W3100V

One-port ADSL 2+ Wireless Router

User Manual

Contents

1 Introduction 1
- 1.1 Application 1
- 1.2 Features 2
- 1.3 Wireless Specifications 3
- 1.4 Compliance Certificates 4
- 1.5 Standards Compatibility and Compliance 4
- 1.6 Supported Encapsulation 5
- 1.7 Environment Requirements 5
- 1.8 System Requirements 6
- 1.9 Safety Cautions 9
- 1.10 LED Status Description 10
  - 1.10.1 Front Panel 10
  - 1.10.2 Rear Panel 11

2 Hardware Installation 11
- 2.1 Choosing the Best Location for Wireless Operation 12
- 2.2 Connecting the ADSL Router 13
- 2.3 Factory Reset Button 13

3 Introduction to Web Configuration 17
- 3.1 Preparation Before Login 17
- 3.2 Logging In to the Modem 18
  - 3.2.1 First-Time Login 18
- 3.3 DSL Router Device Information 19
  - 3.3.1 Summary of Device Information 19
  - 3.3.2 WAN Interface Information 20
  - 3.3.3 Statistics of LAN 21
  - 3.3.4 Statistics of WAN 21
  - 3.3.5 Statistics of ATM 22
  - 3.3.6 Statistics of ADSL 22
  - 3.3.7 Route Table Information 26
  - 3.3.8 ARP Table Information 27
- 3.4 Advanced Setup 27
  - 3.4.1 WAN Configuration 27
  - 3.4.2 LAN Configuration 50
  - 3.4.3 NAT 51
  - 3.4.4 Security 59
  - 3.4.5 Parental Control 65
  - 3.4.6 Quality of Service 66

3.4.7 Routing 78
3.4.8 DNS 81
3.4.9 DSL 83
3.4.10 IPSec 84
3.4.11 Certificate 85
3.5 Wireless 88
3.5.1 Wireless LAN Basics 89
3.5.2 Wireless – Basic 92
3.5.3 Wireless – Security 93
3.5.4 Wireless - MAC Filter 103
3.5.5 Wireless – Bridge 105
3.5.6 Wireless – Advanced 106
3.5.7 Wireless -- Authenticated Stations 109
3.6 Diagnostics 110
3.7 Management 111
3.7.1 Settings 111
3.7.2 System Log 113
3.7.3 TR-069 Client 115
3.7.4 Internet Time 116
3.7.5 Access Control 117
3.7.6 Update Software 119
3.7.7 Save/Reboot 120
4 Networking Topology 121
4.1 PPP over ATM (PPPoA) Mode 121
4.2 PPP over Ethernet (PPPoE) Mode 123
4.3 MER + DHCP Mode 124
4.4 IP over ATM (IPoA) + NAT Mode 126
4.5 Leased Line Mode 128
5 Q&A 129

1 Introduction

The Router is a highly ADSL2+ Integrated Access Device and can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g/802.11b wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Modem connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

The embedded 802.11g wireless access point provides Internet access and connectivity to the Ethernet for 802.11g and 802.11b wireless workstations. IEEE 802.11g is fully compatible with IEEE 802.11b wireless devices. The 802.11g standard supports data transfer with rate up to 54 Mbps. The wireless access point of router supports common security protocols that are used for wireless LAN including 64/128 bits WEP encryption, 802.1x, WPA and WPA2.

1.1 Application

- Home gateway
- SOHOs
- Small enterprises
- TV over IP (IPTV)
- Higher data rate broadband sharing

- Shared broadband internet access
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

1.2 Features

- ADSL2+ interface complied with G.dmt, G.lite, T1.413, G.992.3 (ADSL/ADSL2), G.992.5(ADSL2+), Annex A, Annex L.
- Hardware ATM segmentation & reassembly engine with CBR, rt- VBR, nrt-VBR, UBR- with-PCR, UBR
- 1 x 10/100BASE-T/TX Ethernet switch ports
- IEEE802.11 b/g compatible Wireless Access Point
- Support 64/128-bit WEP, 802.1x, WPA, and WPA2 for wireless security
- Telnet, HTTP Web Management, TFTP, FTP for Firmware Upgrade
- VPN Pass Through on L2TP, PPTP, IPSec
- Transparent Bridging among 10/100 Mbps Ethernet, USB, and 802.11g wireless LAN
- Configuration file backup and restore
- Simple web based status page displays a snapshot of your system configuration, and links to the configuration pages.
- Support DHCP server/client/relay
- Support self-learning bridge (IEEE 802.1D Transparent Bridging)
- Support 64 learning MAC addresses at least
- Support IP source and destination routing
- Support address Filtering, UPnP, NAT, NAPT, DMZ, IP QoS
- Supporting up to 16 PVCs
- Support ATM forum UNI3.0, 3.1 and 4.0 Permanent Virtual Circuits (PVCs)
- Support ITU-T i.610F4/F5 OAM
- Command Line Interface via serial port, telnet, or ssh
- Date/time update from SNTP Internet Time Server
- Three level login including local admin, local user and remote technical support access
- Service access control based on incoming interface: WAN or LAN
- Protect DOS attacks from WAN/LAN: SYN flooding, IP surfing, ping of Death, fraggle,- UDP ECHO (port 7) , teardrop, land.

= PAP (RFC1334), CHAP (RFC1994), MSCHAP for PPP session.
= Support auto channeling for wireless
= Support a main SSID and a guest SSID for wireless
= Support RTS/CTS, Segment function for wireless
= Support STA Mutual isolation for wireless
= Support SES for wireless
= support WDS for wireless
= Support Hide SSID for wireless
= Support MAC Access/Deny List for wireless
= WMM support for wireless
= PRE 54M: -66 dBm@10%PER; 11M: -80 dBm@8%PER for wireless
= Industry standard and interoperable DSL interface

1.3 Wireless Specifications

Item	**Description**	
Network Standard	= IEEE 802.11b = IEEE 802.11g	
Frequency Range	2.40 GHz~2.4835 GHz ISM Band	
Modulation	= 802.11b: DBPSK, DQPS, CCK = 802.11g: BPSK, QPSK, 16QAM, 64QAM	
RF Power	20 dBm (Max). 802.11bType. 16.5+/-1.5 dBm @Normal Temp Range, 802.11gType. 15+/-1.5 dBm @ Normal Temp Range	
AP Capacity	Access User Quantity	50 Pcs~80 Pcs/AP (Proposal)
	Channels	= 11 (US and Canada)
	Auto-sensing Data Rate	= 802.11.b: 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps = 802.11g: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps
Payload Rate	1 Mbps	DBPSK @ 0.81 Mbps

Item	Description	
	2 Mbps	DQPSK @ 1.58 Mbps
	5.5 Mbps	CCK @ 4.07 Mbps
	6 Mbps	BPSK @ 4.64 Mbps
	9 Mbps	BPSK @ 6.55 Mbps
	11 Mbps	CCK @ 7.18 Mbps
	12 Mbps	BPSK @ 8.31 Mbps
	18 Mbps	QPSK @ 11.5 Mbps
	24 Mbps	6QAM @ 14.18 Mbps
	36 Mbps	16QAM @ 18.31 Mbps
	48 Mbps	64QAM @ 23.25 Mbps
	54 Mbps	64QAM @ 26.12 Mbps
Security	64-bit/128-bit WEP, 802.1x, WPA, WPA2	
User Isolation	MAC Level	
MAC Filter	= Eth Interface MAC Filter: Support = Vacancy MAC Filter: Support	
Authentication	= DHCP Client & Static IP: Support = 802.1X and Radius Client: Support = DHCP Server: Support	
Radio Cover Rage	= Outdoor: 120m~400m = Indoor: 35m~100m	
Antenna Type	Internal Diversity with Connector. 2 dBi	

1.4 Compliance Certificates

- FCC Class B
- CE Mark

1.5 Standards Compatibility and Compliance

- RFC 2684 multi-protocol Encapsulation over ATM Adaptation Layer 5
- RFC1483 Multi-protocol Encapsulation over ATM Adaptation Layer 5
- RFC2364 PPP over ATM ALL5 (PPPoA)

- RFC2516 PPP Over Ethernet (PPPoE)
- RFC1662 PPP in HDLC-like Framing
- RFC1332 PPP Internet Protocol Control Protocol
- RFC1577/2225 Classical IP and ARP over ATM (IPoA)
- RFC1483R
- RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC1042 A standard for the Transmission of IP Datagrams over IEEE 802 Networks
- MER (a.k.a IP over Ethernet over AAL5)
- Support ALG (Application Level Gateways)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 issue 2
- IEEE802.3
- IEEE802.3u
- IEEE 802.11b
- IEEE 802.11g

1.6 Supported Encapsulation

- RFC 1483 bridge
- RFC 1483 Router
- Classical IP over ATM (RFC 1577)
- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)

1.7 Environment Requirements

- Operating temperature: 0ºC~40ºC (32ºF to 104ºF)
- Storage temperature: -20ºC~70ºC (-4ºF to 158ºF)
- Operating humidity: 10%~95%, non-condensing
- Storage humidity: 5%~95%, non-condensing

1.8 System Requirements

Recommended system requirements are as follows:

- Pentium 233 MHZ or above
- Memory: 64 Mbps or above
- 10M Base-T Ethernet or above
- Windows 9x, Windows 2000, Windows XP, Windows ME, Windows NT
- Ethernet network interface card

The following information is very helpful for your ADSL configuration. To keep a record for reference, fill in the column as follows.

Collect the following information from your ADSL service provider.

Item	Description	Enter Information in This Column
VPI	Most users are not required to change this setting. The virtual path identifier (VPI) is used in conjunction with the virtual channel identifier (VCI) to identify the data path between the network of your ADSL service provider and your computer. If you set up the Router for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional connections. You can change this setting by accessing the WAN menu of the web management interface.	
VCI	Most users are not required to change this setting. The VCI used in conjunction with the VPI to identify the data path between the network of your ADSL service provider and your computer. If you set up the Router for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional	

Item	Description	Enter Information in This Column
	connections. You can change this setting by accessing the WAN menu of the web management interface.	
Connection and Encapsulation Type	This is the method your ADSL service provider uses to transmit data between the Internet and your computer. Most users use the default PPPoE/PPPoA connection type. The Setup Wizard can be used to configure a PPPoE/PPPoA connection type. You may need to specify one of the following connection types: PPPoE LLC, PPPoA LLC and PPPoA VC-MUX. Other available connections and encapsulation combinations must be configured by using the Web manager. These include the Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-MUX), Static IP (Bridged IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP LLC, 1483 Routed IP VC-MUX or IPoA), etc.	
Username	This is the user name used to log in to the network of your ADSL service provider. It is usually in the form of user@isp.com. Your ADSL service provider uses this to identify your account.	
Password	This is the password used, in conjunction with the user name previously mentioned, to log in to the network of your ADSL service provider. It is used to verify the identity of your account.	

Necessary information about your DSL Router Residential Gateway is as follows.

Item	**Description**	**Enter Information in This Column**
LAN IP addresses for the DSL Router	This is the IP address you enter in the **Address** field in the Web browser to access the configuration graphical user interface (GUI) of the gateway. The default IP address is **192.168.1.1** and it is referred to as the "Management IP" address in this User Manual. You can change this to suit any desired IP address scheme. This address is the basic IP address used for DHCP service on the LAN when DHCP is enabled.	
LAN Subnet Mask for the DSL Router	This is the subnet mask used by the DSL Router, and is used throughout your LAN. The default subnet mask is **255.255.255.0**. You can change it later.	
Username	This is the user name used to access the management interface of the gateway, when you attempt to connect to the device through a web browser. The default username of the Router is **admin**. It cannot be changed.	
Password	This is the password required when you access the management interface of the gateway. The default password is **admin**. It cannot be changed.	

Necessary information about your LAN or computer is as follows.

Item	**Description**	**Enter Information in This Column**
Ethernet NIC	If your computer has an Ethernet NIC, you can connect the DSL Router to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL Router to connect to other computer or Ethernet devices.	

Item	Description	Enter Information in This Column
DHCP Client status	By default, your DSL Router Residential Gateway is configured as a DHCP server. This means that it can assign an IP address, a subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses that the DSL Router assigns is from **192.168.1.2** to **192.168.1.254**. You need to set your computer (or computers) to **Obtain an IP address automatically** (that is, to set computers as DHCP clients.)	

1.9 Safety Cautions

Follow the announcements below to protect the device from risks and damage caused by fire and electric power.

= Use volume labels to mark the type of power.

= Use the power adapter that is packed within the device package.

= Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.

= Proper space left for heat radiation is necessary to avoid any damage caused by overheating to the device. The holes are designed for heat radiation to ensure that the device works normally. Do not cover these heat radiant holes.

= Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.

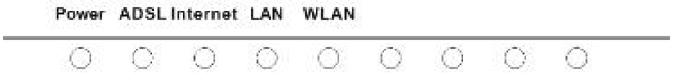
= Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.

= Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.

= Do not place this device on an unstable surface or support.

1.10 LED Status Description

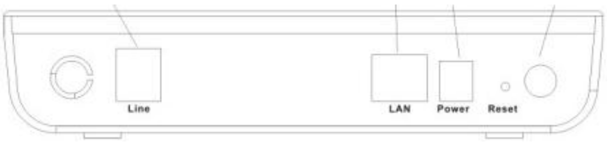
1.10.1 Front Panel



Indicator	Status	Description
Power	Off	The power is off.
	Green	The power is on and the device operates normally.
	Red	The power is self-testing.
		The device enters the console mode of the boot loader.
		The self-testing of the power fails if the LED is always red.
	Blink Red	Upgrading software.
ADSL	Off	No signal is detected.
	Slow Blink Green	The DSL line is transferring.
	Fast Blink Green	The DSL line is training.
	Green	The DSL line connection is established.
Internet	Off	No PPPoA or PPPoE connection
	Green	The PPPoA or PPPoE connection is established. The users can access the Internet.
	Red	Device attempts to become IP connected but fails (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Indicator	Status	Description
LAN	Off	No Ethernet signal is detected.
	Blink Green	The user data is passing through Ethernet port.
	Green	Ethernet interface is ready to work
WLAN	Off	No radio signal is detected.
	Blink Green	The user data is passing through WLAN port.
	Green	WLAN interface is ready to work.

1.10.2 Rear Panel



Interface	Description
ANT	Wireless antenna
LINE	RJ-11 port, using the telephone line to connect the modem with the ADSL cable or splitter.
Ethernet	RJ-45 port, connect the modem to a PC or other network device.
PWR	Power supplied port, plug in for power adapter that the power input is 12V DC, 800m A.
Reset	To restore the factory default, keep the device powered on and push a needle into the hole. Press down the button about 3 seconds and then release.
⏻	Power switch

2 Hardware Installation

The DSL Router has three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL (WAN) interfaces. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it is exposed to moisture or excessive heat. Ensure that cables and the power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting.

2.1 Choosing the Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the DSL Router. If this is the first time that you set up a wireless network device, read the following information.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business. For optimum range and signal strength, use these basic guidelines.

= Keep the numbers of walls and ceilings to the minimum:

  The signal emitted from wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of wireless LAN devices from 1 ~ 30 miters. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.

= Consider the direct line between access points and workstations:

  A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it appears over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.

= Building materials make difference:

  Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signals can pass through drywall or open doorways. Avoid positioning them in the way that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.

= Position the antenna for best reception:
Play around with the antenna position to see if signal strength improves. Some adapters or access points allow you to judge the strength of the signal.

= Keep your product away (at least 1~2 meters) from electrical devices:

= Keep wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

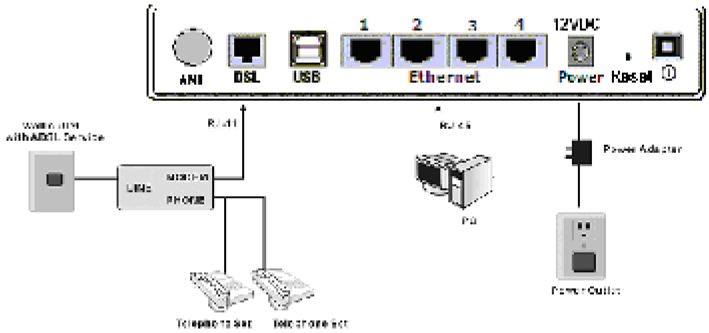
2.2 Connecting the ADSL Router

= See the following figure. Connect the DSL port of the DSL Router with a telephone cable.

= Connect the LAN port of the DSL Router to the network card of the PC via an Ethernet cable.

= Plug one end of the power adapter to the wall outlet and connect the other end to the PWR port of the DSL Router.

The following figure displays the connection of the DSL Router, PC, and telephones.


1
2
3
4
12VDC
ANT
DSL
USB
Ethernet
Power
Reset
Wall Jack
with ADSL Service
RJ-11
RJ-45
LINE
MODEM
PHONE
Power Adapter
PC
Power Outlet
Telephone Set
Telephone Set

2.3 Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this wipes out any settings stored in the flash memory, including user account information and LAN IP settings. The device settings are restored to the following factory defaults: the IP address is *192.168.1.1*, subnet mask is *255.255.255.0*, user name for management is **admin**, and password is **admin**.

3 Introduction to Web Configuration

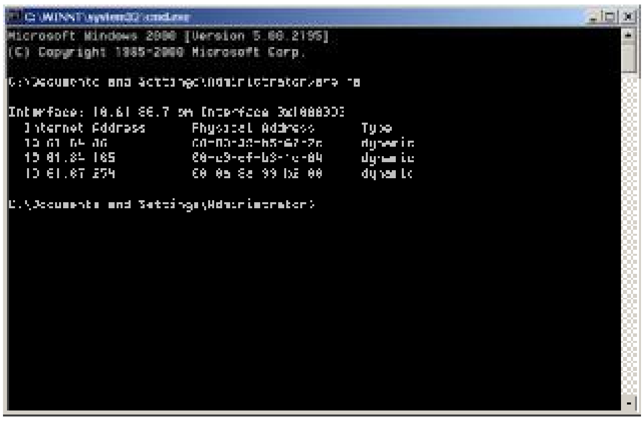
The first time you setup the Router. It is recommended that you configure the WAN connection using a single computer, to ensure that both the computer and the Router are not connected to the LAN. Once the WAN connection operates properly, you may continue to make changes to Router configuration, including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router, including how to change IP settings and DHCP server setup.

3.1 Preparation Before Login

Before accessing the Modem, ensure the communication between PC and Modem is normal. Check the communication as follows.

= Configure the IP address of the PC as 192.168.1.X (2~254), net mask as 255. 255.255.0, gateway address as 192. 168.1.1 (for customized version, configure them according to the actual version).

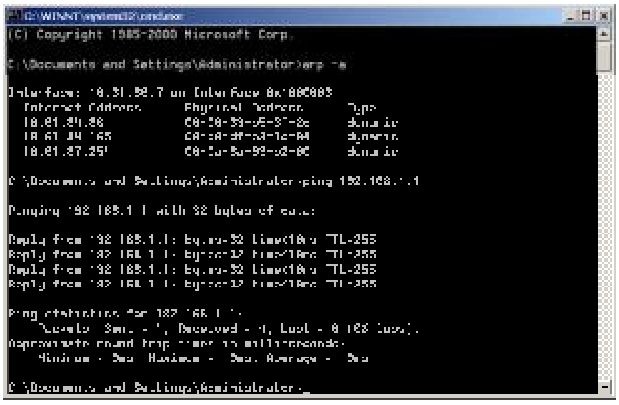
= Enter **arp -a** in the DOS window to check whether the PC can read the MAC address of the Modem.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a

Interface: 10.61.86.7 on Interface [illegible]
  Internet Address      Physical Address      Type
  [illegible]           [illegible]           dynamic
  [illegible]           [illegible]           dynamic
  [illegible]           [illegible]           dynamic

C:\Documents and Settings\Administrator>
```

= Ping the management IP address (192.168.1.1 by default) of the Modem.

If the PC can read the MAC address of the Modem and can ping through the management IP address of the Modem, that means the communication of the PC and the Modem is normal.



```
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a
```

Note: When you manage the Modem through Web, you must keep the Modem power on. Otherwise, the Modem may be damaged.

3.2 Logging In to the Modem

The following description is a detail "How-To" user guide and is prepared for first time users.

3.2.1 First-Time Login

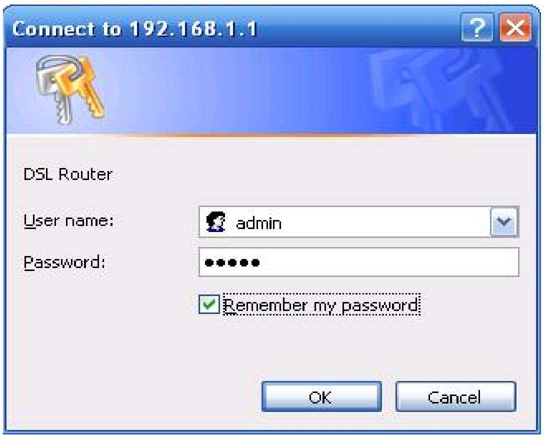
When you log in to the DSL Router for the first time, the login wizard appears.

Step 1 Open a Web browser on your computer.

Step 2 Enter **http://192.168.1.1** (DSL router default IP address) in the address bar. The login page appears.

Step 3 Enter a user name and the password. The default username and password of the super user are **admin** and **admin**. The username and password of the common user are **user** and **user**. You need not enter the username and password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 4 Click OK to log in or click Cancel to exit the login page.



Connect to 192.168.1.1

DSL Router

User name: admin

Password: •••••

☑ Remember my password

After logging in to the DSL router as a super user, you can query, configure, and modify all configurations, and diagnose the system.

You need to reboot the DSL router to enable your modification or configuration effective in some cases, for example, after you modify the PVC configuration. Some modification, such as adding a static route, takes effect at once, and does not require modem reboot.

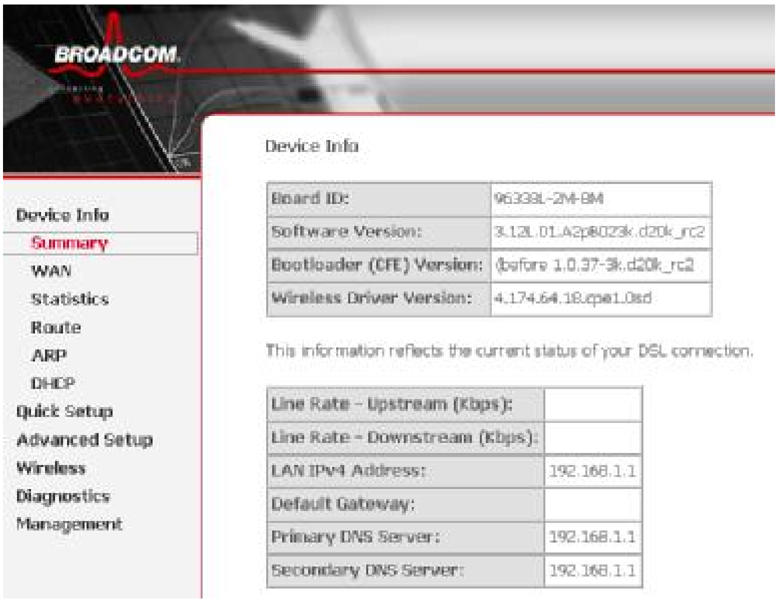
3.3 DSL Router Device Information

Click **Device Info** and you can view the following information.

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP

3.3.1 Summary of Device Information

Click **Summary** and the following interface appears.


BROADCOM
Device Info
Summary
WAN
Statistics
Route
ARP
DHCP
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Device Info

Board ID:	96338L-2M-8M
Software Version:	3.12L.01.A2pB023k.d20k_rc2
Bootloader (CFE) Version:	(before 1.0.37-3k.d20k_rc2
Wireless Driver Version:	4.174.64.18.cpe1.0sd

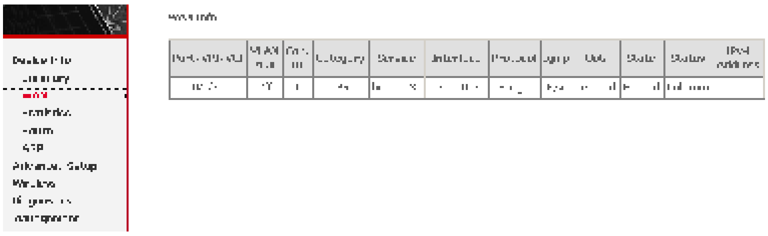
This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

- **LAN IPv4 Address**: the management IP address.
- **Default Gateway**: In the bridging mode there is no gateway. In other modes, it is the address of the uplink equipment, for example, PPPOE/PPPOA.
- **DNS Server**: In the PPPoE / PPPoA mode, it is obtained from the uplink equipment. In the bridging mode, there is no DNS Server address and you can manually enter the information.

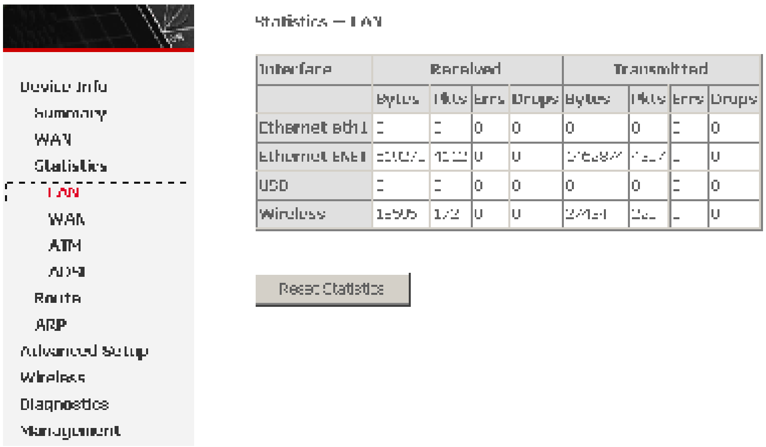
3.3.2 WAN Interface Information

Click **WAN** and the following page appears. The **WAN Info** page displays the status and the connect or disconnect button, depending on the selected connection mode.



3.3.3 Statistics of LAN

Choose **Statistics** > **LAN** and the following page appears. You can query information of packets recevied at the Ethernet and wireless interfaces. Click **Reset Statistics** to restore the values to zero and recount them.

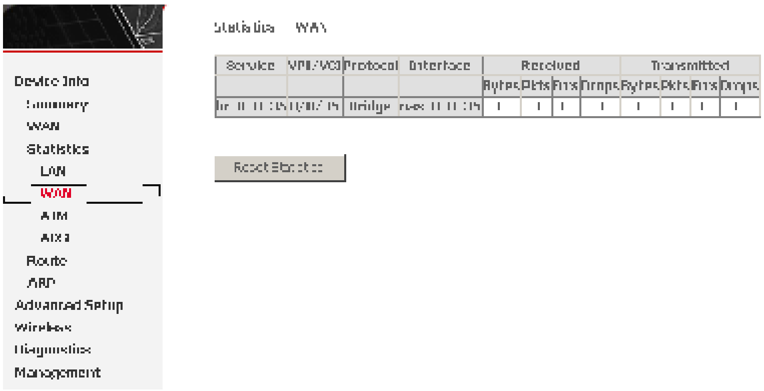

Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management
Reset Statistics

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth1	0	0	0	0	0	0	0	0
Ethernet ENET	[illegible]	[illegible]	0	0	[illegible]	[illegible]	0	0
USB	0	0	0	0	0	0	0	0
Wireless	[illegible]	172	0	0	[illegible]	[illegible]	0	0

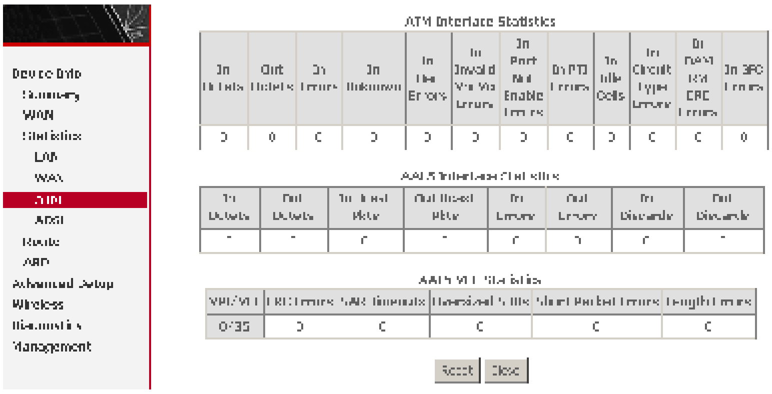
3.3.4 Statistics of WAN

Click **Statistics** > **WAN** and the following page appears. You can query information of packets recevied at the WAN interfaces. Click **Reset Statistics** to restore the values to zero and recount them.


Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management
Statistics -- WAN
Service
VPI/VCI
Protocol
Interface
Received
Transmitted
Bytes
Pkts
Errs
Drops
Bridge
Reset Statistics

3.3.5 Statistics of ATM

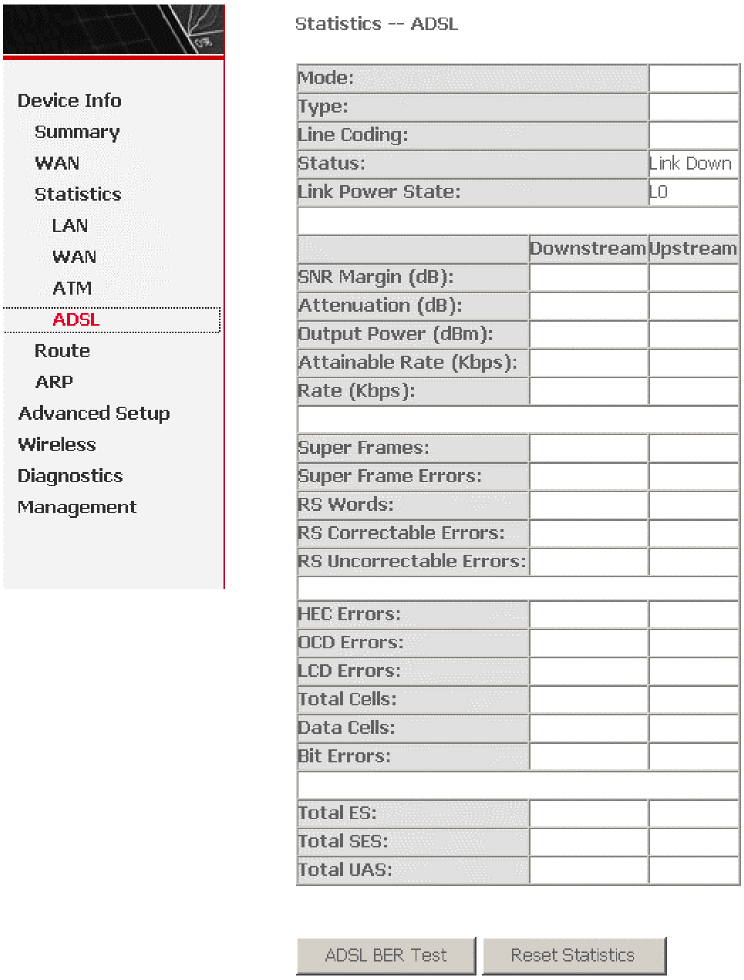
Click **Statistics** > **ATM** and the following page appears. You can query information of packets recevied at the ATM interfaces. Click **Reset** to restore the values to zero and recount them.


Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management
ATM Interface Statistics
In Octets
Out Octets
In Errors
In Unknown
In Hec Errors
In Invalid Vpi Vci Errors
In Port Not Enable Errors
In PTI Errors
In Idle Cells
In Circuit Type Errors
In OAM RM CRC Errors
In GFC Errors
AAL5 Interface Statistics
In Octets
Out Octets
In Ucast Pkts
Out Ucast Pkts
In Errors
Out Errors
In Discards
Out Discards
AAL5 VCC Statistics
VPI/VCI
CRC Errors
SAR Timeouts
Oversized SDUs
Short Packet Errors
Length Errors
0/35
Reset
Close

3.3.6 Statistics of ADSL

Click **Statistics** > **ADSL** and the following page appears.

If the DSL line is activated, the window shows as follows.


Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management
ADSL BER Test
Reset Statistics

Statistics -- ADSL

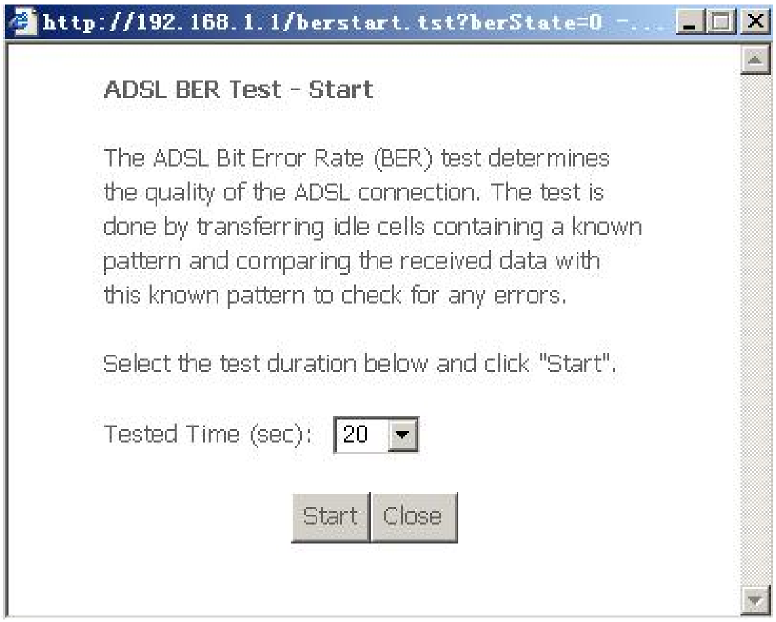
Mode:	
Type:	
Line Coding:	
Status:	Link Down
Link Power State:	L0

	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (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:		

Click **Reset Statistics** at the bottom to restore the values to zero and recount them.

3.3.6.1 ADSL BER Test

Click **ADSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows.



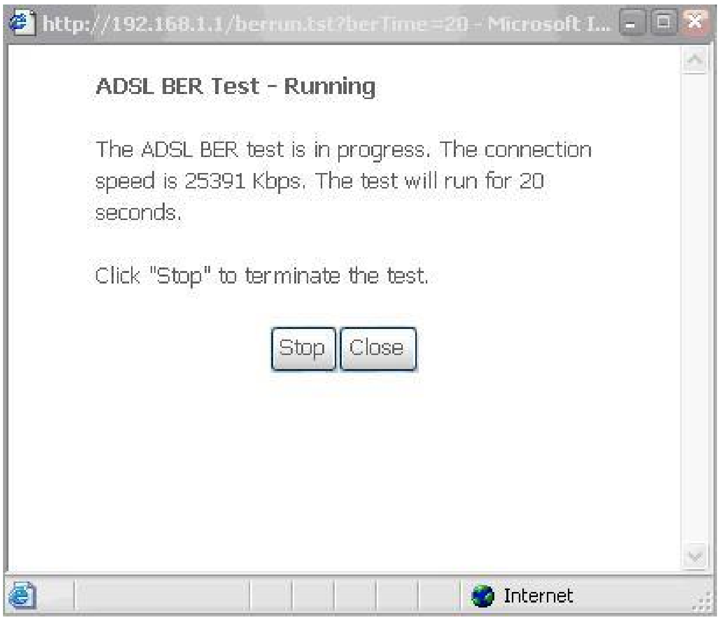
ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time and click **Start**. The following pages appear.

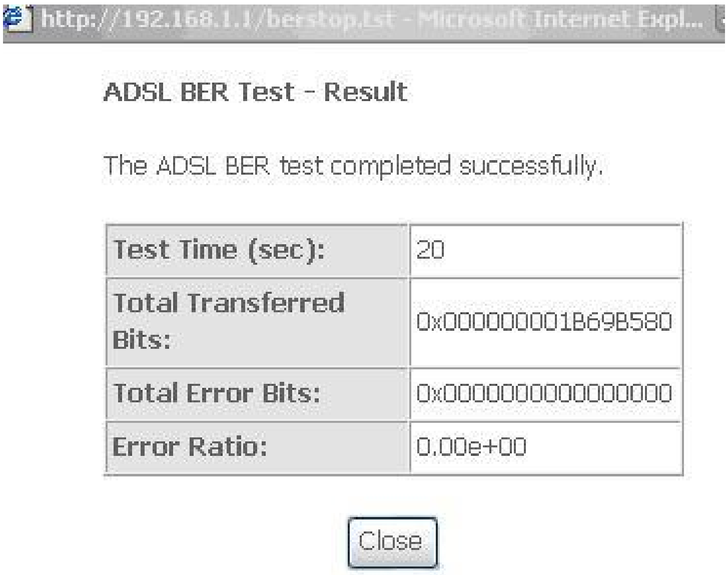

http://192.168.1.1/berrun.tst?berTime=20 - Microsoft I...
Internet

ADSL BER Test - Running

The ADSL BER test is in progress. The connection speed is 25391 Kbps. The test will run for 20 seconds.

Click "Stop" to terminate the test.

Stop
Close


http://192.168.1.1/berstop.tst - Microsoft Internet Expl...
Close

ADSL BER Test - Result

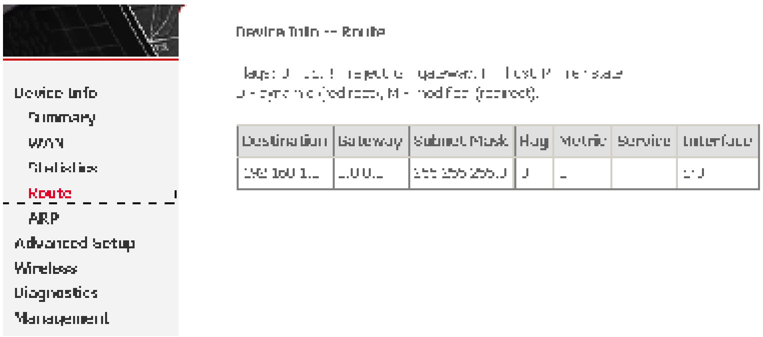
The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x000000001B69B580
Total Error Bits:	0x0000000000000000
Error Ratio:	0.00e+00

***Note**: If the BER reaches e-5, you cannot access the Internet.*

3.3.7 Route Table Information

Click **Route**, and if the system is in the default configuration, the following page appears.


Device Info
Summary
WAN
Statistics
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management

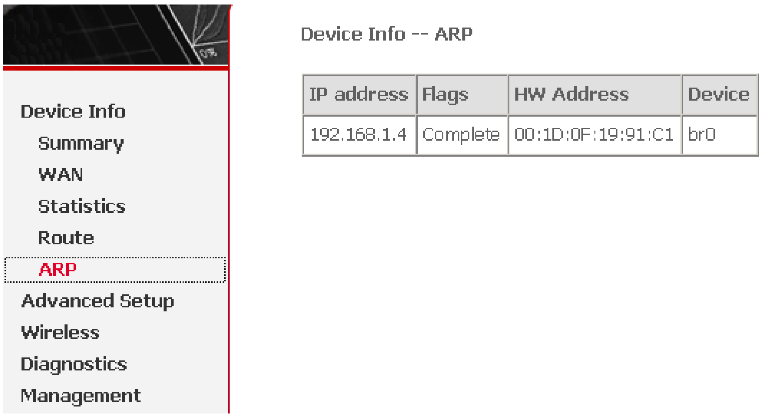
Device Info -- Route

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]

If the configuration of modem is as PPPoE/PPPoA dial-up, the page shows different.

3.3.8 ARP Table Information

Click **ARP** and the following page appears. You can query the MAC and IP address information of the equipment attached to the modem.


Device Info
Summary
WAN
Statistics
Route
ARP
Advanced Setup
Wireless
Diagnostics
Management

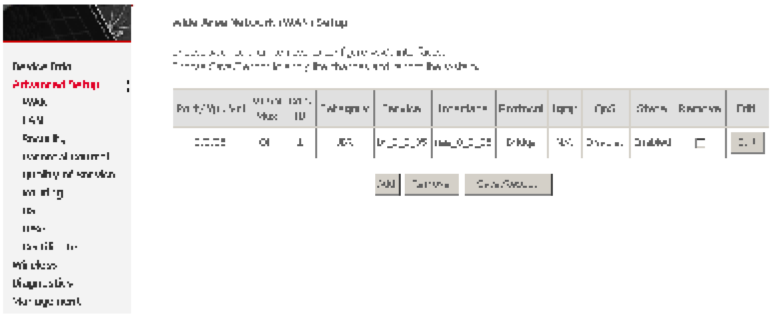
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.4	Complete	00:1D:0F:19:91:C1	br0

3.4 Advanced Setup

3.4.1 WAN Configuration

Click **Advanced Setup > WAN**, and the following page appears, so you can modify and configure the WAN interface.



***Note:** After a PVC is deleted or modified, the system must be rebooted. Otherwise, the modification does not take effect.*

Click **Add**, **Edit**, or **Remove** to configure WAN interface.

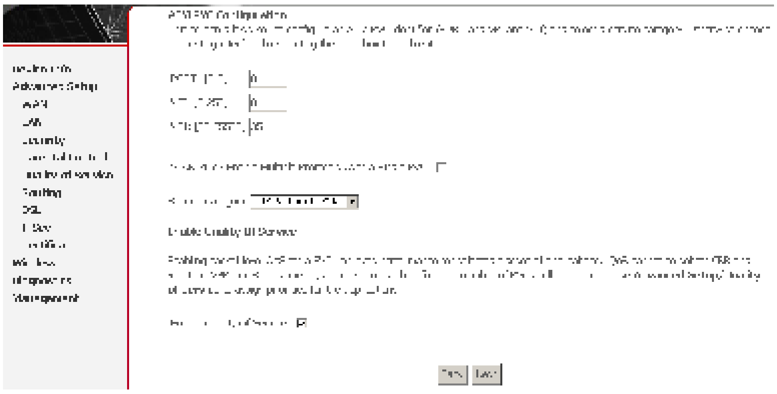
Click **Save/Reboot** to save the modification, and reboot the modem to make the modification effective.

The section shows you how to add PVC.

3.4.1.1 PPPoE Configuration

This section describes the procedure for adding PVC 8/35 (PPPoE mode).

Step 1 Click **Add** and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.



= **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.

= **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

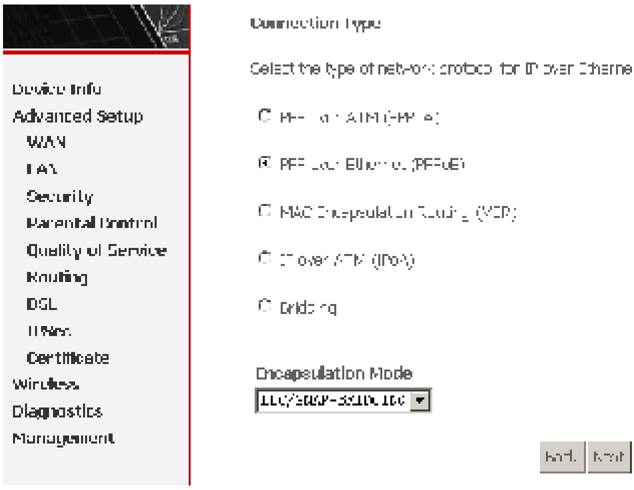
= **Service Category**: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

= **Enable Quality Of Service**: Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

Step 2 In this page, you can modify the Internet connection type and encapsulation type.


Device Info
Advanced Setup
WAN
LAN
Security
Parental Control
Quality of Service
Routing
DSL
IPSec
Certificate
Wireless
Diagnostics
Management
Back
Next

Connection Type

Select the type of network protocol for IP over Ethernet as WAN Interface

○ PPP over ATM (PPPoA)

● PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

○ Bridging

Encapsulation Mode: LLC/SNAP-BRIDGING

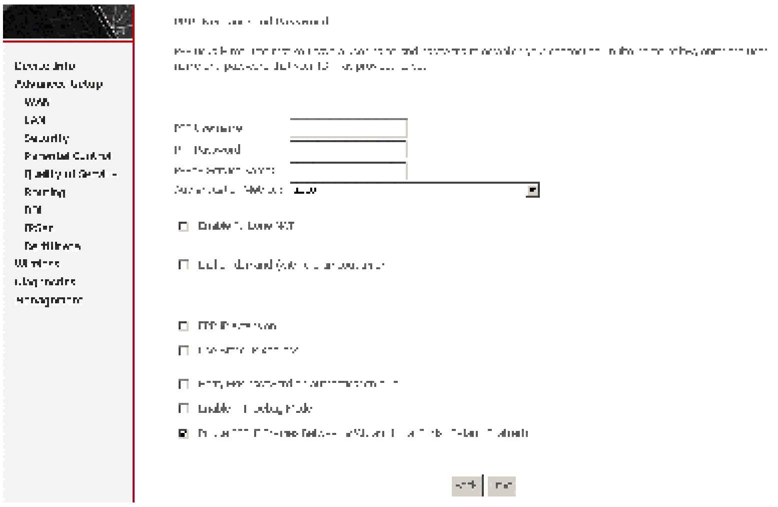
Change the connection type of PVC 8/35 to PPP over Ethernet (PPPoE) and set the Encapsulation Mode to LLC/SNAP-BRIDGING (according to the uplink equipment).

Enable the 802.1q VLAN tag value.

***Note**: that 802.1q VLAN tagging is only available for PPPoE, MER, and Bridge.*

Click **Next** and the following page appears.

Step 3 In this page, you can modify the PPP user name, PPP password, authentication method, and so on.



PPP Username: The correct user name that your ISP provides to you.

PPP Password: The correct password that your ISP provides to you.

PPPoE Service Name: If your ISP provides it to you, please enter it. If not, do not enter any information.

Authentication Method: The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.

Dial on demand (with idle timeout timer): If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPOE dialup.

If this function is disabled, the modem performs PPPOE dial-up all the time. The PPPOE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.

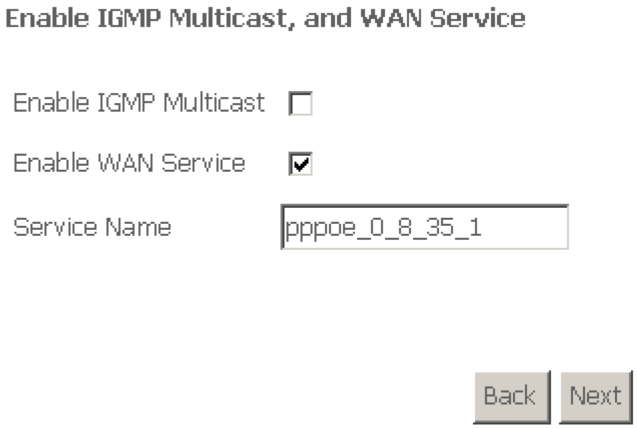
PPP IP extension: If this function is enabled, the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached to the modem (at this time, the modem connects to only one PC). From the aspect of the PC user, the PC dials up to obtain an IP addres. But actually, the dial-up is done by the modem.

If this function is disabled, the modem itself obtains the WAN IP address.

Use Static IP Address: If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up.If this function is enabled, the modem uses this IP address as the WAN IP address.

After entering the PPP user name and password, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.



Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☑

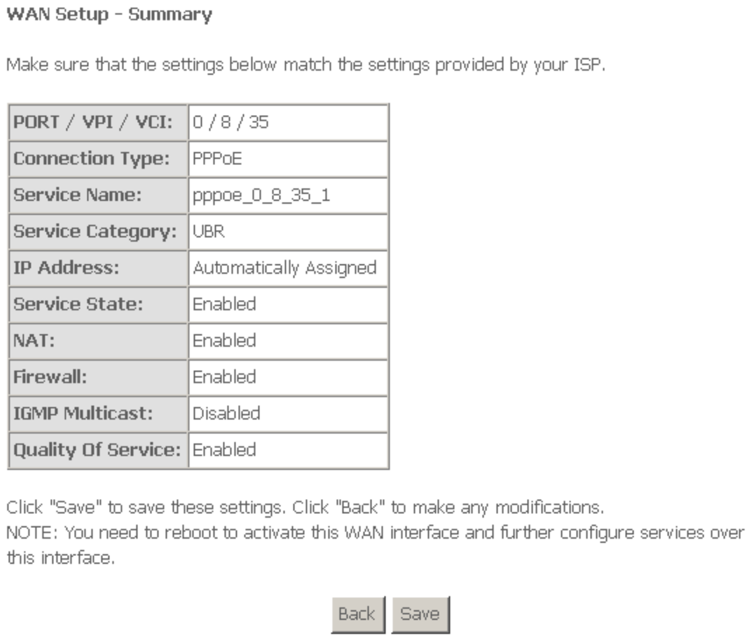
Service Name pppoe_0_8_35_1

Enable IGMP Multicast: IGMP proxy. For example, if you wish that the PPPoE mode supports IPTV, enable this function.

Enable WAN Service: Enable it, unless you do not want to active the PVC.

Click **Nex**t and the following page appears.

This page shows all the configuration. You can view the default values of NAT enable and Firewall enable.



WAN Setup - Summary

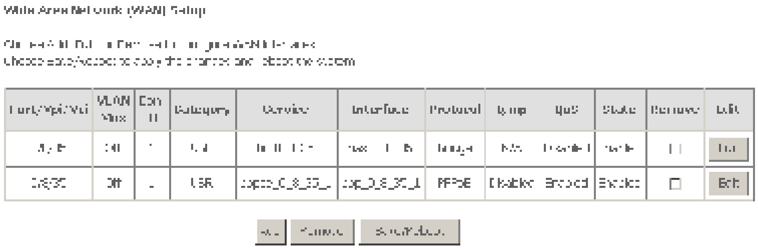
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_8_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

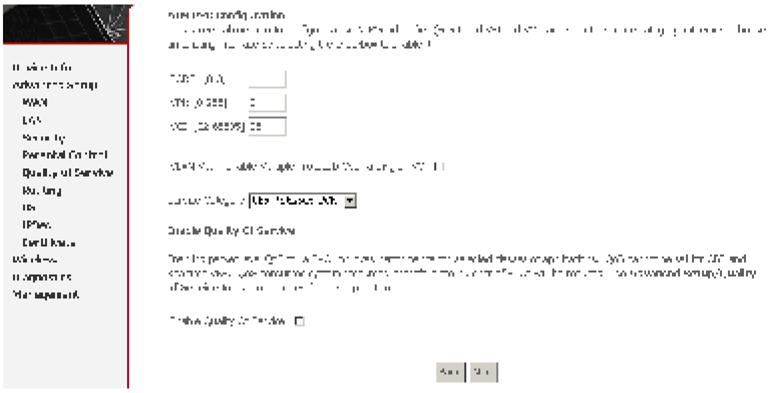
To save the settings, click **Save**. To make any modifications, click **Back**. After you click **Save**, the following page appears.

Note: *You need to reboot the modem to activate this WAN interface and further configure services in this interface.*



3.4.1.2 PPPoA Configuration

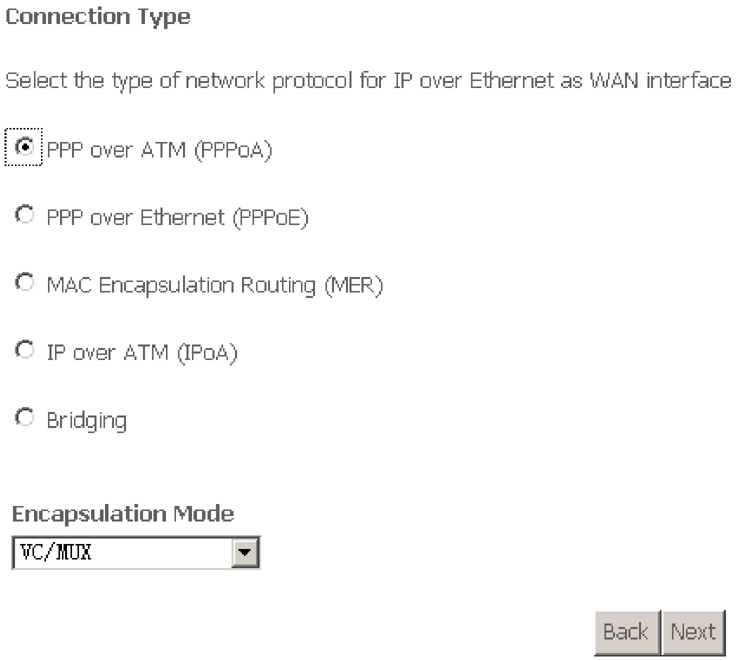
This section describes the procedure for adding PVC 8/35 (PPPOA mode). Click **Add** and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.



In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet Connection Type and Encapsulation Type.



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

● PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

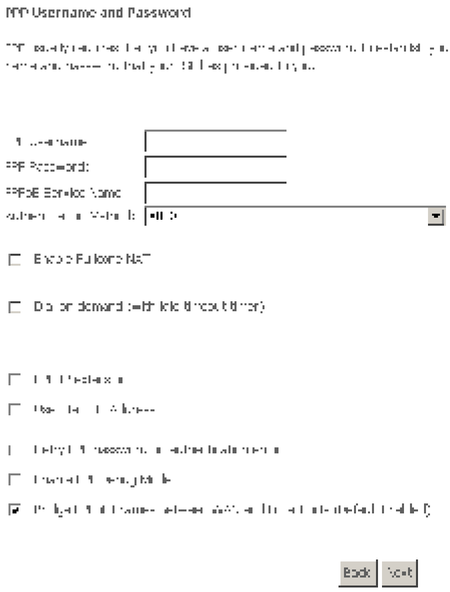
○ Bridging

Encapsulation Mode

VC/MUX

Change the connection type of PVC 8/35 to PPP over ATM (PPPoA) and set the Encapsulation Mode to VC/MUX (according to the uplink equipment). Click **Next** and the following page appears.

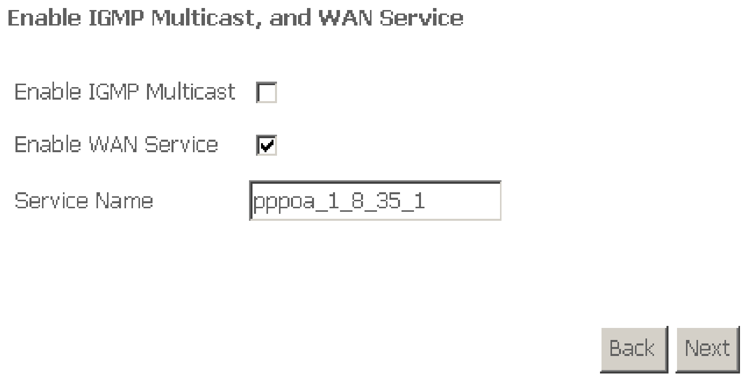
In this page, you can modify the PPP Username, PPP Password, Authentication Method, and so on.



PPP Username and Password

After entering the PPP user name and password, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.



Enable IGMP Multicast, and WAN Service

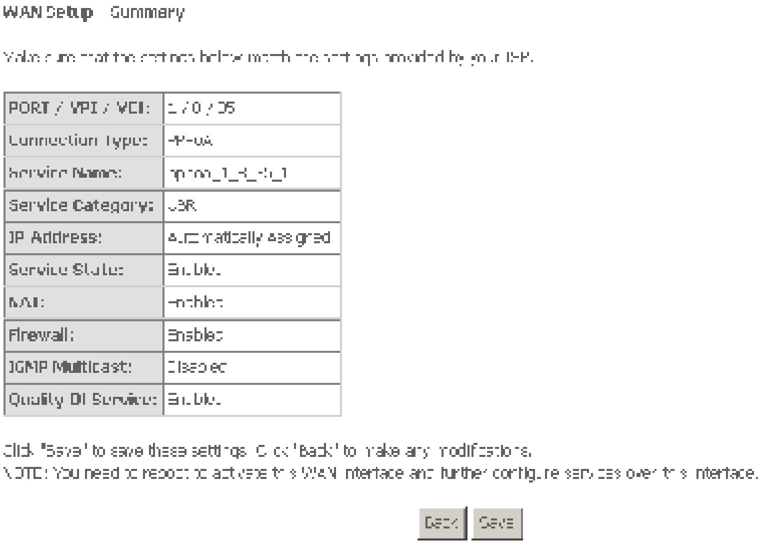
Enable IGMP Multicast ☐

Enable WAN Service ☑

Service Name pppoa_1_8_35_1

Click **Next** and the following page appears.

This page shows all the configuration. You can view the default values of NAT enable and Firewall enable.



WAN Setup - Summary

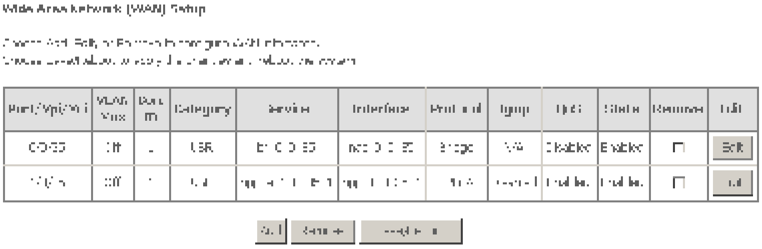
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	1 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_1_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**. After you click **Save**, the following page appears.

***Note**: You need to reboot the modem to activate this WAN interface and further configure services in this interface.*



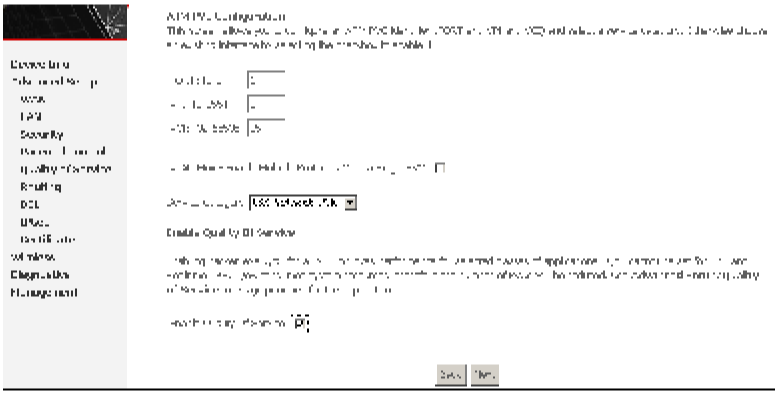
Wide Area Network (WAN) Setup

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Disabled	Enabled	☐	Edit
[illegible]	Off	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	☐	Edit

3.4.1.3 MER Configuration

This section describes the procedure for adding PVC 8/35 (MER mode).

Click **Add** and the following page appears. In this page, you can modify VPI/VCIs, service categories and QoS.

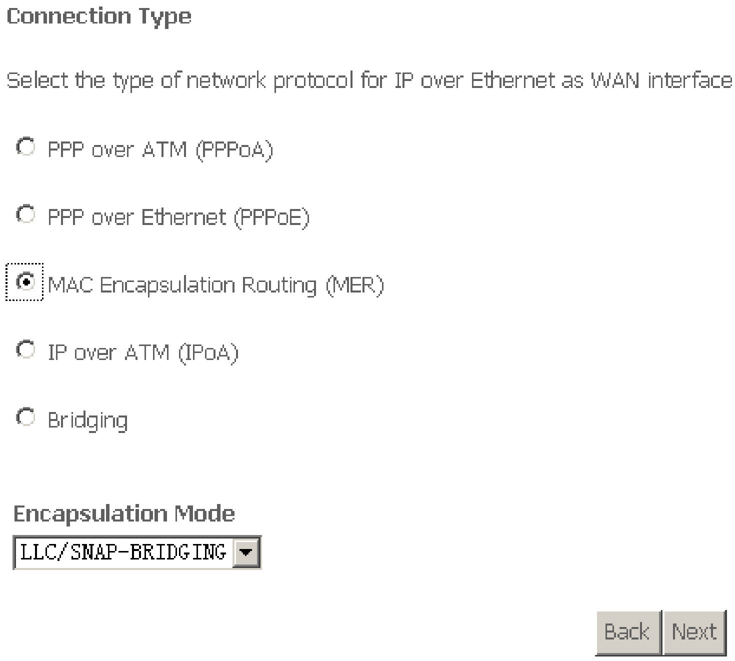


In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet connection type and encapsulation type.

Change the connection type of PVC 8/35 to **MAC Encapsulation Routing (MER)** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (according to the uplink equipment).



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

● MAC Encapsulation Routing (MER)

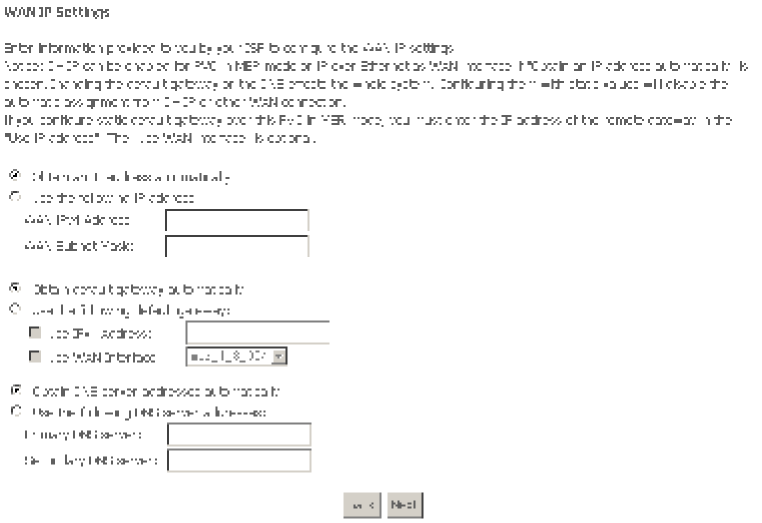
○ IP over ATM (IPoA)

○ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Click **Next** and the following page appears.
In this page, you can modify the WAN IP address, default gateway, and DNS server settings.



Obtain an IP address automatically: The modem obtains a (WAN) IP address automatically and at this time it enables DHCP client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP server functions.

Use the following IP address: If you want to manually enter the WAN IP address, select this check box and enter the information in the field.

WAN IPv4 Address: Enter the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Obtain default gateway automatically: Obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.

Use the following default gateway: If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.

Use IPv4 Address: Enter the gateway of the WAN interface provided by your ISP.

Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.

Obtain DNS server address automatically: To obtain the IP address of the DNS server assigned by the uplink equipment such as BAS.

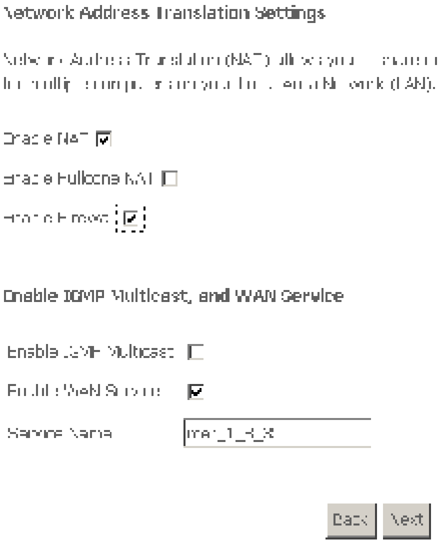
Use the following DNS server addresses: If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

Primary DNS server: Enter the IP address of the primary DNS server.

Secondary DNS server: Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT ☑

Enable Fullcone NAT ☐

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☑

Service Name mer_1_4_32

Enable NAT: Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. It is normal to enable NAT.

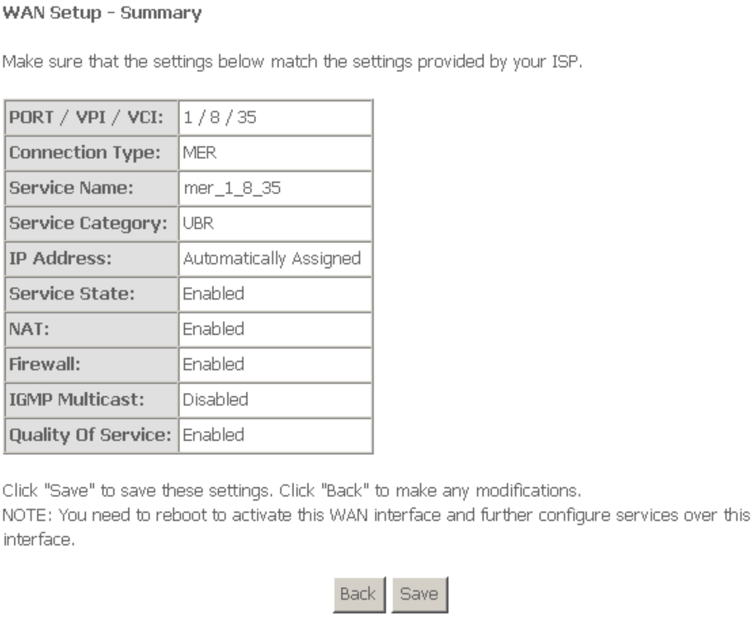
Enable Firewall: Enable or disable IP filtering.

Enable IGMP Multicast: IGMP proxy. For example, if you wish that the MER mode supports IPTV, enable this function.

Enable WAN Service: Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.

This page shows all the configuration.



WAN Setup - Summary

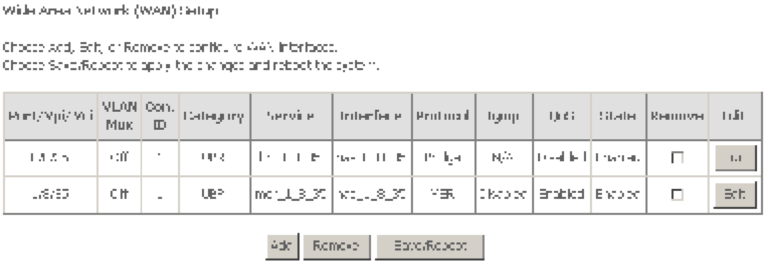
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	1 / 8 / 35
Connection Type:	MER
Service Name:	mer_1_8_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**. After you click **Save**, the following page appears.

Note: You need to reboot the modem to activate this WAN interface and further configure services in this interface.



Wide Area Network (WAN) Setup

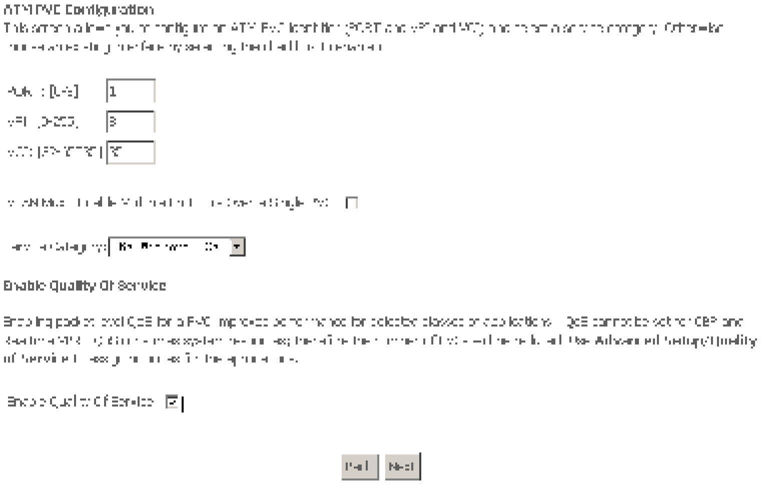
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
[illegible]	Off	[illegible]	[illegible]	[illegible]	[illegible]	Bridge	N/A	Disabled	Enabled	☐	Edit
1/8/35	Off	1	UBR	mer_1_8_35	nas_1_8_35	MER	Disabled	Enabled	Enabled	☐	Edit

3.4.1.4 IPoA Configuration

This section describes the procedure for adding PVC 8/35 (IPoA mode).

Click **Add** and the following page appears. In this page, you can modify VPI/VCIs, service categories, and QoS.



ATM PVC Configuration

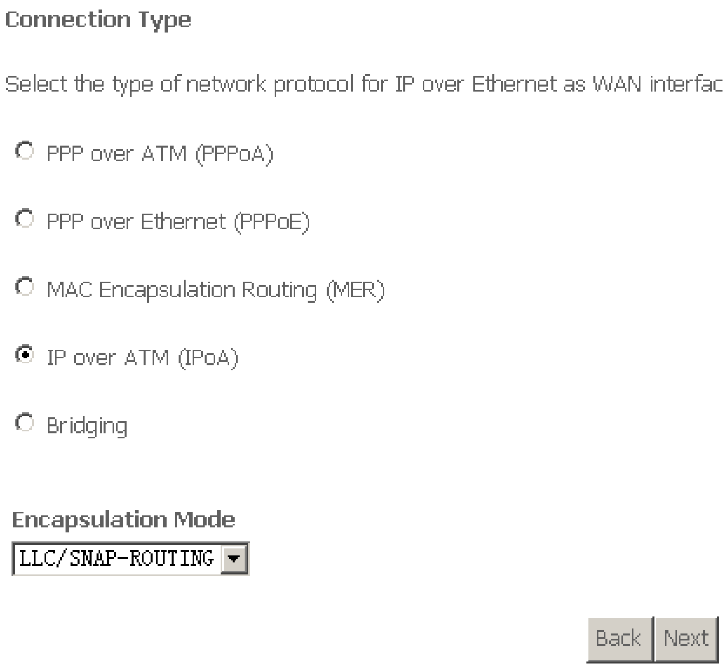
Enable Quality Of Service

In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet connection type and encapsulation type.

Change the connection type of PVC 8/35 to **IP over ATM (IPoA)** and set the **Encapsulation Mode** to **LLC/SNAP-ROUTING** (according to the uplink equipment).



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

● IP over ATM (IPoA)

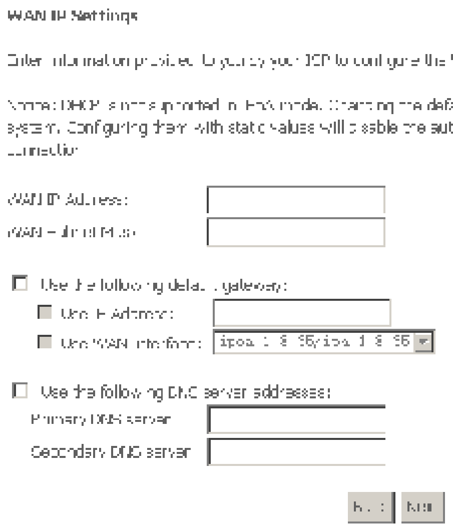
○ Bridging

Encapsulation Mode

LLC/SNAP-ROUTING

Click **Next** and the following page appears.

In this page, you can modify the WAN IP, default gateway, and DNS server settings.



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

☐ Use the following default gateway:

☐ Use IP Address:

☐ Use WAN Interface: ipoa 1 8 35/ipa 1 8 35

☐ Use the following DNS server addresses:

Primary DNS server

Secondary DNS server

WAN IP Address: Enter the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Use the following default gateway: If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.

Use IP Address: Enter the gateway of the WAN interface provided by your ISP.

Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.

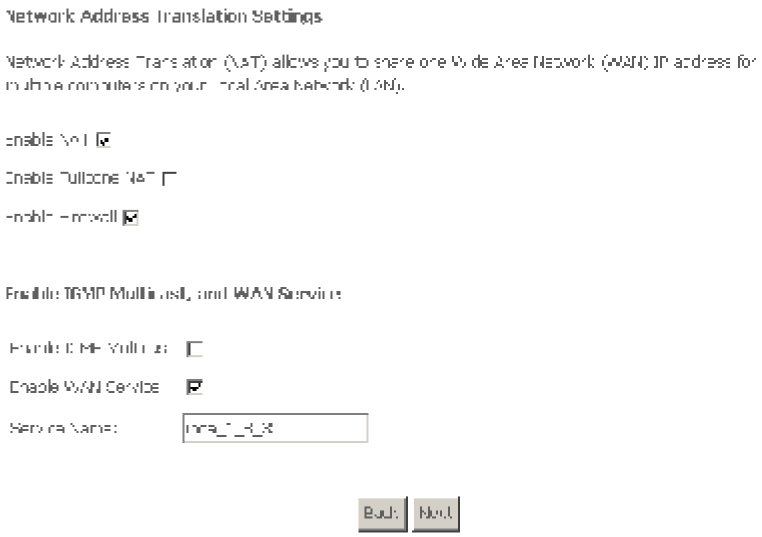
Use the following DNS server addesses: If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

Primary DNS server: Enter the IP address of the primary DNS server.

Secondary DNS server: Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT ☑

Enable Fullcone NAT ☐

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☑

Service Name: [illegible]

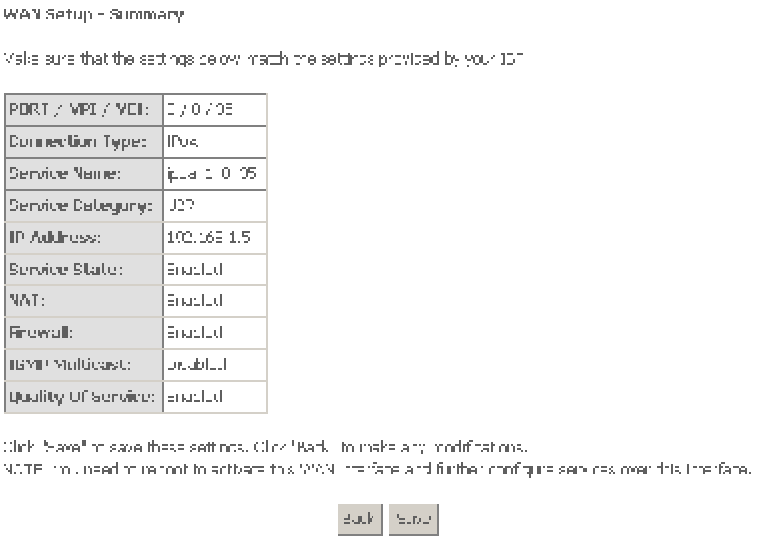
Enable NAT: Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.

Enable Firewall: Enable or disable IP filtering.

Enable IGMP Multicast: IGMP proxy. For example, if you wish that the IPoA mode supports IPTV, enable this function.

Enable WAN Service: Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.This page shows all the configuration.



WAN Setup - Summary

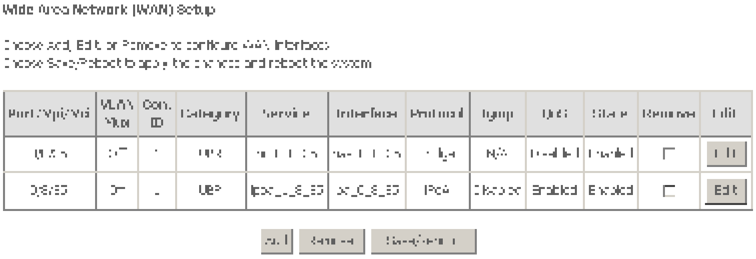
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	192.168.1.5
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**. After you click **Save**, the following page appears.

***Note**: You need to reboot to the modem to activate this WAN interface and further configure services in this interface.*



Wide Area Network (WAN) Setup

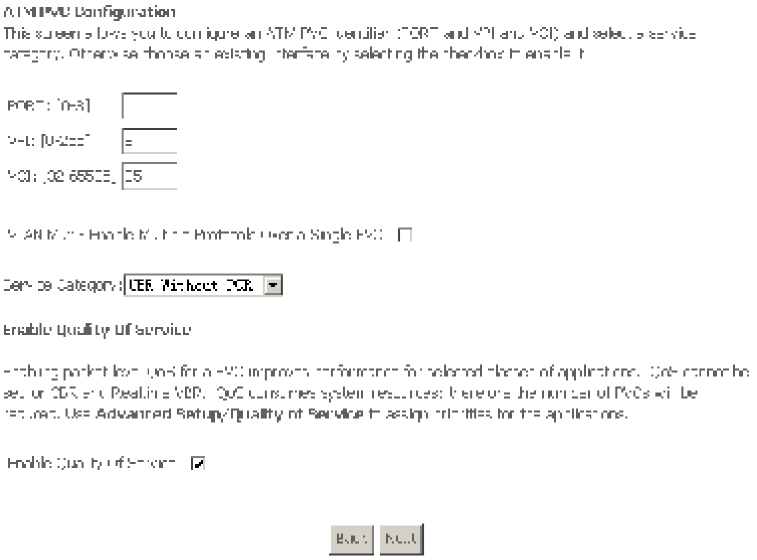
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	N/A	[illegible]	[illegible]	☐	Edit
0/8/35	Off	1	UBR	ipoa_0_8_35	ipa_0_8_35	IPoA	Disabled	Enabled	Enabled	☐	Edit

3.4.1.5 Bridge Configuration

This section describes the procedure for adding PVC 8/35 (IPoA mode).

Click **Add,** and the following page appears. In this page, you can modify VPI/VCIs, service categories, and QoS.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

PORT: [0-3]

VPI: [0-255] 8

VCI: [32-65535] 35

VLAN Mux - Enable Multiple Protocols Over a Single PVC ☐

Service Category: UBR Without PCR

Enable Quality Of Service

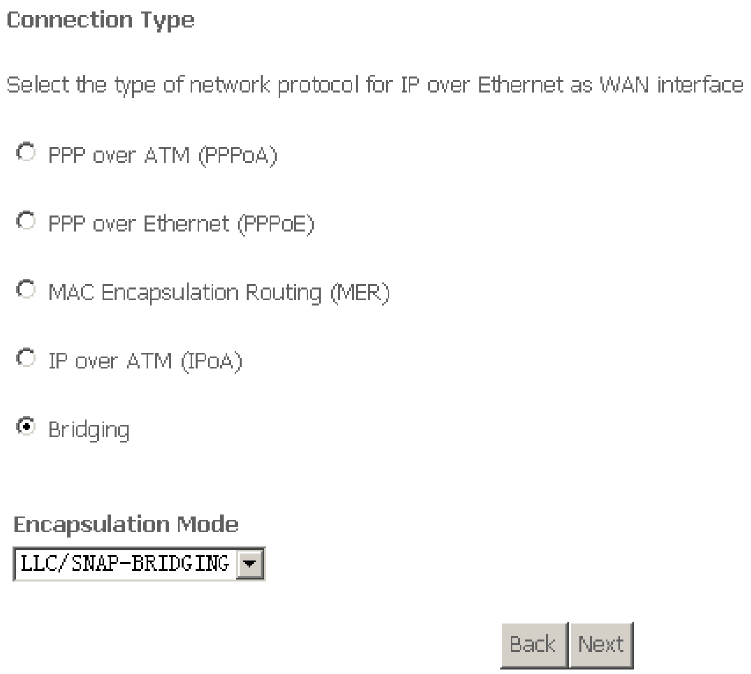
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.

Enable Quality Of Service ☑

In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet connection type and encapsulation type.



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

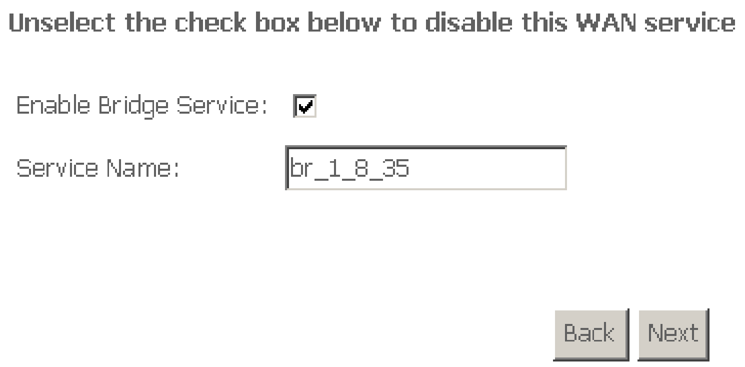
● Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Click **Next** and the following page appears.

In this page, you can modify the service name.



Unselect the check box below to disable this WAN service

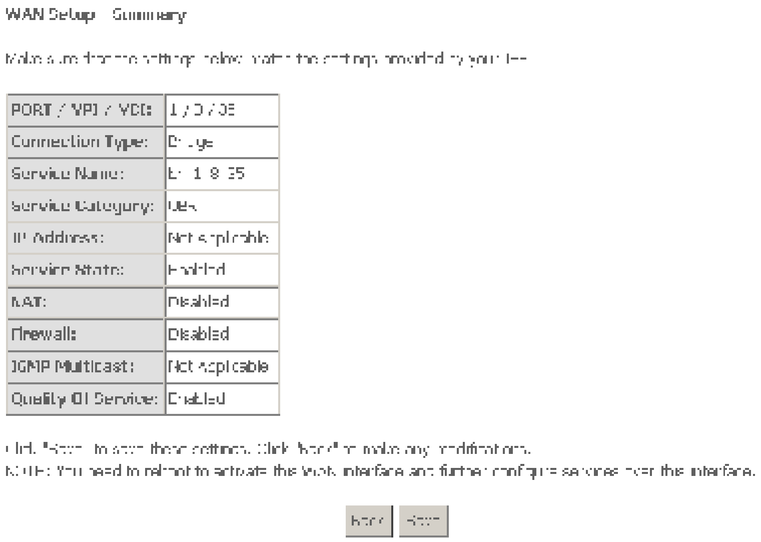
Enable Bridge Service: ☑

Service Name: br_1_8_35

Enable Bridge Service: Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.

This page shows all the configuration.



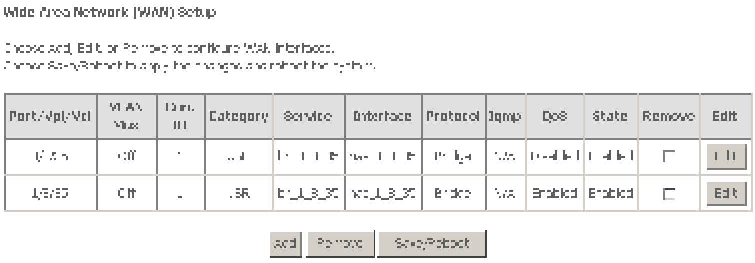
WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	1 / 8 / 35
Connection Type:	Bridge
Service Name:	br_1_8_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**. After you click **Save**, the following page appears.



Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

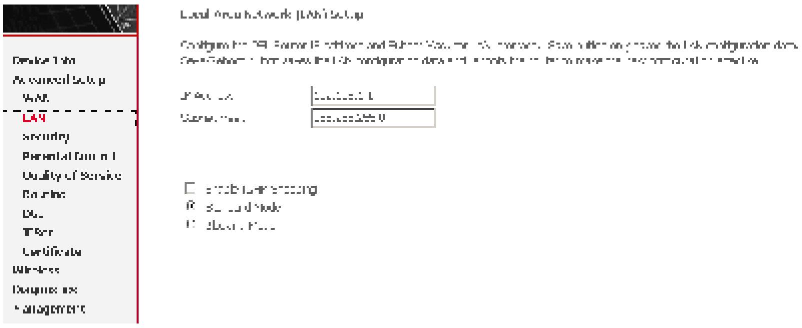
Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
[illegible]	Off	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	N/A	[illegible]	[illegible]	☐	Edit
1/8/35	Off	1	UBR	br_1_8_35	nas_1_8_35	Bridge	N/A	Enabled	Enabled	☐	Edit

***Note**: You need to reboot the modem to activate this WAN interface and further configure services in this interface.*

3.4.2 LAN Configuration

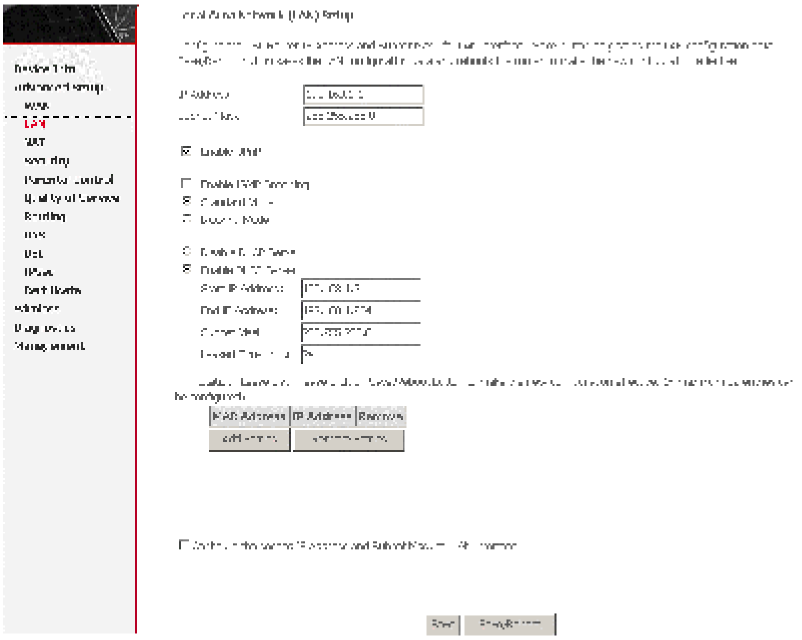
In this interface, you can modify and configure IP Address and DHCP Server.

If the mode is bridge, the interface shows as below.


Device Info
Advanced Setup
WAN
LAN
Security
Parental Control
Quality of Service
Routing
DSL
IPSec
Certificate
Wireless
Diagnostics
Management

Enable IGMP Snooping: It is used to Bridge mode.

If the mode is router, the interface shows as follows.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Wireless
Diagnostics
Management
MAC Address
IP Address
Remove

3.4.3 NAT

3.4.3.1 Overview

Setting up the NAT Function

= The DSL router is equipped with the network address translation (NAT) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the public IP address of the router by default.

= One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it is explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data to pass through. The router opens one specific port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

= If an external application tries to send a call to a PC in the local network, the router blocks it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links (that is. several ports), so that players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot run if NAT is activated.

= Using port forwarding (the forwarding of requests to particular ports), the router is forced to send requests from the Internet for a certain service, for example, a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service. Where configuration is concerned, you must define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses.

You then assign the public ports that are to be opened for the application to this trigger port. The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it opens the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it to pass through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

***Note**:*

= An application that is configured for port triggering can only be run by one user in the local network at a time.

= After public ports are opened, they can be used by unauthorized persons to gain access to a PC in the local network.

= When the DSL router is supplied, the NAT function is activated. For example, all IP addresses of PCs in the local network are converted to the public IP address of the router when accessing the Internet. You can use NAT settings to configure the DSL router to carry out the following tasks.

= For functions described as follows, IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the DSL router, you must disable DHCP server as the settings in the local network menu entry for the lease time or assign static IP addresses for the PCs.

You can enable or disenable the NAT function. By default, the NAT function is enabled.

3.4.3.2 NAT-Virtual Server Setup

By default, DSL router blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into the network and damage it.

However, you may want to expose your network to the Internet in limited and controlled ways in order to enable some applications to work from the LAN (for example, game, voice, and chat applications) and to enable Internet access to servers in the home network. The port forwarding feature supports both functionalities. This topic is also referred as Local Servers.

The port forwarding page is used to define applications that require special handling by DSL router. All you need to do is to select the application protocol and the local IP address of the computer that is using or providing the service. If required, you may add new protocols in addition to the most common ones provided by DSL router.

For example, if you wanted to use a file transfer protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at DSL router from the Internet henceforth is forwarded to the specific computer.

Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that provide it. This is useful, for example, if you want to host a Web server inside your home network.

When an Internet user points his/her browser to DSL router external IP address, the gateway forwards the incoming HTTP request to your Web server. With one external IP address (DSL router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer.

For example, you can define that FTP uses address X to reach computer A and Telnet also uses address X to reach computer A. But attempting to define FTP to use address X to reach both computer A and B fails. DSL router, therefore, provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the IP addresses pool. Then, you can define FTP to use address X to reach computer A and address Y to reach computer B.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. For example, if you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses DSL router via HTTP.

To accomplish this, do as follows:

Step 1 Define a port forwarding rule for the HTTP service, with the PC IP or host name.

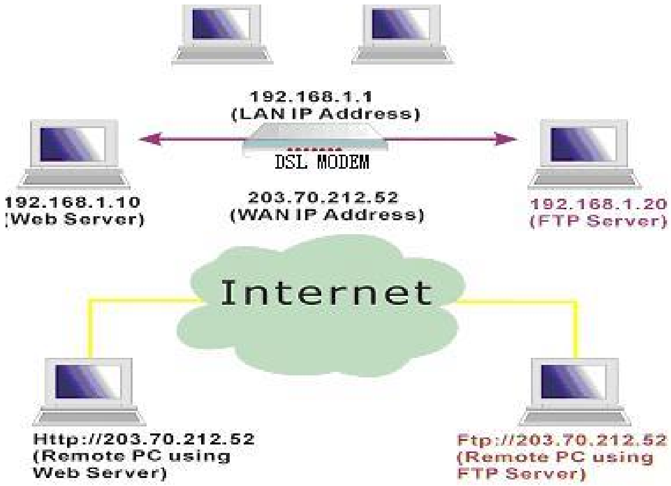
Step 2 Specify 8080 in the **Forward to Port** field.

All incoming HTTP traffic is forwarded to the PC running the Web server on port 8080. When setting a port forwarding service, ensure that the port is not used by another application, which may stop functioning. A common example is when using

SIP signaling in Voice over IP, the port used by the gateway VoIP application (5060) is the same port, on which port forwarding is set for LAN SIP agents.

Note*: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific application level gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. DSL router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.*

Virtual servers are configured for this purpose.


192.168.1.1
(LAN IP Address)
DSL MODEM
192.168.1.10
(Web Server)
203.70.212.52
(WAN IP Address)
192.168.1.20
(FTP Server)
Internet
Http://203.70.212.52
(Remote PC using
Web Server)
Ftp://203.70.212.52
(Remote PC using
FTP Server)

Adding Port Forwarding

Step 1 To set up virtual servers for a service, select **Advanced Setup** > **NAT** > **Virtual Servers**, and click **Add**.

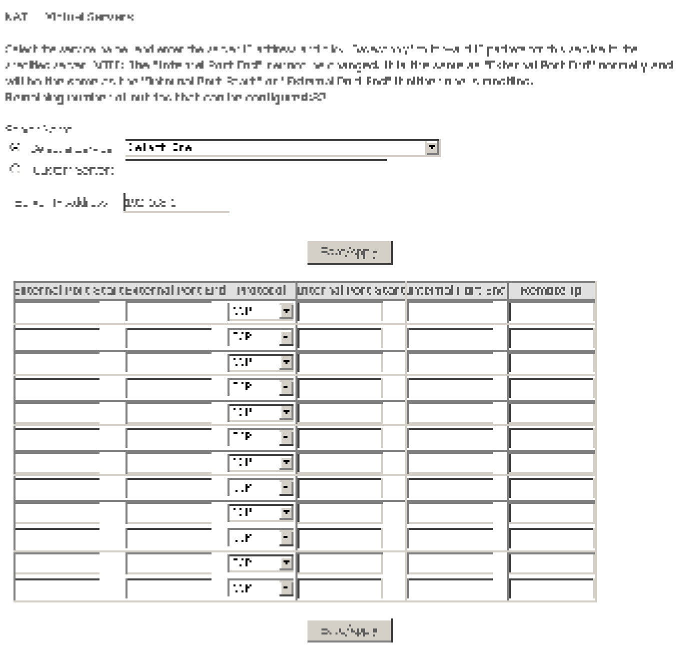


Figure 1 Adding virtual servers

Step 2 Select a service or enter a custom server.

Step 3 Set **Server IP Address**.

Step 4 Enter the server IP address of the computer that provides the service (the server in the local host field). Note that unless an additional external IP address is added, only one LAN computer can be assigned to provide a specific service or application.

Step 5 Set **External Port Start** and **External Port End**.

Step 6 Select **Protocol**.

Step 7 Set **Internal Port Start** and **Internal Port End**.

Step 8 Enter **Remote IP**.

Step 9 Click **Save/apply** to apply the settings.

If the application you require is not in the list, manually enter the information.

Select the protocol for the service you are providing from the **Protocol** drop-down list. Under **External Port**, enter the port number of the service you are providing. In the **Internal Port** field, enter the internal port number, to which service requests are to be forwarded. In the **Local IP Address** field, enter the IP address of the PC that provides the service.

Example

The Web server is configured to react to requests on port 8080. However, the requests from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with port 80 on the Web server of the PC you have defined with port 8080.

Deleting Port Forwarding

Step 1 Select the **Remove** check box.

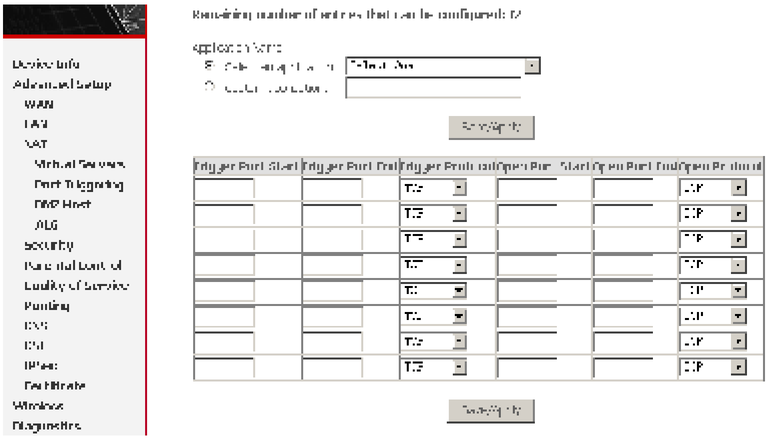
Step 2 Click **Remove** to apply the settings.

3.4.3.3 Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or manually assign ports or port blocks.

Adding Port Triggering

Step 1 To set up port triggering for a service, select **Advanced Settings** > **NAT** > **Port Triggering**, and click **Add**.


Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Wireless
Diagnostics
Trigger Port Start
Trigger Port End
Trigger Protocol
Open Port Start
Open Port End
Open Protocol

Step 2 Select the required application from the **Select an application** drop-down list, or manually enter the information in the **Custom application** field.

= **Trigger Port Start and Trigger Port End**: enter the port that is to be monitored for outgoing data traffic.

= **Trigger Protocol**: select the protocol that is to be monitored for outgoing data traffic.

= **Open Protocol**: select the protocol that is to be allowed for incoming data traffic

= **Open Port Start and Open Port End**: enter the port that is to be opened for incoming traffic.

Step 3 Click **Save/Apply** to apply the settings.

Removing Port Triggering

Step 1 Select the **Remove** check box.

Step 2 Click **Save/Apply** to apply the settings.

3.4.3.4 DMZ Host

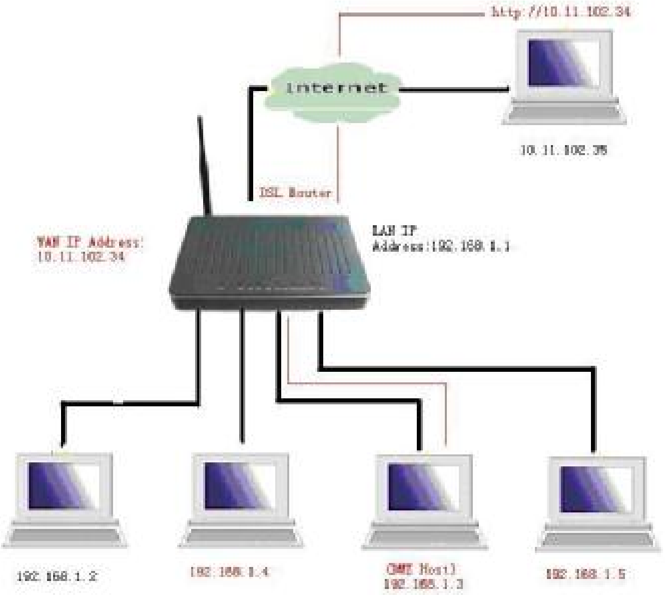

http://10.11.102.34
internet
10.11.102.35
DSL Router
WAN IP Address:
10.11.102.34
LAN IP
Address:192.168.1.1
192.168.1.2
192.168.1.4
DMZ Host)
192.168.1.3
192.168.1.5

Figure 2 DMZ host

The demilitarized military zone (DMZ) host feature allows one local computer to be exposed to the Internet. This function is applicable for:

- Users who want to use a special-purpose Internet service, such as an on-line game or video conferencing program, that is not presented in the port forwarding list and for which no port range information is available.
- Users who are not concerned with security and wish to expose one computer to all services without restriction.

***Note**: A DMZ host is not protected by the firewall and may be vulnerable to attack. This may also put other computers in the home network at risk. Hence, when designating a DMZ host, you must consider the security implications and protect it if necessary.*

You can set up a client in your local network as a so-called DMZ host. Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (for example, hacker attacks). Enable this function only when necessary (for example, to operate a Web server) and when other functions (for example, port forwarding) are inadequate. In this case, you should take appropriate measures for the clients concerned.

***Note**: Only one PC per public IP address can be set up as an exposed host.*

Adding a DMZ Host

Step 1 To set up a PC as a DMZ host, select **Advanced Setup** > **NAT** > **DMZ host**.

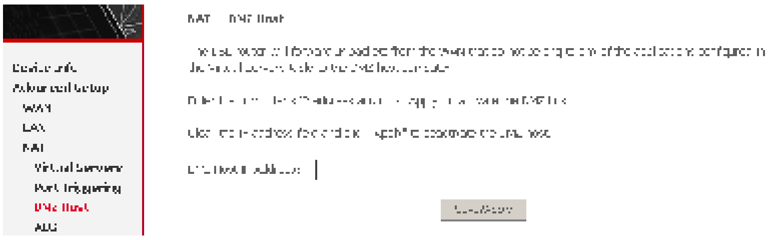


Figure 3 DMZ host configuration

Step 2 Enter the local IP address of the PC that is to be enabled as an exposed host.

Step 3 Click **Save/Apply** to apply the settings.

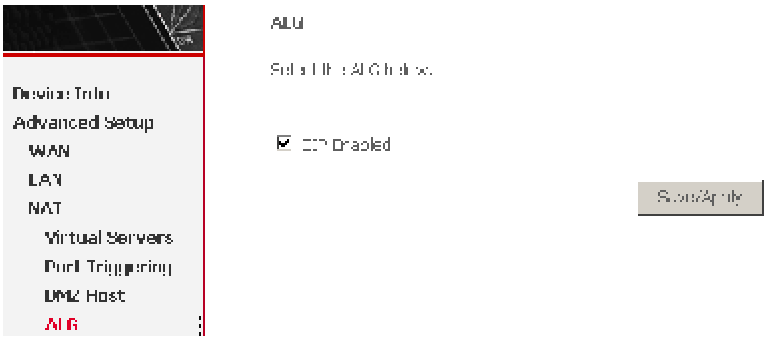
Remove DMZ host

Step 1 Clear the DMZ Host Address.

Step 2 Click **Save/Apply** to apply the settings.

3.4.3.5 NAT – ALG

Click **ALG**, the following page appears. In this interface, you can enable SIP ALG.



ALG

Select the ALG below.

☑ SIP Enabled

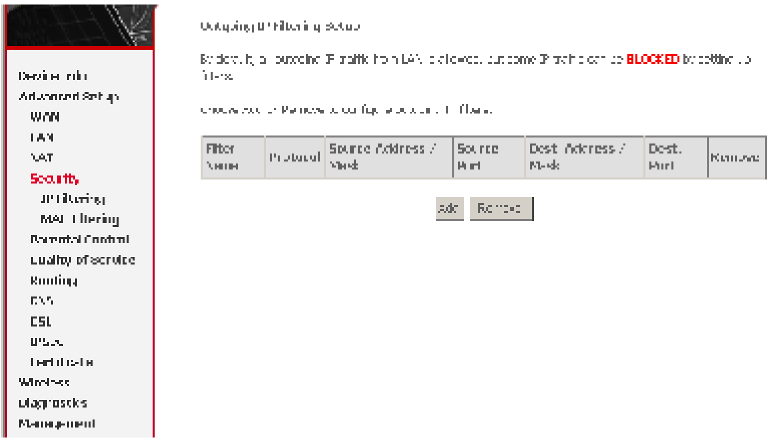
Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
Save/Apply

3.4.4 Security

Click **Security** > **IP Filtering** and the following interface appears. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and permits only authorized documents to be sent to the LAN.

***Note**: If the modem is configured to bridge mode only, IP filtering is disabled and the IP filtering interface does not appear.*

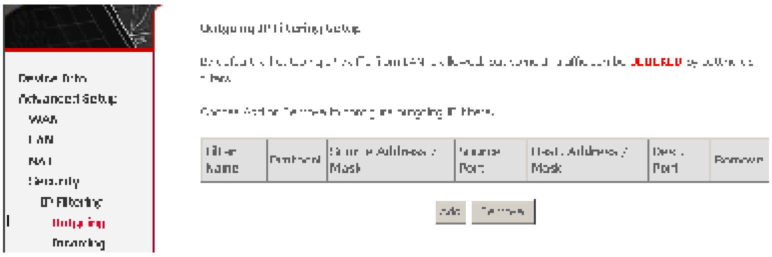
If the modem does not configure a PVC of Bridge mode, MAC filtering is disabled and the MAC Filtering interface does not appear.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Wireless
Diagnostics
Management
Outgoing IP Filtering Setup
BLOCKED
Filter Name
Protocol
Source Address / Mask
Source Port
Dest. Address / Mask
Dest. Port
Remove
Add
Remove

3.4.4.1 Outgoing IP Filtering Setup

Click **Security** > **IP Filtering** > **Outgoing** and the following page appears.

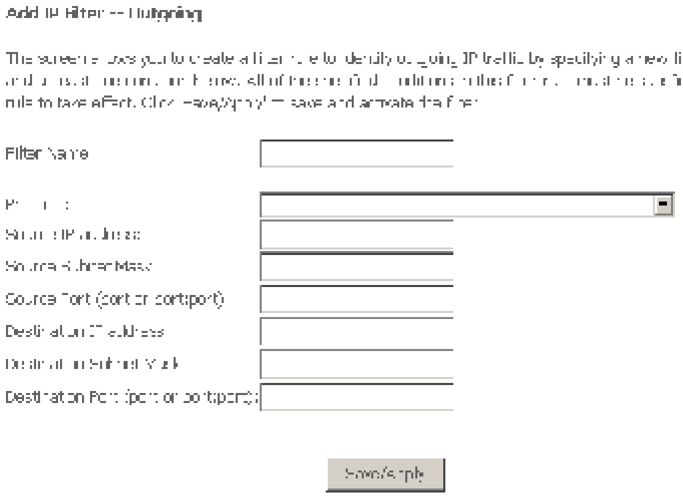
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
Outgoing IP Filtering Setup
BLOCKED
Filter Name
Protocol
Source Address / Mask
Source Port
Dest. Address / Mask
Dest. Port
Remove
Add
Remove

Click **Add** and the page for defining the IP filtering rule appears.

In this page, you can create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All specified conditions in the filtering rule must be complied with the rule to take effect.

Click **Save/Apply** to save and activate the filter.

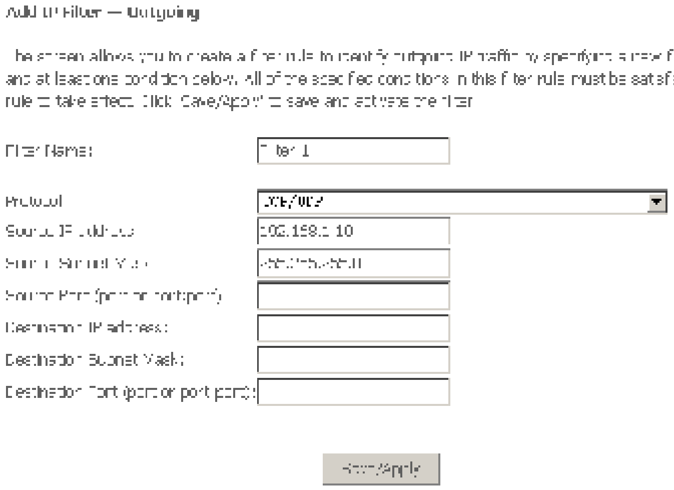


Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:	
Protocol:	
Source IP address:	
Source Subnet Mask:	
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

For example: if you need to block a PC whoese IP address is 192.168.1.10. All outgoing IP traffic from that PC(192.168.1.10) is disallowed. The confiuration is as follows.

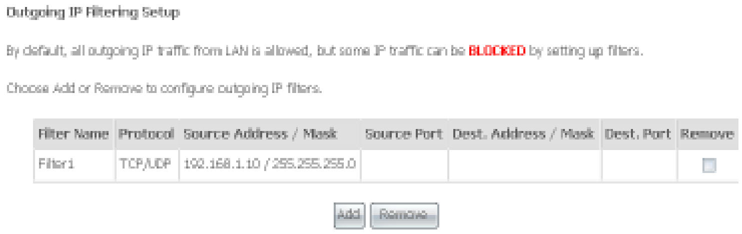


Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:	Filter 1
Protocol:	TCP/UDP
Source IP address:	192.168.1.10
Source Subnet Mask:	255.255.255.0
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

Click **Save/apply**, the following interface appears.



Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

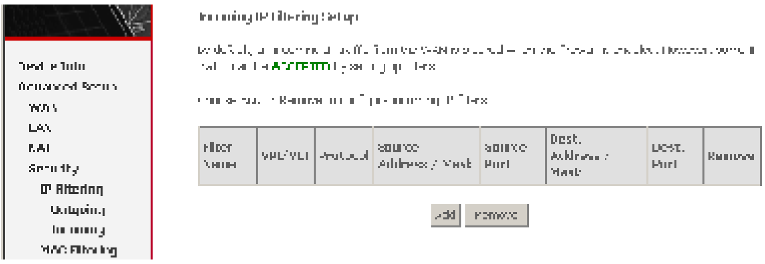
Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Filter1	TCP/UDP	192.168.1.10 / 255.255.255.0				☐

3.4.4.2 Incoming IP Filtering Setup

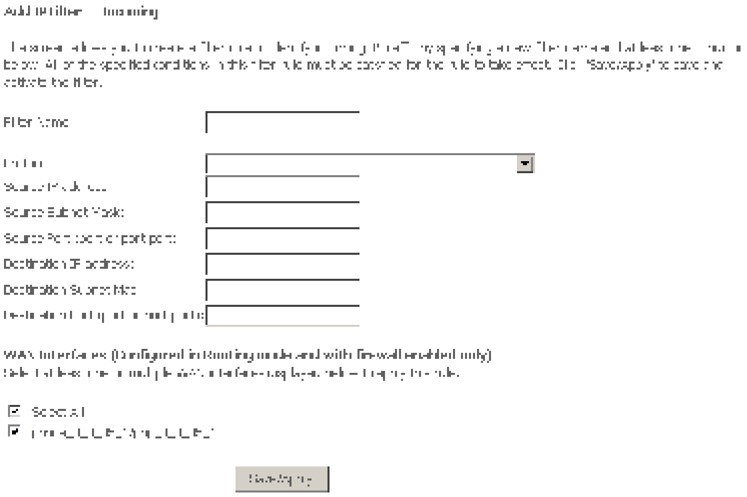
Click **Security** > **IP Filtering** > **Incoming** and the following page appears.

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



Click **Add**, the following page appears. In this page, you can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All specified conditions in this filter rule must comply with the rule. Click **Save/Apply** to save and activate the filter.

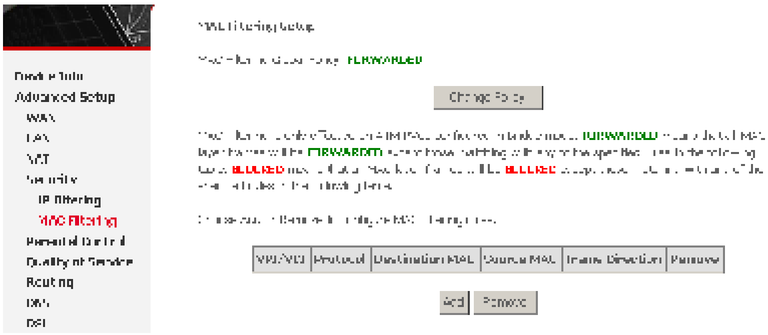
You should select at least one WAN interface to apply this rule.


Add IP Filter -- Incoming
Filter Name
Protocol
Source IP address
Source Subnet Mask
Source Port (port or port:port)
Destination IP address
Destination Subnet Mask
Destination Port (port or port:port)
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select All
Save/Apply

3.4.4.3 MAC Filtering Setup

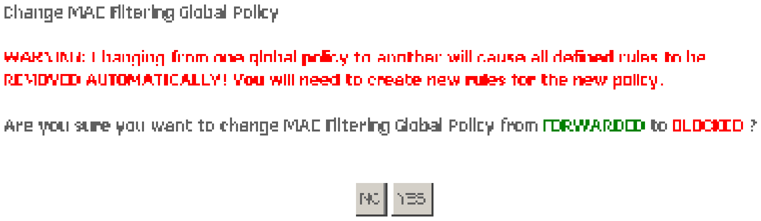
Click **Security** > **MAC Filtering**, and the following page apperas.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. Forwarded means that all MAC layer frames are forwarded except those matching with any of the specified rules in the following table. Blocked means that all MAC layer frames are blocked except those matching with any of the specified rules in the following table.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
MAC Filtering Setup
FORWARDED
Change Policy
FORWARDED
FORWARDED
BLOCKED
BLOCKED
Add
Remove

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Click **Change Policy** and the following page apperas.Then you can change the MAC Filtering Global Policy from FORWARDED to BLOCKED.



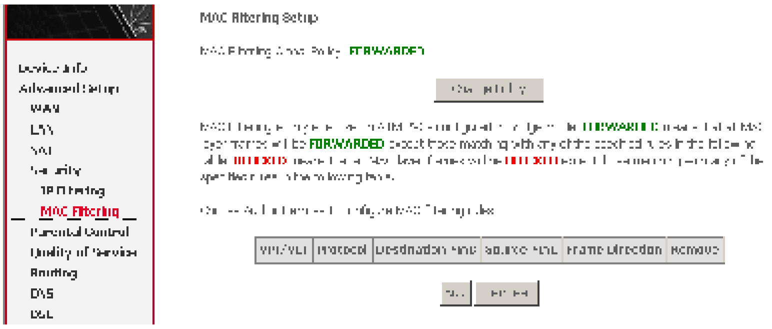
Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from FORWARDED to BLOCKED ?

Read the warning information. Click **Yes** to change the MAC filtering global policy from **Forwarded** to **Blocked**. Click **No** to cancel.

For example, to forbid the PC whose MAC address is 00:13:20:9E:0F:10 through PPPoE dial-up, begin with the following page.



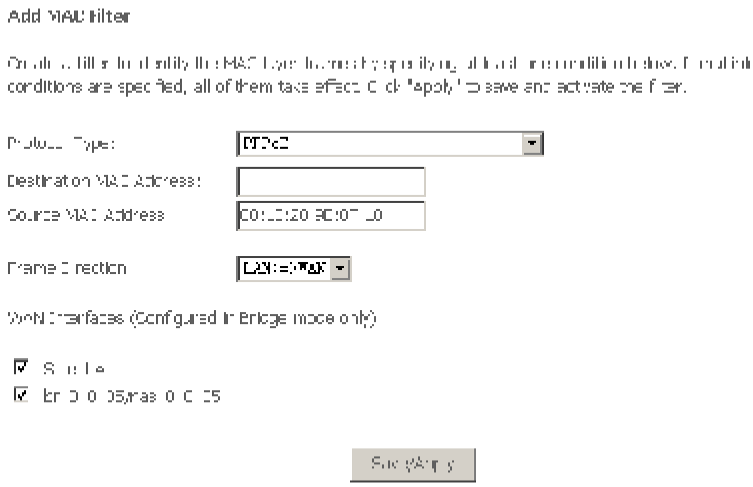
MAC Filtering Setup

MAC Filtering Global Policy: FORWARDED

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Change Policy
Add
Remove

Click **Add** to configure the interface as follows.



Add MAC Filter

[illegible] conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type: PPPoE

Destination MAC Address:

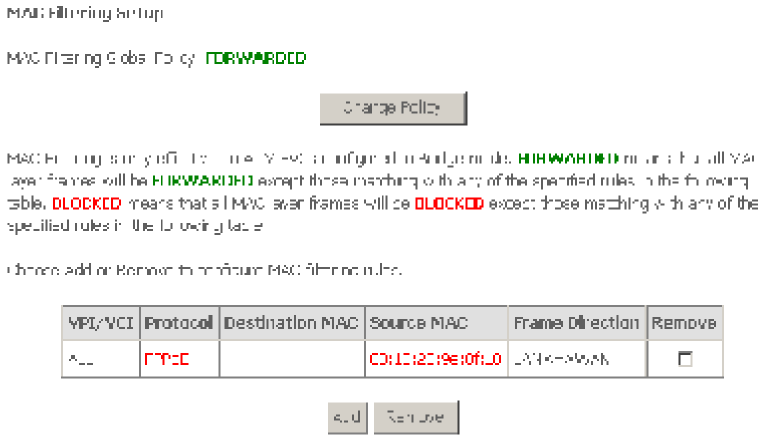
Source MAC Address: [illegible]

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

☑ [illegible]
☑ [illegible]

Click **Save/Apply** and the following page appears.



MAC Filtering Setup

MAC Filtering Global Policy: FORWARDED

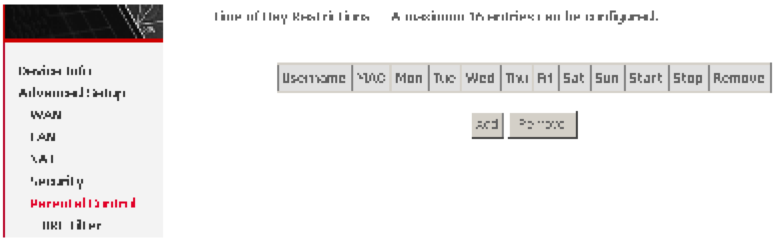
[illegible] FORWARDED [illegible] FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

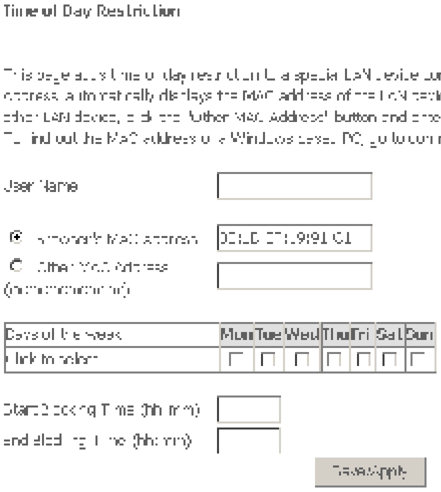
VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	PPPoE		[illegible]	LAN<=>WAN	☐

3.4.5 Parental Control

Click **Security**>**Parental Control** and the following page appears.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
URL Filter
Time of Day Restrictions -- A maximum 16 entries can be configured.
Username
MAC
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Start
Stop
Remove
Add
Remove

Click **Add** and the following page appears.


Time of Day Restriction
User Name
Browser's MAC Address
Other MAC Address
Days of the week
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply

In this page, you can add time of day restriction to a special LAN device connected to the Router. The **Browser's MAC Address** automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click **Other MAC Address** and enter the MAC address of the another LAN device. To obtain the MAC address of a Windows based PC, enter **ipconfig /all** in the DoS window.

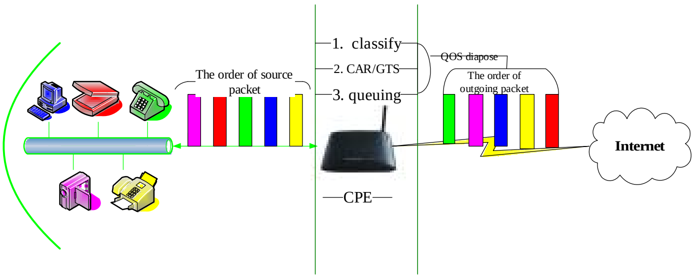
3.4.6 Quality of Service

Many communication and multimedia applications require large, high-speed bandwidths to transfer data between the local network and the internet. However, for many applications there is often only one internet connection available with limited capacity. QoS divides this capacity between the different applications and provides undelayed, continuous data transfer in situation where data packets with higher priority are given preference.

Click **Quality of Service** and the following page appears. Under **Quality of Service**, there are two network share modes: **Queue Config** and **QoS Classification**.

Network QoS is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

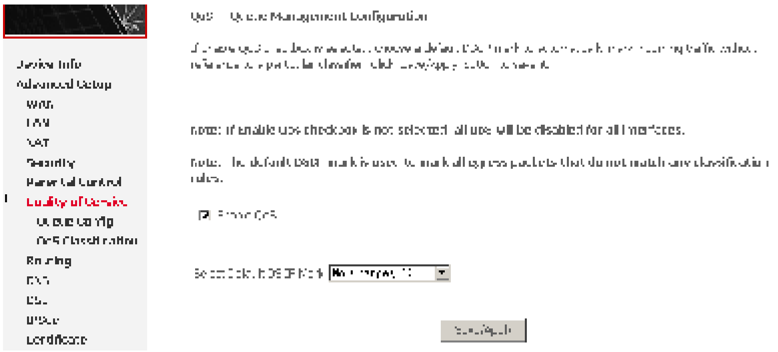
Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network’s best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.



3.4.6.1 Enabling QoS

In this page, you can perform QoS queue management configuration. By default, the system enables QoS and sets a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

Select **Advanced Setup** > **Quality of Service** and the following page appears.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
UPnP
Certificate
Enable QoS
Save/Apply

Select **Enable QoS** to enable QoS and set the default DSCP mark.

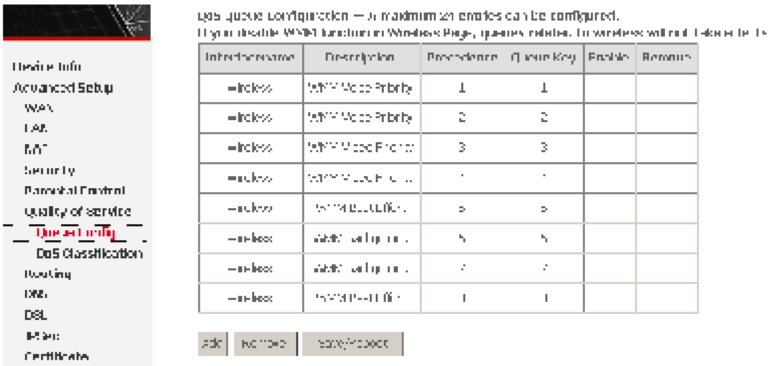
Click **Save/Apply** to activate QoS.

3.4.6.2 QoS-Queue Configuration

The queuing in packet QoS becomes effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

Click **Queue Config,** and the following page appears. In this page, you can configure QoS queue. A maximum of 24 entries can be configured.

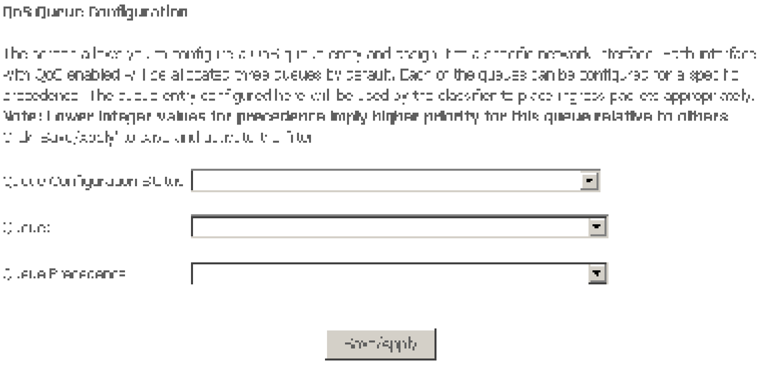
QoS Queue Configuration can allocate four queues. Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured is used by the classifier to place ingress packets appropriately.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
IPSec
Certificate
Add
Remove
Save/Reboot

Note: *Lower integer values for precedence imply higher priority for this queue relative to others.*

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/0/35). Set integer values for queue precedence to 1.

Step 1 Click **Add,** and the following page appears.


QoS Queue Configuration
Note: Lower integer values for precedence imply higher priority for this queue relative to others.
Queue Configuration Status:
Queue:
Queue Precedence:
Save/Apply

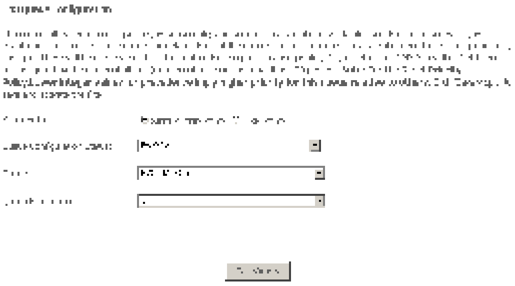
= **Policy Select**: you can select Strict Priority Policy or WRR Policy.

= **Queue Configuration Status**: set to enable or disable a QoS queue.

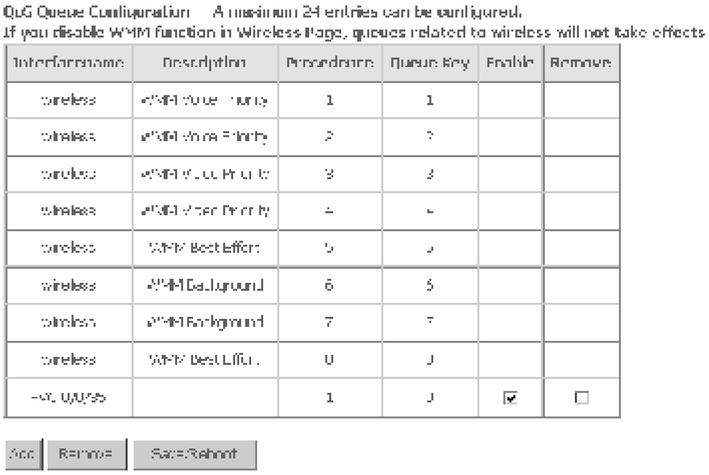
= **Queue**: select a specific network interface. When you have already selected a network interface, the specific network interface selected automatically allocates to the queue.

= **Queue Precedence**: select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

Step 2 Add a QoS queue entry and assign it to a specific network interface (PVC 0/0/35), and set integer values for queue precedence to 1. See the following figure:



Step 3 After proper modifications, click **Save/Apply** and the following page appears. This configuration takes effective at once.



QoS Queue Configuration A maximum 24 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

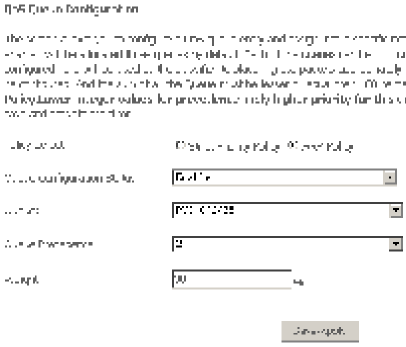
Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	[illegible]		
wireless	WMM Background	6	5		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	0	[illegible]		
PVC 0/0/35		1	[illegible]	☑	☐

To delete a certain queue, disable it, select it, and then click **Remove**.

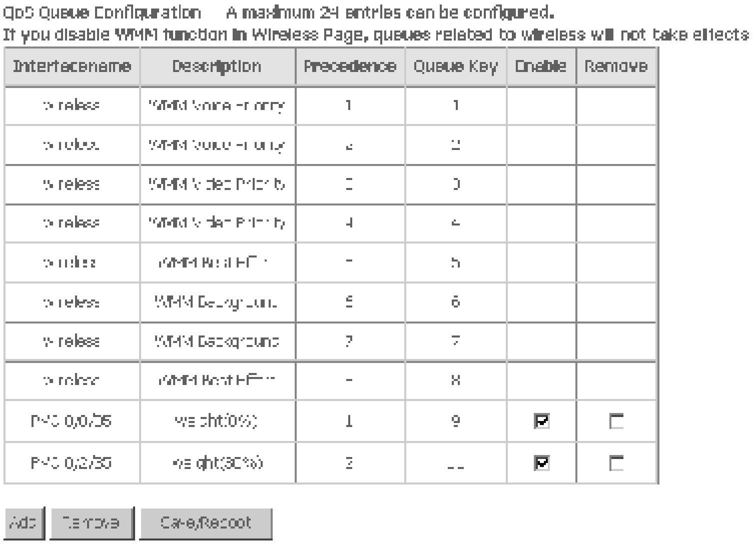
After the queue is configured, you can create several traffic class rules to classify the upstream traffic.

WRR (Weighted Round Robin): this is another QoS method. If you want to set WRR, you must disable the **Strict-Priority Queue** (PQ). The WRR is mutex to PQ. Only one QoS method can exist at the same time. Select WRR in **QoS Queue Configuration** page. The following interface appears.

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/2/35). Set queue precedence to 2 and weight value to 30%.



After proper modifications, click **Save/Apply** and the following page appears.



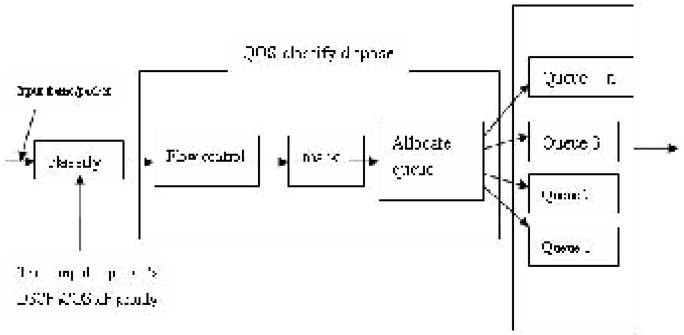
QoS Queue Configuration A maximum 24 entries can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	-	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	-	8		
PVC 0/0/35	weight(0%)	1	9	☑	☐
PVC 0/2/35	weight(30%)	2	10	☑	☐

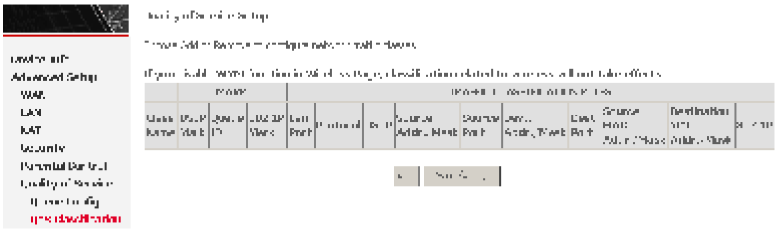
The weighted round robin (WRR) queue schedule divides each port into several output queues. Queues are scheduled in turn to ensure that each queue obtains a certain service time. WRR configures a weighted value (w3, w2, w1 and w0) for each queue. The weighted value represents the proportion of the obtained resources. For example, the weighted value of WRR queue schedule algorithm of a 100M port is configured as 50, 30, 10 and 10 (corresponding to w3, w2, w1 and w0), so that the queue with minimum priority obtains a bandwidth of at least 10Mbps, which avoids the disadvantage that a message in queue with low priority during PQ schedule may not obtain service for a long time. WRR queue still has another advantage. Although the schedule of these queues are conducted in turn, each queue is not assigned with a fixed service time slice-if a certain queue is null, it is immediately changed to the next queue. In this way, the bandwidth resources can be fully utilized.

3.4.6.3 QoS-QoS Classification

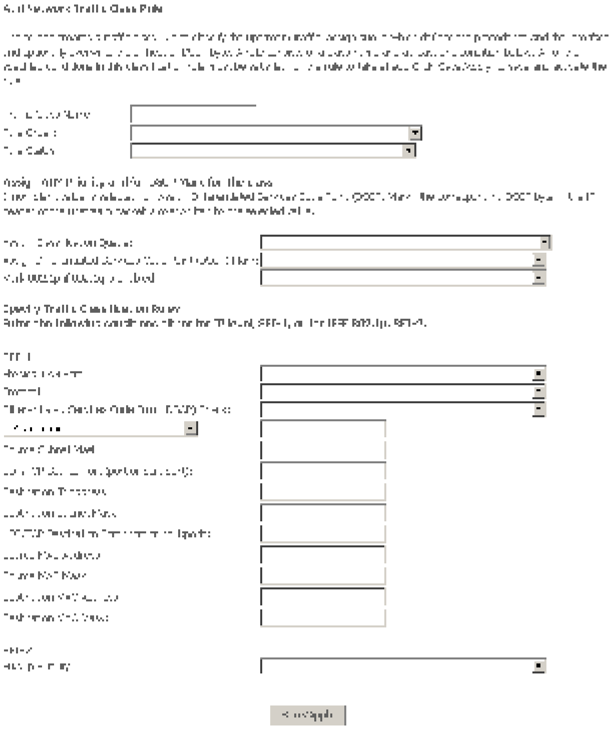
Some applications require specific bandwidth to ensure its data be forwarded in time. QoS classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. After QoS classification, QoS divides capacity between different applications and provides undelayed, continuous data transfer where data packet with higher priority is given preference. The follow figure shows QoS classification.



Click **QoS Classification** and the following page appears. In this page, you can configure network traffic classes.


Advanced Setup
WAN
LAN
NAT
Security
Parental Control

Click **Add** and the following page appears.



- = Traffic Class Name: Enter a name of the class.
- = Rule Order: Select order for queue.
- = Rule Status: Enable or disable this traffic class rule.
- = Assign Classification Queue: Select a classification queue.

- Assign Differentiated Service Code Point (DSCP) Mark: Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS-Mark IP Precedence, AF-Assured Forwarding, EF-Expedited Forwarding)
- Mark 802.1p if 802.1q is enabled: Select an 802.1p priority number that serves as the 802.1p value.

There are two sets of classification rules. Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port; Set-2 is based on MAC layer IEEE 802.1p priority field.

Set-1 Rules contain the following:

- Physical LAN Port: Select one among USB port, Ethernet ports and wireless port.
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols.
- Source IP Address
- Source subnet mask
- UPD/TCP Source Port
- Destination IP Address
- Destination Subnet Mask
- UPD/TCP destination port or a range of ports
- Source Mac Address
- Source Mac Mask
- Destination Mac Address
- Destination Mac Mask

Set-2 Rules contain the following:

802.1p Priority: the 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

QoS-DSCP Setting

In order to understand what is differentiated services code point (DSCP), you should be familiar with the differentiated services model (Diffserv).

Diffserv is a class of service (CoS) model that enhances best-effort Internet services via differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

As displayed in following diagram, the IPV4 packet has a TOS filed. Diffserv defines TOS field in IP packet headers referred to as DSCP. Hosts or routes that pass traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handing or scheduling behavior.

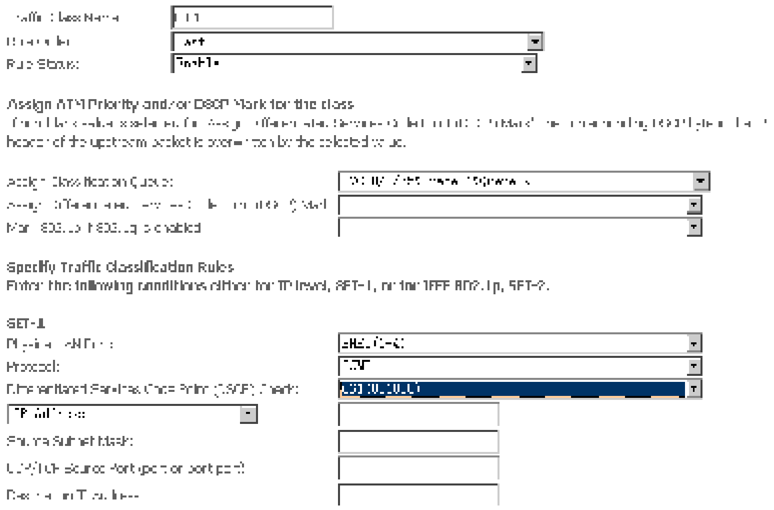
Layer 3 IPV4 packet

Version/length	TOS (1 word)	length	ID	Offset /mark	TTL	protocol	Check sum	IP-SA	IP-DA	data

TOS filed-IP priority (TOS front 3 bit) or DSCP (front 6 bit)

7	6	5	4	3	2	1	0
IP priority			Undefined				
DSCP						Flow control	

For example, mark each transmitted ICMP packet which passes traffic to 0-35class with an appropriate DSCP (CS1).



Rule Status:

Assign ATM Priority and/or DSCP Mark for the class

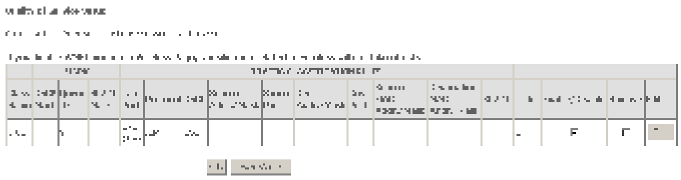
Specify Traffic Classification Rules

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Protocol:

After proper modifications, click **Save/Apply** and the following page appears.



Click **Save/Apply**. This configuration takes effective at once.

QoS-802.1p Setting

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The follow diagram shows the structure of 802.1Q Frame. The 802.1Q header includes a 3-bit prioritization field, which allows packets to be grouped to be grouped into eight levels of priority (0-7), where level 7 is the highest one. In addition, DSL maps these eight levels to priority queues, where queue 1 has the highest priority.

Layer 2 802.Q frame

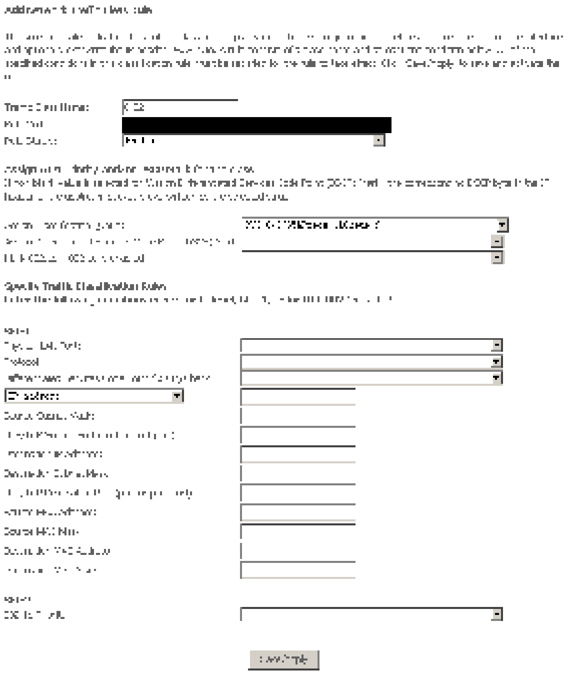
Preamble	SFD	DA	SA	mark (4	Len/Etype (2 word)	DATA	FCS

				word)			

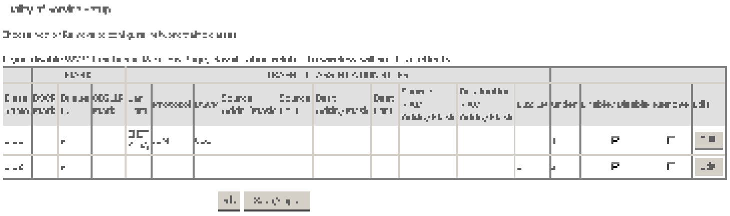
Mark

TPID(0x8100)	Priority(3bit)	CFI (1bit)	VLAN ID (12bit)

For example: mark the frame of 802.1p that queued to Queue 9 on value 2.


[redacted]

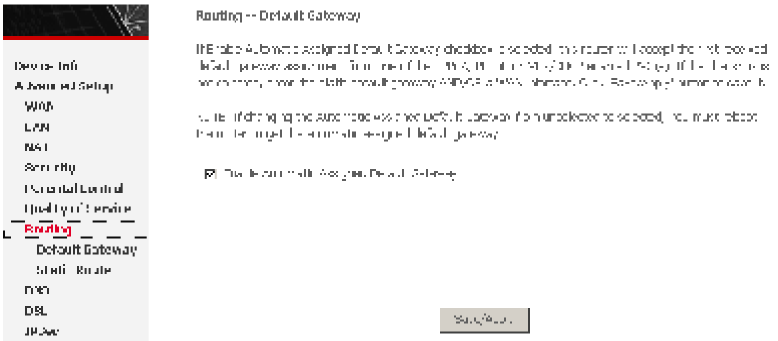
After proper modifications, click **Save/Apply** to show the following interface.



Click **Save/Apply**. This configuration takes effective at once.

3.4.7 Routing

Click **Routing** and the following page appears.



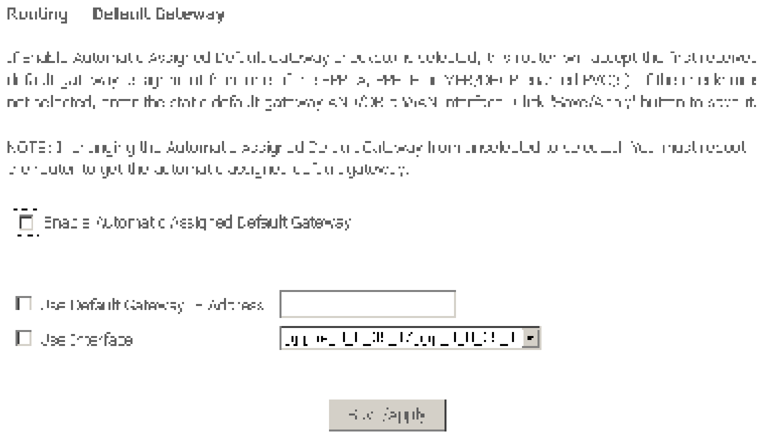
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
DNS
DSL
IPSec
Routing -- Default Gateway
Save/Apply

☑ Enable Automatic Assigned Default Gateway

3.4.7.1 Routing - Default Gateway

In this page, you can modify the default gateway settings.

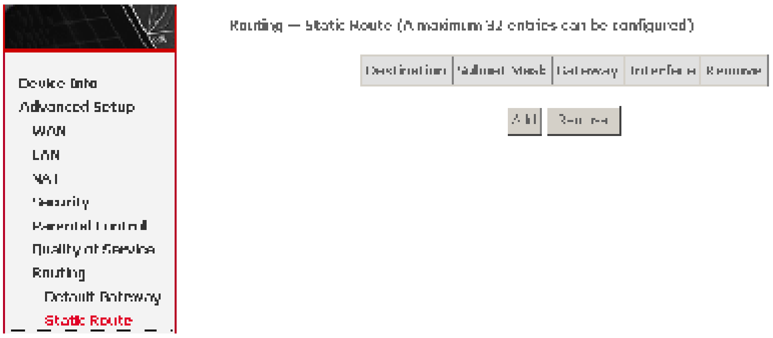
If you select **Enable Automatic Assigned Default Gateway**, this router can accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the check box is not selected, you need to enter the static default gateway and/or a WAN interface. Then, click **Save/Apply**.


Routing -- Default Gateway
☐ Enable Automatic Assigned Default Gateway
☐ Use Default Gateway IP Address
☐ Use Interface
Save/Apply

Note*: If the Automatic Assigned Default Gateway check box is changed from deselected to selected, you need to reboot the router to obtain the automatic assigned default gateway.*

3.4.7.2 Routing - Static Route

In this interface, you can modify the static route settings.

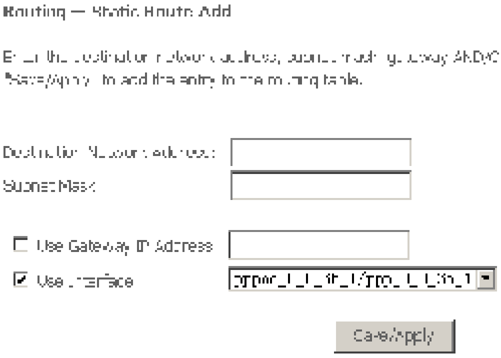

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Routing -- Static Route (A maximum 32 entries can be configured)
Destination
Subnet Mask
Gateway
Interface
Remove
Add
Remove

In this interface, you can query the preset static routes, delete an existing static route, or add a new static route. By default, the system has no static route information.

- **Destination**: The IP address to which packets are transmitted.
- **Subnetmask**: The subnet mask of the destination IP address.

- **Gateway**: The gateway that the packets pass by during transmission.
- **Interface**: The interface that the packets pass through on the modem.

Click **Add** and the following page appears.



Routing — Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

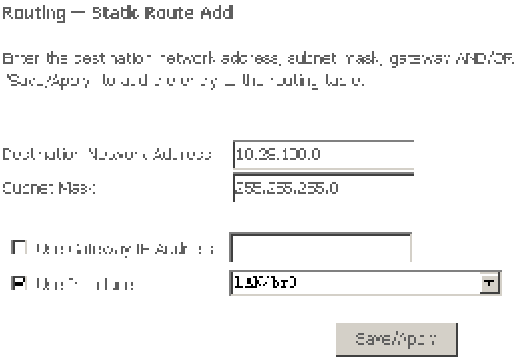
Destination Network Address:

Subnet Mask:

☐ Use Gateway IP Address

☑ Use Interface

To add a static route rule, the configuration is as follows.



Routing — Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

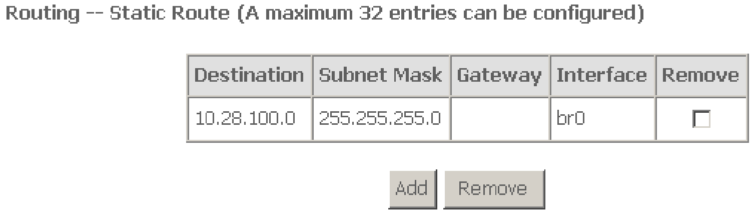
Destination Network Address: 10.28.100.0

Subnet Mask: 255.255.255.0

☐ Use Gateway IP Address

☑ Use Interface LAN/br0

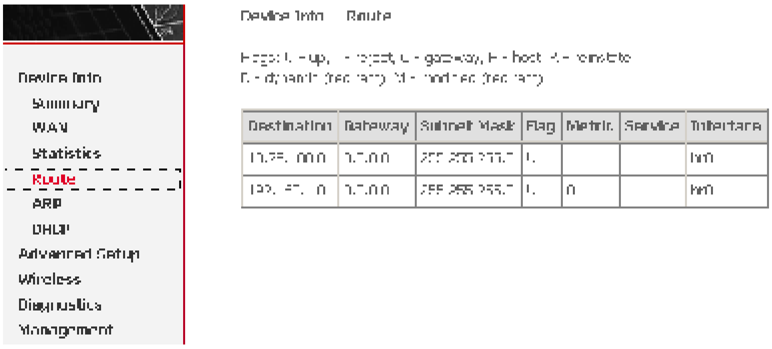
Click **Save/Apply** and the following page appears.



Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove
10.28.100.0	255.255.255.0		br0	☐

In the route status interface, the following page appears.


Device Info
Summary
WAN
Statistics
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management

Device Info -- Route

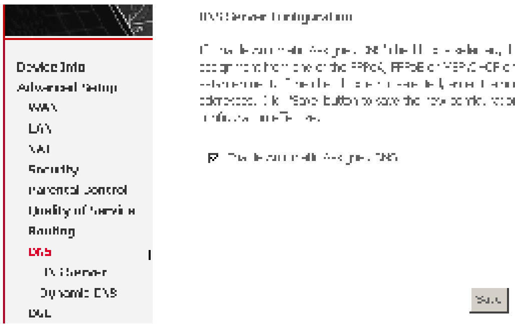
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect)

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
[illegible]	0.0.0.0	[illegible]	U			br0
[illegible]	0.0.0.0	[illegible]	U	0		br0

3.4.8 DNS

3.4.8.1 DNS Server

In this interface, you can modify the DNS server settings.

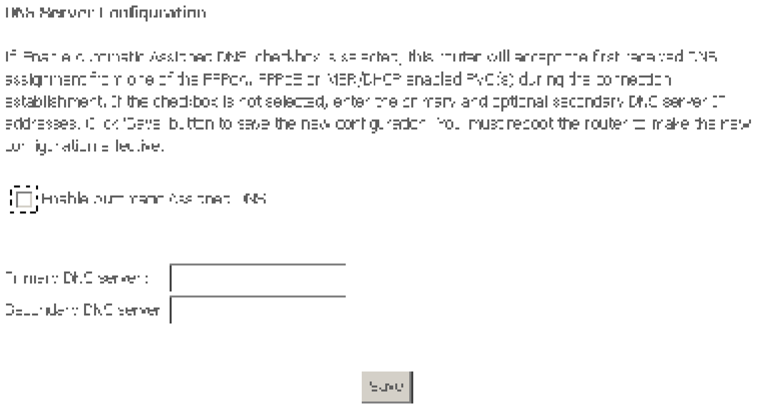

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Save

DNS Server Configuration

☑ Enable Automatic Assigned DNS

If select **Enable Automatic Assigned DNS**, this router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is as follows.



DNS Server Configuration

☐ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

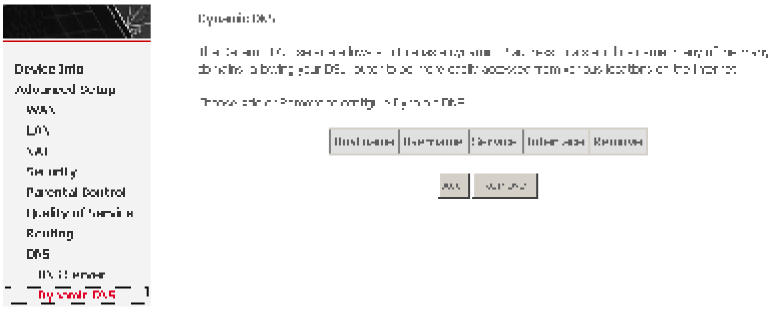
Click **Save** to save the new configuration.

***Note**: You must reboot the router to make the new configuration effective.*

3.4.8.2 Dynamic DNS

In this interface, you can modify the Dynamic DNS settings.

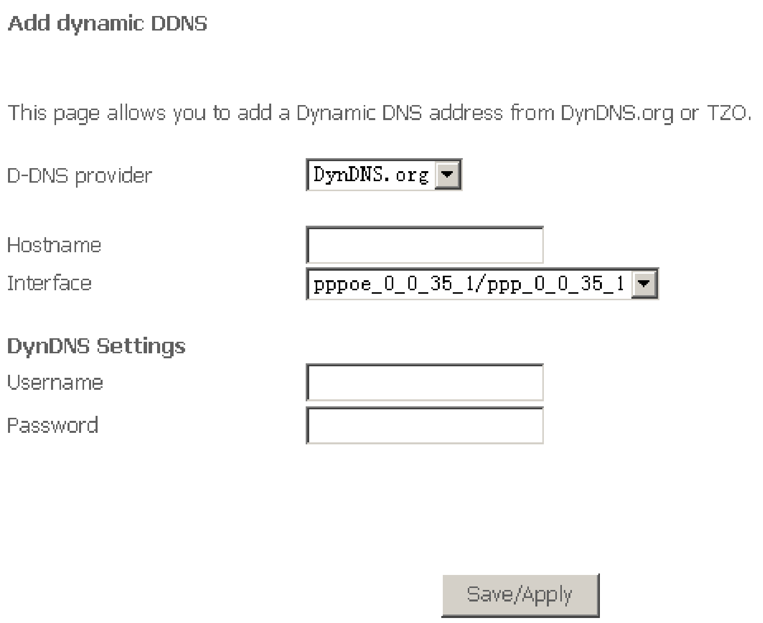
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



Dynamic DNS

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
Hostname
Username
Service
Interface
Remove
Add
Remove

Click **Add** to add dynamic DDNS.



Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_0_35_1/ppp_0_0_35_1

DynDNS Settings

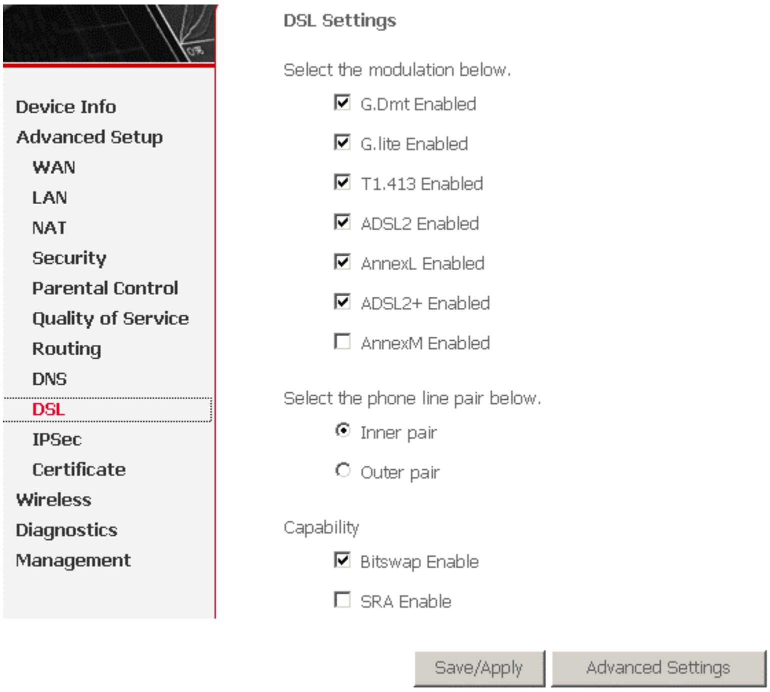
Username:

Password:

3.4.9 DSL

In this interface, you can modify the DSL settings.

Select one you need. But the default setting can check G.dmt/ G.lite/ T1.413/ ADSL2/AnnexI/ ADSL2+/ Inner pair/ Bitswap. The modem can negotiate the modulation mode with the DSLAM.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Wireless
Diagnostics
Management

DSL Settings

Select the modulation below.

☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
☐ AnnexM Enabled

Select the phone line pair below.

● Inner pair
○ Outer pair

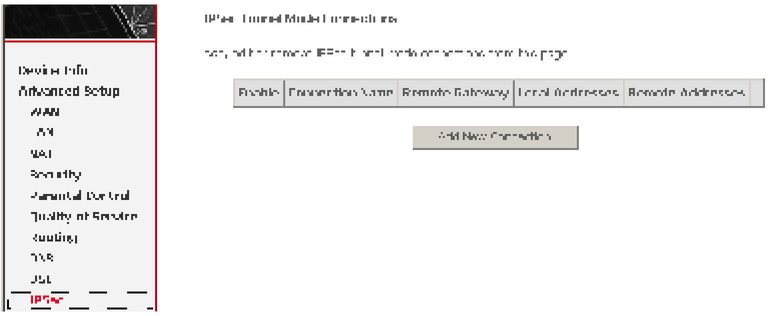
Capability

☑ Bitswap Enable
☐ SRA Enable

Save/Apply
Advanced Settings

3.4.10 IPSec

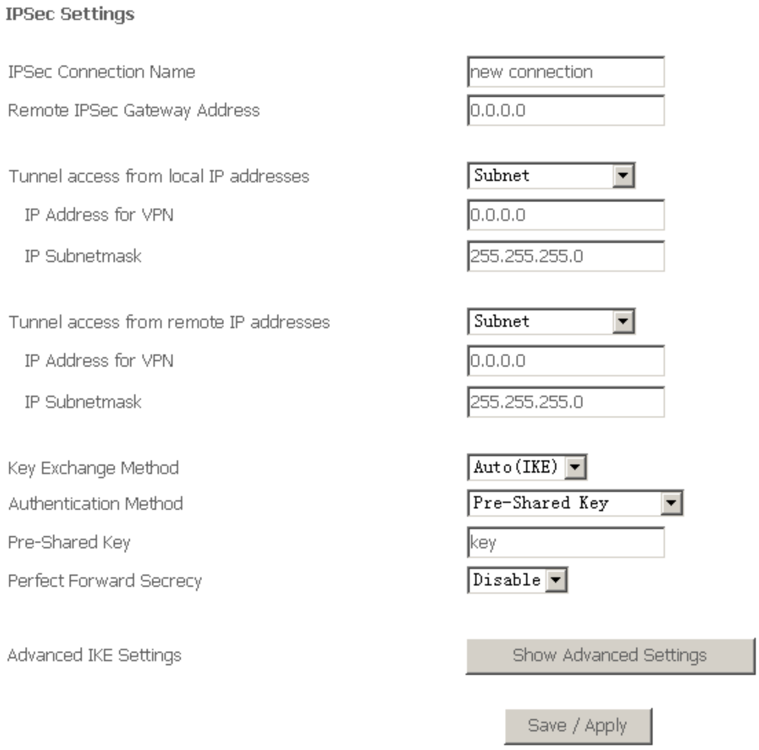
Click **IPSec**, and the following page appears.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Add New Connection

IPSec Tunnel Mode Connections

Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	

Click **Add New Connection** to add a new IPSec connection.



IPSec Connection Name	new connection
Remote IPSec Gateway Address	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

You can click **Show Advance Settings** to view some advance parameters and modify them to match the other side of this connection.

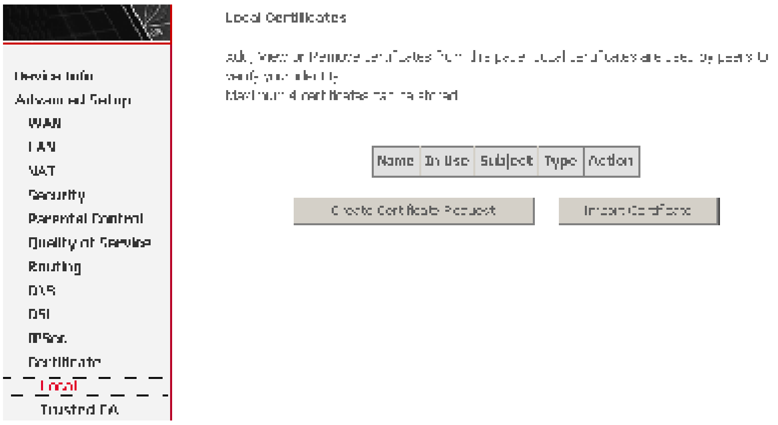
Click **Save/Apply** to save this connection, then you can check the checkbox of enable column to enable this IPSec connection. And the communication is established.

3.4.11 Certificate

3.4.11.1 Local Certificates

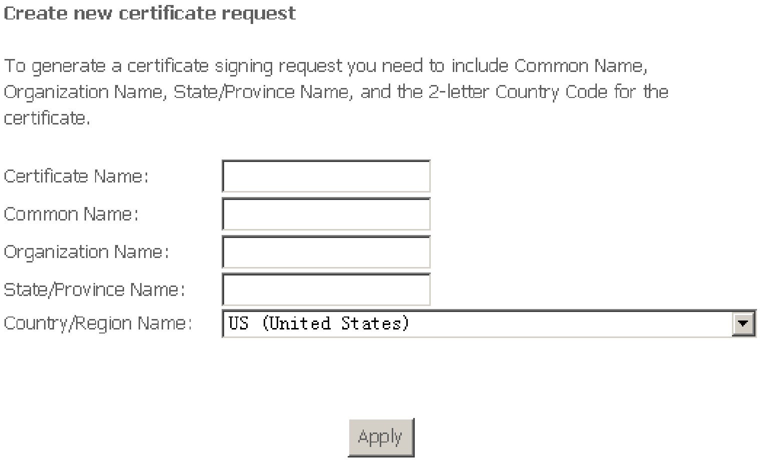
Click **Certificate** > **Local** and the following page appears.

Local certificates are used by peers to verify your identity. It can store maximum 4 certificates.


Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Local
Trusted CA
Local Certificates
Name
In Use
Subject
Type
Action
Create Certificate Request
Import Certificate

Click **Create Certificate Request** and the following page appears.

To generate a certificate signing request, you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

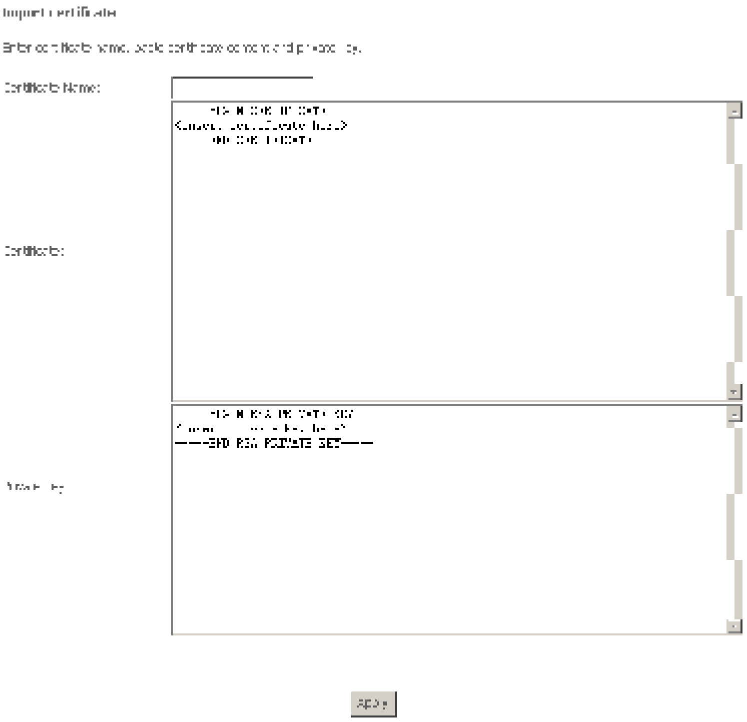


Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:
Common Name:
Organization Name:
State/Province Name:
Country/Region Name: US (United States)

If click **Import Certificate**, the following page appears. Then you can enter certificate name, paste certificate content and private key.


Import certificate
Certificate Name:
Certificate:
Private Key:
Apply

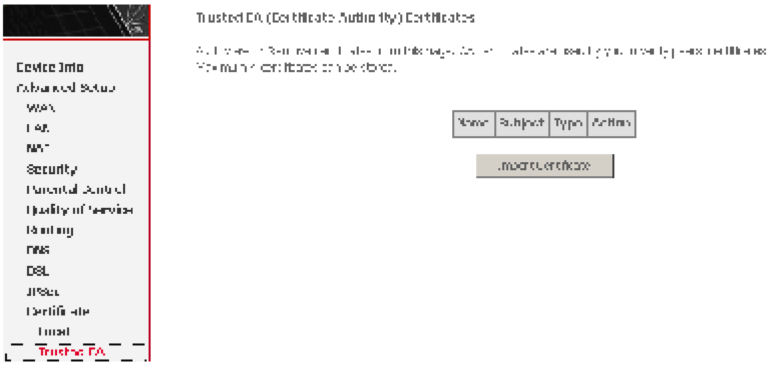
Enter certificate name, paste certificate content and private key.

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

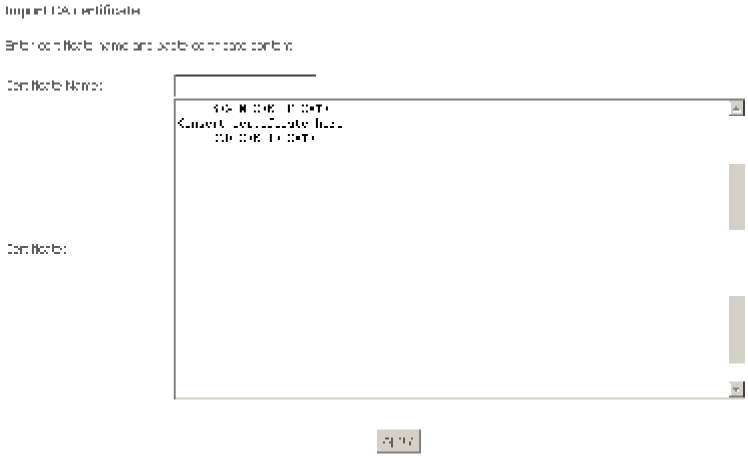
```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

3.4.11.2 Trusted CA Certificates

Click **Certificate** > **Trusted CA** and the following page appears. CA certificates are used by you to verify certificates of peers. It can store maximum 4 certificates.


Trusted CA (Certificate Authority) Certificates
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
IPSec
Certificate
Local
Trusted CA
Name
Subject
Type
Action
Import Certificate

Click **Import Certificate** and the following page appears. Then you can enter certificate name, paste certificate content.


Import CA certificate
Certificate Name:
Certificate:
Apply

3.5 Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LAN can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points (AP) that bridge network traffic to the wired LAN.

The Modem Wi-Fi® certified IEEE 802.11g compliant wireless access point allows multiple computers to connect wirelessly to your local network over the Modem Wireless LAN environment. The Modem is backward compatible with IEEE 802.11b, which means 802.11b and 802.11g devices can coexist in the same wireless network. The Wireless Distribution System (WDS) on your Modem allows you to extend the range of your wireless network. To be able to use WDS, you will need to introduce an additional WDS-enabled access point into your wireless network. To be able to connect the computers, make sure that a wireless client adapter (WLAN client) is installed on each computer you want to connect via the WLAN.

3.5.1 Wireless LAN Basics

Some basic understanding of 802.11b/g wireless technology and terminology is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

3.5.1.1 Wireless client requirements

All wireless client adapters compliant to 802.11g and/or 802.11b can communicate with the Modem (W) LAN environment. However, be aware that only 802.11g compliant wireless clients are able to gain full profit of the 54 Mb/s (Max) bandwidth delivered by the Modem. It is highly recommended to use only wireless client adapters that are Wi-Fi™ certified to ensure smooth interoperability with the Modem's WLAN.

3.5.1.2 Radio Transmission

Wireless LAN or WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. Digital data is superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread

Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. See the expert technical specifications for more details on wireless operation.

3.5.1.3 Antennas

Direct the external antenna to allow optimization of the wireless link. If for example the antenna is erect, wireless links in the horizontal plane are favored. Please note that the antenna characteristics are influenced by the environment, that is, by reflections of the radio signal against walls or ceilings. It is advisable to use the received signal strength as indicated by the wireless client manager to optimize the antenna position for the link to a given client. Concrete walls weaken the radio signal and thus affect the connection.

3.5.1.4 Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the Router in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

3.5.1.5 SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network. The Modem operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default the Modem broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting the wireless menu of web management.

3.5.1.6 Radio channels

The 802.11g standard allows several WLAN networks using different radio channels to be co-located. The Modem supports multiple radio channels and is able to select the best radio channel at each startup. You can choose to set the channels automatically or manually.

The different channels overlap. To avoid interference with another access point, make sure that the separation (in terms of frequency) is as high as possible. It is recommended to keep at least 3 channels between 2 different access points.

The Modem supports all channels allowed for wireless networking. However, depending on local regulations, the number of channels actually allowed to be used may be additionally restricted, as shown in the table below.

Regulatory Domain	**Allowed Radio Channels**
USA / Canada	1 to 11

3.5.1.7 Wireless Security

Various security options are available on the Modem including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. Authentication may use an open system or a shared key. For details on these methods and how to use them, please read the wireless LAN configuration information in Section 3.5.3 (Wireless Security Configuration).

3.5.1.8 About 802.11g Wireless

802.11b is an IEEE standard, operating at 2,4 GHz at a speed of up to 11 Mb/s. 802.11g, a newer IEEE standard also operating at 2,4 GHz, gives you up to 54 Mb/s speed, more security and better performance.

Today's 11-megabits-per-second 802.11b wireless networks are fine for broadband Internet access (which typically tops out at about 1 mbps) but rather slow for large internal file transfers or streaming video. However, 54-mbps, corporate-oriented 802.11a is expensive and because its radio uses the 5-GHz band and 802.11b uses the 2.4 GHz band, upgrading to an 802.11a network means either scrapping 802.11b gear or buying even-pricier hardware that can support both standards.

But 802.11g promises the same speed as 802.11a and the ability to coexist with 802.11b equipment on one network, since it too uses the 2.4-GHz band. 802.11g is an extension to 802.11b, the basis of many wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You should be able to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

***Note**: Maximum wireless signal rate based on IEEE Standard 802.11g specifications is 54 Mbps. But actual data throughput varies depending on.network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead will cause lower actual data throughput rate.*

3.5.1.9 Access Point and Wireless Fidel

The Wi-Fi certification ensures that your Modem will interoperate with any Wi-Fi certified 802.11g and 802.11b compliant wireless device.

The Modem Wireless LAN Access Point (AP) behaves as a networking hub allowing to wirelessly interconnect several devices to the local (W) LAN and to provide access to the Internet.

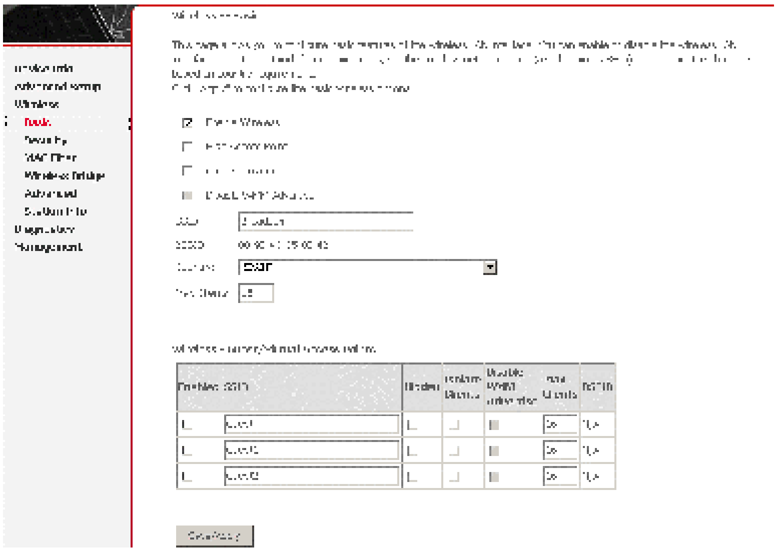
3.5.2 Wireless – Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Following is a description of the different options:

= **Enable Wireless**: If you want to make wireless be available, you have to check this box first. Otherwise, the Hide Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID box will not be displayed.

- **Hide Access Point**: Check this box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.
- **SSID**: The SSID (Service Set Identification) is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network.
- **Country**: The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Guest SSID**: The SSID (Service Set Identification) is the unique name shared among all devices in a guest wireless network. The SSID must be identical for all devices in the guest wireless network.



Click **Save/Apply** to save the basic wireless options and make the modification effect.

3.5.3 Wireless – Security

This page allows you can configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled and authentication is open. Before enabling the security, consider your network size, complexity, and existing authentication infrastructure and then determine which solution applies to it.

Following is a description of the different options.

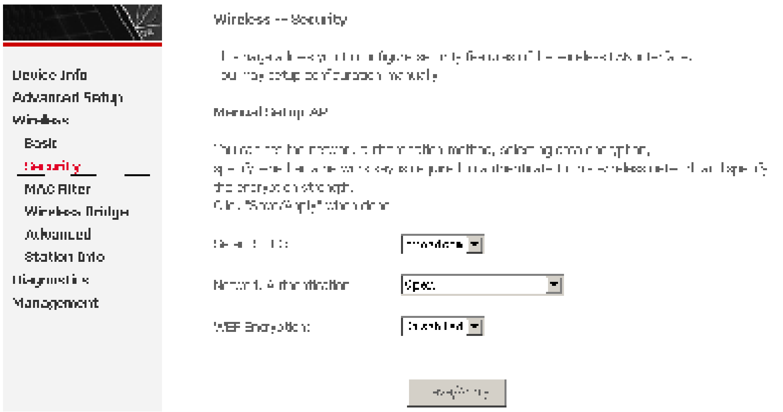
= Select SSID: Select the wireless LAN of SSID to configure security features.

= No Encryption: Please refer to below for details of configuration

= Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open.

= WEP Encryption: Disable WEP Encryption.

The data is not encrypted when it is transferred from the device to the client station. This is the default option.



Wireless -- Security

Manual Setup AP

Network Authentication: Open

WEP Encryption: Disabled

Click **Save/Apply** to save the wireless security options and make the modification effect.

64-bit WEP

= Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.

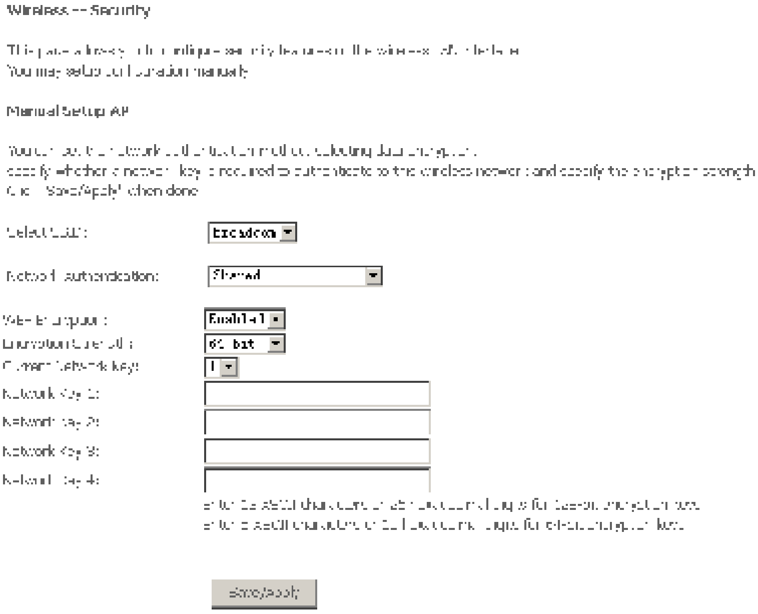
= WEP Encryption: Enable WEP Encryption.

= Encryption Strength: click the desired Data Security level to be 64-bit.

= Current Network Key: Select one of network key that you set on the Key boxes as default one.

- = Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

Manual Setup AP

Select SSID: broadcom

Network Authentication: Shared

WEP Encryption: Enabled

Encryption Strength: 64-bit

Current Network Key: 1

Network Key 1:

Network Key 2:

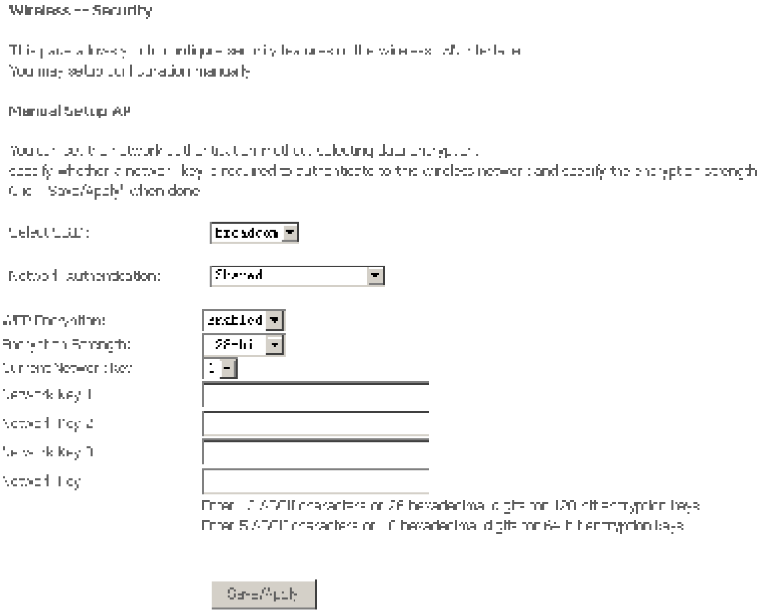
Network Key 3:

Network Key 4:

128-bit WEP

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.
- = WEP Encryption: Enable WEP Encryption.
- = Encryption Strength: Click the desired Data Security level to be 128-bit.
- = Current Network Key: Select one of network key that you set on the Key boxes as default one.
- = Network Key 1 to 4: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

You may setup configuration manually

Manual Setup AP

Click "Save/Apply" when done.

Select SSID: broadcom

Network Authentication: Shared

WEP Encryption: enabled

Encryption Strength:

Current Network Key: 1

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

802.1x Authentication

= Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be 802.1x.

= Radius Server IP Address: Enter the IP Address of the authentication server.

= Radius Port: Enter the port number of the authentication server. The default port number is 1812.

= Radius Key: Enter the same key as the Radius server's.

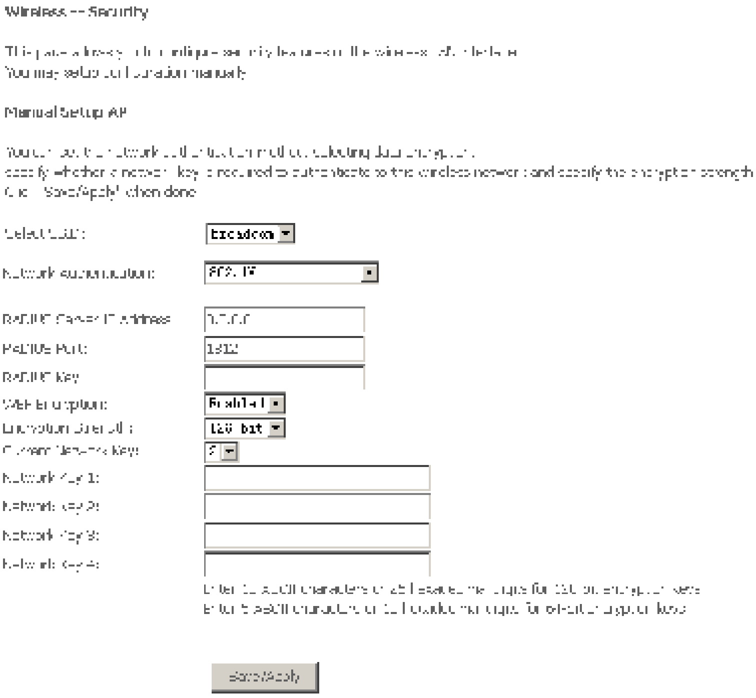
= WEP Encryption: Enable WEP Encryption. This is default

= Encryption Strength: click the desired Data Security level to be 64-bit or 128-bit.

= Current Network Key: Select one of network key that you set on the Key boxes as default one.

= Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys or enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID: broadcom

Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:
WEP Encryption: Enabled
Encryption Strength: 128-bit
Current Network Key: 2
Network Key 1:
Network Key 2:
Network Key 3:
Network Key 4:

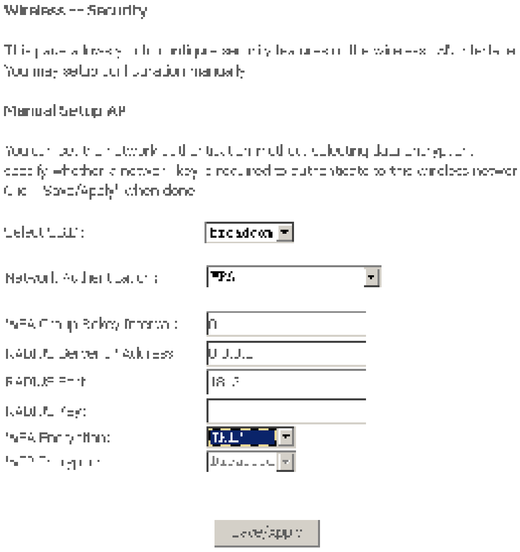
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

WPA Authentication

- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA.
- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- Radius Server IP Adress: Enter the IP Address of the authentication server.
- Radius Port: Enter the port number of the authentication server. The default port number is 1812.

- = Radius Key: Enter the same key as the Radius server's.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

Manual Setup AP

Select SSID: broadcom

Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP

WEP Encryption: Disabled

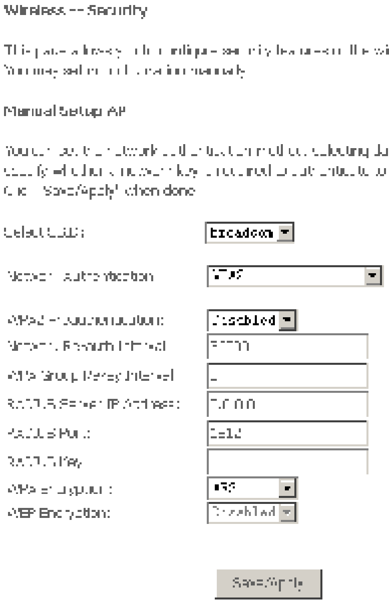
WPA2 Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA2.
- = WPA2 Preauthentication: Selec Enable or Disenable.
- = Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = RADIUS Server IP Adress: Enter the IP Address of the authentication server.
- = RADIUS Port: Enter the port number of the authentication server. The default

port number is 1812.

- = RADIUS Key: Enter the same key as the Radius server's.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.


Wireless -- Security
Manual Setup AP
broadcom
Disabled
WEP Encryption:
Disabled
Save/Apply

Mixed WPA2/WPA Authentication

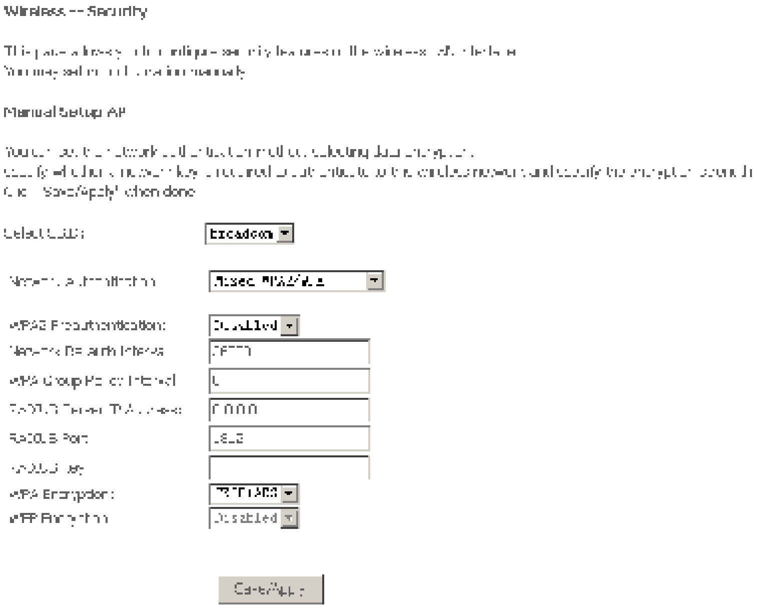
This authentication mode means AP auto adjust to use WPA2 or WPA according to wireless clients.

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA.
- = WPA2 Preauthentication: Selec Enable or Disenable.
- = Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If

the value set 0, no need to change. The change is done automatically between the server and the client.

- Radius Server IP Adress: Enter the IP Address of the authentication server.
- Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- Radius Key: Enter the same key as the Radius server’s.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



WPA-PSK Authentication

- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA-PSK.
- WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table

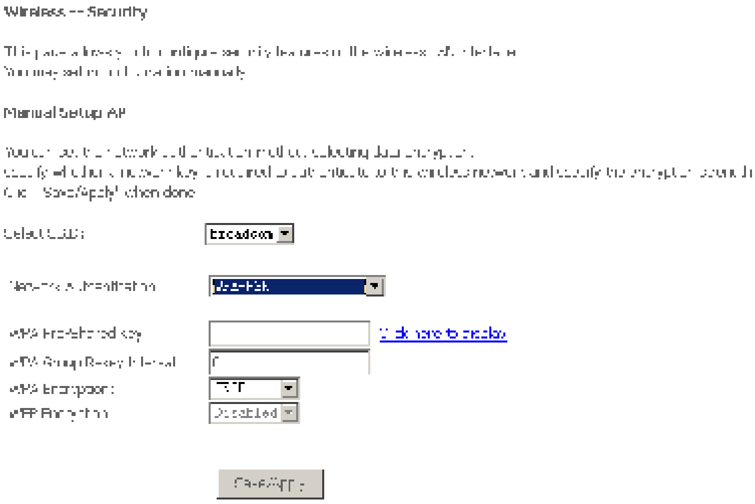
below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

= WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.

= WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

Manual Setup AP

WPA2-PSK Authentication

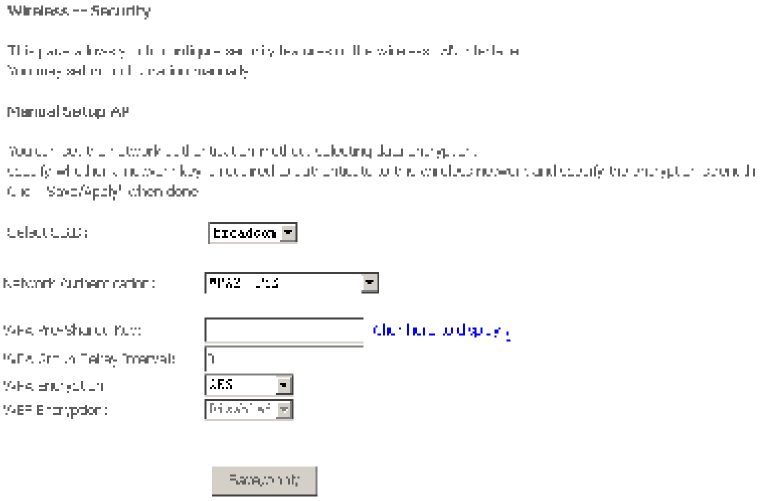
= Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2-PSK.

= WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

Manual Setup AP

Click "Save/Apply" when done.

Select SSID: broadcom

Network Authentication: WPA2 -PSK

WPA Pre-Shared Key:

WPA Group Rekey Interval: 0

WPA Encryption: AES

Mixed WPA2/WPA-PSK Authentication

This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients.

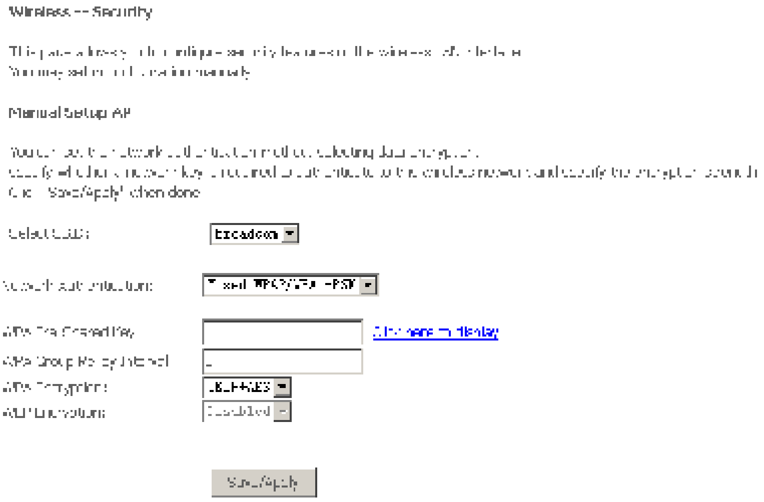
- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA-PSK.
- WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table

below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Wireless -- Security

Manual Setup AP

Select SSID: broadcom

Network Authentication: Mixed WPA2/WPA -PSK

WPA Pre-Shared Key:

WPA Group Rekey Interval: 0

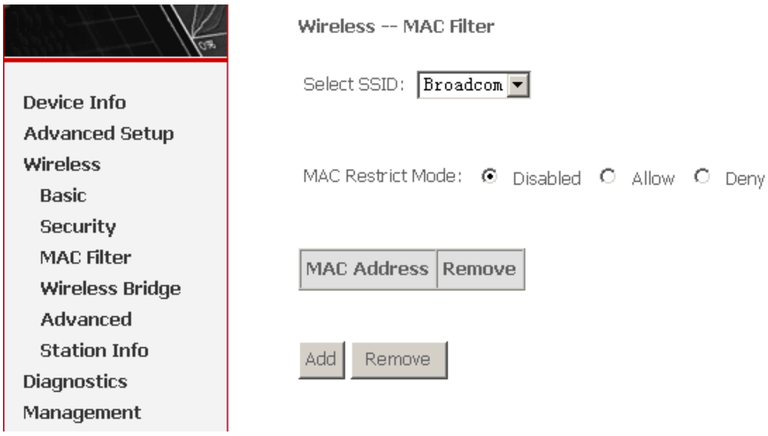
WPA Encryption: TKIP+AES

WEP Encryption: Disabled

3.5.4 Wireless - MAC Filter

The web page allows you to create a list of MAC addresses that are banned or allowed association with the wireless access point.

- = **MAC Restrict Mode: The function can be turn on/off,** Check **Disabled** to disable this function. Vice versa, to enable the function. After enabling the function, you can filter wireless users according to their MAC address, either allowing or denying access. Check **Allow** to make any wireless MAC address in the Wireless Access Control List can be linked to. And Check **Deny** to banned any wireless MAC address in the Wireless Access Control List to be linked to.


Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- MAC Filter

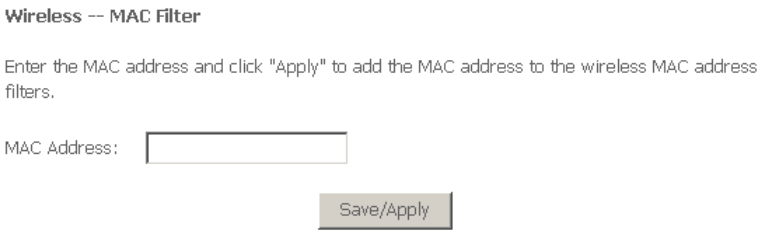
Select SSID: Broadcom

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

Add
Remove

= **Add a MAC Access Control:** To add a new MAC address to your wireless MAC address filters, click **Add** to show next page. Type in the MAC Address in the entry field provided. Click **Save/Apply** to add the MAC address to the list. The MAC address appears listed in the table below.



Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

= **Remove a MAC Access Control:** Select the **Remove** checkbox in the right column of the list for the MAC address to be removed and click **Remove**.

3.5.5 Wireless – Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface.

The Wireless Distribution System (WDS) allows you to extend the range of your wireless network by introducing one or more WDS-enabled devices into your wireless network. You can only establish WDS links with WDS-enabled devices.

- **AP Mode:** Select Access Point's functionality to be Access Point or pure Wireless Bridge. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality and Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
- **Bridge Restrict:** Select **Disabled** in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in Remote Bridges are granted access.

You can manually enter Remote Bridges MAC Address to the list. You can also do it automatically in the following steps:

Step 4 In the Bridge Restrict list, click Enabled (Scan).

Step 5 Click Refresh to update the remote bridges.

The router waits for a few seconds to update. And then lists the results in the Accessible Access Points table.

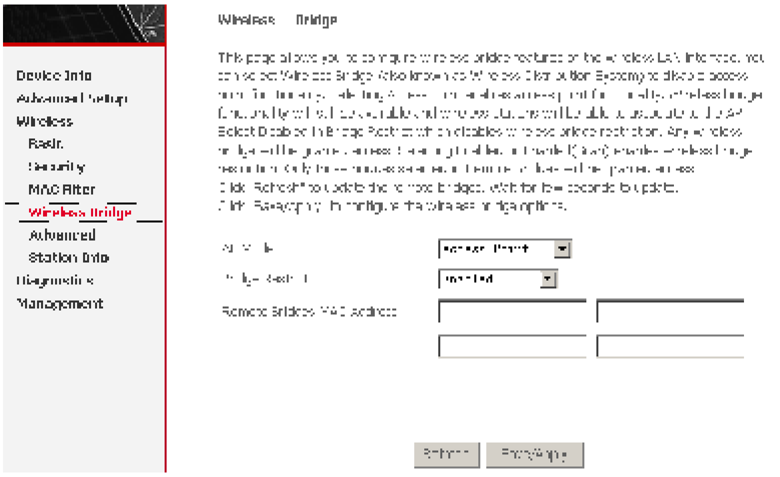
Step 6 Check on the box in the left column of the list for selecting the Access Point to which you want to establish a WDS connection.

Step 7 Click **Save/Apply**.

You must configure all Bridges Access Point with:

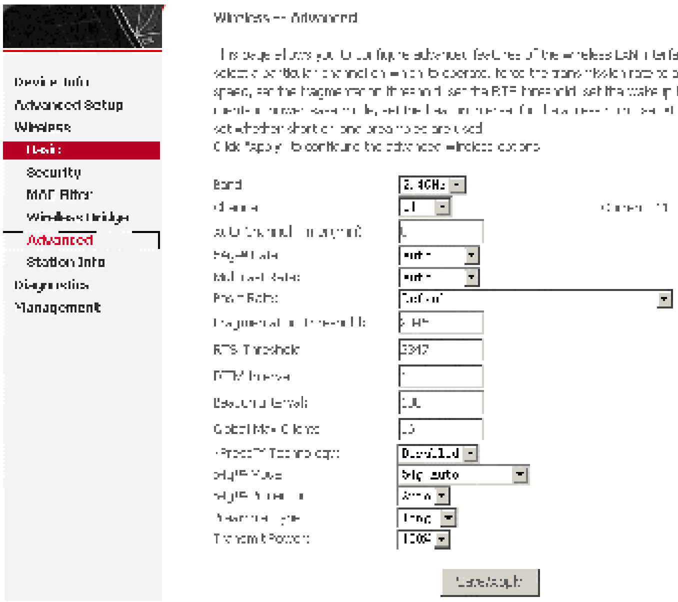
- The same encryption and authentication mode as Open, Shared, WEP, WPA-PSK or WPA2-PSK.
- The same fixed channel.

Click **Save/Apply** to configure the wireless bridge options and make the modification effect.


Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Wireless -- Bridge
Remote Bridges MAC Address

3.5.6 Wireless – Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.


Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Save/Apply

Wireless -- Advanced

Band 2.4GHz

RTS Threshold 2347

- **Band:** Select 802.11b/g using wireless frequency band range. The radio frequency remains at 2.437 GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. 11 is the default channel. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer(min):** Specifies the timer of auto channelling.
- **54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or

you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

= **Basic Rate:** Select the basic transmission rate ability for the AP.

= **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

= **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.

= **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

= **Beacon Interval:** Beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.

= **Global Max Clients:** Specifies maximum wireless client stations to be enble to link with AP.

= **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.

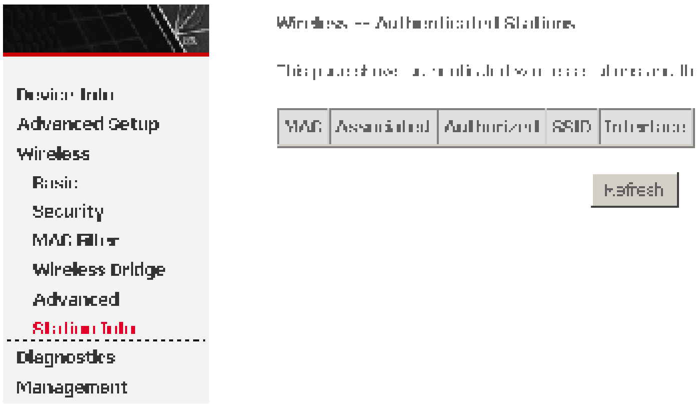
= **54g™ Mode:** Compatible with IEEE 802.11b, IEEE 802.11g. Select a Standards from the drop-down list box. Its default setting is 54g Auto. The drop-down list box includes below mode.

- **802.11b Only**: Only stations that are configured in 802.11b mode can associate. If you select it, the rate of transmission only has selected values: 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps. For other selections, the rate of transmission has lots of selected values: 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 9Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.
- **54g LRS**: This is a special compatibility mode for 802.11b/g and is in fact designed for older types of b-clients. Use this mode if you are experiencing problems with wireless clients that connect to the Access Point. If you select it, the preamble type will be disabled, which cannot be set.
- **54g Auto**: Only stations that are configured in 802.11b/g mode can associate.
- **54g Perfomance**: Only stations that are configured in 802.11g mode can associate. It is the same as 54g LRS, if you select it, the preamble type will be disabled, which cannot be set.
- **54g™ Protection**: The 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **Preamble Type**: Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble only if the 54g mode is set to 802.11b.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.

Click **Save/Apply** to configure the advanced wireless options and make the changes take effect.

3.5.7 Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status about Association and authentication.


Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Refresh

Wireless -- Authenticated Stations

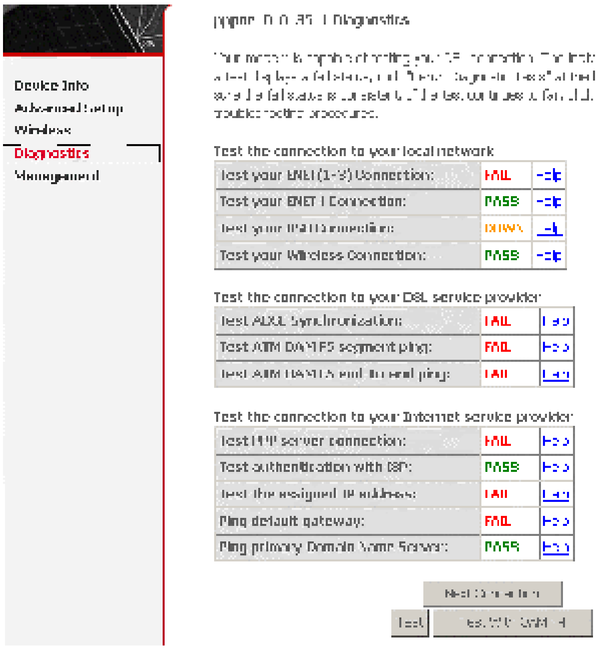
This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

3.6 Diagnostics

Click **Diagnostics** to show the interface.

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.


Device Info
Advanced Setup
Wireless
Diagnostics
Management
Next Connection
Test
Test With OAM F4

pppoe_0_0_35_1 Diagnostics

Test the connection to your local network

Test your ENET(1-3) Connection:	FAIL	Help
Test your ENET 1 Connection:	PASS	Help
Test your USB Connection:	DOWN	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test the connection to your Internet service provider

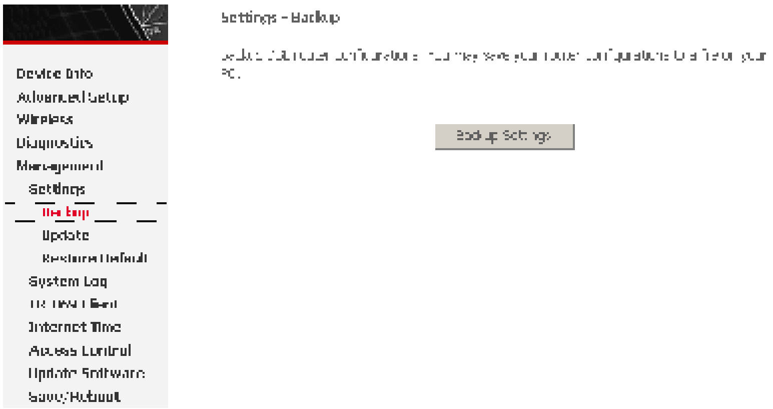
Test PPP server connection:	FAIL	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	PASS	Help

3.7 Management

3.7.1 Settings

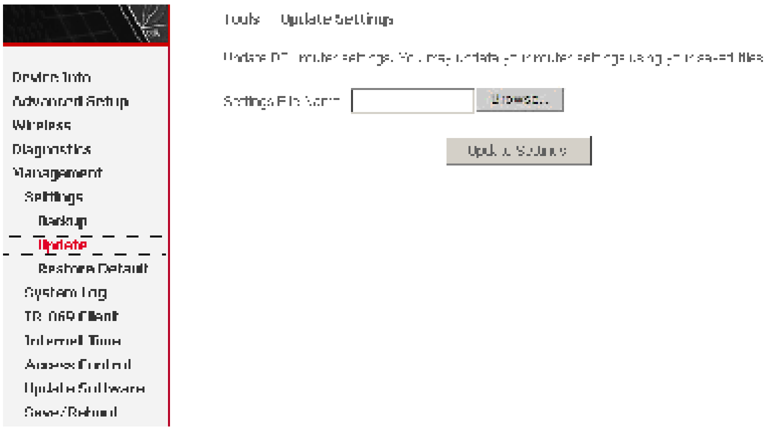
3.7.1.1 Settings Backup

Click **Backup Settings** to back up the DSL router configuration.


Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
Backup
Update
Restore Default
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Settings - Backup
Backup Settings

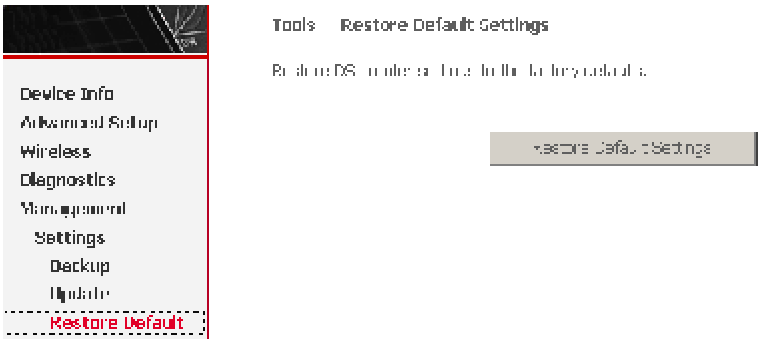
3.7.1.2 Settings Update

Click **Browser** and select the correct update configure settings file. Then, click **Update Settings** to update the modem settings.


Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
Backup
Update
Restore Default
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Tools -- Update Settings
Settings File Name:
Browse...
Update Settings

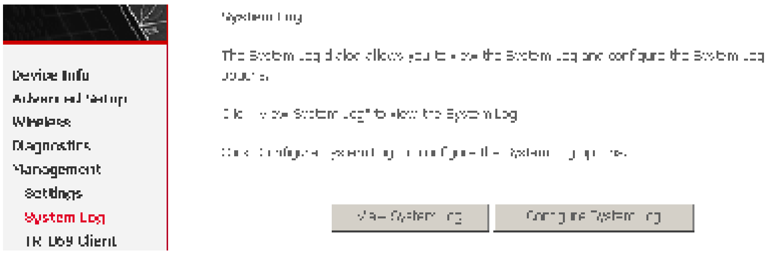
3.7.1.3 Settings Restore Default

Click **Restore Default Settings** to restore DSL router settings to the factory defaults.

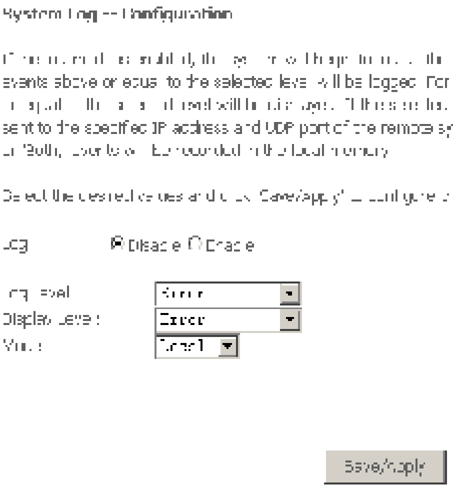

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
Backup
Update
Restore Default
Tools Restore Default Settings
Restore Default Settings

3.7.2 System Log

Click **System Log** to show the following interface. The system log dialog allows you to view the system log and configure the system log options.


Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
System Log
View System Log
Configure System Log

Click **Configure System Log** to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click **Apply** to end your configurations.



System Log -- Configuration

Log: ● Disable ○ Enable

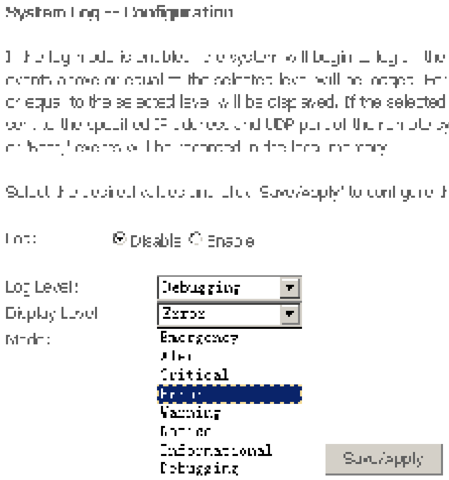
Log Level: Error

Display Level: Error

Mode: Local

Both the log level and display level have eight choices. The default log level is **Debugging** and the default display level is **Error**.

The mode options are **Local**, **Remote**, and **Both**. The default is **Local**.



System Log -- Configuration

Log: ● Disable ○ Enable

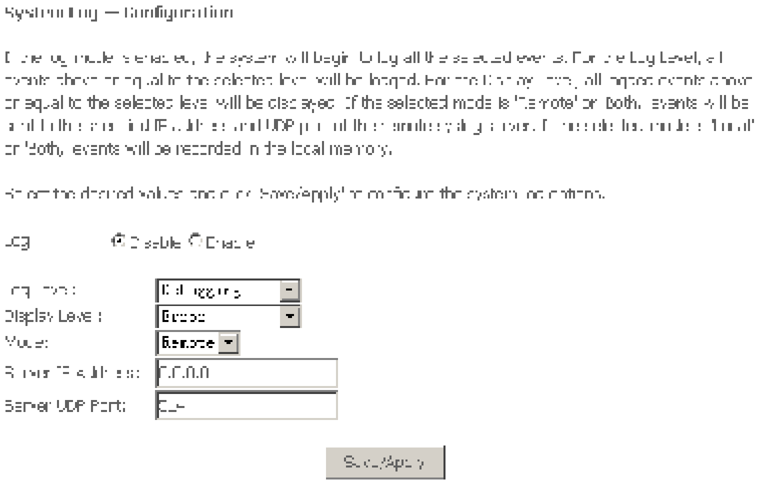
Log Level: Debugging

Display Level: Error

Mode:

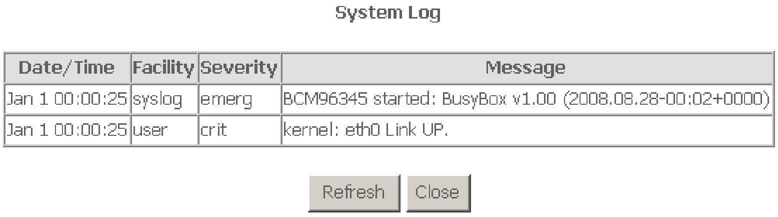
Emergency
Alert
Critical
Error
Warning
Notice
Informational
Debugging
Save/Apply

If you select **Remote** or **Both**, all events are transmitted to the specified UDP port of the specified log server.



After operations under **Configure System Log**, click **View System Log** to query the system logs. In this example, the **View System Log** is the default.

***Note**: The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as Debugging.*

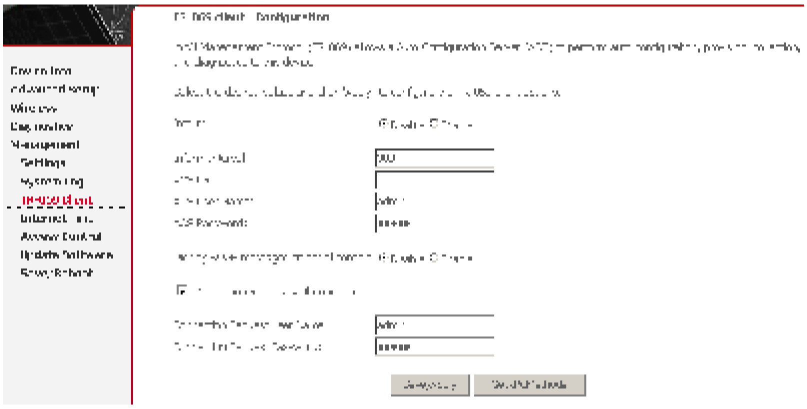

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:25	syslog	emerg	BCM96345 started: BusyBox v1.00 (2008.08.28-00:02+0000)
Jan 1 00:00:25	user	crit	kernel: eth0 Link UP.

Click **Refresh** to refresh the system event logs or click **Close** to exit from this interface.

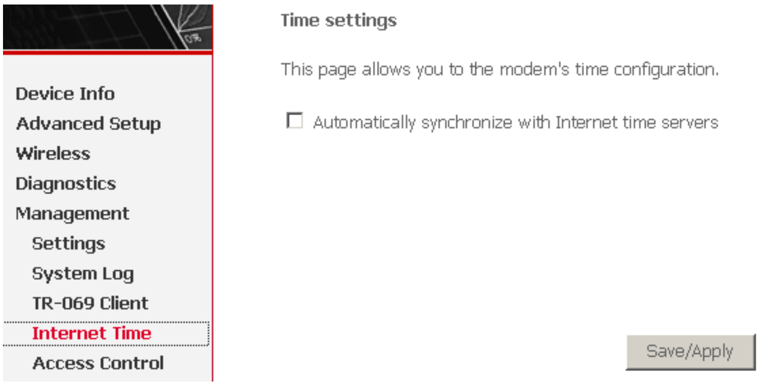
3.7.3 TR-069 Client

Select the desired values and click **Save/Apply** to configure the TR-069 client options.



3.7.4 Internet Time

Click **Internet Time** to show the following page. In this page, the modem can synchronize with Internet time servers.

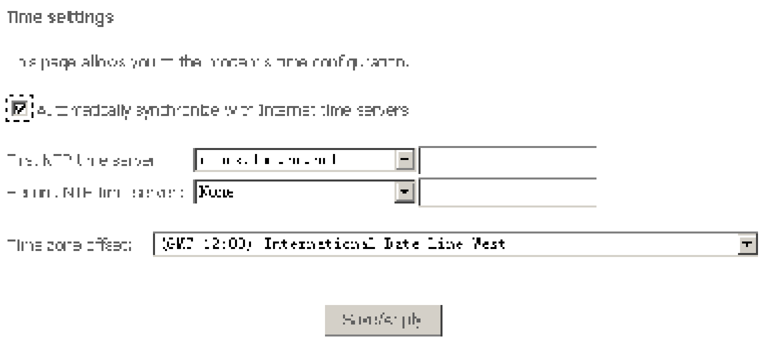

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Save/Apply

Time settings

This page allows you to the modem's time configuration.

☐ Automatically synchronize with Internet time servers

After enable **Automatically synchronize with Internet time servers**, the interface show below. Enter proper configurations and click **Save/Apply**.



Time settings

☑ Automatically synchronize with Internet time servers

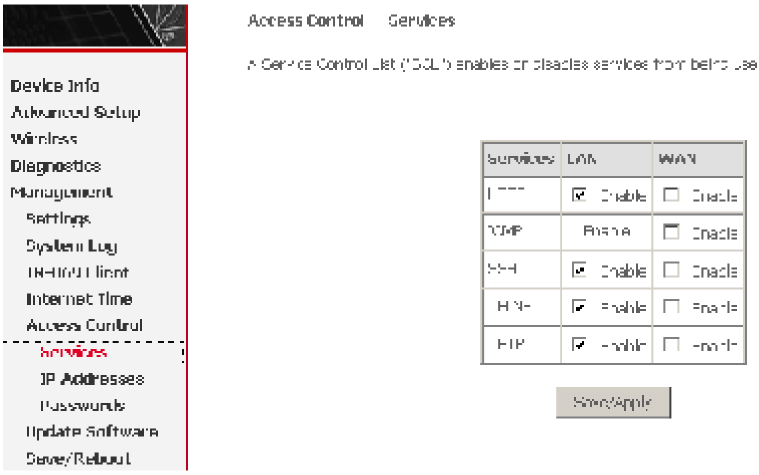
Second NTP time server: None

Time zone offset: (GMT-12:00) International Date Line West

3.7.5 Access Control

3.7.5.1 Access Control – Services

Click **Access Control** > **Services** to show the following interface. In the interface, you can enable or disable HTTP, ICMP, SSH, TELNET and TFTP services. And the LAN side and WAN side can have different configurations.



Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

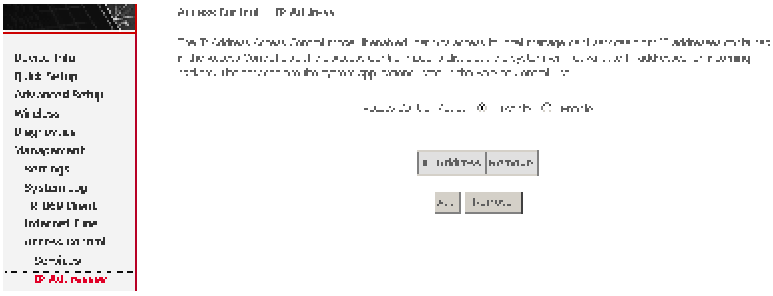
Services	LAN	WAN
HTTP	☑ Enable	☐ Enable
ICMP	Enable	☐ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☑ Enable	☐ Enable

Save/Apply

***Note**: If the connection is PPPoE PVC, you can view the information of WAN side.*

3.7.5.2 Access Control -- IP Addresses

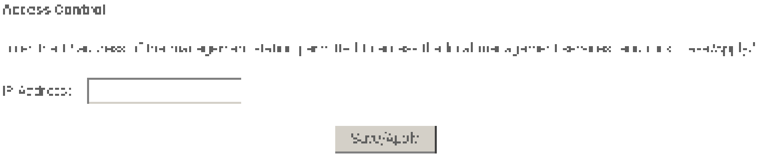
Click **Access Control** > **IP Addresses** to show the following interface.


Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
Internet Time
Access Control
Services
IP Addresses

If enabled, permits access to local management services from IP addresses contained in the Access Control List.

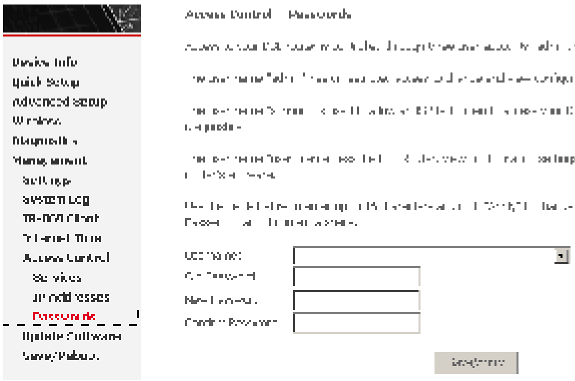
If the Access Control mode is disabled, the system does not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click **Add** to show the following interface. In the interface input the IP address of the management station permitted to access the local management services, and click **Save/Apply**.


Access Control
IP Address:
Save/Apply

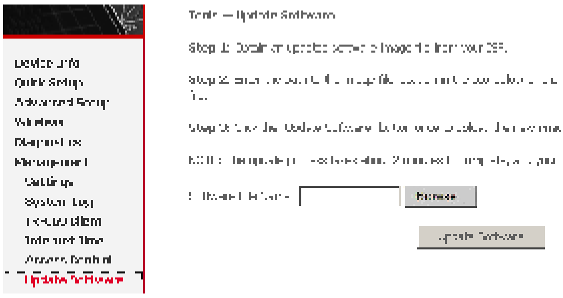
3.7.5.3 Access Control – Passwords

Click **Access Control** > **Passwords** to show the following interface. In the interface, you can modify the accounts passwords.


Access Control -- Passwords
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot

3.7.6 Update Software

Click **Update Firmware** to show the following interface. In this interface, you can update the modem firmware. Click **Browse** to find the right version file and click **Update Firmware** to update.

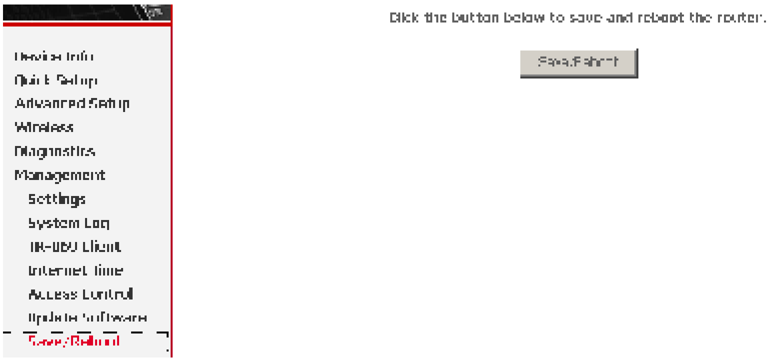

Tools -- Update Software
Browse
Update Software
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Update Software

Note*: Do not turn off your modem during firmware updates. When the update is finished, the modem reboots automatically. Do not turn off your modem either before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.*

After update software, it is suggested to restore the modem to the factory defaults and configure it again.

3.7.7 Save/Reboot

Click **Save/Reboot** to show the following interface. Click **Save/Reboot** to save and reboot the router.

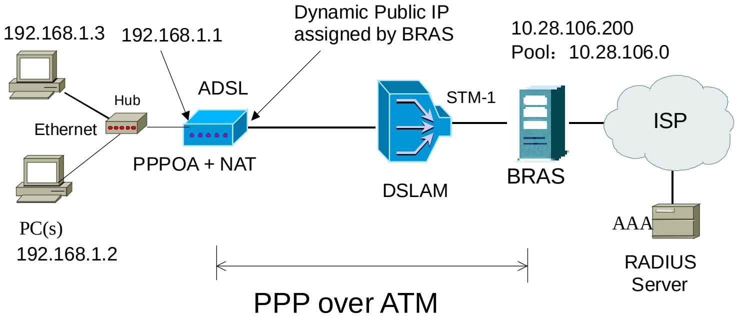

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Save/Reboot

Click the button below to save and reboot the router.

4 Networking Topology

Before configuring the Modem, you must clearly determine that the Modem is used for Bridging mode or Routing mode. This chapter introduces some applications. And see the Introductions to WEB Configuration Management for detailed configurations.

4.1 PPP over ATM (PPPoA) Mode


192.168.1.3
192.168.1.1
Dynamic Public IP
assigned by BRAS
10.28.106.200
Pool：10.28.106.0
Hub
ADSL
STM-1
ISP
Ethernet
PPPOA + NAT
BRAS
DSLAM
AAA
PC(s)
192.168.1.2
RADIUS
Server
PPP over ATM

Descriptions

In this example, the Modem is connected to the DSLAM through PVC 8/35 and the access mode is the built-in PPPOA+NAT. The encapsulation of the BRAS downlink port is PPP OVER ATM, the authentication is AUTO, the IP address is 10.28.106.200, the IP Pool is 10.28.106.*, and the IP address of uplink port is 10.61.92.157. The IP of the WAN port on the Modem is assigned by BRAS through the built-in PPPOA dial-up dynamically. The PC that the Modem is attached is assigned with a private IP address (within the same segment with the management IP of the Modem). The NAT functions of the Modem are enabled and the private PC address is translated to the public address 10.28.106.* (2 ~ 254) assigned by BRAS dynamically for accessing ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP server of the Modem. If it is assigned by DHCP server, the DHCP functions of the MODEM must be enabled. The IP address of the DHCP address pool is

192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting Procedure

Step 1 Activate your browser and enter *192.168.1.1* in the address bar to login in to the Modem.

Step 2 Click **Advanced Setup** > **WAN**, then click **Add**.

Step 3 In the **ATM PVC Configuration** interface, configure VPI/VCI as 8/35 and then click **Next**.

Step 4 In the **Connection Type** interface, select **PPP over ATM** (**PPPoA**) and **VC MUX** as the encapsulation, and then click **Next**.

Step 5 In the **PPP User name and Password** interface, enter the user name and password provided by your ISP. And then click **Next**.

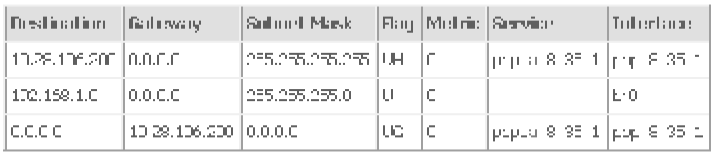
Step 6 In the **Enable IGMP Multicast and WAN Service** interface, keep the default configuration unchanged and then click **Next**.

Step 7 Check the network configurations and ensure that all settings comply with the information provided by your ISP, and then click **Save**.

Step 8 Click **Save/Reboot** to apply the changes and reboot the system.

You can also modify the PVC 8/35. If you need to modify the LAN IP address and DHCP server information, you can operate in **LAN** in **Advanced Setup**.

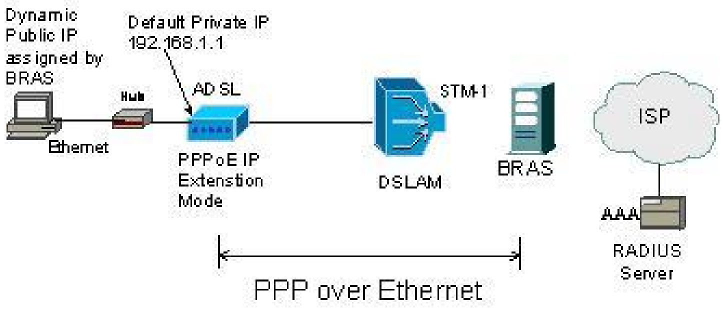
After the dial-up is complete, the IP address that the Modem obtains at the WAN-side port ppp_8_35_1. Query **Device Info** > **Route,** and the route interface is as follows.



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.28.106.200	0.0.0.0	255.255.255.255	UH	0	pppoa_8_35_1	ppp_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.28.106.200	0.0.0.0	UG	0	pppoa_8_35_1	ppp_8_35_1

After the built-in PPPoA dial-up is successful, the created WAN-side port is ppp_8_35_1.

4.2 PPP over Ethernet (PPPoE) Mode


Dynamic Public IP assigned by BRAS
Default Private IP 192.168.1.1
Hub
ADSL
Ethernet
PPPoE IP Extenstion Mode
STM-1
DSLAM
BRAS
ISP
AAA
RADIUS Server
PPP over Ethernet

Description

In this example, the modem is connected to the DSLAM through PVC 8/35 and the access mode is the built-in PPPOE+NAT. The encapsulation of the BRAS downlink port is PPP over Ethernet, the authentication is AUTO, the IP address is 10.28.106.200, the IP Pool is 10.28.106.*, and the IP address of uplink port is 10.61.92.157. The IP of the WAN port on the modem is dynamically assigned by BRAS through the built-in PPPOE dial-up. The PC attached to the modem is assigned with a private IP address (within the same segment as the management IP of the modem). The NAT function of the modem is enabled and the private address of the PC is translated to the public address 10.28.106.* (2~254) dynamically assigned by BRAS for accessing ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the modem. If it is assigned by the DHCP server, the DHCP functions of the modem must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting Procedure

Step 1 Open the Internet browser and enter ***192.168.1.1*** in the address bar to log in to the modem.

Step 2 Choose **Advanced Setup** > **WAN** and click **Add**.

Step 3 In the **ATM PVC Configuration** page, set VPI/VCI to 8/35 and click **Next**.

Step 4 In the Connection Type page, select PPP over Ethernet (PPPoE) and set the Encapsulation Mode to LLC/SNAP-BRIDGING, and then click Next.

Step 5 In the **PPP User name and Password** page, enter the user name and password provided by your ISP. Then, click **Next**.

Step 6 In the **Enable IGMP Multicast and WAN Service** page, keep the default settings and click **Next**.

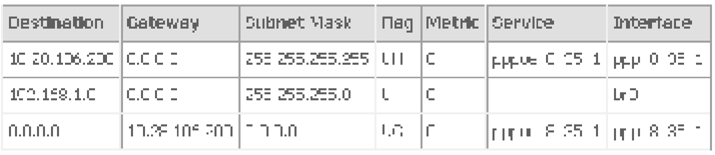
Step 7 Confirm the network configuration and ensure that all settings are consistent with the data provided by your ISP. Then, click **Save**.

Step 8 Click **Save/Reboot** to apply the changes and reboot the modem.

You can also modify the PVC 8/35. To modify the LAN IP address and DHCP server information, set in **LAN** in **Advanced Setup**.

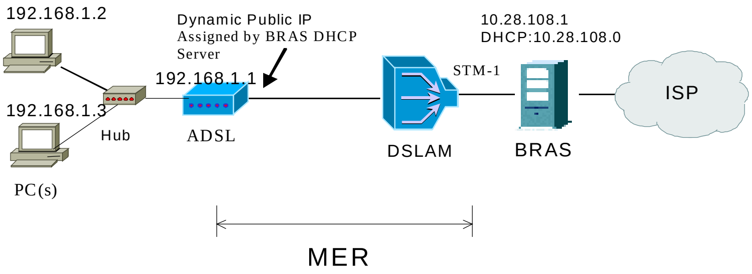
After the dial-up is successful, the modem obtains the IP address at the WAN-side port ppp_8_35_1.

Choose **Device Info** > **Route** and the route table is as follows.



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.20.136.200	0.0.0.0	255.255.255.255	UH	0	pppoe_8_35_1	ppp_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.20.136.200	0.0.0.0	UG	0	pppoe_8_35_1	ppp_8_35_1

4.3 MER + DHCP Mode


192.168.1.2
192.168.1.3
PC(s)
Hub
Dynamic Public IP
Assigned by BRAS DHCP
Server
192.168.1.1
ADSL
DSLAM
STM-1
10.28.108.1
DHCP:10.28.108.0
BRAS
ISP
MER

Description

In this example, the modem is connected to the DSLAM through PVC 8/35 and the access mode is the MER+NAT. The downlink interface of BRAS is encapsulated in 1483B, the IP address is 10.28.108.1 and the DHCP Server is enabled, the address pool is 10.28.108.* (2~254), and the IP address of the uplink interface is

10.61.92.157. The WAN IP address of the modem is automatically obtained through DHCP. The PC attached to the modem is assigned with a private IP address (within the same segment as the management IP address 192.168.1.1). The NAT functions of the modem is enabled and the private address of the PC is translated to the public address 10.28.108.* (2~254) dynamically assigned by BRAS for accessing ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP server of the modem. If it is assigned by the DHCP server, the DHCP functions of the modem must be enabled. The IP address of the DHCP address pool is 192.168.1.* (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting Procedure

Step 1 Open the Internet browser and enter *192.168.1.1* in the address bar to log in to the modem.

Step 2 Choose **Advanced Setup** > **WAN** and click **Add**.

Step 3 In the **ATM PVC Configuration** page, set **VPI/VCI** to **8/35** and click **Next**.

Step 4 In the **Connection Type** page, select **MAC Encapsulation Routing (MER)** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING**, and then click **Next**.

Step 5 In the WAN IP Settings page, select Obtain an IP address automatically, Obtain default gateway automatically and Obtain a DNS server address automatically. Then, click Next.

Note*: You can manually configure the WAN IP address, default gateway, and DNS server address.*

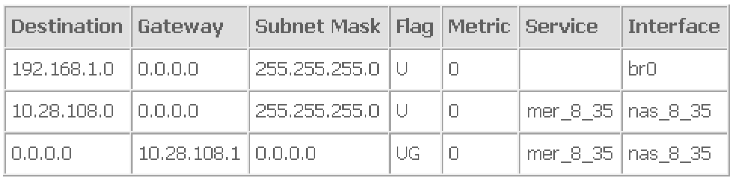
Step 6 In the **Network Address Translation Settings** page, enable the NAT and firewall. Keep default settings for other fields. Then, click **Next**.

Step 7 Confirm the network configuration and ensure that all settings are consistent with the data provided by your ISP. Then, click **Save**.

Step 8 Click **Save/Reboot** to apply the changes and reboot the modem.

You can also modify the PVC 8/35. To modify the LAN IP address and DHCP server information, set in **LAN** in **Advanced Setup**.

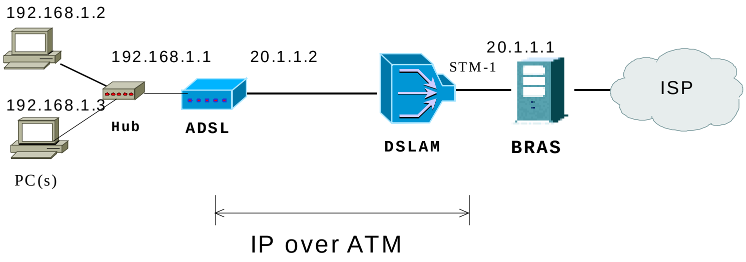
After the configuration is complete, the modem obtains the IP address at the WAN-side port nas_8_35. Choose **Device Info** > **Route** and the routing table is as follows.



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
10.28.108.0	0.0.0.0	255.255.255.0	U	0	mer_8_35	nas_8_35
0.0.0.0	10.28.108.1	0.0.0.0	UG	0	mer_8_35	nas_8_35

If **Enable NAT** is disabled during the configuration, you must configure the route on the BRAS. Otherwise, you cannot access your ISP. In actual application, **Enable NAT** must be selected.

4.4 IP over ATM (IPoA) + NAT Mode



Description

In this example, the modem is connected to the DSLAM through PVC 8/35 and the access mode is the IPOA+NAT. The downlink interface of BRAS is encapsulated in 1483R, the IP address is *20.1.1.1*, the IP address of the uplink interface is *10.61.92.157*, and the WAN IP address of the modem is assigned as *20.1.1.2*. The PC attached to the modem is assigned with a private IP address (within the same segment as the management IP address *192.168.1.1*) . The NAT functions of the modem is enabled, and the private address of the PC is translated into the public address 20.1.* (2~254) dynamically assigned by BRAS for accessing ISP.

The IP address of the PC can be fixed (as in this example) or assigned through DHCP Server of the modem. If it is assigned by DHCP server, the DHCP functions of the modem must be enabled. The IP address of the DHCP address pool is *192.168.1.** (2~254). The functions are enabled by default and at the same time the PC is configured to obtain IP and DNS addresses dynamically.

Setting Procedure

Step 1 Open the Internet browser and enter *192.168.1.1* in the address bar to log in to the modem.

Step 2 Choose **Advanced Setup** > **WAN** and click **Add**.

Step 3 In the **ATM PVC Configuration** page, set VPI/VCI to 8/35 and click Next.

Step 4 In the Connection Type page, select IP over ATM (IPoA) and set the Encapsulation Mode to LLC/SNAP-ROUTING, and then click Next.

Step 5 In the **WAN Setting**s page, enter the IP address, subnet mask, and DNS server address provided by your ISP. Do not select **Use the following default gateway**. Then, click **Next**.

WAN IP Address: *20.1.1.2*
WAN Subnet Mask: *255.255.255.0*
Primary DNS server: *168.95.1.1*
Secondary DNS server: *168.95.192.1*

Step 6 In the **Network Address Translation Settings** page, enable the NAT and firewall. Keep default settings for other fields. Then, click **Next**.

Step 7 Confirm the network configuration and ensure that all settings are consistent with the data provided by your ISP. Then, click **Save**.

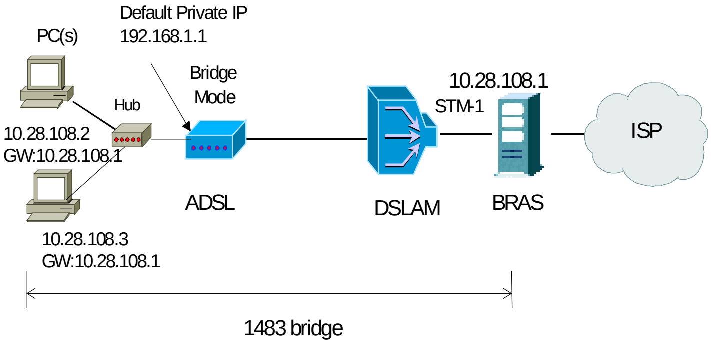
Step 8 Click **Save/Reboot** to apply the changes and reboot the modem.

You can also modify the PVC 8/35. To modify the LAN IP address and DHCP server information, set in **LAN** in **Advanced Setup**.

After the configuration is complete, the modem WAN-side interface is ipa_8_35.

If **Enable NAT** is disabled during the configuration, you must configure the route on the BRAS. Otherwise, you cannot access your ISP. In actual application, **Enable NAT** must be selected.

4.5 Leased Line Mode


Default Private IP
192.168.1.1
PC(s)
Bridge
Mode
Hub
10.28.108.2
GW:10.28.108.1
10.28.108.3
GW:10.28.108.1
ADSL
10.28.108.1
STM-1
DSLAM
BRAS
ISP
1483 bridge

Description

In this example, the modem is connected to the DSLAM through PVC 8/35 and the access mode is pure Bridging. The uplink interface of BRAS is encapsulated as 1483B, the IP address is *10.28.108.1*, and the IP address of the uplink interface is *10.61.92.157*. The PC attached to the modem is assigned a public IP address and the gateway is *10.28.108.1*.

Setting Procedure

Step 1 Open the Internet browser and enter *192.168.1.1* in the address bar to log in to the modem.

Step 2 Choose **Advanced Setup** > **WAN** and click **Add**.

Step 3 In the **ATM PVC Configuration** page, set VPI/VCI to 8/35 and click Next.

Step 4 In the Connection Type page, select Bridging and set the Encapsulation Mode to LLC/SNAP-BRIDGING, and then click Next.

Step 5 In the Unselect the check box below to disable this WAN service page, keep the default settings and click Next.

Step 6 Confirm the network configuration and ensure that all settings are consistent with the data provided by your ISP. Then, click **Save**.

Step 7 Click **Save/Reboot** to apply the changes and reboot the modem.

You can also modify the PVC 8/35. To modify the LAN IP address and DHCP server information, set in **LAN** in **Advanced Setup**.

Note*: In the pure Bridging mode, there is no interface at the WAN side of the modem.*

5 Q&A

(1) **Q**: Why all LED indicators are off?

A:

= Check the connection between the power adaptor and the power socket.

= Check the power switch is on or not.

(2) **Q**: Why Ethernet LED is not lighting?

A:

= Check the connection between the ADSL modem and your computer, hub, or switch.

= Check the running status of your PC, hub, or switch, and ensure that they are working normally.

(3) **Q**: Why DSL LED is not lighting?

A: Check the connection between the ADSL "LINE" port and the wall jack.

(4) **Q**: Why cannot visit Internet with ADSL LED is on?

A: Ensure that the following information is correctly entered.

= VPI/VCI

= Username/password.

(5) **Q**: Why cannot open the Modem Web configuration page?

A: Follow below steps to check the communication between the computer and modem.

= Choose **Start** > **Run** from the desktop, and ping *192.168.1.1* (the IP address of the modem).

= If the modem cannot be reached, please check following configuration:

- Type of the network cable
- Connection between the modem and computer
- TCP/IP configuration of you computer

(6) **Q**: How to load the default setting after incorrect configuration?

A:

= To restore the factory default, keep the device powered on and push a needle into the hole. Press down the button about 3 seconds and then release.

- The default IP address and subnet mask of the modem are *192.168.1.1* and *255.255.255.0* respectively.
- The Username and password are **admin** and **admin** respectively.

FCC Information

This equipment complies with CFR 47, Part 15.19 of the FCC rules. Operation of the equipment is subject to the following conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

This device must not be co-located or operating in conjunction with any other antenna or transmitter

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER’S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

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

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

---Reorient or relocate the receiving antenna.

---Increase the separation between the equipment and receiver.

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

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

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

Safety Information

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.