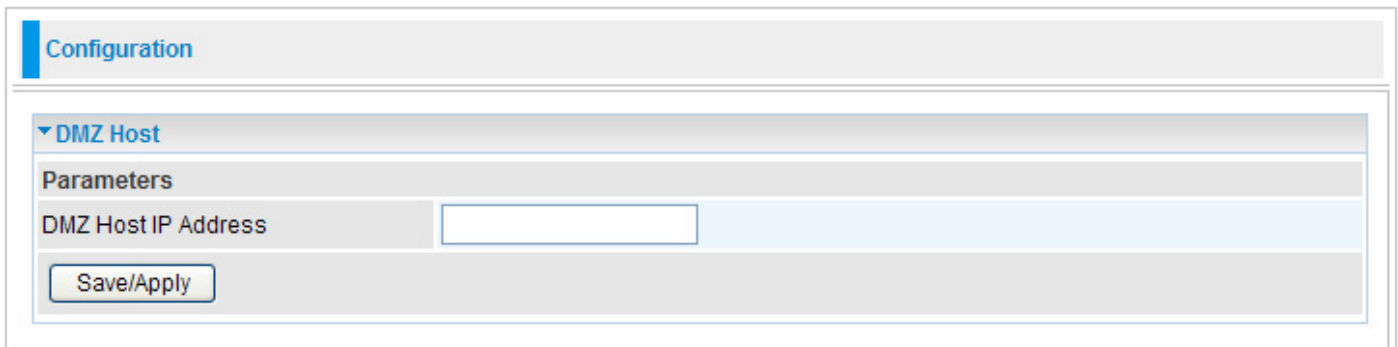
**Remove:** To delete the port mapping entry from the table, check Remove checkbox then click Remove button to delete the selected item.

Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed 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 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 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

## DMZ Host

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 that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host. When this is done, press Apply to save the changes.



The screenshot shows a configuration window titled "Configuration". Underneath, there is a section for "DMZ Host" with a dropdown arrow. Below that is a "Parameters" section containing a text input field labeled "DMZ Host IP Address" and a "Save/Apply" button.

**DMZ Host IP Address:** Enter the computer's IP address and click Save/Apply to activate the DMZ host. Or you can clear this field and click Save/Apply to inactivate the DMZ host.



### Attention

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



Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore advised to use specific Virtual Server entries just for those ports that your applications require.



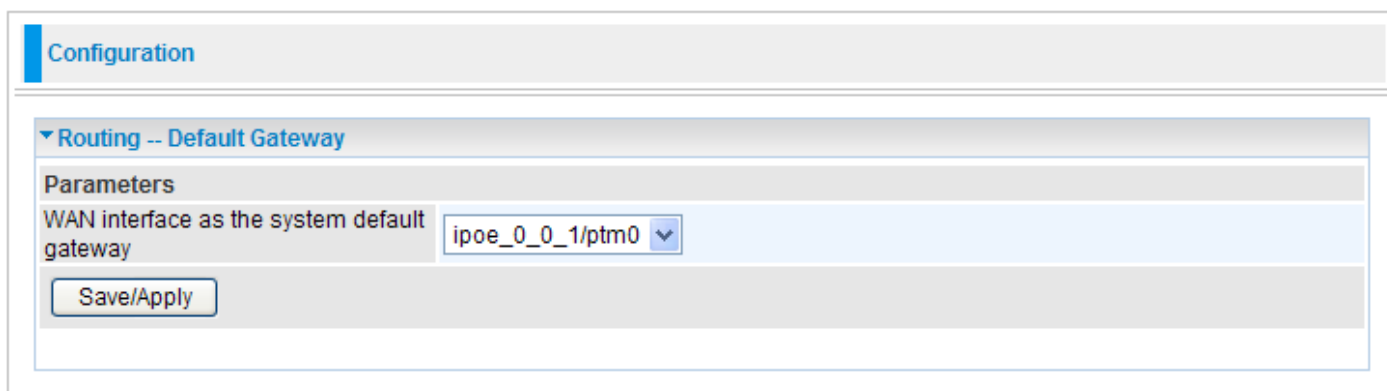
# Advanced

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.

Here are the items within the Advanced section: [Routing](#), [DNS](#), [Interface Grouping](#), [Device Management](#), [System Log Server](#) and [TR-069 client](#).

## Routing

### Default Gateway



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Routing -- Default Gateway' is expanded. Under this section, there is a 'Parameters' area. The first parameter is 'WAN interface as the system default gateway', which is set to 'ipoe\_0\_0\_1/ptm0' via a dropdown menu. A 'Save/Apply' button is located at the bottom of the configuration area.

**WAN interface as the system default gateway:** Select an appropriate WAN interface as the default gateway.

Click Save/Apply to confirm the settings.

## Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.

**Configuration**

▼ Routing -- Static Route

**Parameters**

Destination Network Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Use Interface	LAN/br0 ▼
Use Gateway IP Address	<input type="text"/>

#	Destination	Subnet Mask	Gateway	Interface	Edit	Remove <input type="checkbox"/>
<input type="button" value="Remove"/>						

**Destination:** Enter the destination IP where the traffic is to be forwarded.

**Netmask:** Enter the netmask of the destination.

**Gateway:** Enter the gateway address for the traffic.

**Interface:** Select an appropriate interface for the new routing rule from the drop-down menu.

Click Add to confirm the settings.

**#:** This is the rule number for each static router entry.

**Edit:** Check the Edit radio button to display the parameters of the selected application. Then change the items you want and click on Edit button to apply the changes.

**Remove:** To delete a static route entry, check the Remove box of the selected entry and then click on Remove button.

# RIP

Configuration

Routing -- RIP

Interface	Version	Operation	Enabled
ptm0	2	Passive	<input type="checkbox"/>

Apply/Save

**Interface:** Displays the interface for the RIP rule.

**Version:** Select the desired RIP version for this interface.

**Gateway:** Select the desired RIP operation for this interface.

**Enabled:** Check Enabled check box for the interface.

Click Apply/Save to confirm the settings.

# DNS

## DNS Server

On the Internet, Domain Name System (DNS) servers are used to translate a hostname or a domain name to its corresponding binary identifier.

The screenshot shows a web interface for configuring the DNS server. At the top, there is a 'Configuration' tab. Below it, the 'DNS Server' section is expanded. Under the 'Parameters' heading, there are two radio button options. The first option, 'Obtain DNS info from a WAN interface:', is selected. Below this, a dropdown menu shows 'ipoe\_0\_0\_1/ptm0' as the selected WAN interface. The second option, 'Use the following Static DNS IP address:', is unselected. Below this, there are two text input fields for 'Primary DNS server:' and 'Secondary DNS server:', both of which are currently empty. At the bottom of the configuration area, there is an 'Apply/Save' button.

If you check "Obtain DNS info from a WAN interface", this router will accept the first received DNS assignment from one of the WAN interface during the connection establishment. If you check "Use the following Static DNS IP address", enter the primary and optional secondary DNS server IP addresses.

Click Apply/Save to confirm the settings.

## 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 when hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

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



The screenshot shows a web interface with a 'Configuration' header. Below it is a section titled 'Dynamic DNS' which contains a table with the following columns: Hostname, Username, Service, Interface, and Remove. Below the table are two buttons: 'Add' and 'Remove'.

Click Add to enter Add Dynamic DNS screen.



The screenshot shows the 'Add Dynamic DNS' configuration form. It has a 'Parameters' section with the following fields: 'D-DNS provider' (a dropdown menu with 'DynDNS.org' selected), 'Hostname' (a text input field), 'Interface' (a dropdown menu with 'ipoe\_0\_0\_1/ptm0' selected), 'Username' (a text input field), and 'Password' (a text input field). At the bottom of the form is an 'Apply/Save' button.

**Dynamic DNS Server:** Select the DDNS service you have registered an account with.

**Hostname:** Enter your registered hostname for this service.

**Interface:** Select an appropriate interface for the DDNS service from the drop-down menu.

**Username/Password:** Enter username and password for this service.

Click Apply/Save to confirm the settings and you will be returned to Dynamic DNS table.

**Remove:** To delete the DDNS entry from the table, check Remove checkbox then click Remove button to delete the selected item.

# Interface Grouping

This function allows you to set new interface group.

The screenshot shows the 'Configuration' page with a section for 'Interface Grouping'. It contains a table with the following data:

Group Name	Remove	WAN Interface	LAN Interface	DHCP Vendor IDs
Default		ptm0	eth2	
			eth3	
			eth1	
			eth0	

Below the table are two buttons: 'Add' and 'Remove'.

Click Add to create a new interface grouping.

The screenshot shows the 'Configuration' page with a section for 'Interface Grouping' containing a configuration form. The form includes the following fields and controls:

- Group Name:** A text input field.
- WAN Interface used in the grouping:** A dropdown menu with 'ipoe\_0\_0\_1/ptm0' selected.
- Grouped LAN Interfaces:** An empty list box.
- Available LAN Interfaces:** A list box containing 'eth0', 'eth1', 'eth2', and 'eth3'.
- Navigation:** '<- Add' and '-> Remove' buttons between the grouped and available LAN interfaces.
- Automatically Add Clients With the following DHCP Vendor IDs:** A section with five input fields labeled 'Vendor #0' through 'Vendor #4'.
- Apply/Save:** A button at the bottom of the form.

**Group Name:** Enter the name that you want this interface group to have.

**WAN Interface used in the grouping:** Select appropriate WAN interface.

**Grouped LAN Interfaces:** Displays the list of selected ethernet ports in this group. To delete services from the list, select the interface and click Remove.

**Available LAN Interfaces:** Displays the list of available ethernet ports which you can add to this group. Select the services you want and click Add.

Note: Ethernet port needs to be part of port mapping group and bridge interface

**Automatically Add Clients With the following DHCP Vendor IDs:** Enter the IDs in the fields.

Click on Save/Apply button to finish the configuration and you will be returned to Interface Grouping table.

Configuration

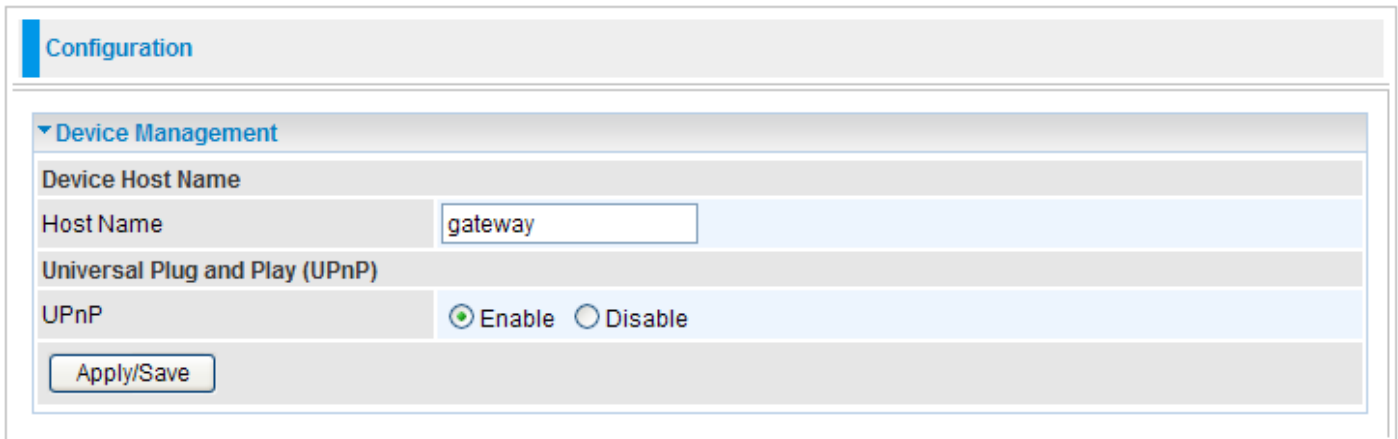
▼ Interface Grouping

Group Name	Remove	WAN Interface	LAN Interface	DHCP Vendor IDs
Default			eth2	
			eth3	
			eth1	
test	<input type="checkbox"/>	ptm0	eth0	

**Remove:** To delete the Interface Grouping from the table, check Remove checkbox then click Remove button to delete the selected item.

## Device Management

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



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a section titled 'Device Management' is expanded. Under 'Device Management', there are two main sections: 'Device Host Name' and 'Universal Plug and Play (UPnP)'. The 'Device Host Name' section has a 'Host Name' field containing the text 'gateway'. The 'Universal Plug and Play (UPnP)' section has a 'UPnP' field with two radio buttons: 'Enable' (which is selected) and 'Disable'. At the bottom of the configuration area, there is an 'Apply/Save' button.

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

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UPnP feature. Windows 2000 does not support UPnP.

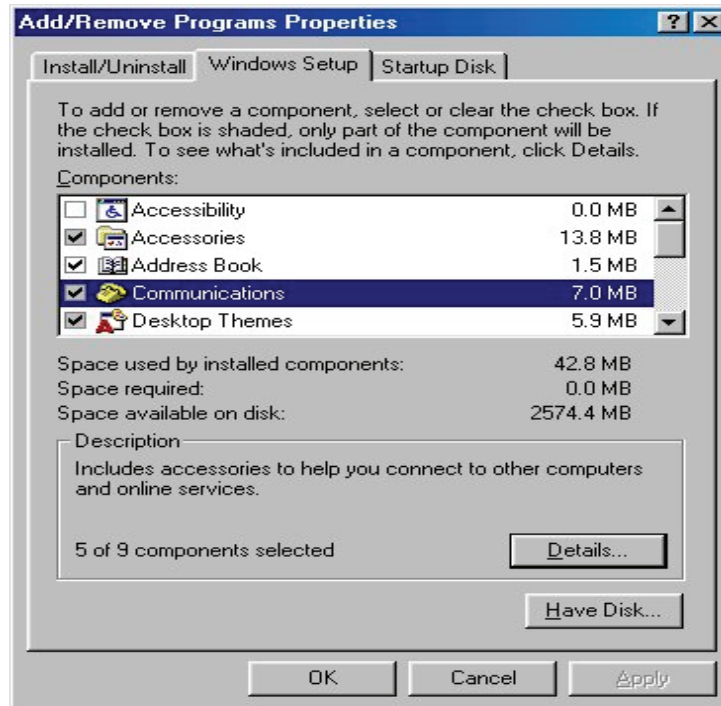


## Installing UPnP in Windows Example

### 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.

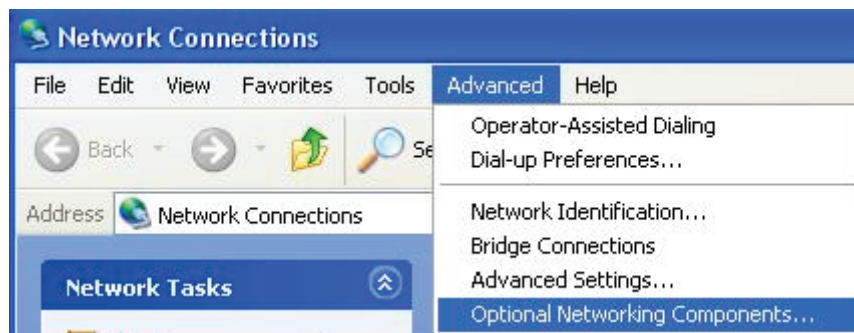
Step 5: Restart the computer when prompted.

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

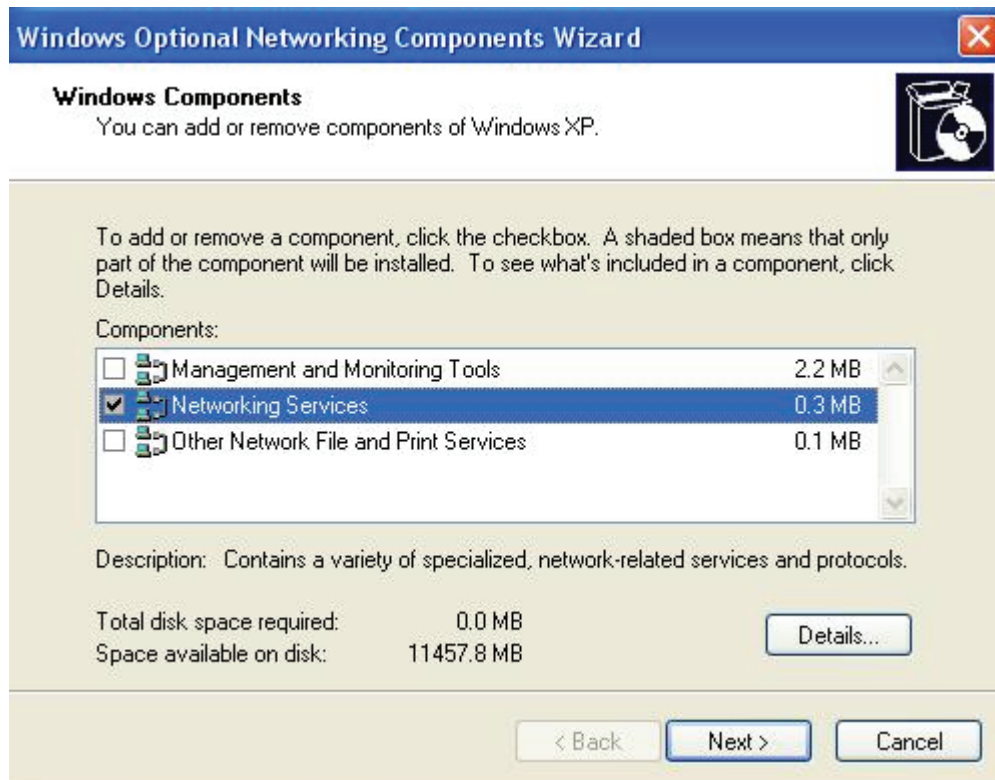
Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

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

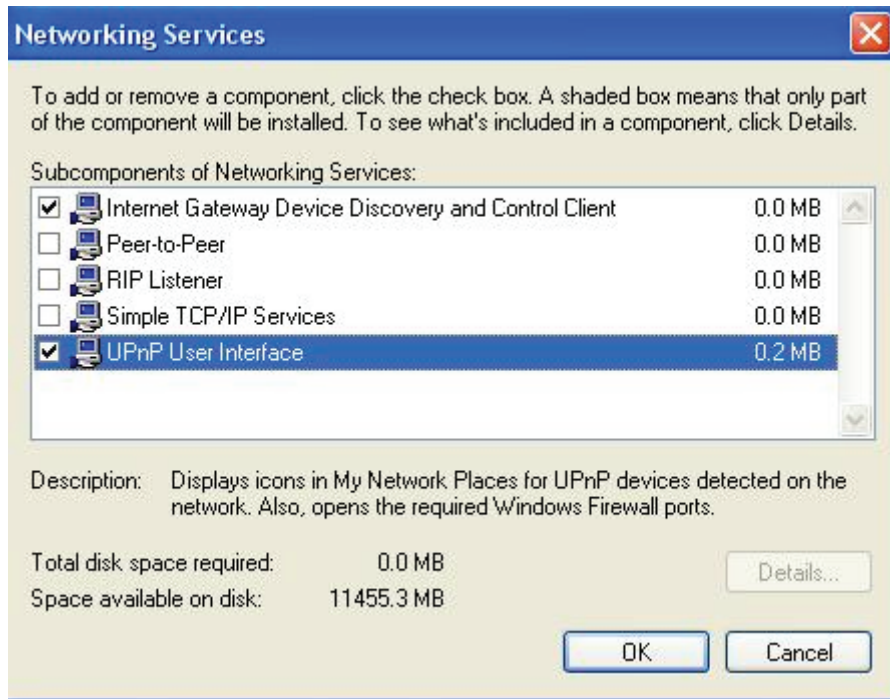


Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



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

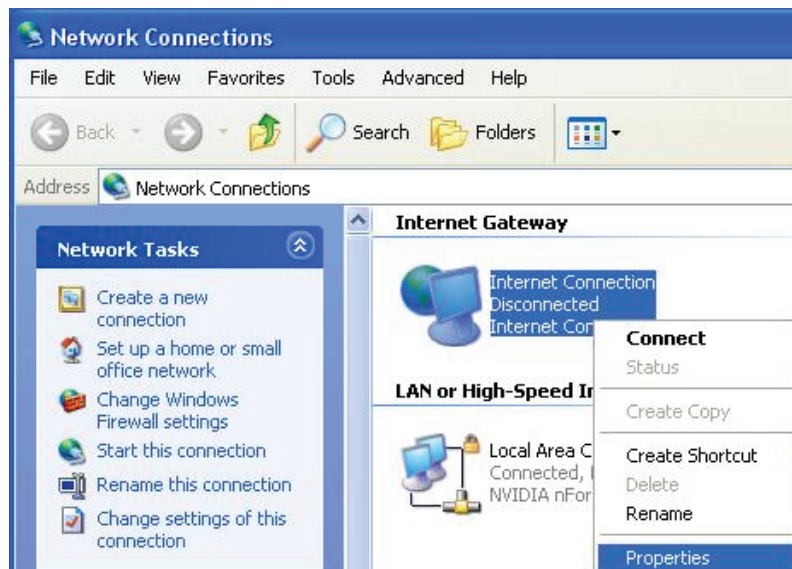
Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



## Auto-discover Your UPnP-enabled Network Device

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

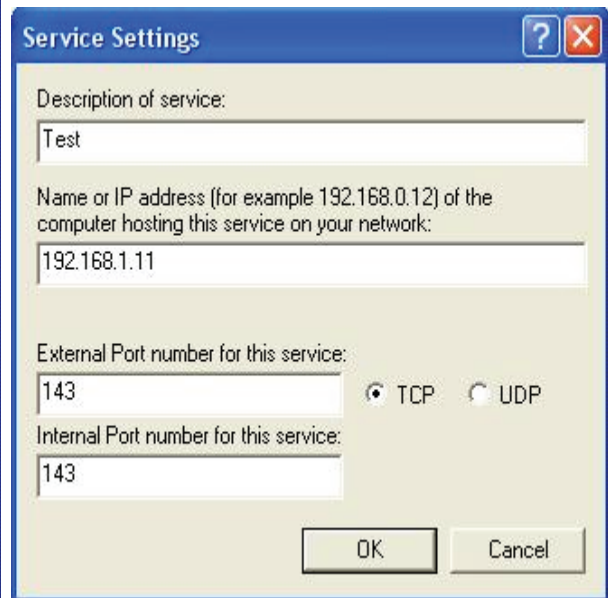
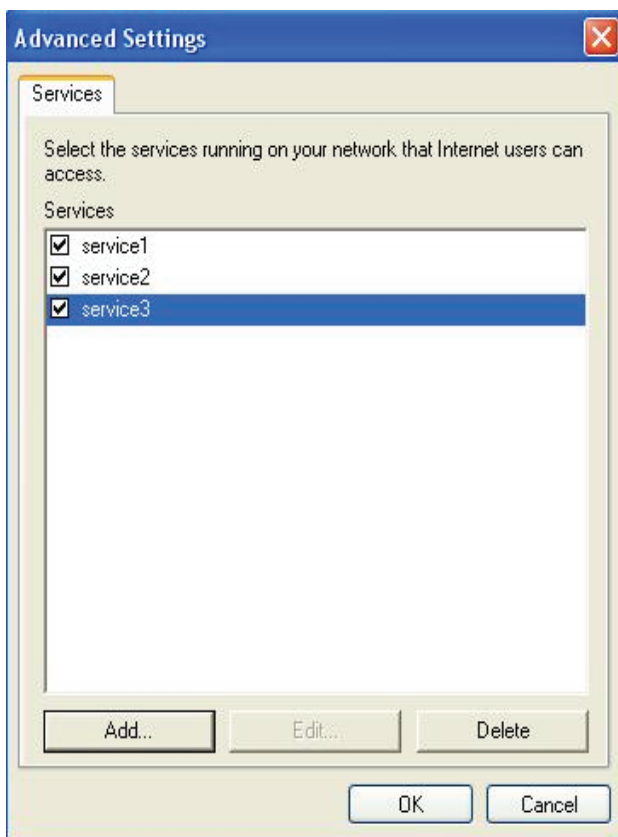
Step 2: Right-click the icon and select Properties.



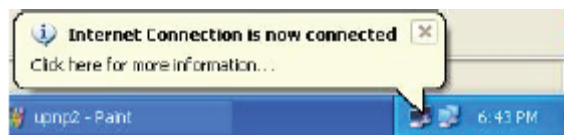
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



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

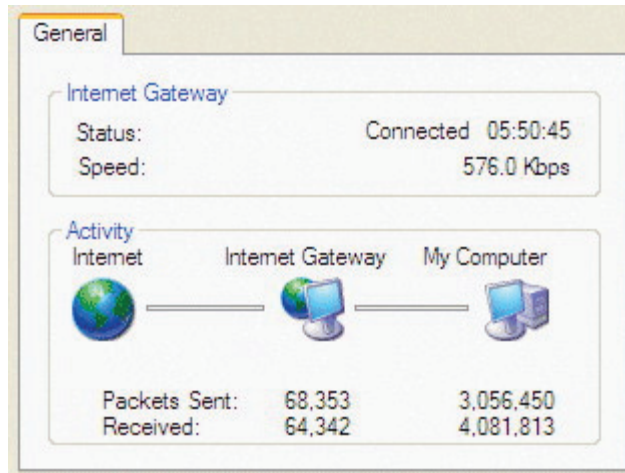


Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.



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





## Web Configurator Easy Access

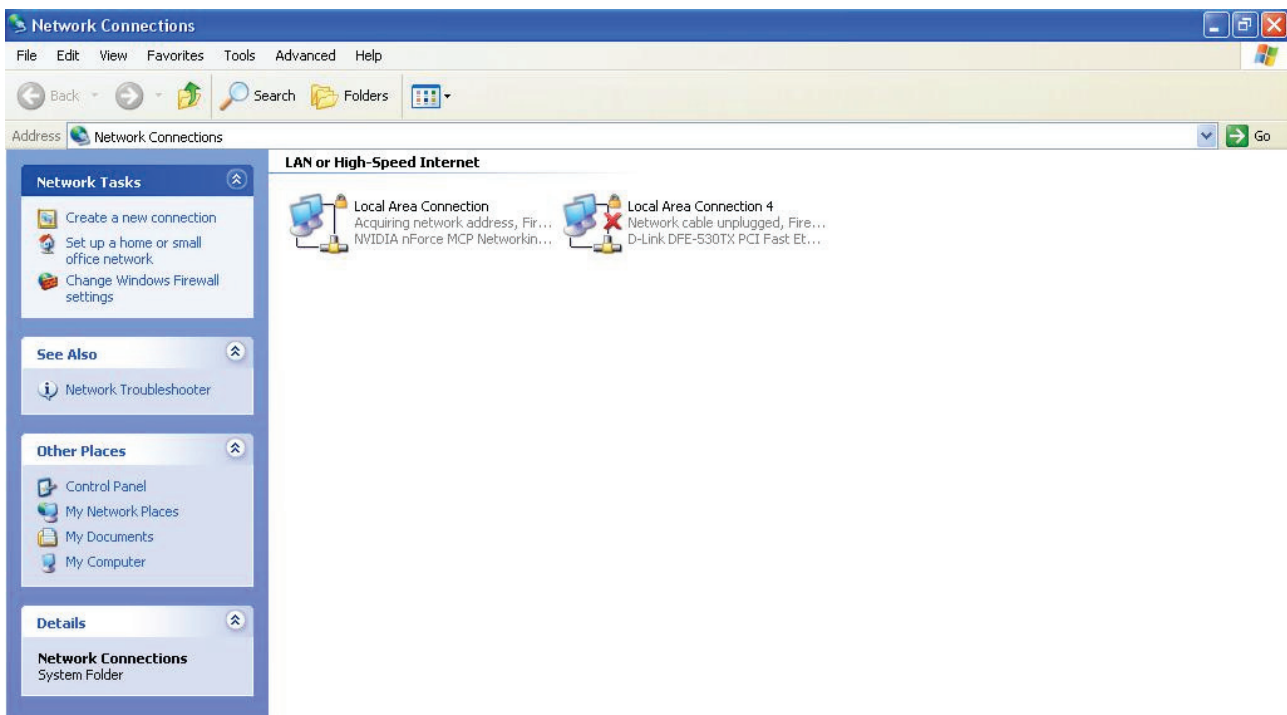
With UPnP, you can access web-based configuration for the BEC 8800N without first finding out the IP address of the router. This helps if you do not know the router's IP address.

### 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.



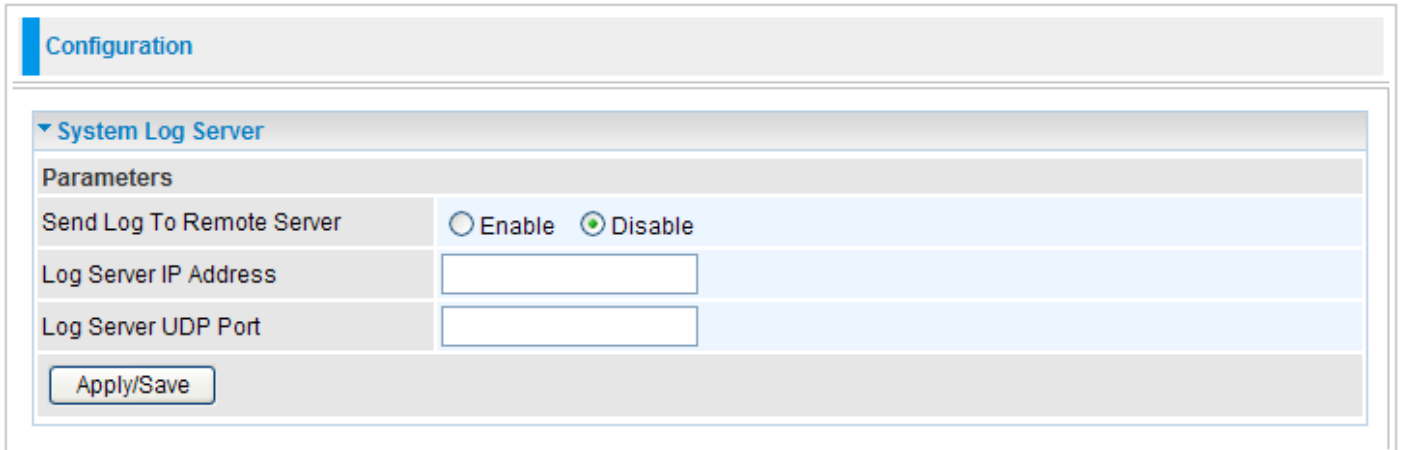
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BEC 8800N and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BEC 8800N and select Properties. A properties window displays basic information about the BEC 8800N.

# System Log Server

This screen allows you to view the system events log or to configure the system log options.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'System Log Server' is expanded. Under this section, there is a 'Parameters' area. The first parameter is 'Send Log To Remote Server', which has two radio buttons: 'Enable' (which is unselected) and 'Disable' (which is selected). Below this are two text input fields: 'Log Server IP Address' and 'Log Server UDP Port'. At the bottom of the configuration area is a button labeled 'Apply/Save'.

**Send Log To Remote Server:** By default, it is disabled. To enable it, tick Enable to activate system log.

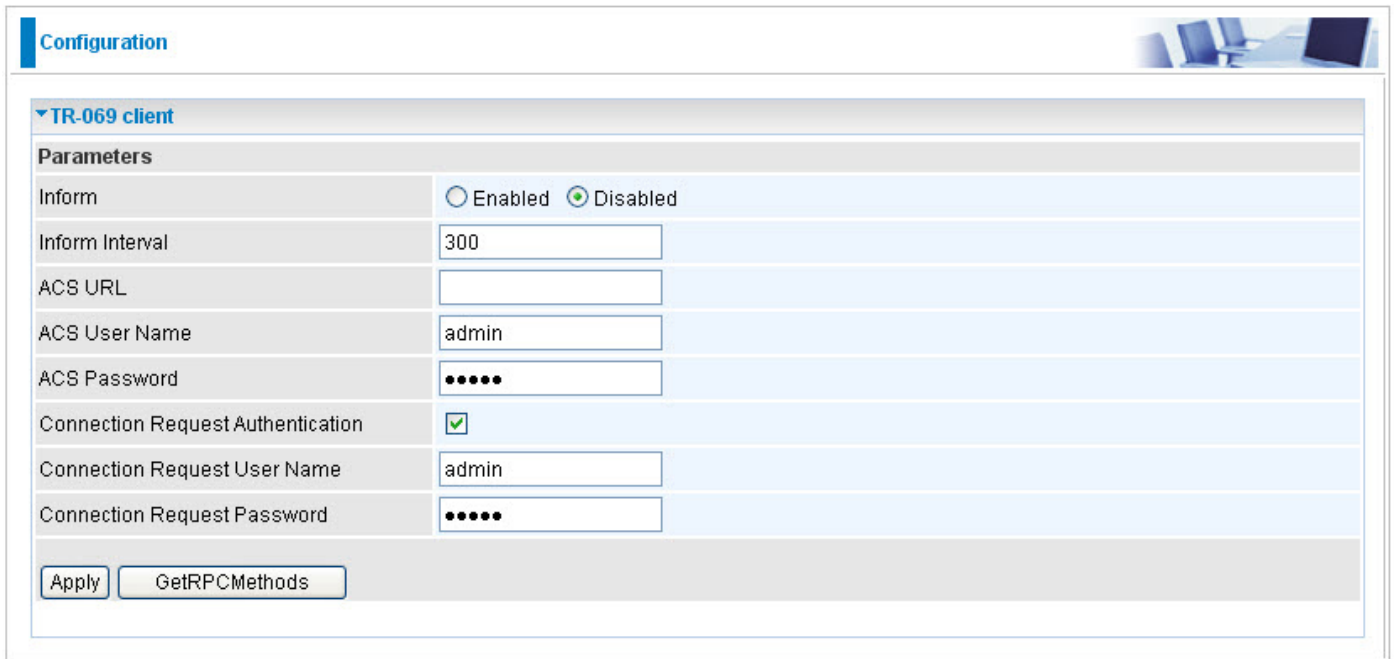
**Log Server IP Address:** Enter the server IP address.

**Log Server UDP Port:** Enter the server UDP port.

Click Apply/Save to confirm the settings.

# TR-069 Client

Please contact your ISP for the information of TR069.



Parameters	
Inform	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Inform Interval	<input type="text" value="300"/>
ACS URL	<input type="text"/>
ACS User Name	<input type="text" value="admin"/>
ACS Password	<input type="password" value="....."/>
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request User Name	<input type="text" value="admin"/>
Connection Request Password	<input type="password" value="....."/>

**Inform:** You can enable or disable the periodic inform feature.

**Inform Interval:** Enter the length of the periodic inform interval (unit: seconds).

**ACS URL:** Enter the ACS URL address.

**ACS Username:** Enter the ACS server login name.

**ACS Password:** Enter the ACS server login password.

**Connection Request Authentication:** Check to enable connection request authentication feature.

**Connection Request User Name:** Enter the username for ACS server to make connection request.

**Connection Request Password:** Enter the password for ACS server to make connection request.

**GetRPCMethods:** Detect the types of methods that ACS supports and is in communication with.

Click Apply to confirm the settings.

# Diagnostics

Here are 2 items within this section: [Diagnostics](#) and [Fault Management](#).

## Diagnostics

This page allows users to test the Ethernet port connection, DSL port connection, and connection to the Internet Service Provider. If a test displays a FAIL status, click "Test" again or "Test With OAM F4" to make sure the fail status is consistent.

ipoe\_0\_0\_1 Diagnostics

Local Network	
Test your eth2 Connection	FAIL
Test your eth3 Connection	FAIL
Test your eth1 Connection	PASS
Test your eth0 Connection	FAIL

DSL service provider	
Test xDSL Synchronization	FAIL
Test ATM OAM F5 segment ping	DISABLED
Test ATM OAM F5 end-to-end ping	DISABLED

Internet service provider	
Ping default gateway	PASS
Ping primary Domain Name Server	FAIL



# Fault Management

IEEE 802.1ag Ethernet Connectivity Fault Management protocols comprise three protocols: continuity check, link trace and loopback protocols that work together to help administrators debug Ethernet networks. On this screen, you can configure 802.1ag CFM and use this function.

**Diagnostics**

**802.1ag Connectivity Fault Management (only for VDSL PTM Mode)**

Maintenance Domain (MD) Level	2
Destination MAC Address	
802.1Q VLAN ID (0-4095)	0
VDSL Traffic Type	Inactive

**Test the connection to another Maintenance End Point (MEP)**

Loopback Message (LBM)	
------------------------	--

**Find Maintenance End Points (MEPs)**

Linktrace Message (LTM)				

Set MD Level    Send Loopback    Send Linktrace

# Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or BEC for support.

Problem	Suggested Action
<b>The power LED is not on</b>	Make sure the connection of power supply is good, the switch of power supply is turned on and the output of power supply is correct.
<b>None of the LEDs lit when the router is turned on</b>	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
<b>I can not access Internet or remote networks</b>	Make sure that the power is turned on and the software configuration of the router is correct. Ensure that the device has been restarted after configuration change. Check IP connection using ping command and that the DNS of the computer is correct.
<b>I can not access some web server</b>	This problem is often caused by one of the following issues: <ul style="list-style-type: none"> <li>• The MTU of operating system might be too large.</li> <li>• Some operating systems might need to be patched.</li> </ul>
<b>I can not log on to the configuration page</b>	<ul style="list-style-type: none"> <li>• Check the connection between the PC and the router.</li> <li>• Ensure your PC's IP address is on the same subnet as the router.</li> <li>• Check to see if your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to ensure that the Java applet is loaded.</li> <li>• Make sure you are using the correct user name and password. User names and passwords are case sensitive, so make sure that CAPS LOCK is not on when entering this information.</li> <li>• Reset the device.</li> </ul>
<b>I have forgotten my login username or password</b>	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the Reset button for 3~5 seconds.

# Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

## Contact BEC

<http://www.bectechnologies.net>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.