DSL-6540U
User Manual

VER: 1.0

Contents

1 Introduction

The VDSL DSL-6540U is a high-speed VDSL2 router, uplink rate up to 40 Mbps and downlink rate up to 80 Mbps. It provides sufficient bandwidth for high performance connection to the Internet, online gaming, video on demand (VOD), video conferencing, and high definition television (HDTV). It has Web-based graphic user interface (GUI), in which you can easily modify the settings and connect to your ISP. It also provides flow statistics, connection status, and other detailed information. The VDSL DSL-6540U is easily upgraded and provides terminal users and ISP with the guarantee of future.

The VDSL DSL-6540U provides one RJ11 telephone interface, one RJ45 Ethernet WAN interface, four RJ45 Ethernet LAN interfaces. The telephone interface is used for connecting to the Internet provided by the telecom carrier. The Ethernet is used for connecting to computers, through which you can access the Internet. Computers that are connected with the router through the Ethernet can establish a small local network area (LAN). Those computers can communicate with each other, sharing resources and files. The VDSL DSL-6540U is an ideal broadband CPE solution for both home users who wish to share high-speed Internet access and small offices that wish to do business on the Internet.

1.1 Application

- VOD and video-conferencing
- Network online gaming
- IP over television (IPTV)and HDTV
- High Internet access sharing
- High rate broadband sharing
- Small enterprises application
- Home networking application

1.2 Features

- User-friendly GUI for web configuration
- Support IPSec for virtual private network (VPN)
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Configurable as a DHCP server on your network
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Support virtual server, IP filter, DMZ host, and much more
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 16 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support SNMP v2, RIP v1 & RIP v2, NAT

1.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- 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+)
- ITU G.993.1 (VDSL)
- ITU G993.2 (VDSL2)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u

1.4 Safety Cautions

Follow the following announcements 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 dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation 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.

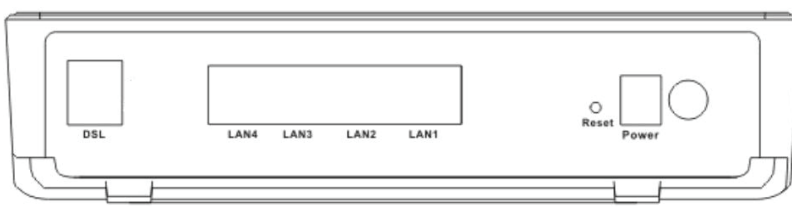
1.5 LED Status Description

1.5.1 LED Status

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 self-testing of the power fails if the LED is always red.
	Blink Red	Upgrading software.
VDSL	Off	No signal is detected.
	Blink Green	The VDSL line is transferring.

Indicator	Status	Description
	Green	The DSL line connection is established.
Internet	Off	No internet connection.
	Blink Red	The DSL line tries to activate or fails to activate.
	Blink Green	Data is being transmitted through the WAN interface.
	Green	The connection is established. The users can access the Internet.
LAN1/2/3/4	Off	No Ethernet signal is detected.
	Blink Green	The user data is passing through Ethernet port.
	Green	Ethernet interface is ready to work

1.5.2 Rear Panel



Interface	Description
VDSL	VDSL connector, for connecting to VDSL telephone line.
LAN1/2/3/4	LAN interface, for connecting to a computer or switch.
Reset	Keep power on, put a thin needle in-to the hole to press the button for about 1 second, then the device restores to the factory default configuration.
Power	Power supplied port, for connecting the power adapter. The power adapter output is: 12 V DC, 1A.
⏻	Power switch.

2 Hardware Installation

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. Place the DSL Router in a location where it can be connected to the various devices as well as to a power source. The DSL Router should not be placed where it is exposed to moisture or excessive heat. Ensure the cables and power cord are placed safely to avoid tripping hazard. As with any electrical appliance, observe common sense safety procedures.

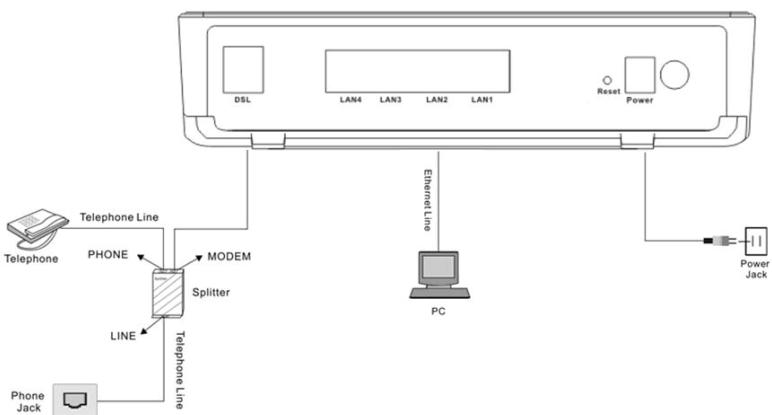
2.1 Connecting the DSL Router

Step 1 See the following figure. Connect the DSL port of the Router with a telephone cable.

Step 2 Connect the LAN port of the DSL Router to the network card of the PC via an Ethernet cable.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the DSL Router.

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



2.2 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

3.1 About DSL router

DSL router is a scalable suite of software infrastructure and technologies that original equipment manufacturers (OEMs) require in order to bring residential gateways to market.

DSL router leverages a wide range of compelling broadband-based applications and services and includes an operating system, drivers, and remote management capabilities. DSL router delivers a set of highly integrated solutions, required for homes and small companies, such as:

- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM/PTM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Virtual private network (VPN): IPSec
- Secure socket layer virtual private network (SSL VPN)
- Universal plug-and-play
- File server for network attached storage (NAS) devices
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Simple network management protocol (SNMP)

- Command line interface (CLI)
- TR-069 WAN management protocol
- TR-064-LAN-side DSL CPE configuration

- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modem and bridge.

3.2 Setup

Connecting your computer or home network to the DSL router is a simple procedure, varying slightly depending on the operating system. This chapter guides you to seamlessly integrate DSL router with your computer or home network. The Windows default network settings dictate that in most cases the setup procedure described as follows is unnecessary. For example, the default DHCP setting in Windows 2000 is 'client', requiring no further modification. However, it is advised to follow the setup procedure described as follows to verify that all communication parameters are valid and that the physical cable connections are correct. The setup procedure consists of three consecutive configuration stages:

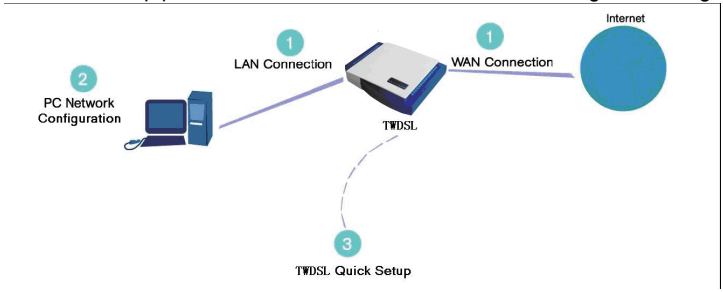


Figure 1 Hardware configuration

(1) Setting up WAN and LAN connections
(2) PC network configuration
(3) DSL router quick setup, via Web-based management

3.2.1 Setting Up WAN and LAN Connections

WAN Connection

Your can connect DSL interface of the router to the wall socket by using a telephone cable. If it has an Ethernet socket for the wide area network (WAN), connect it to the external modem you have, or to the Ethernet socket you might have, by using an Ethernet cable.

LAN Connection

The connection is Ethernet, with most platforms featuring four such ports. Use an Ethernet cable to connect an Ethernet port of your DSL router and the network card of your computer.

3.2.2 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box as it appears on Windows XP.

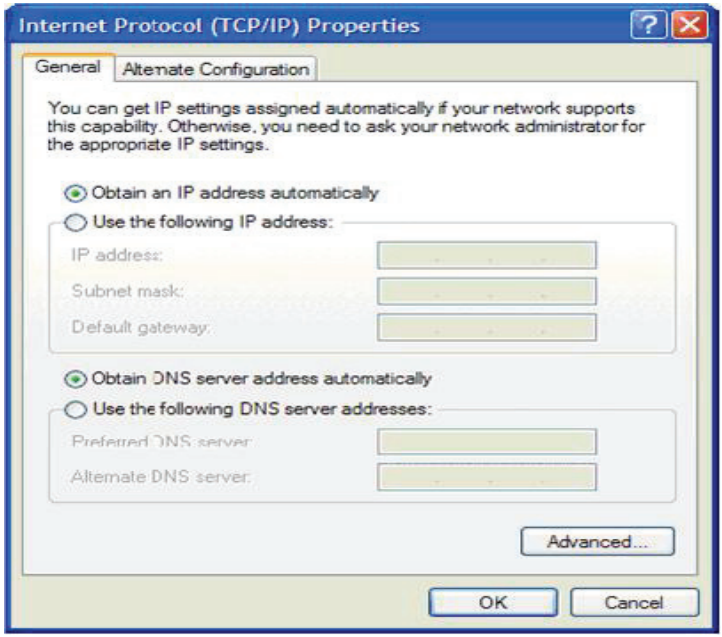


Figure 2 IP and DNS configuration

TCP/IP configuration instructions for Windows XP are as follows.

Step 1 Choose **Start** > **Control Panel** > **Access Network Connections** from the desktop.

Step 2 Right-click the Ethernet connection icon and choose **Properties**.

Step 3 On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step 4 The **Internet Protocol (TCP/IP) Properties** window appears.

Step 5 Select the **Obtain an IP address automatically** radio button.

Step 6 Select the **Obtain DNS server address automatically** radio button.

Step 7 Click **OK** to save the settings.

4 Web-Based Management

Note:

This project is hardware project, the Web interface of software is for reference only.

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

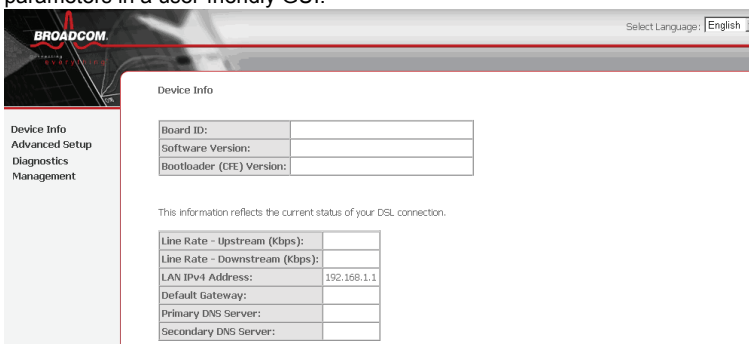


Figure 3 Web-based management - home page

4.1 Logging In to the Modem

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

4.1.1 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://192.168.0.1* (default IP address of the DSL router) 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 **(blank)**. 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.

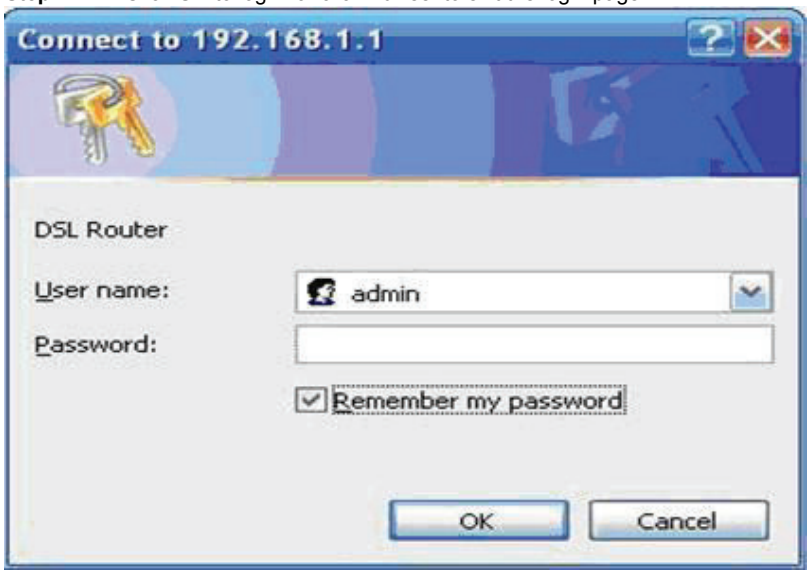


Figure 4 WBM login authentication

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

4.2 DSL Router Device Information

Choose **Device Info**, the following page appears.

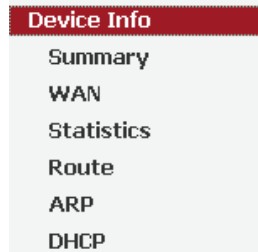
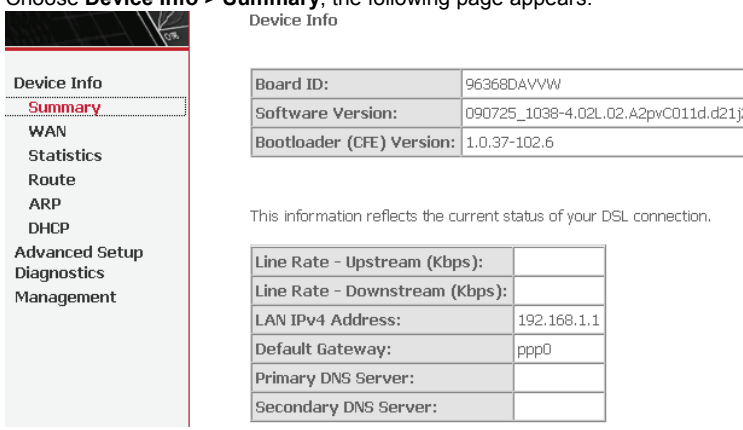


Figure 5 Device Info menu

4.2.1 Summary of Device Information

Choose **Device Info > Summary**, the following page appears.



- **LAN IPv4 Address:** the management IPv4 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 address:** 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.

4.2.2 WAN Interface Information

Choose **Device Info > WAN** and the following page appears.

WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
atm1	br_0_0_35	Bridge	Disabled	Disabled	Disabled	Disabled	Connecting	
ppp0	pppoe_0_0_32	PPPoE	Disabled	Enabled	Enabled	Enabled	Connecting	

- **Description:** Descripte this interface with protocol and PVC.
- **Type:** The connection type of WAN, such as PPPoE, PPPoA.

4.2.3 Statistics

This page contains the following four parts:

- Statistics of LAN
- Statistics of WAN Service
- Statistics of ATM
- Statistics of xDSL

4.2.3.1 Statistics of LAN

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

Statistics -- LAN

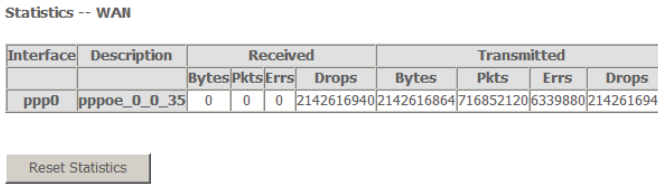
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	302961	3159	0	0	4146047	4336	0	0
eth1	0	0	0	0	0	0	0	0
usb0	0	0	0	0	0	0	0	0

Reset Statistics

Figure 6 Statistics of LAN

4.2.3.2 Statistics of WAN

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


Statistics -- WAN

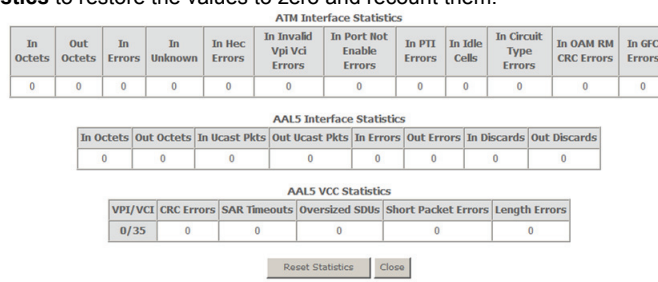
Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0	pppoe_0_0_35	0	0	0	2142616940	2142616864	716852120	6339880	2142616940

Reset Statistics

Figure 7 Statistics of WAN

4.2.3.3 Statistics of ATM

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


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
0	0	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0

Reset Statistics Close

Figure 8 Statistics of ATM

4.2.3.4 Statistics of xDSL

Choose **Device Info > Statistics** > **xDSL** and the following page appears.
If the DSL line is activated, the following window appears.

Statistics -- xDSL

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

xDSL BER Test Reset Statistics

- **Traffic Type:** ATM, or PTM.
- **Status:** Link Down, NoSignal, Training
- **Link Power State:** L0, L1, L2
- **Line Coding:** Trallis on, etc.
- **Rate (Kbps):** Upstream Line Rate/Downstream Line Rate.

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

Click **xDSL BER Test** to test xDSL Bit Error Rate.

4.2.3.5 xDSL BER Test

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

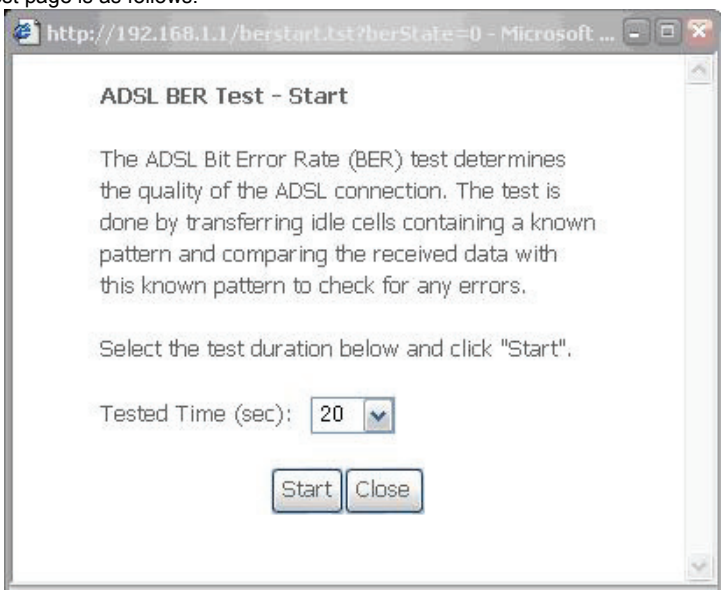


Figure 9 ADSL BER test

The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360.

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

4.2.4 Route Table Information

Choose **Device Info > Route** and the following page appears.

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
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 10 Route table

4.2.5 ARP Table Information

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

Device Info -- ARP

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

Figure 11 ARP table

4.2.6 DHCP IP Lease Information

Choose **Device Info > DHCP** and the following page appears. You can query the IP address assignment for MAC address at the LAN side of the DSL router and obtain the IP Address from the DHCP server through Ethernet in the DSL router.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

Figure 12 DHCP leases list

- **Expires In:** Time that the device leases the IP Address for the MAC Address.

4.3 Advanced Setup

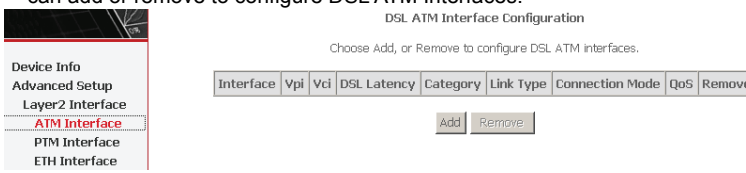
4.3.1 Layer2 Interface

Choose **Advanced Setup** > **Layer2 Interface** and three items appear.

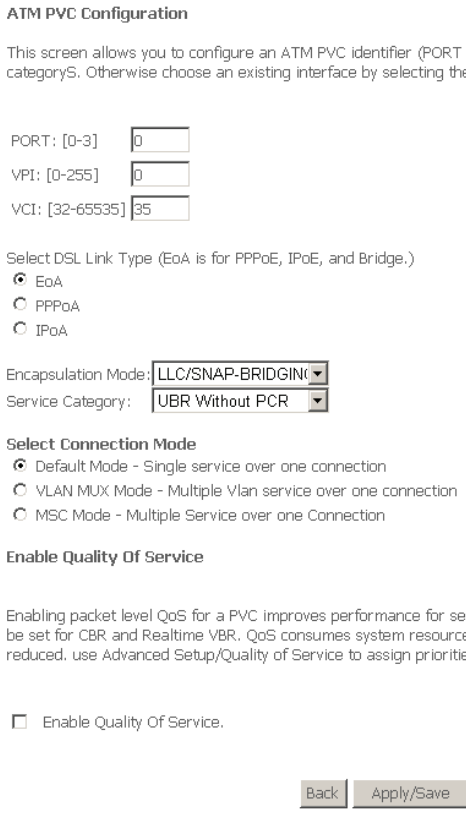
- ATM Interface
- PTM Interface
- ETH Interface

4.3.1.1 ATM Interface

Choose **Advanced Setup** > **Layer2 Interface > ATM Interface** . In this page, you can add or remove to configure DSL ATM Interfaces.



Click **Add** to add ATM Interface and the following page appears.



In this page, you can enter this PVC (VPI and VCI) value, and select DSL link type (EoA is for PPPoE, IPoE, and Bridge.), encapsulation mode, service category, connection Mode.

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **DSL Link Type**: EoA (it is for PPPoE, IPoE, and Bridge), PPPoA, or IPoA

- **Encapsulation Mode**: LLC/SNAP-BRIDGING, or VC/MUX
- **Service Category:** UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR.
- **Connection Mode:** Default mode, VLAN MUX mode, or MSC mode
- **Enable Quality Of Service:** enable/disable.

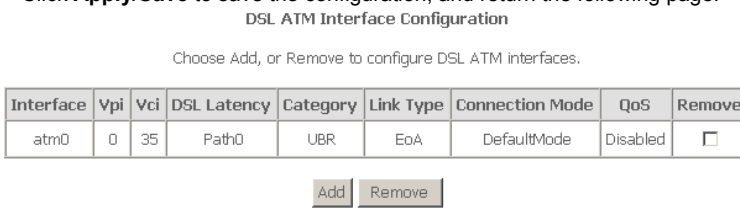
In actual applications, you can modify them depending on your requirement.

You can also select the **Enable Quality Of Service** check box in to enable the packet level QoS for a PVC. This improves performance for selected classes of applications.

Note:

QoS cannot be set for CBR and Realtime VBR.

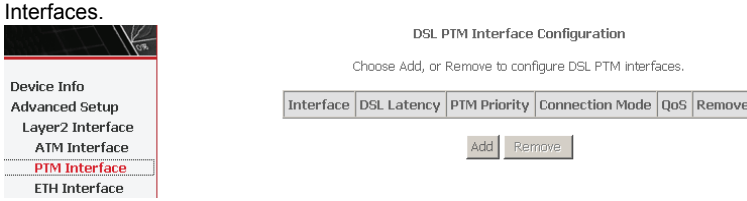
Click **Apply/Save** to save the configuration, and return the following page:



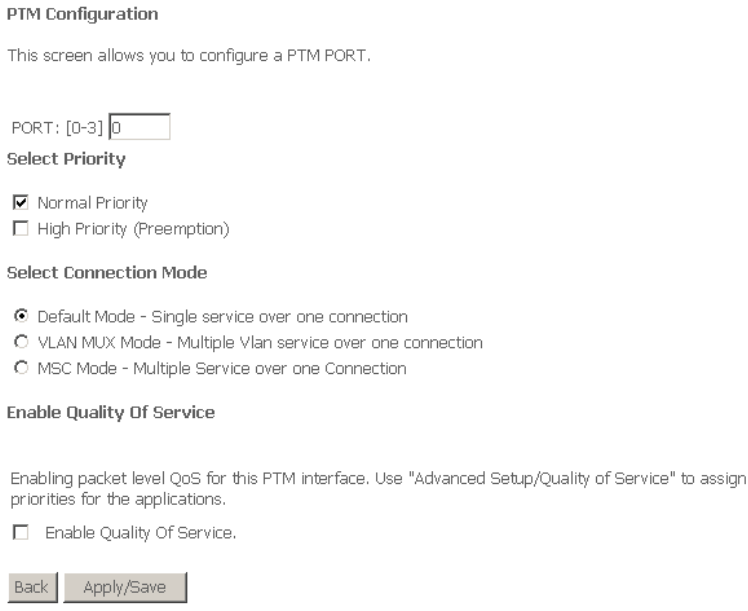
If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

4.3.1.2 PTM Interface

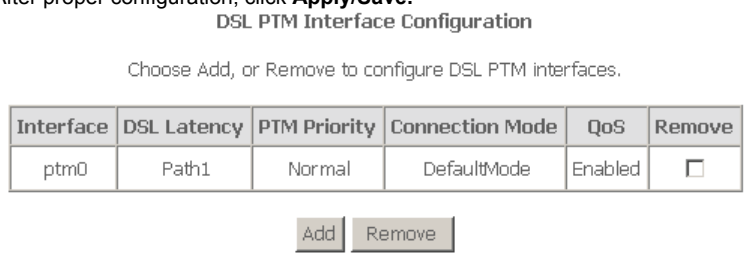
Choose **Advanced Setup** > **Layer2 Interface > PTM Interface**, and the following page appears. In this page, you can add or remove to configure PTM WAN Interfaces.



Click **Add** to add PTM Interface and the following page appears.

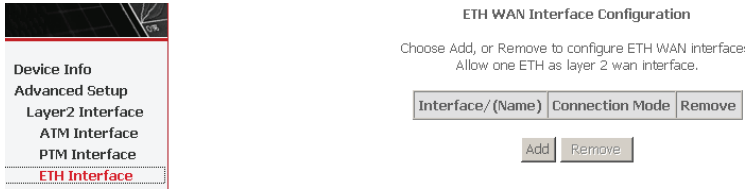


After proper configuration, click **Apply/Save.**

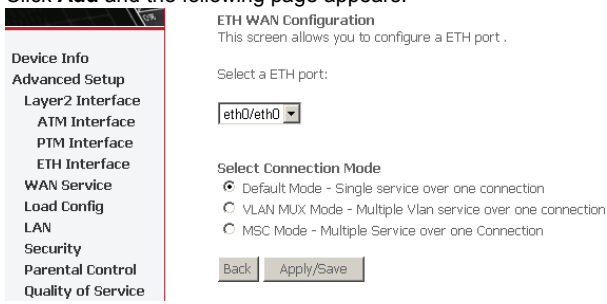


4.3.1.3 ETH Interface

Choose **Advanced Setup** > **Layer2 Interface > ETH Interface**, and the following page appears. In this page, you can add or remove to configure ETH WAN Interfaces.



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



In this page, you can select a ETH port, such as eth0/ENET4, and select connection mode. Click **Apply/Save** to save configuration.

4.3.2 WAN Configuration

Choose **Advanced Setup** > **WAN Service,** and the following page appears.

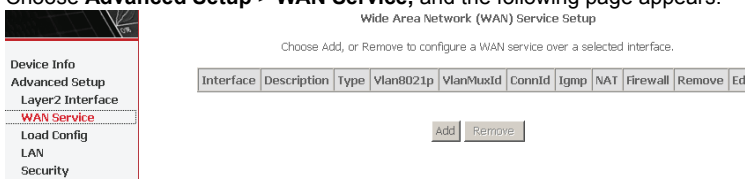


Figure 13 WAN configuration

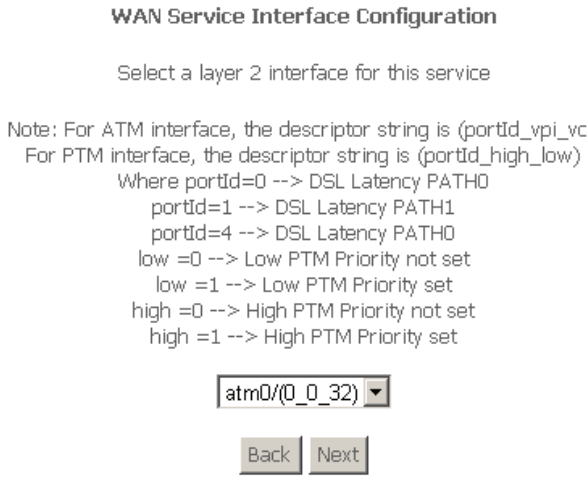
Click **Add** to configure PPPoE, PPPoA, Mer (IPoE), Bridge, IPoA WAN configuration.

Note: ETH and PTM/ATM sevice can not be coexist.

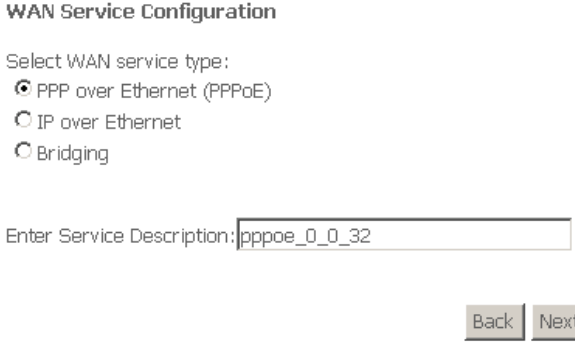
4.3.2.1 Adding a PPPoE WAN Configuration

In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding pppoe_0_0_32 (PPPoE mode).

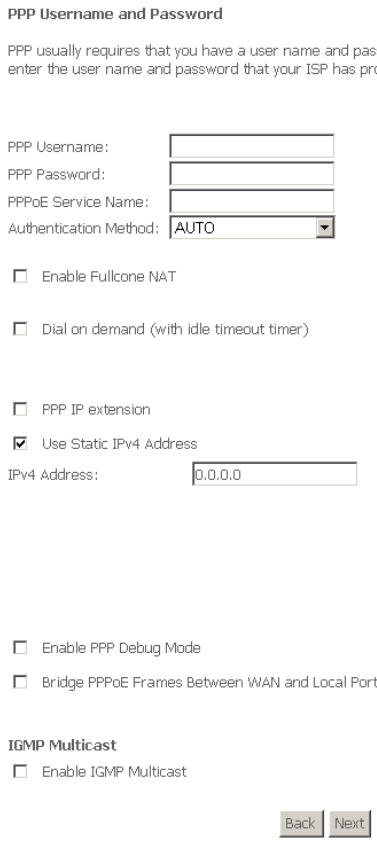
Step 1 Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.) In this page, you can select ATM Interface .



Step 2 After proper selection, click **Next**, and the following page appears.



Step 3 In this page, select WAN service type **PPP over Ethernet(PPPoE)**. Click **Next**, and the following page appears.

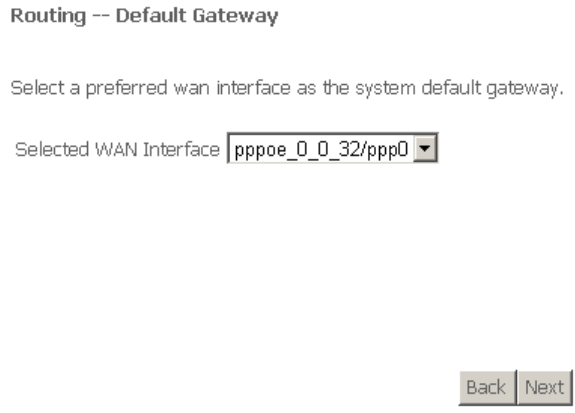


Step 4 In this page, you can modify the PPP username, PPP password, and authentication method.

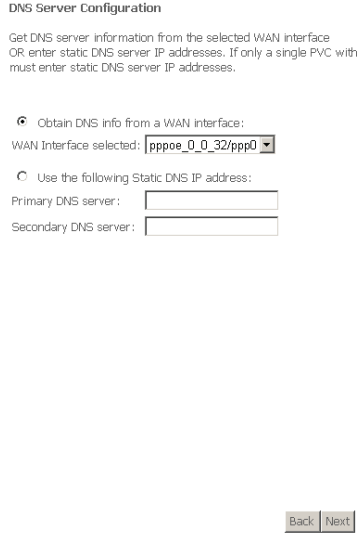
- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.

- **Enable Fullcone NAT:** A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **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:** After **PPP IP extension** is enabled, the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached with the modem (at this time, the modem has only one PC). From the view of the PC user, this is even with that 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 automatically.
- **Use Static IPv4 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.
- **IGMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

After enter the PPP Username and PPP Password, click **Next**, and the following page appears.

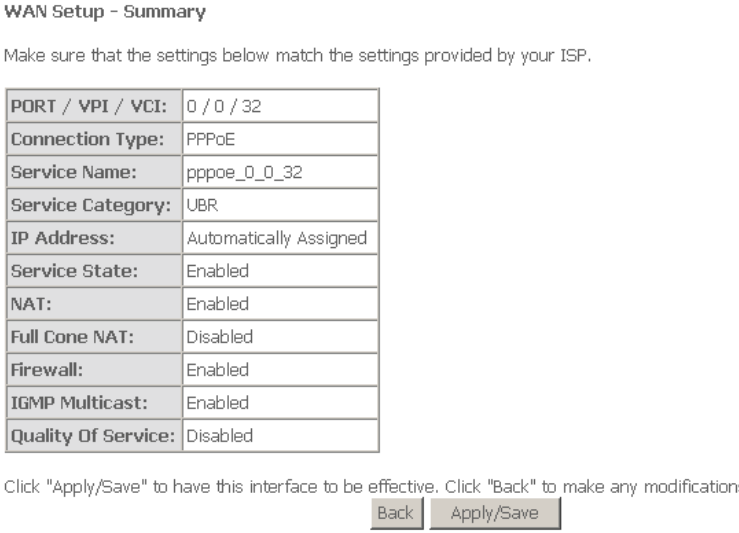


Step 5 In this page, select a preferred WAN interface as the system default gateway. Click **Next,** and the following page appears.

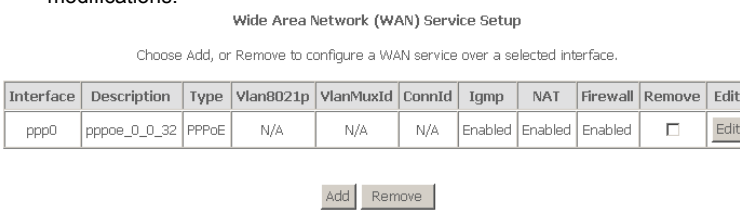


Step 6 In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC

with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next**, and the following page appears.



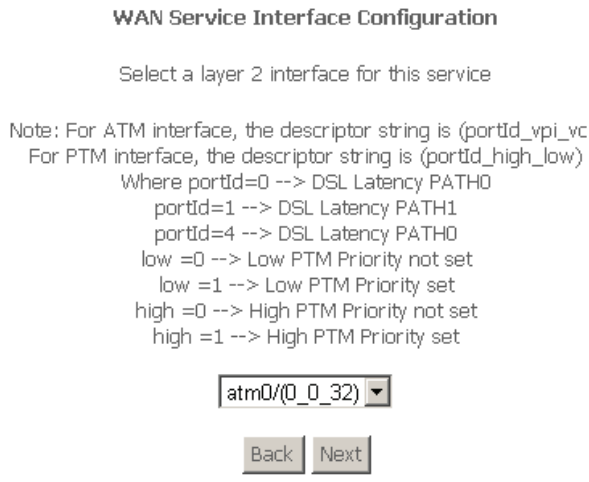
Step 7 In this page, it shows all the configurations. Click **Apply/Save** to all the configurations, and the following page appears. Click **Back** to make any modifications.



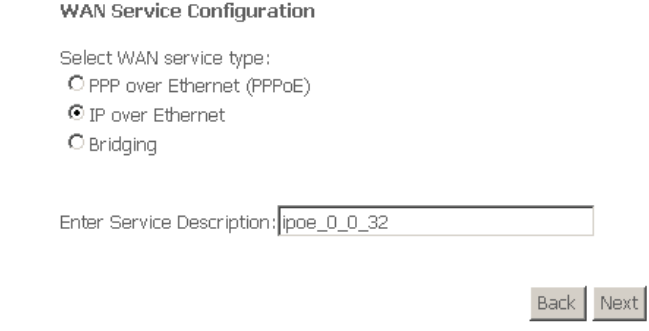
4.3.2.2 Adding a MER (IPoE) Configuration

In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding ipoe_0_0_32 (Mer mode).

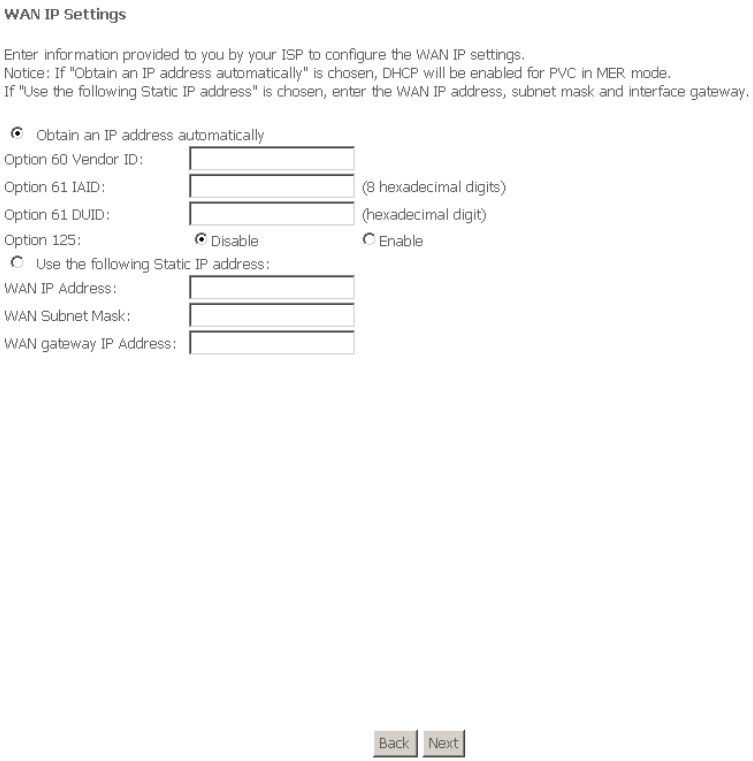
Step 1 Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.)



Step 2 Select an ATM Interface, such as atm0/ (0_0_32). Click **Next** and the following page appears.

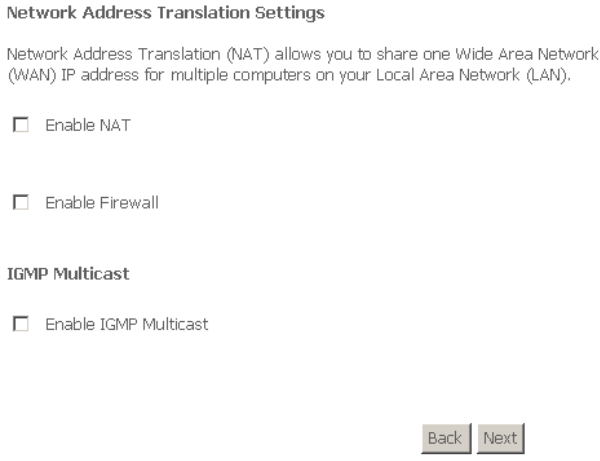


Step 3 In this page, you can modify the **WAN service type** and **Service Description**. Click **Next** and the following page appears.

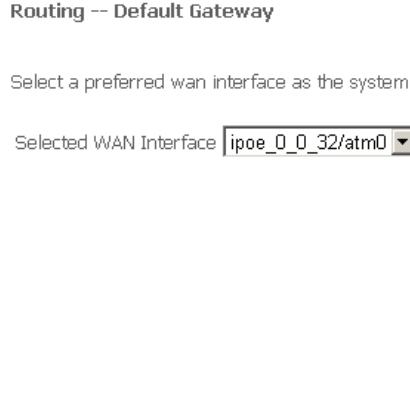


Step 4 In this page, you can modify the **IP Settings**. Enter information provided by your ISP to configure the WAN IP settings. Click **Next** and the following page appears.

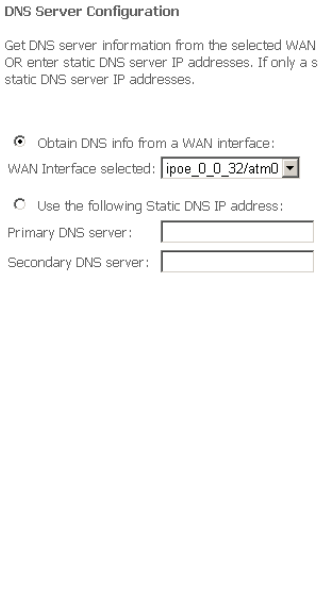
Note: If select Obtain an IP address automatically is chosen, DHCP will be enabled for PVC in MER mode.
If Use the following Static IP address is chosen, enter the WAN IP address, subnet mask and interface gateway.



Step 5 In this page, you can modify the **Network Address Translation Settings.** Click **Next** and the following page appears.



Step 6 In this page, select a preferred wan interface as the system default gateway. Click **Next** and the following page appears.



Step 7 In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next** and the following page appears.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 32
Connection Type:	IPoE
Service Name:	ipoe_0_0_32
Service Category:	UBR
IP Address:	192.168.1.12
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

Step 8 In this page, click **Apply/Save** to save all the configurations, and the following page appears. If you want to make any modifications, click **Back**.

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

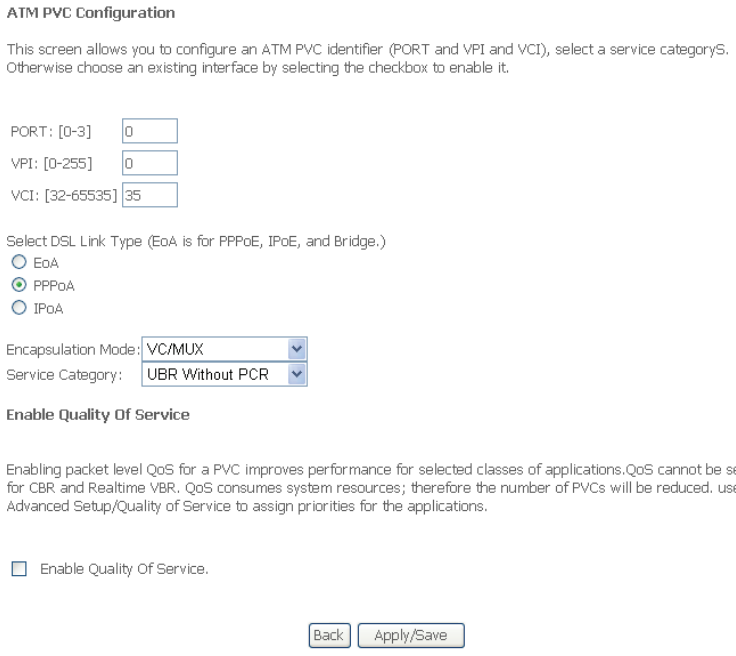
Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
atm0	ipoe_0_0_32	IPoE	N/A	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit

Add Remove

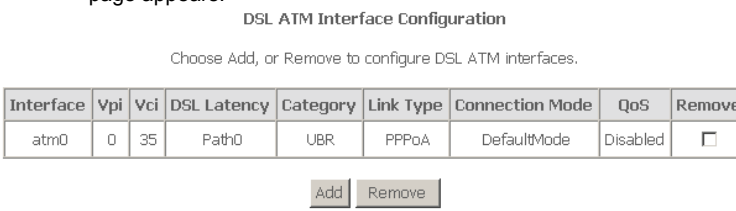
4.3.2.3 Adding a PPPoA Configuration

This section describes the procedure for adding pppoa_0_0_35 (PPPoA mode).

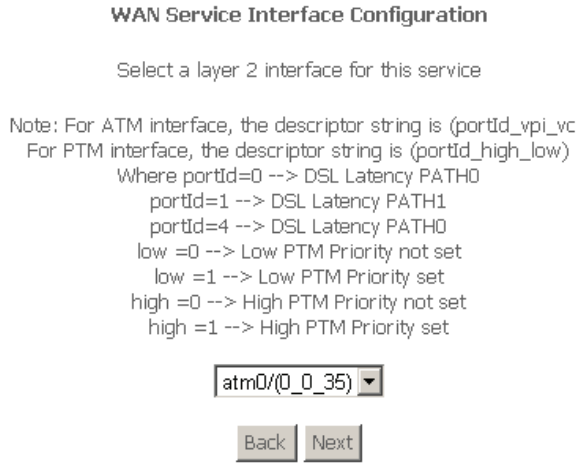
Step 1 You need to open the **Layer2 Interface > ATM Interface** page to add a PVC for PPPoA mode. Click **Add** and the following page appears.



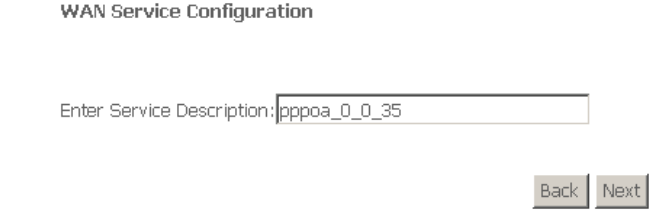
Step 2 Select the DSL link type to **PPPoA,** the Encapsulation Mode to **VC/MUX** (according to the uplink equipment). Click **Apply/Save,** and the following page appears.



Step 3 Return to the **WAN Service** page, and click **Add**. The following page appears.

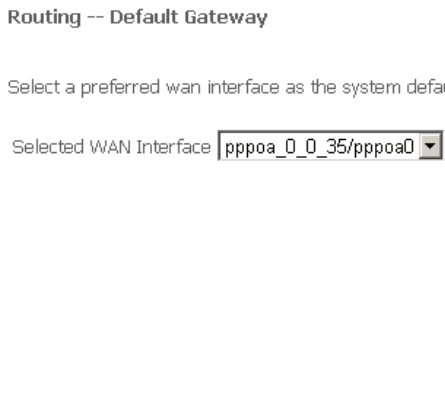


Step 4 After proper selection, click **Next,** and the following page appears.

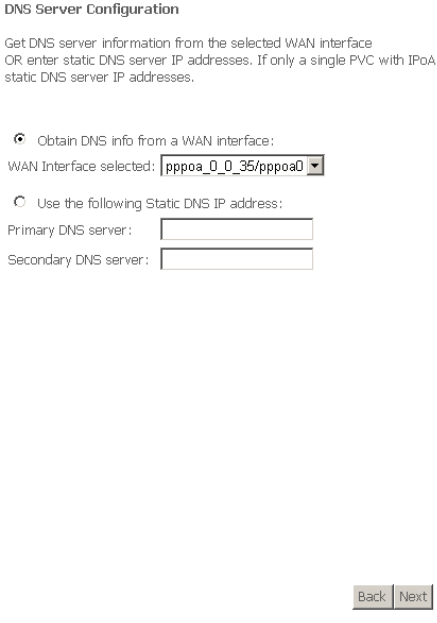


Step 5 In this page, you can modify the service description in the text box. Click **Next**, and the following page appears.

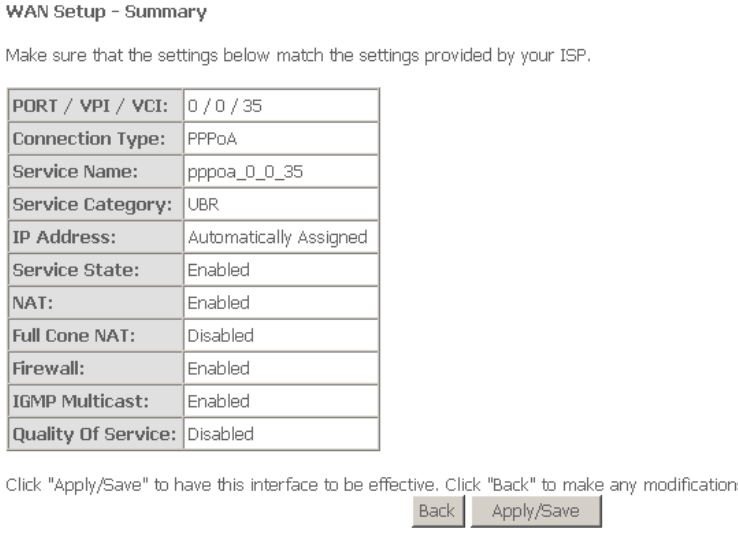
Step 6 In this page, you can modify the PPP Username, PPP Password, Authentication Method according to your requirement. Click **Next**, and the following page appears.



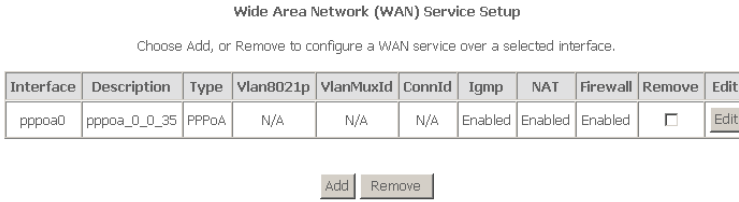
Step 7 In this page, select a preferred wan interface as the system default gateway. Click **Next**, and the following page appears.



Step 8 In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next** and the following page appears.



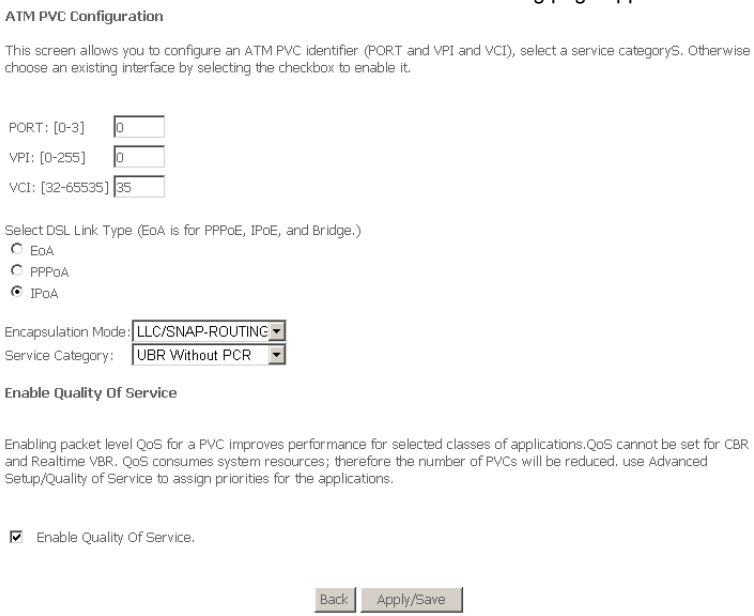
Step 9 In this page, click **Apply/Save** to save all the configurations, and the following page appears. If you want to make any modifications, click **Back**.



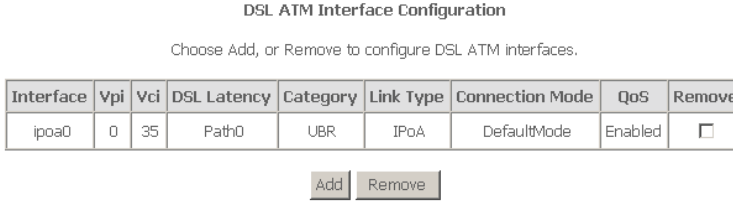
4.3.2.4 Adding an IPoA Configuration

This section describes the procedure for adding ipoa_0_0_35 (IPoA mode).

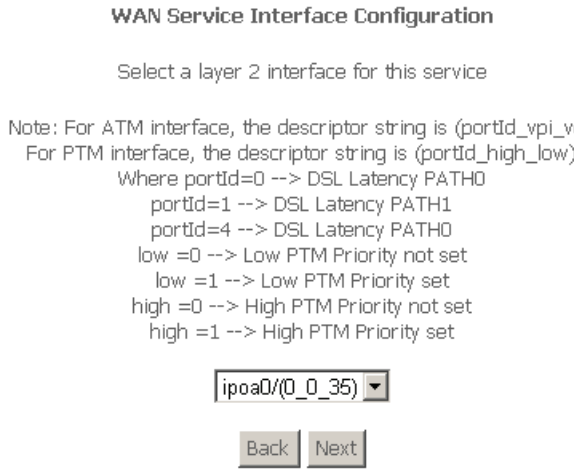
Step 1 You need to open the **Layer2 Interface > ATM Interface** page to add a PVC for IPoA mode. Click **Add** and the following page appears.



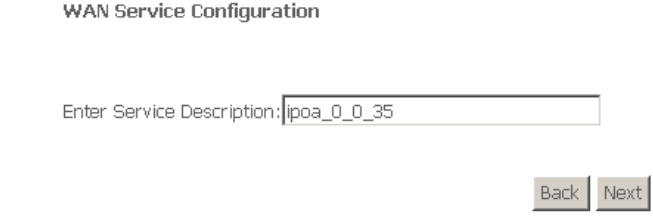
Step 2 Select the DSL link type to **IPoA,** the Encapsulation Mode to **LLC/SNAP-ROUTING** (according to the uplink equipment). Click **Apply/Save,** and the following page appears.



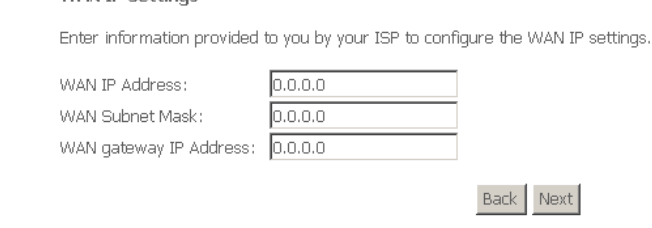
Step 3 Return to the **WAN Service** page, and click **Add**. The following page appears.



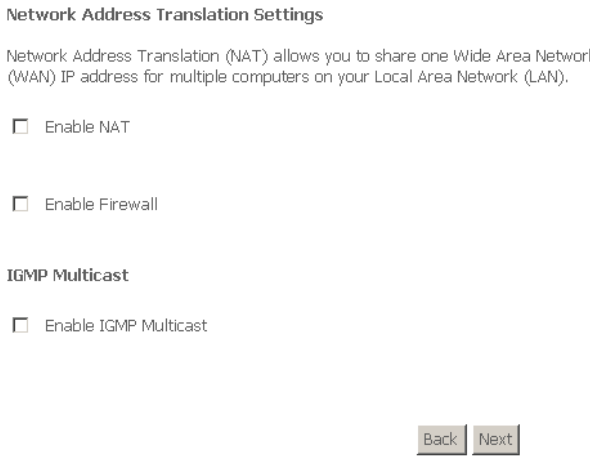
Step 4 After proper modifications, click **Next**, and the following page appears..



Step 5 In this page, you can modify the service description. Click **Next**, and the following page appears.



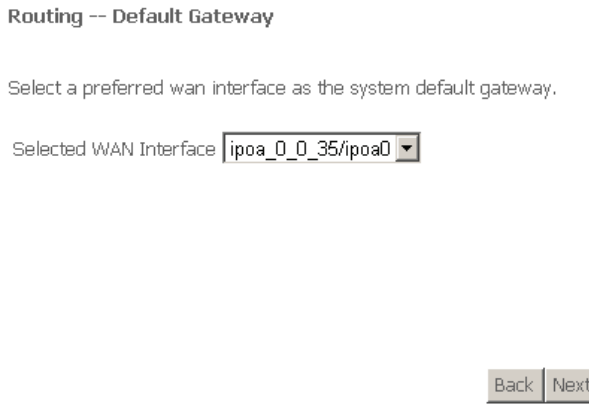
Step 6 In this page, enter information provided to you by your ISP to configure the WAN IP settings. Click **Next**, and the following page appears.



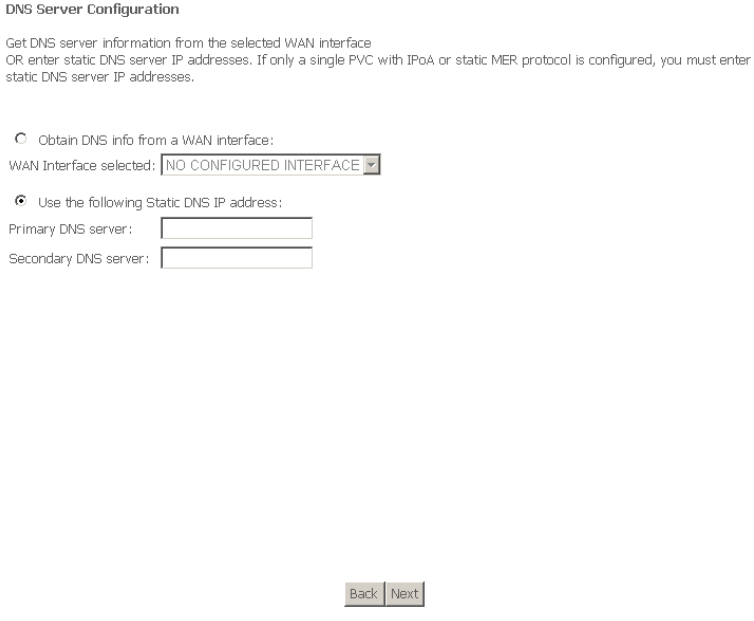
In this page, Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

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

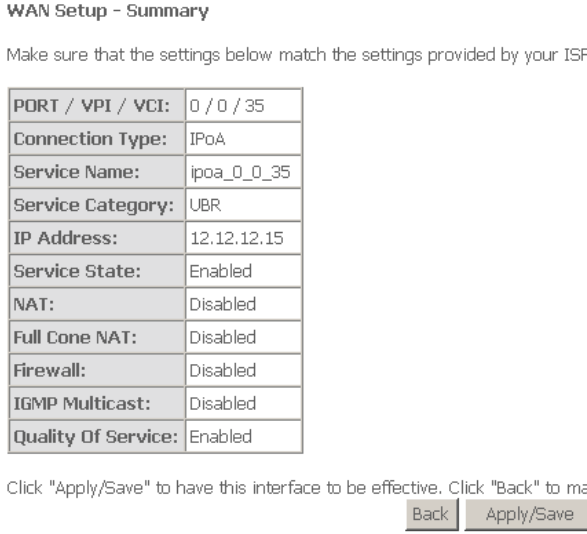
Step 7 After proper selection, click **Next**, and the following page appears.



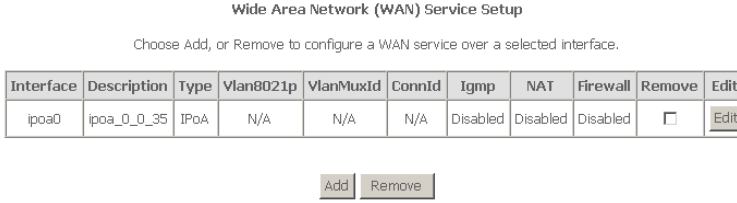
Step 8 In this page, select a preferred WAN interface as the system default gateway. Click **Next,** and the following page appears.



Step 9 In this page, you should use static DNS IP address for IPoA mode. Enter primary DNS server and secondary DNS server. Click **Next,** and the following page appears.



Step 10 Click **Apply/Save** to save all the configurations. And the following page appears. If you want to make any modifications, click **Back**.

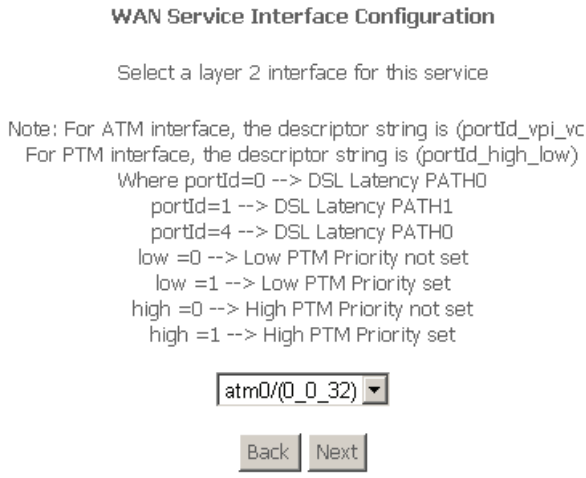


4.3.2.5 Adding a Bridge Configuration

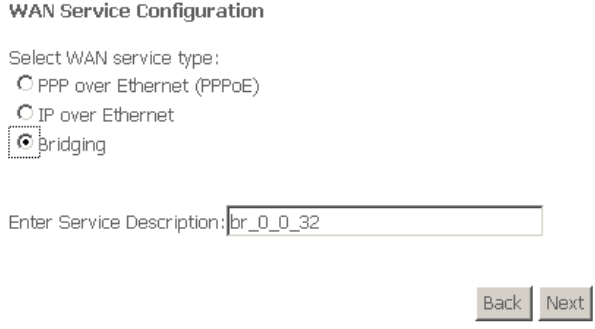
In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding br_0_0_32 (Bridge mode).

Step 1 Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.) In this page, you can

select ATM Interface.



Step 2 Select an ATM Interface, such as atm0/(0_0_32). Click **Next,** and the following page appears.



Step 3 In this page, you can modify the **WAN service type** and **Service Description**. Click **Next,** and the following page appears.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 32
Connection Type:	Bridge
Service Name:	br_0_0_32
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

Step 4 Click **Apply/Save** to save all the configurations, and the following page appears. To make any modifications, click **Back**.

Wide Area Network (WAN) Service Setup

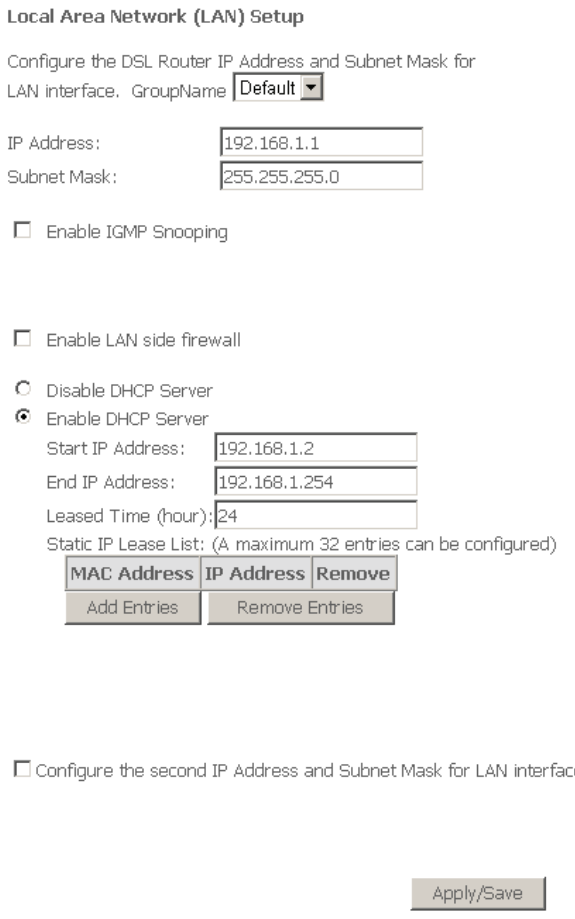
Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
atm0	br_0_0_32	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	☐	Edit

Add Remove

4.3.3 LAN Configuration

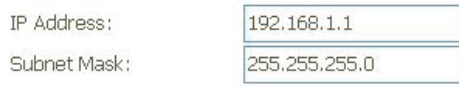
Choose **Advanced Setup > LAN,** and the following page appears. In this page, you can configure an IP address for the DSL Router and enable DHCP server.



4.3.3.1 Configuring the Private IP Address for the DSL Router

In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1. This is the private IP address of the DSL Router, under which the device can be reached in the local network. It can be freely assigned from the block

of available addresses. The IP address under which the Router can be reached from outside is assigned by the ISP.



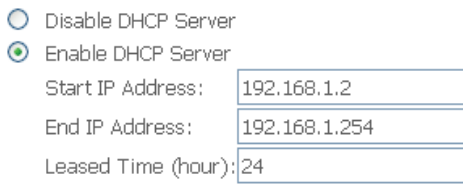
4.3.3.2 Enabling IGMP Snooping

Internet Group Management Protocol (IGMP) is an Internet protocol that enables an Internet computer to inform neighboring routers that it is a member of a multicast group.

Note: **If IGMP snooping function is enabled, the DSL Router capability improves.**

4.3.3.3 Configuring the DHCP Server

The DSL Router has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the DSL Router.



4.3.3.4 Configuring DHCP Static IP Lease

View the following part for static IP Lease List.

Note*:* A maximum 32 entries can be configured.

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

4.3.3.5 Configuring the Second IP Address and Subnet Mask for LAN Interface

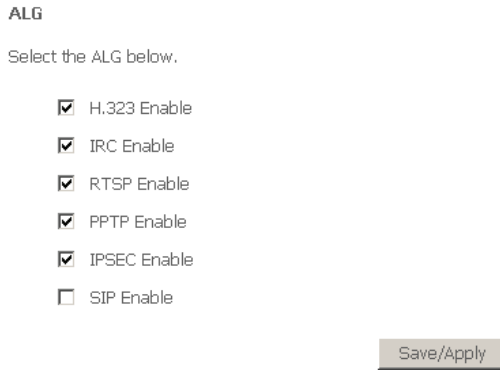
View the following part for second IP address and subnet mask for LAN interface.

4.3.4 NAT

Note: Only the mode of configuration PVC is PPPoE or PPPoA, NAT service appears.

4.3.4.1 ALG

Click **Advanced Setup > NAT > ALG**, and the following page appears. This part contains NAT Application-Layer Gateway (ALG).



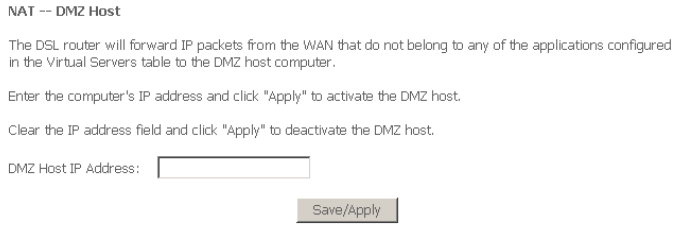
- **H.323 Enable:** The H.323 ALG is a flexible application layer gateway that allows H.323 devices such as H.323 phones and applications to make and receive calls between each other, when connected to private networks secured by clavister security gateways.
- **IRC Enable:** The IRC ALG is a flexible application layer gateway that allows Internet Relay Chat (IRC).
- **RTSP Enable:** Allows applications that use Real Time Streaming Protocol (RTSP) to receive streaming media from the internet.
- **PPTP Enable:** Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server.
- **IPSEC Enable:** Allows multiple VPN clients to connect to their corporate networks using IPSec.
- **SIP Enable:** Allows devices and applications to use VoIP (Voice over IP) to communicate through NAT.

4.3.4.2 DMZ Host

Adding a DMZ Host

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

host.



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 configurations.

Remove DMZ host

Step 1 Clear the **DMZ Host Address**.

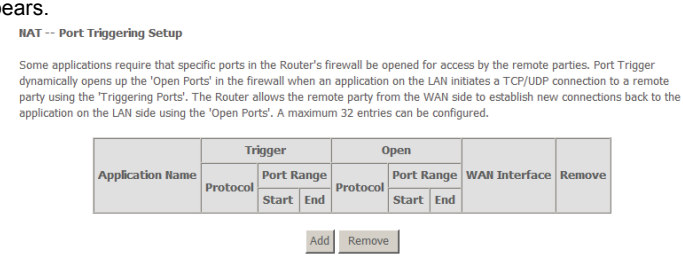
Step 2 Click **Save/Apply** to apply the settings.

4.3.4.3 Port Triggering

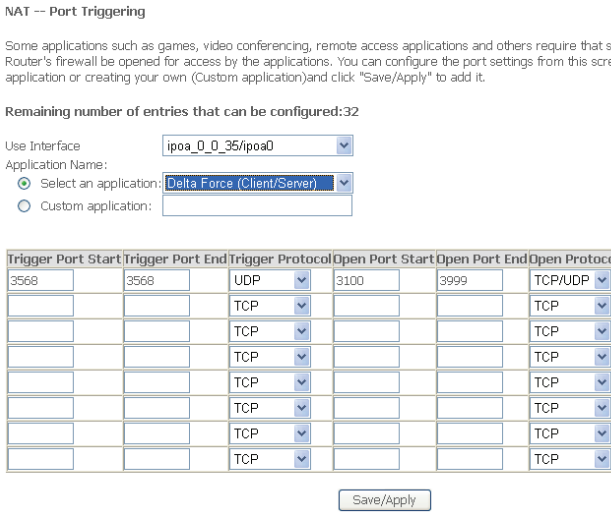
If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or manually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

Adding Port Triggering

Choose **Advanced Settings** > **NAT** > **Port Triggering**, and the following page appears.



Step 1 To set up port triggering for a service, click **Add**.



Step 2 Select the use Interface like that ipoa_0_0_35/ipoa0 and 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.

Note: You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

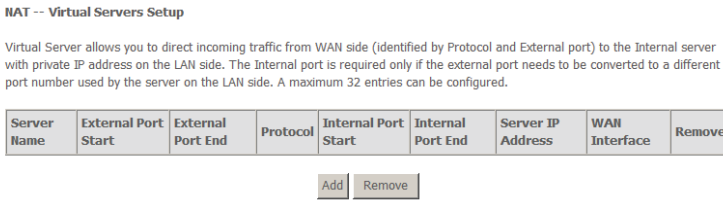
Step 3 Click **Save/Apply** to apply the settings.

Removing Port Triggering

Select the **Remove** check box. Click **Save/Apply** to apply the settings.

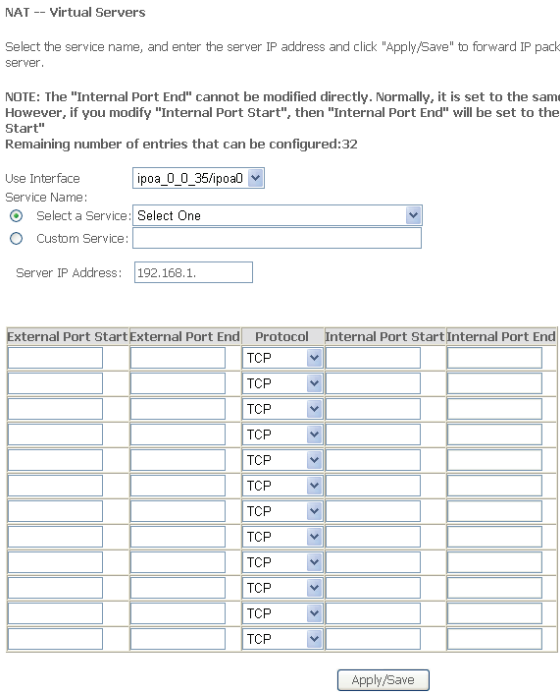
4.3.4.4 NAT - Virtual Server Setup

Click **Advanced Setup > NAT > Virtual Servers**, and the following page appears. The port forwarding (virtual server) page is used to define applications that require special handling by DSL router.



Adding Virtual Servers

Step 1 To set up virtual servers for a service, click **Add**.



Step 2 Select the use Interface like that ipoa_0_0_35/ipoa0 and 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 **Apply/Save** 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 **Public Port**, enter the port number of the service you are providing. In the **Local 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.

Deleting Virtual Servers

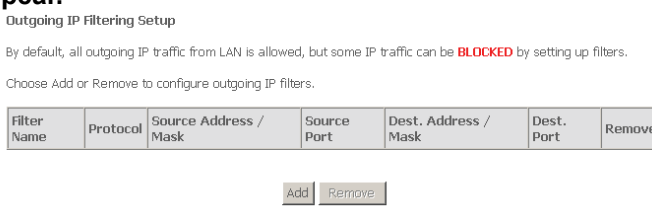
Step 1 Select the **Remove** check box.

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

4.3.5 Security

Choose **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.**

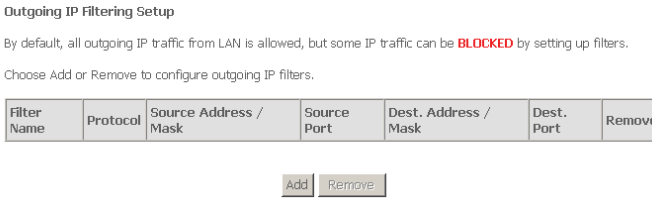


4.3.5.1 Outgoing IP Filtering Setup

When setup of outgoing IP filtering rules is enabled on the modem, various security functions for the local network are enabled at the same time.

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

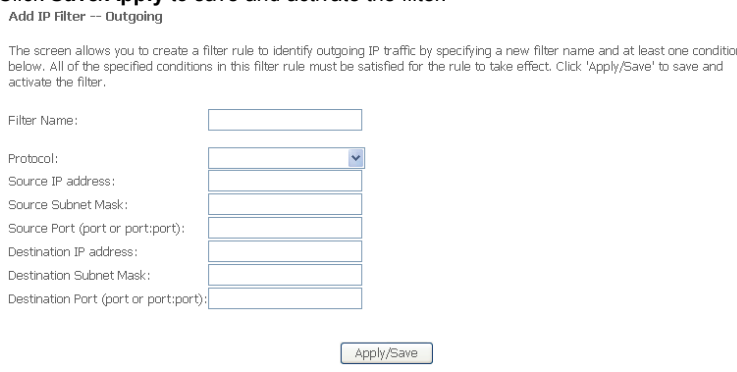
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.



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.

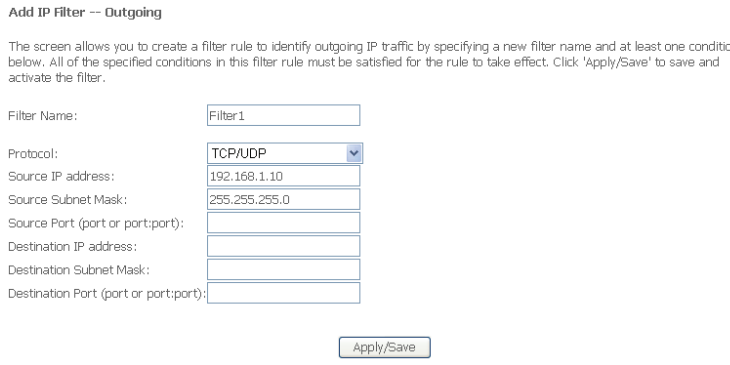


- **Source IP address**: Enter an IP address. After you set the IP address, outgoing packets (protocol selected packets) are blocked.
- **Source port**: UPD/TCP source port or a range of ports.
- **Destination port**: UPD/TCP destination port or a range of ports.

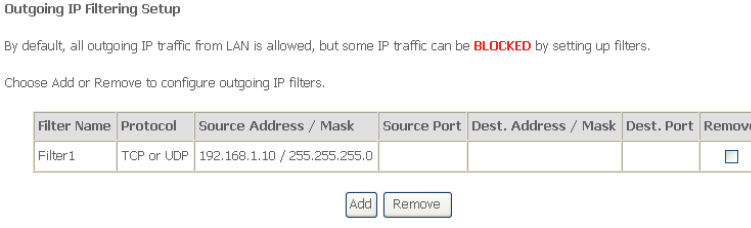
Configuration

Step 1 By default, all outgoing IP traffic from LAN is allowed.

Step 2 The following page shows the detailed configuration.



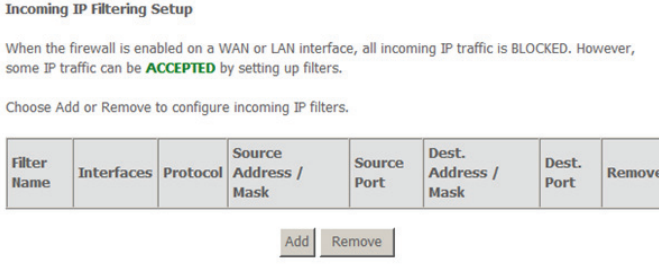
Step 3 Click **Save/Apply** and the following page appears.



4.3.5.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmisstion from internet.

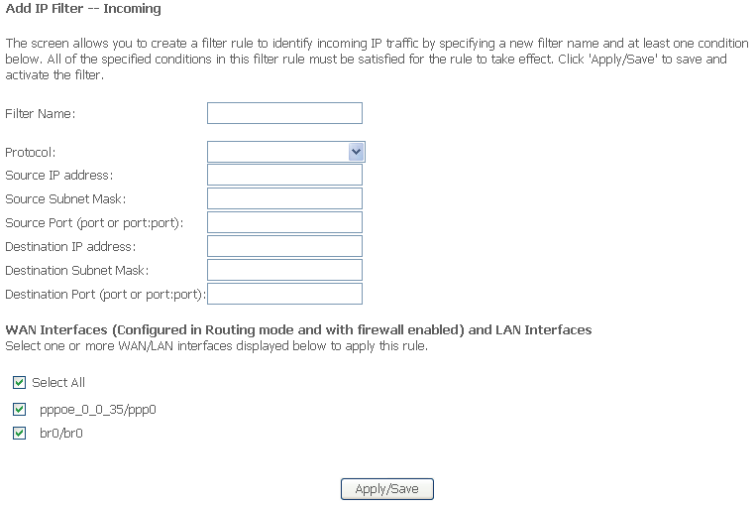
Choose **Security** > **IP Filtering** > **Incoming** and the following page appears.



Click **Add** and the page for defining the IP filtering rule 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 the filter rule must be complied with the rule to take effect. Click **Save/Apply** to save and activate the filter.

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

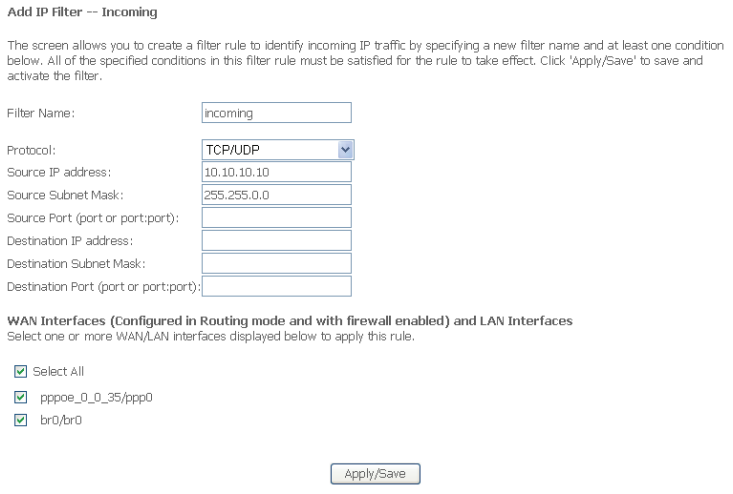


- **Source IP address**: Enter an IP address. After you set the IP address, the incoming packets (protocol selected packets) are allowed.
- **Source port**: UPD/TCP source port or a range of ports.
- **Destination IP address**: destination IP (default: null).
- **Destination port**: UPD/TCP destination port or a range of ports.
- **WAN interfaces**: You can select WAN interfaces and PVC.

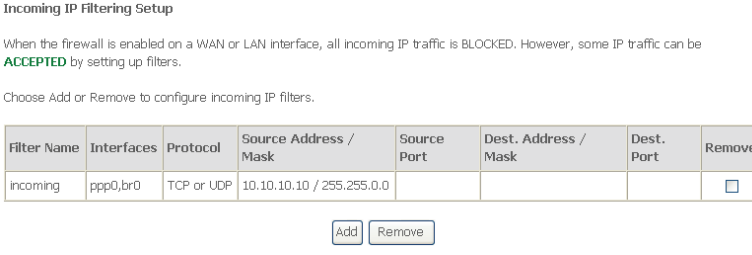
Configuration

Step 1 By default, all incoming IP traffic from Internet is blocked.

Step 2 The detailed configuration steps are as follows:



Step 3 Click **Save/Apply** and the following page appears.



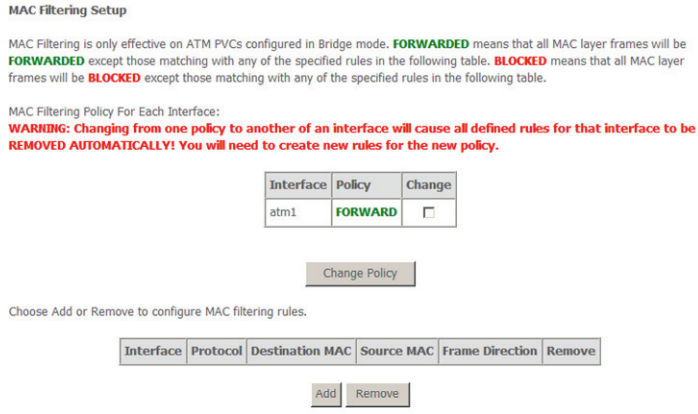
4.3.5.3 MAC Filtering Configuration

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the modem serves as a firewall that works at layer 2.

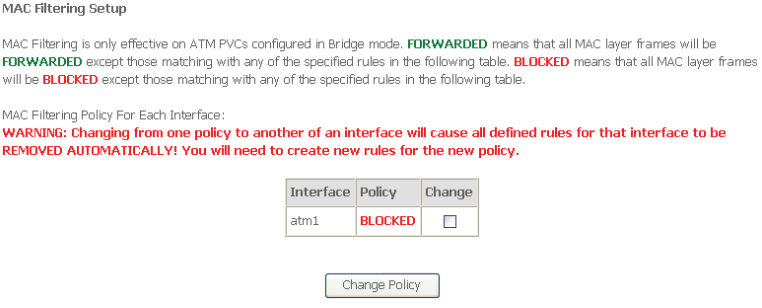
Choose **Security** > **MAC Filtering** and the following page appears.

Note: MAC filtering is only effective on ATM PVCs configured in Bridge mode. If the ATM PVCs are configured in other routing modes (such as PPPoE mode), the MAC

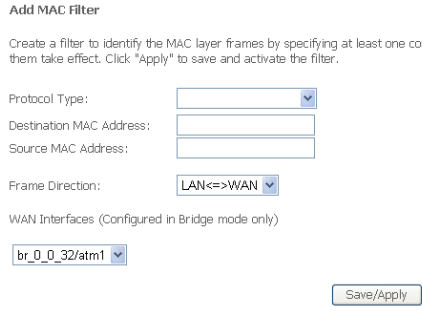
Filtering Setup page does not appear.



Click **Change Policy** and the following page appears. You can change the **MAC Filtering Global Policy** from **FORWARDED** to **BLOCKED**.



Click **Add** to add MAC filter rules. See the following figure.

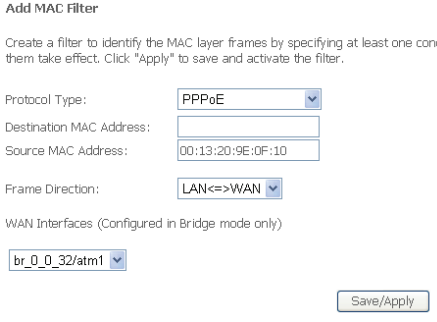


Frame Direction: Direction of transmission frame.

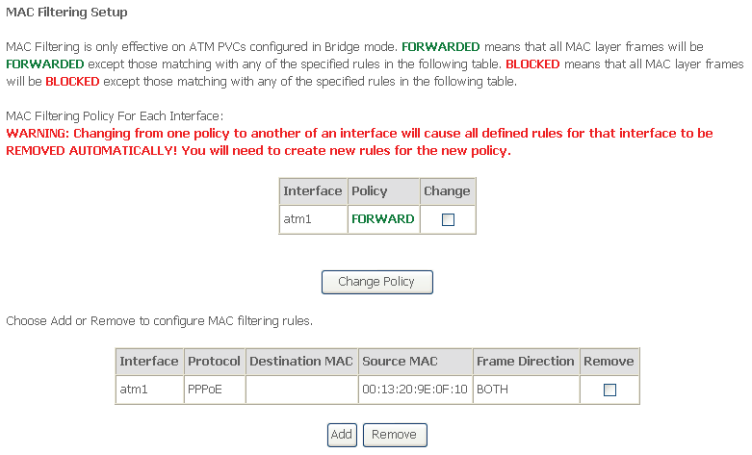
MAC Filtering - Global Policy FORWARDED

This section describes how to prevent the PC whose MAC address is 00:13:20:9E:0F:10 from transmitting PPPoE frames to Internet.

Click **Add** and configure in the following page.



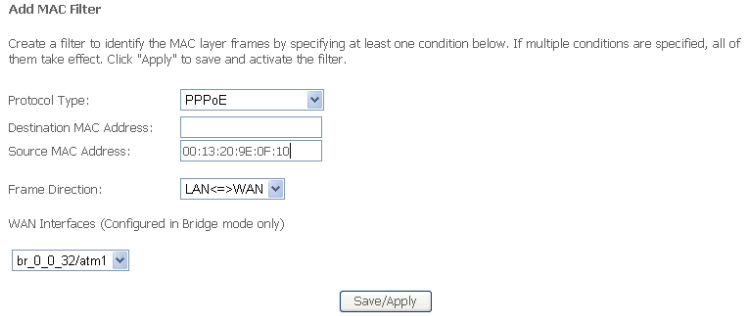
Click **Save/Apply** and the following page appears.



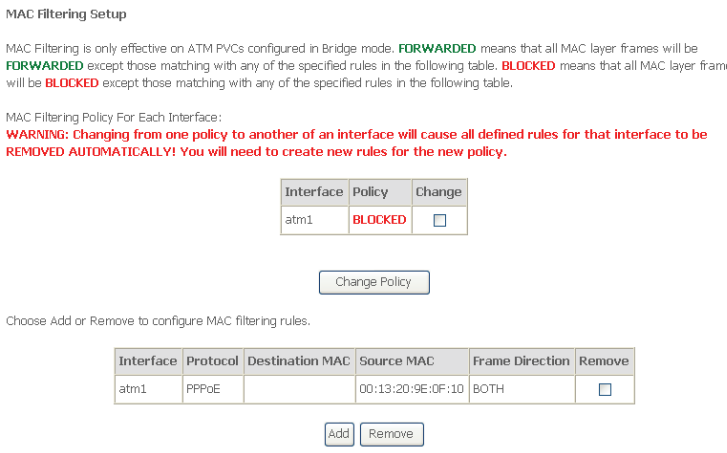
MAC Filtering - Global Policy BLOCKED

This section describes how to permit the PC who has the 00:13:20:9E:0F:10 MAC address transmit PPPoE frame to Internet.

Click **Add** to configure in the following page.



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

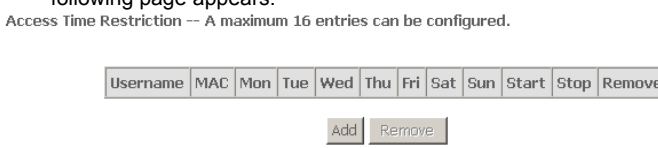


4.3.6 Parental Control

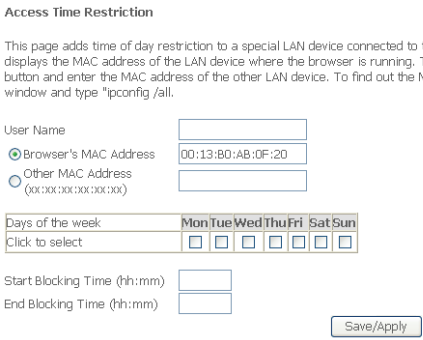
Parental Control restricts a speciel LAN device with its MAC address by setting **Access Time Restriction**, or add URL List to accept or restrict LAN devices accessing URL address by setting **Url Filtering**.

4.3.6.1 Access Time Restriction

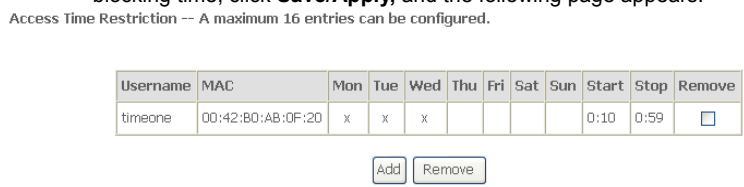
Step 1 Click **Advanced > Parental Control** > **Time Restriction**, and the following page appears.



Step 2 Click **Add,** and the following page appears.



Step 3 In this page, you can add time of day restriction to a special LAN device connected to the Router. After enter user name, select days of week and blocking time, click **Save/Apply,** and the following page appears.

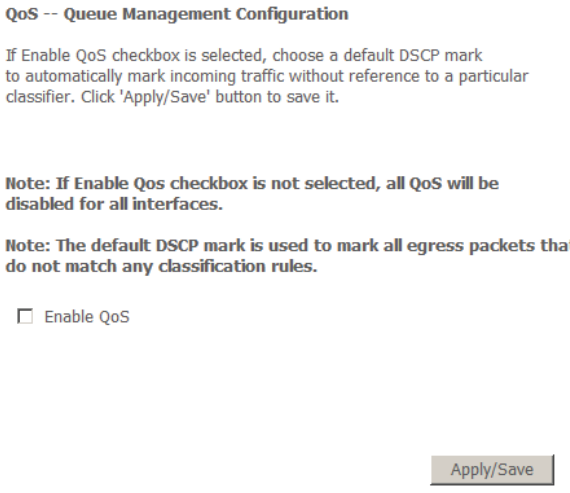


4.3.7 Quality of Service

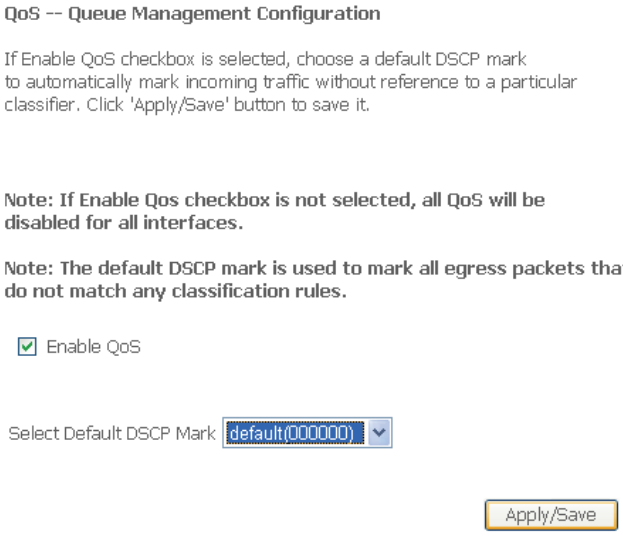
Under **Quality of Service**, there are two network share modes: **Queue Config** and **Qos Classification**.

4.3.7.1 Enabling QoS

In this page, you can perform QoS queue management configuration. Choose **Advance Setup** > **Quality of Service** and the following page appears.



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



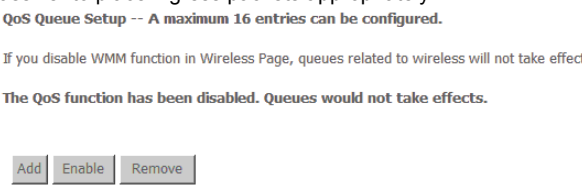
Note: If Enable Qos checkbox is not selected, all QoS is disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

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

4.3.7.2 QOS - Queue Config

Choose **Advanced Setup > Quality of Service > Queue Config,** and the following page appears. In this page, you can configure QoS Queue. A maximum of 24 entries can be configured.

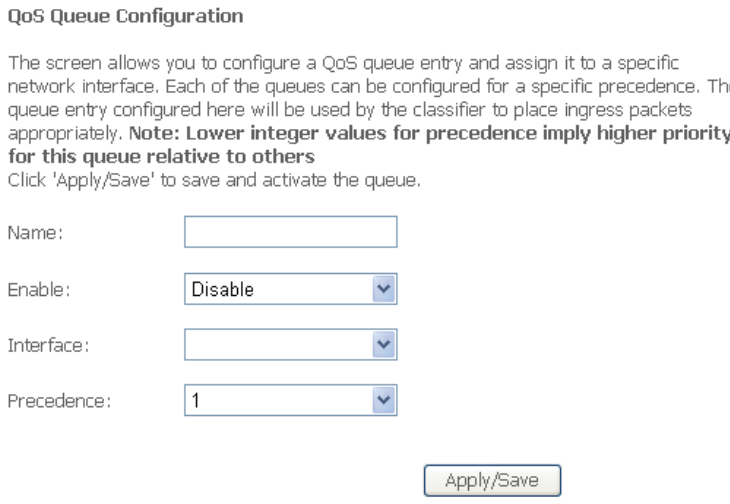
Qos Queue Configuration can allocate three queues. Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured is used by the classifier to place ingress packets appropriately.



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

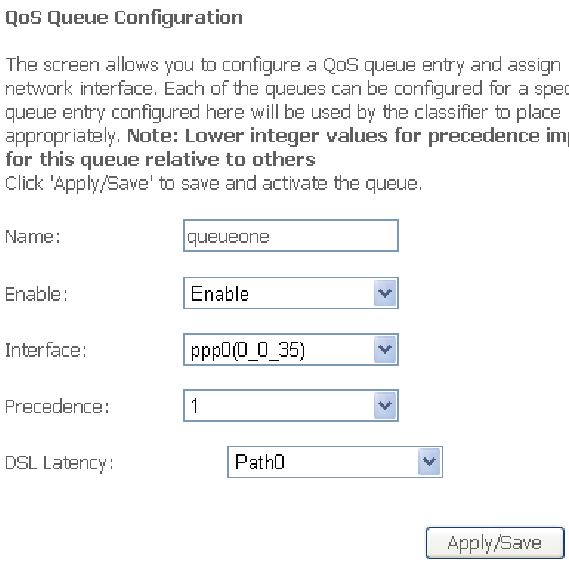
For example, add a QoS queue entry and allocate it to a specific network interface (pppoe_0_0_35). Set integer values for queue precedence to 2.

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

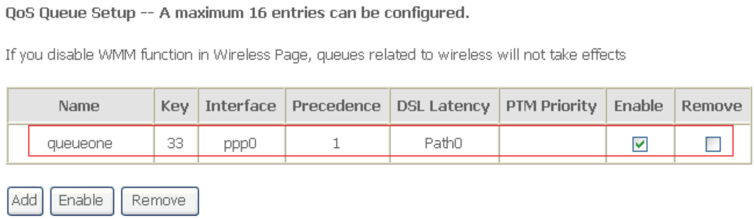


Precedence: Select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

Step 2 Add a QoS queue entry and assign it to a specific network interface (pppoe_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.

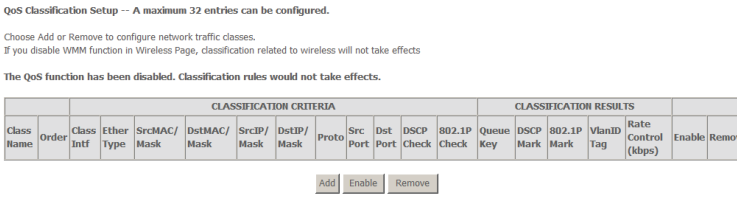


To delete a certain queue, disable it, select it, and then click **Remove**.

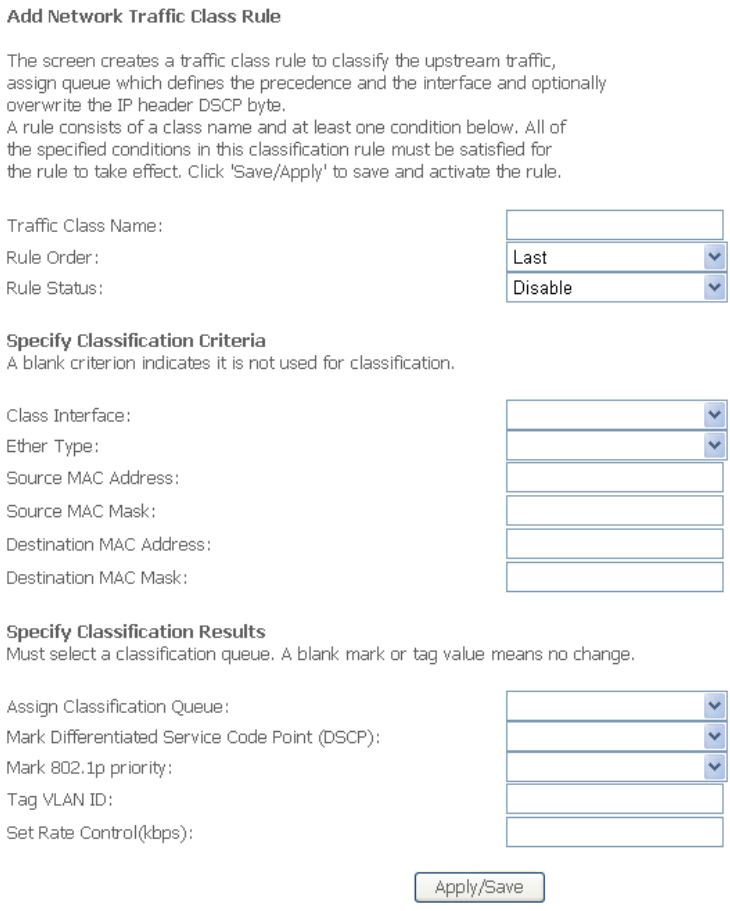
After the queue is configured, you can create several traffic class rules to classify the upstream traffic.

4.3.7.3 QoS--QoS Classification

Choose **Advanced Setup > Quality of Service > Qos Classification** and the following page appears. In this page, you can configure network traffic classes.



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



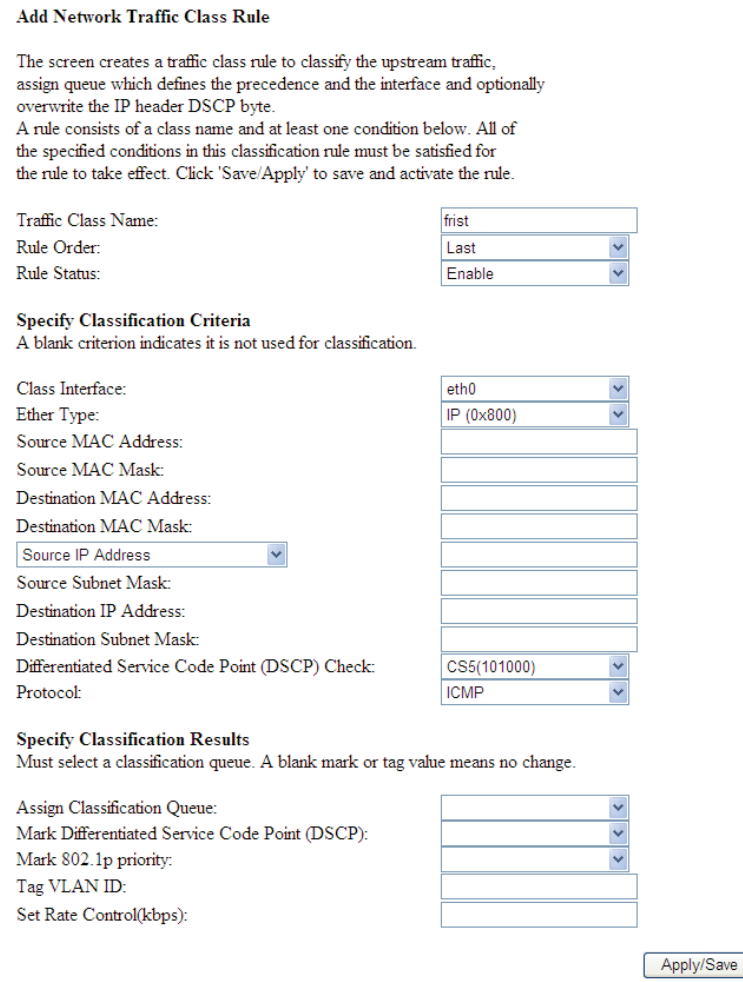
- **Specify Classification Criteria:** A blank criterion indicates it is not used for classification.
- **Specify Classification Results:** Must select a classification queue. A blank mark or tag value means no change.
  - **Mark Differentiated Service Code Point (DSCP):** Select a mark service that 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)

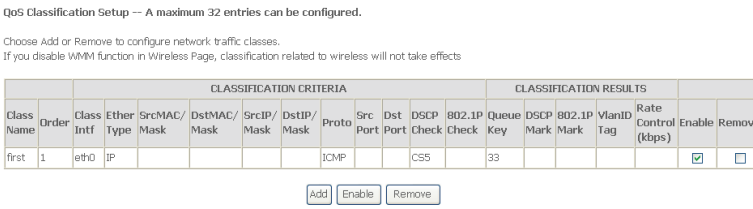
- **Mark 802.1p priority:** Select an 802.1p priority number that serves as the 802.1p value. The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

QoS - DSCP Setting

For example, mark each transmitted ICMP packet which passing traffic to 8-81class with an appropriate DSCP (CS5). See the following figure.



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



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

QoS - 802.1p Setting

For example: Mark the frame of 802.1p that queued to Queue 9 on value 2. See the following figure.

Add Network Traffic Class Rule

The screen creates a 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.
A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:	Second
Rule Order:	Last
Rule Status:	Enable

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:	Local
Ether Type:	IP (0x800)
Differentiated Service Code Point (DSCP) Check:	
Protocol:	

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	ppp0&Prec1&Path0
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	2
Tag VLAN ID:	
Set Rate Control(kbps):	

Apply/Save

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

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove
first	1	eth0	IP					ICMP			CS5		33					☑	☐
Second	2	Local	IP										33		2			☑	☐

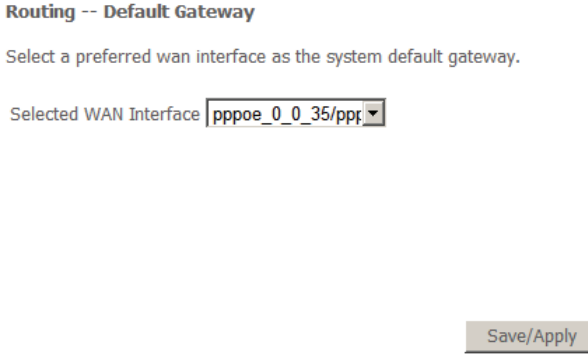
Add Enable Remove

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

4.3.8 Routing

4.3.8.1 Routing – Default Gateway

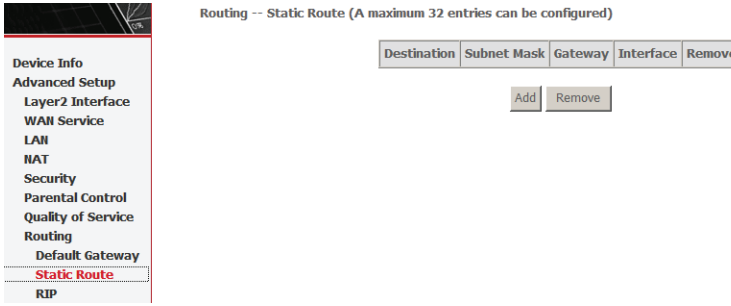
Choose **Advanced Setup > Routing > Default Gateway,** and the following page appears. In this page, you can modify the default gateway settings.
If selected an interface by the **Selected WAN Interface** box, this router accepts the received default gateway assignment from this WAN interface. Click **Save/Apply** to save the configuration.



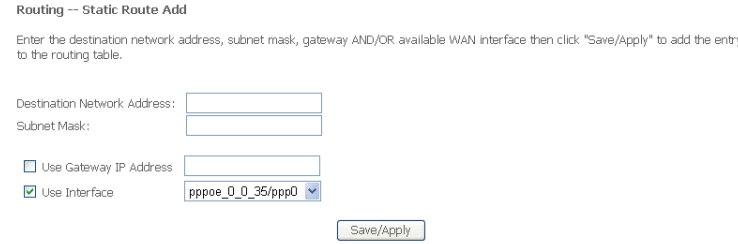
4.3.8.2 Static Route

Adding Static Route

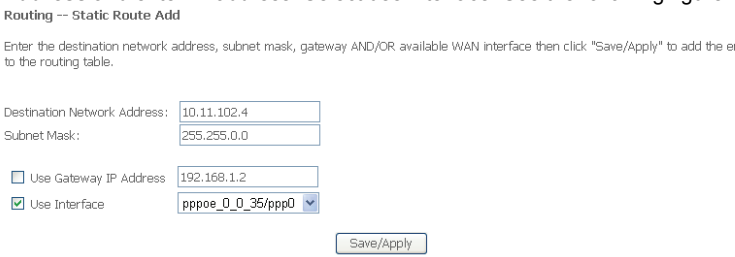
Step 1 Choose **Advanced Setup > Routing > Static Route** and the following page appears.



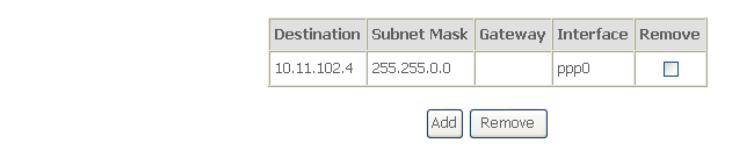
Step 2 Click **Add** and the following page appears.



Enter destination network address and subnet mask. Enable **Use Gateway IP Address** and enter IP address. Select use interface. See the following figure.



Step 3 Click **Save/Apply** to apply the settings and the following page appears.



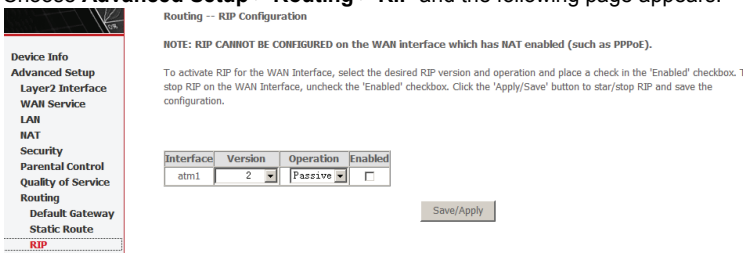
Note: A maximum 32 entries can be configured.

Remove Static Route

Select **Remove** checkbox, and click **Remove** to apply the settings.

4.3.8.3 RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.



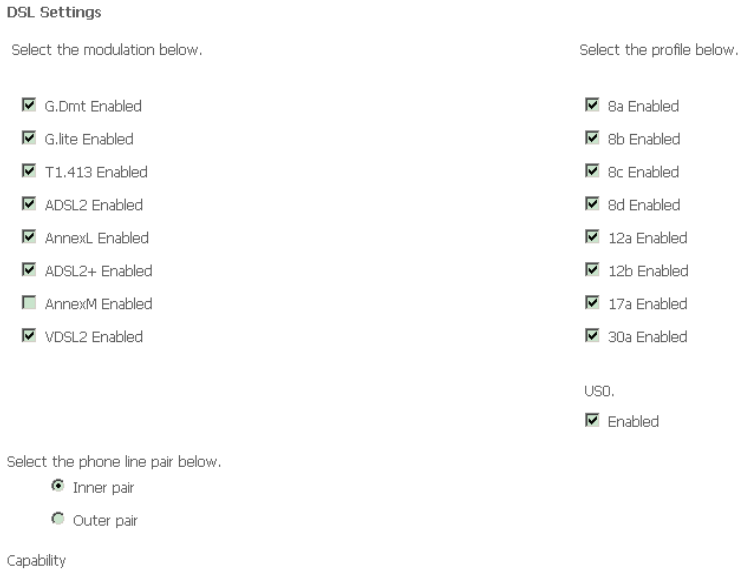
RIP Configuration

- To activate RIP for the device, select **Enabled** for Global RIP Mode.
- To configure an individual interface, select the desired RIP version and operation, followed by selecting the **Enabled** checkbox for the interface.

Click **Save/Apply** to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

4.3.9 DSL

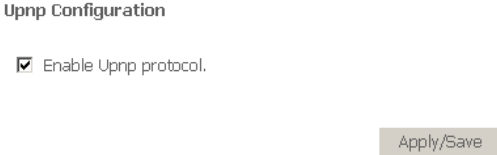
Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM.



4.3.10 UPNP

4.3.10.1 Enabling UPNP

Choose **Advanced Setup** > **UPNP** and the following page appears. In this page, you can enable or disable UPNP protocol.

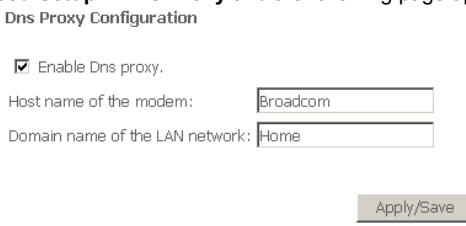


Note: The operating system of the PC should be Windows ME or Windows XP. Check whether the UPnP function is installed in the PC. You may need to retrospectively install the UPnP components, even on systems with Windows XP

or Windows ME. Please refer to the User Guide of your PC.

4.3.11 DNS Proxy

Choose **Advanced Setup > Dns Proxy** and the following page appears.



Enter Host name of the modem and domain name of the LAN network, click **Apply/Save** to save the configuration.

4.3.12 Print Server

A network printer is a printer on which you can print your documents without it being connected to your PC. The advantage of this is that you only need one network printer in your network. All PCs that have the permission to access the network printer can work with it.

In most cases, a printer of this type is connected to another PC, instead of the local PC, in the network. This does indeed offer the advantage referred to above, but it has serious disadvantages:

- The printer can be used by others only when the PC to which it is connected is switched on.
- The print job you send to the PC to which the printer is connected reduces the performance of this PC.

To facilitate this option you must set up a printer port on each PC that is to use the network printer. A printer port is an interface on the PC that forwards the print job to an IP address within the network. Once you set up this port, you must install the printer driver.

4.3.12.1 Configuring a Print Server on DSL Server

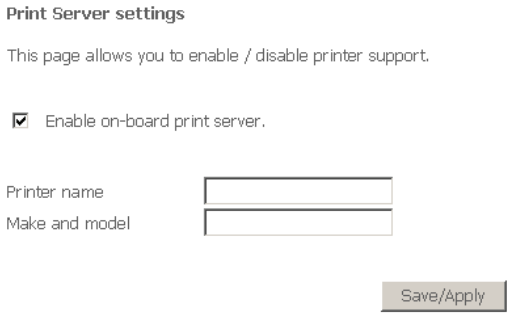
To enable the on-board printer server, do as follows:

Step 1 Enable **Print Server** from modem web page.

Step 2 Select the **Enable on-board printer server** check box and enter the information in **Printer name** and **Make and model**.

Note:

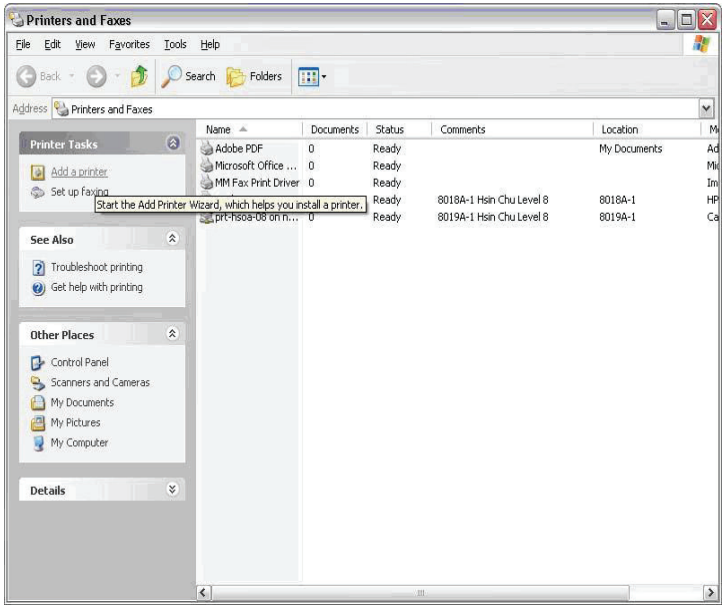
- The **Printer name** can be any text string up to 40 characters.
- The **Make and model** can be any text string up to 128 characters.



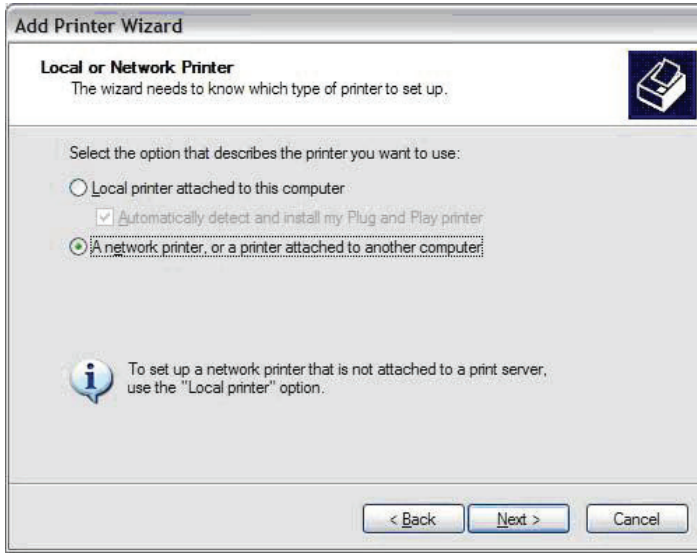
4.3.12.2 Configuring a Print Server on the Windows Host

To configure the print server on the Windows host, do as follows:

Step 1 Choose **Control Panel** > **Add a printer** from the desktop of a Windows XP computer and click **Next**.

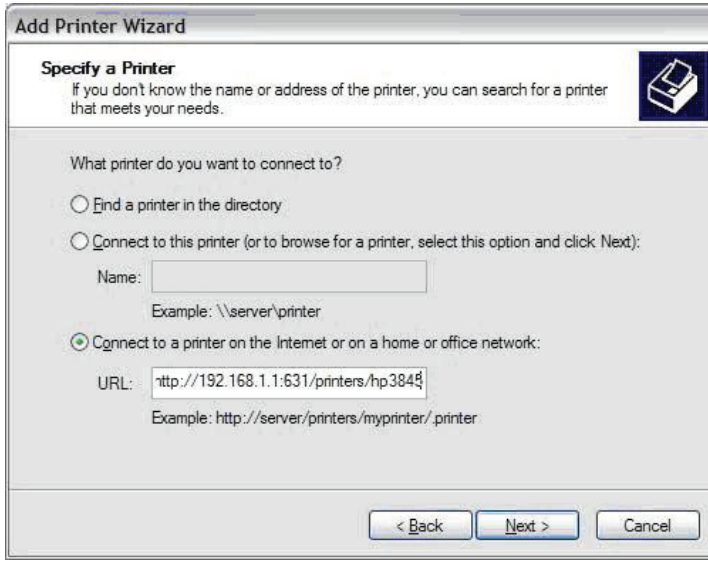

Printers and Faxes
File Edit View Favorites Tools Help
Back Search Folders
Address Printers and Faxes
Printer Tasks
Add a printer
Set up faxing
See Also
Troubleshoot printing
Get help with printing
Other Places
Control Panel
Scanners and Cameras
My Documents
My Pictures
My Computer
Details
Name Documents Status Comments Location
Adobe PDF 0 Ready My Documents
Microsoft Office ... 0 Ready
MM Fax Print Driver 0 Ready
Ready 8018A-1 Hsin Chu Level 8 8018A-1
Ready 8019A-1 Hsin Chu Level 8 8019A-1
Start the Add Printer Wizard, which helps you install a printer.

Step 2 Select **Network Printer** and click **Next**.



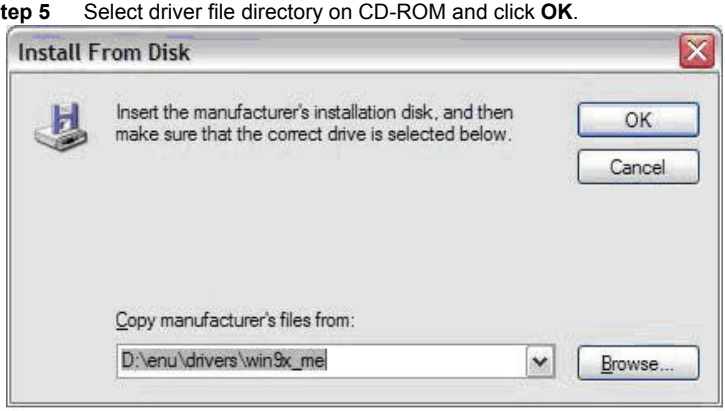
Step 3 Select **Connect to a printer on the Internet**, enter **http://192.168.1.1:631/printers/hp3845** and click **Next**.

The printer name (**hp3845**) must be the same name entered in the **Printer server setting** page as mentioned in Step 1.



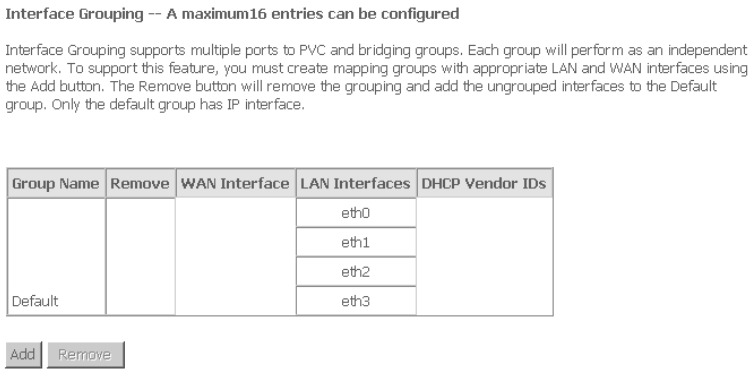
Step 4 Click **Have Disk** and insert the printer driver CD.

Step 5 Select driver file directory on CD-ROM and click **OK**.



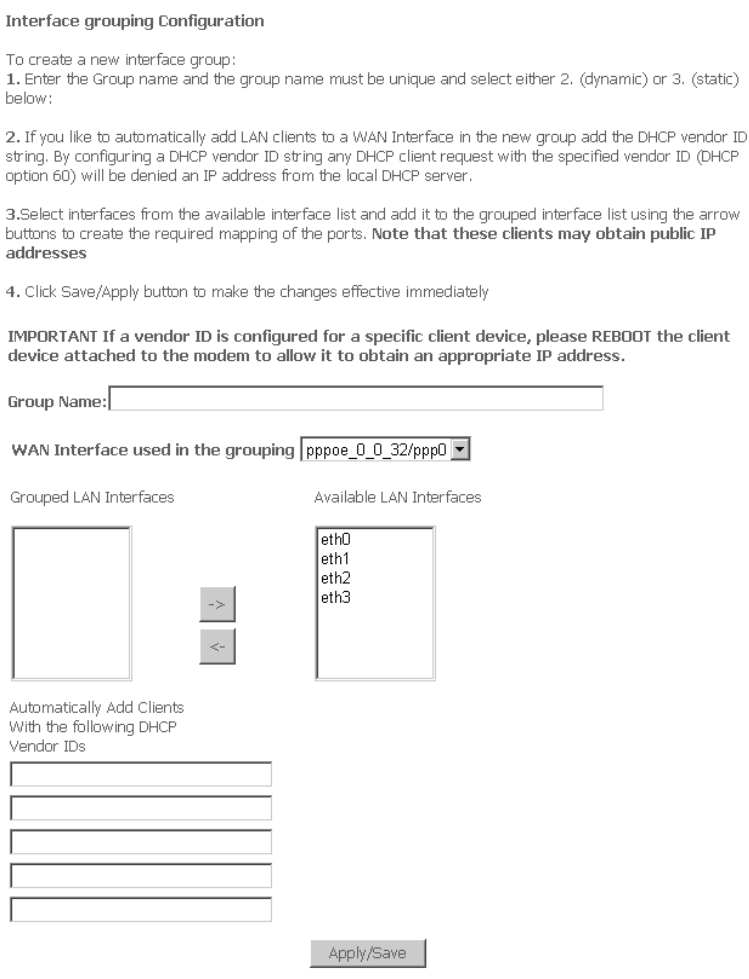
4.3.13 Interface Grouping

Choose **Advanced Setup > Interface Grouping** and the following page appears.

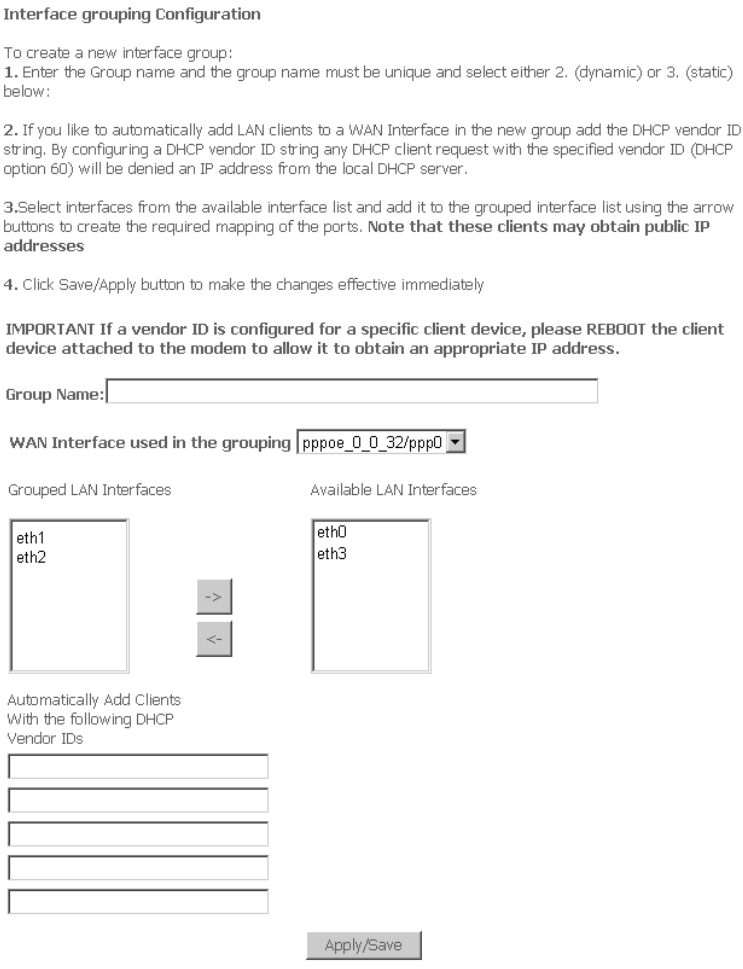


4.3.13.1 Create a new mapping group

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



Automatically Add Clients With the following DHCP Vendor IDs: If a vendor ID is configured for a specific client device, reboot the client device attached to the modem to allow it to obtain an appropriate IP address. (For example, the windows 2000/XP default DHCP client's vender ID is MSFT 5.0.).



Step 1 Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

Note: These clients may obtain public IP addresses.

Step 2 Click **Save/Apply** to apply the configuration immediately.

Note: The selected interfaces are removed from their existing groups and added to the new group.

4.3.14 IPsec

4.3.14.1 How to Use and Configure the IPSec

To use IPSec user interface, choose **Advanced Setup** > **IPSec**. The following page appears.

The table shows current connections. In this page, you can do the following operation.

- Click **Remove** to remove a connection.
- Click **Add New Connection** to add a new connection.

IPSec Setting Parameters

- **Remote IPSec Gateway Address:** IP gateway of the remote modem (which you want to connection) at the WAN side.
- **Tunnel access from local IP addresses:** If you select **Single Address**, it allows only one PC from local to connect remote hosts with IPSEC mode. You must enter the IP address of the PC in fourth item.
  If you select **subnet**, it allows more than one PC from local to connect remote hosts with IPSEC mode.

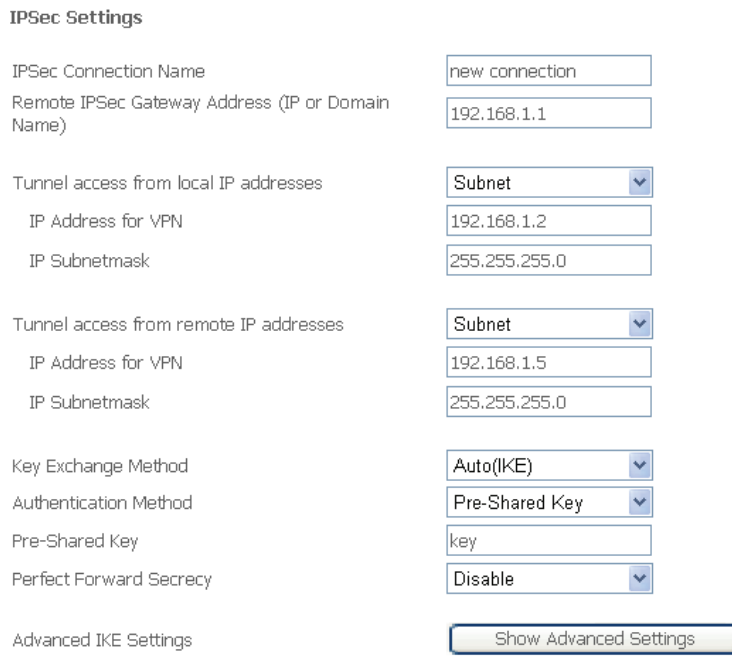
Note: These PCs must in the same subnet, so you must enter the subnet address in fourth item. Enter the subnet mask in the IP Subnet mask that hides when you select

Single Address.

- **IP Address for VPN**: If you select **Single Address**, it is the IP address of the PC. If you choose **Subnet**, it is the subnet address.
- **Tunnel access from remote IP addresses**: same with the third item, but it means remote modem.
- **Key Exchange for VPN**: You can select the encryption mode to **Auto (IKE)** or M**anual**, **Auto (IKE)** sets the encryption automatically, and **Manual** indicates to set the encryption manually.

Example of Configuring IPSec

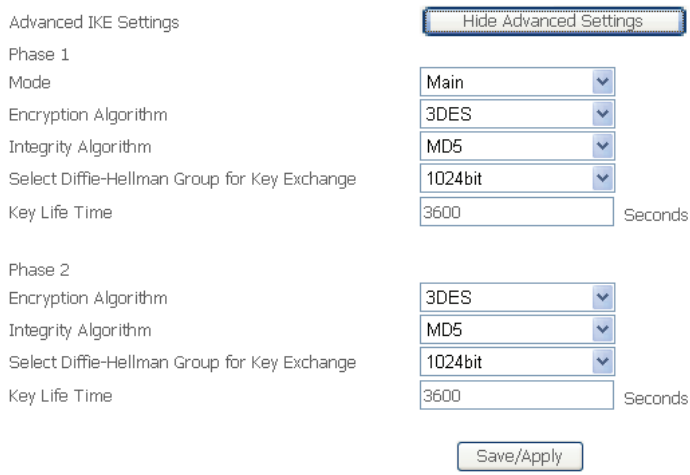
The following page is used to edit configurations when adding or editing an IPSec connection:



This is a dynamic page. The displays are different (some options are shown and hidden) when different types or connections are chosen. You can select automatic

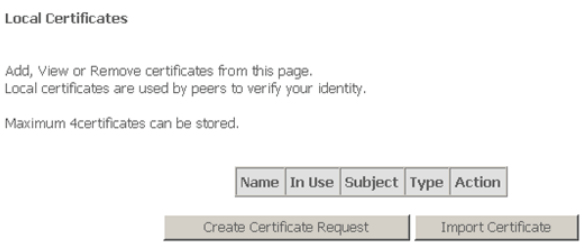
key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.

When automatic key exchange method is used, click **Show Advanced Settings** and more options appear:



4.3.15 Certificate

Choose **Advanced Setup** > **Certificate** and two items appear: **Local** and **Trusted CA**. For either type of certificate, the page shows a list of certificates stored in the modem.



In the menu, **Local** means local certificates. **Trusted CA** means trusted Certificate Authority certificates. Local certificates preserve the identity of the modem. CA certificates are used by the modem to very certificates from other hosts.

Local certificates can be created by two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate.
- Import an existing signed certificate directly.

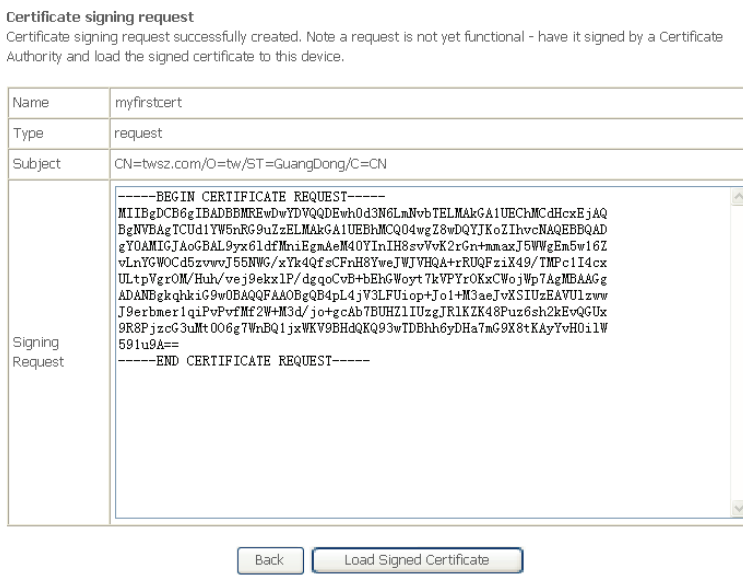
4.3.15.1 Create New Local Certificate

- **Certificate name:** Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.
- **Common Name:** The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specifier "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.
- **Organization Name:** The name of the organization to which the entity belongs (such as the name of a company).
- **State/Province Name:** This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.
- **Country/Region Name:** This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

To create a new certificate, do as follows:

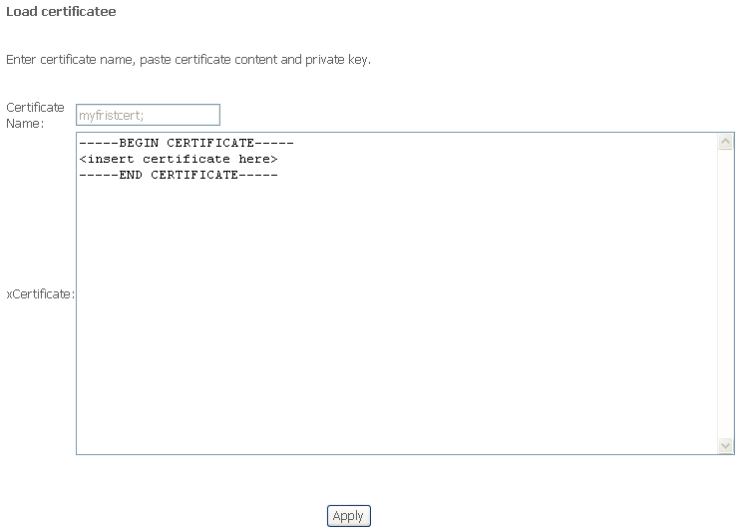
Step 1 Click **Create Certificate Request** and enter necessary information.

Step 2 Wait several seconds and the generated certificate request appears.



The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click **Load Signed Certificate** in the previous page or in the first page, and the load

certificate page appears. Paste the signed certificate, click **Apply**, and a new certificate is created.



4.3.15.2 Importing an Existing Local Certificate

To import existing certificate, click **Import Certificate** and paste both certificate and corresponding private key.

4.3.15.3 Trusted CA Certificates

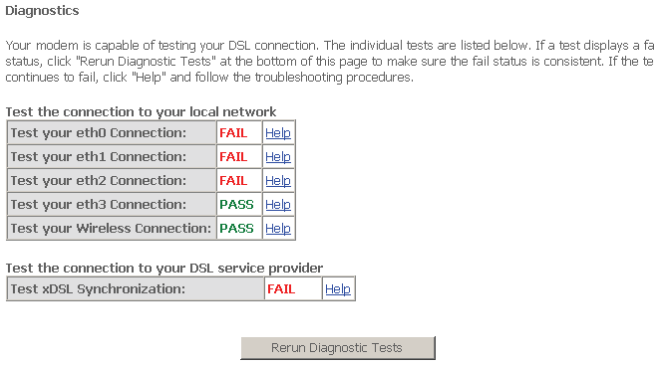
Choose **Certificate** > **Trusted CA** and the following page appears.

Click **Import Certificate** and the following page appears. CA certificate can only be imported.

4.4 Diagnostics

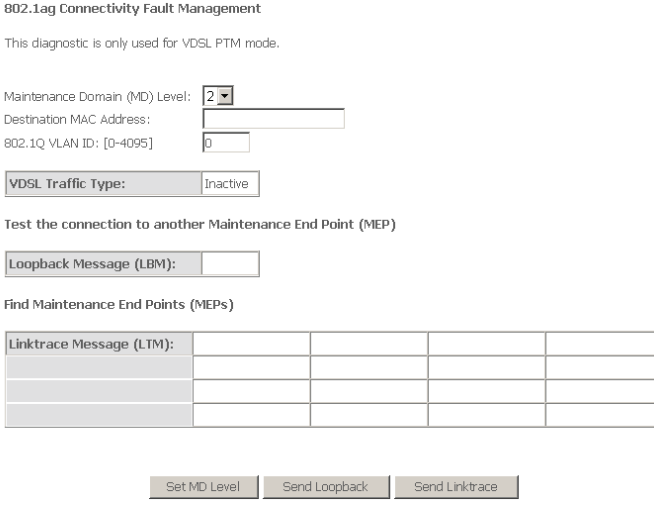
Click **Diagnostics**, and the following page appears.

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click **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.



4.4.1 Diagnostics - Fault Management

Click **Diagnostics > Fault Management**, and the following page appears.

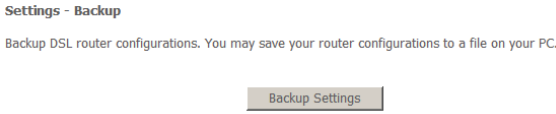


4.5 Management

4.5.1 Settings

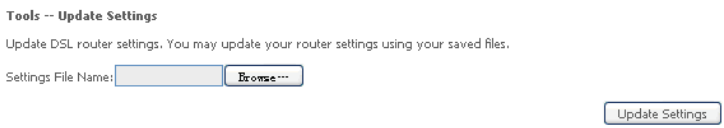
4.5.1.1 Settings Backup

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



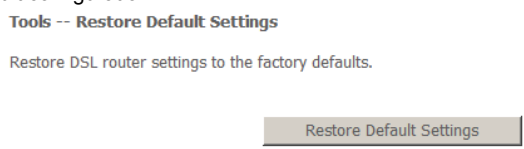
4.5.1.2 Settings Update

Click **Management > Settings > Update**, and the following page appears. Click **Browse** and select the correct update configure settings file. Then, click **Update Settings** to update the modem settings.



4.5.1.3 Settings Restore Default

Click **Management > Settings > Restore Default** to restore DSL router to the factory default configuration.



4.5.2 System Log

Click **Management > System Log**, and the following page appears. The system log dialog allows you to view the system log and configure the system log options.

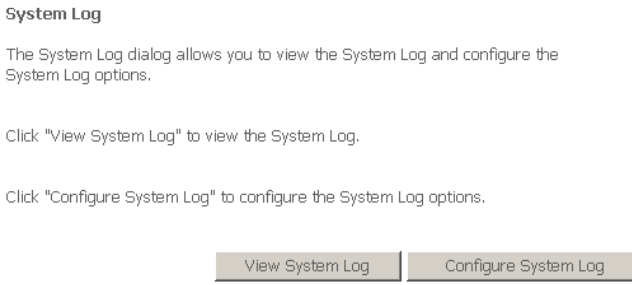
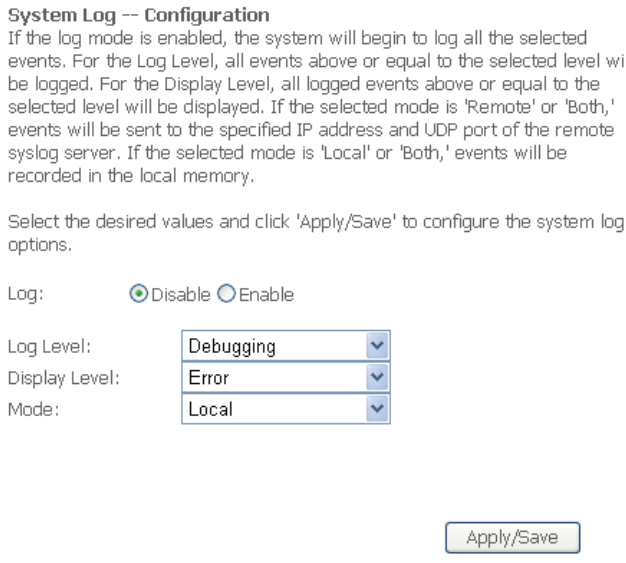


Figure 14 System Log overview

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.



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**.

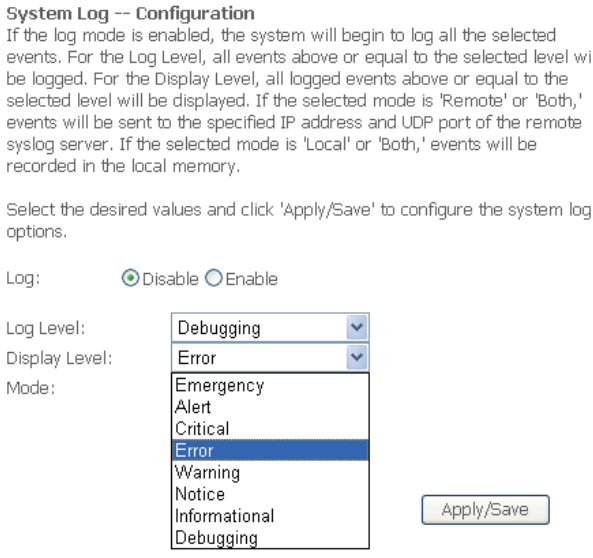


Figure 15 System log configuration (1)

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

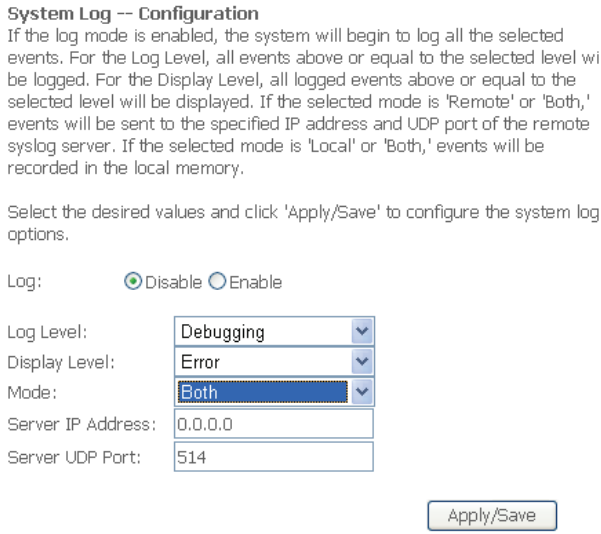


Figure 16 System log configuration (2)

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 want to record all information, you need to set the levels as Debugging.

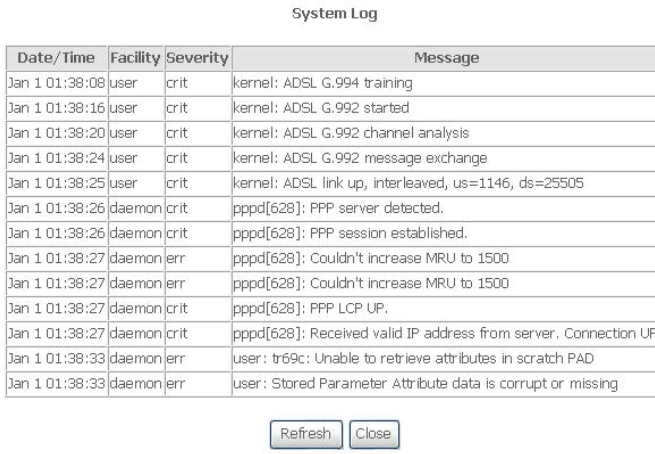


Figure 17 View system event logs

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

4.5.3 TR-69 Client Management

4.5.3.1 Tr-069 Client-configuration

Choose **Management** > **TR-069Client** to show the **TR-069 Client configuration** page.

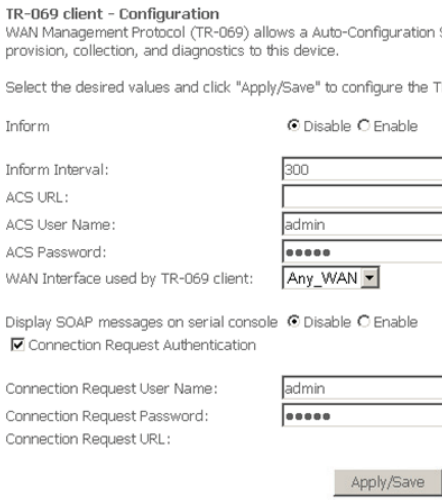


Figure 18 Tr-069 client -configuration

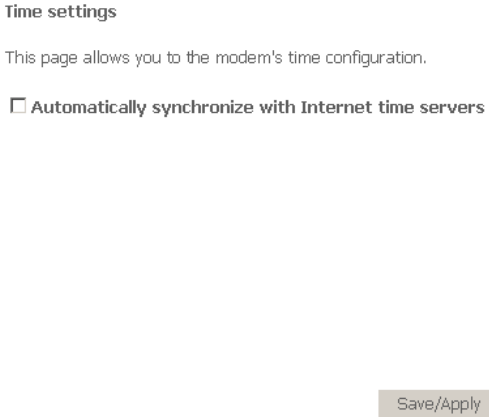
- **Inform:** If the **Enable** option is selected,the CPE accepts the commands from ACS, the CPE does not accept the commands from ACS when the **Disable** option is selected.
- **Inform Interval:** How many seconds does the CPE inform the ACS to connect.
- **ACS URL:** Enter the ACS URL.
- **ACS User Name:** The ACS user name is that the TR-069 Service provide to you.
- **ACS Password:** The ACS password is that the TR-069 Service provide to you.
- **Display SOAP messages on serial console:** When select **Enable** option, the SOAP information displays on the serial console, when select **Disable**, it does not.
- **Connection Request Authentication:** If this checkbox is selected, you need to enter the Connection Request User Name and the Connection Request Password. Or you needn't to enter.
- **Connection Request User Name:** the connection user name that the TR-069 Service provides to you.

- **Connection Request Password:** the Connection Request Password that the TR-069 Service provides to you.

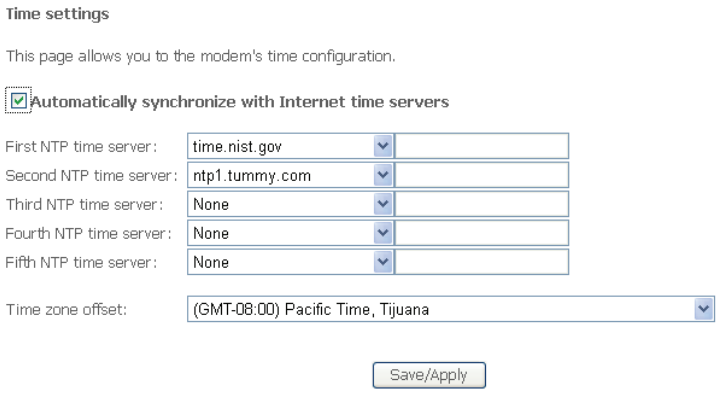
  Click **Save/Apply** to save the he configuration.

4.5.4 Internet Time

Click **Management > Internet Time**, and the following page appears. In this page, the modem can synchronize with Internet time servers.



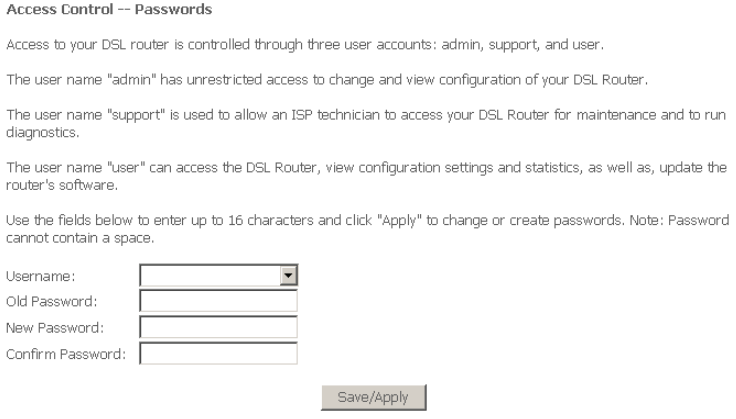
After enable **Automatically synchronize with Internet time servers**, the interface show below. Enter proper configurations and click **Save/Apply**.



4.5.5 Access Control

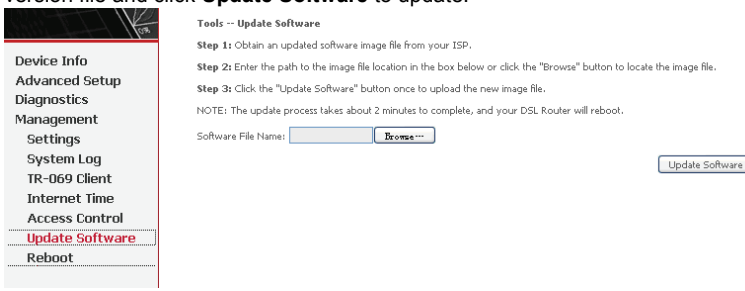
4.5.5.1 Access Control – Passwords

Choose **Management > Access Control > Passwords,** and the following page appears. In the interface, you can modify the accounts passwords.



4.5.6 Update Software

Click **Management > Update Software**, and the following page appears. In this interface, you can update the modem firmware. Click **Browse** to find the right version file and click **Update Software** to update.



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.

4.5.7 Reboot

Choose **Reboot** and the following page appears. Click **Reboot** to reboot the router.