DSL-X11

One Port ADSL Modem Router

User Manual

Contents

1 Introduction

The device is a well-designed high-speed ADSL modem/router.

1.1 Features

- Full rate ADSL router, support Router/ Bridge
- Provides 24Mbps downstream and 1Mbps upstream
- Maximum transmission range: 5.4 Kilometers
- One Ethernet port, 10/100 Mbps Auto-MDI/MDIX
- Friendly GUI for web configuration.
- Configurable as a DHCP Server on Your Network
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of your configuration, and links to the configuration pages.
- Downloadable flash software upgrades
- Support up to 8 Permanent Virtual Circuits (PVC)
- Support up to 8 PPPoE sessions

1.2 ADSL Standard Supports

- ITU G.992.1 (G.dmt) Annex A
- ITU G.992.2 (G.lite)
- ANSI T1.413 Issue 2
- ITU G.992.3(ADSL2)
- ITU G.992.5(ADSL2+)

1.3 Encapsulation Supports

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

1.4 System Requirements

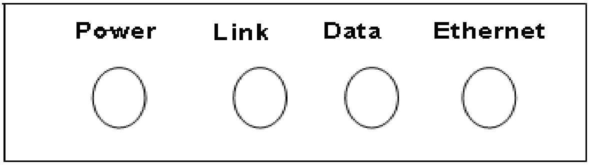
Recommended system requirements are:

- Pentium 300 MHZ or above
- Memory: 128 MB or above
- 10 M Base-T Ethernet or above
- Win9X, Win2000, WinXP, WinMe, WinNT
- Ethernet Network Card

Please collect the following information from your ADSL service provider. This information is very helpful for your ADSL configuration. To keep a record for reference, you can fill in the column as follow:

- VPI
- VCI
- Encapsulation: VCMUX or LLC
- Protocol
- Standard
- User name
- Password
- Password protocol

1.5 LED Status Description



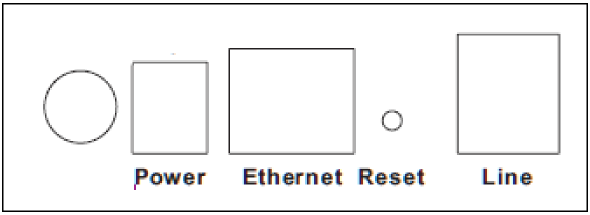
The following table describes the LEDs of the device:

LEDs	Color	Status	Description
Power	Green	On	The device is powered on or the initiation of the device is successful.
		Off	The device is powered off.
	Red	On	The device is self-testing, the self-test is failed or the software is upgrading.
Link	Green	On	The device has established a connection

LEDs	Color	Status	Description
			with the physical layer of the office end.
		Slow Blinks	No signal is being detected.
		Fast Blinks	The device is handshaking with the physical layer of the office end.
Data	Green	On	The device has a successful WAN connection (PPP dial-up is successful) in the routing mode and no data is being transmitted on the Internet.
		Blinks	Data is being transmitted on the Internet in the routing mode.
		Off	The device is in the bridged mode.
	Red	On	In the routing mode, after the successful synchronization, the WAN connection is failed (PPP dial-up is failed).
Ethernet	Green	On	The LAN connection is normal and activated.
		Blinks	Data is being transmitted on the LAN or data is being transmitted on the Internet in the bridged mode.
		Off	The LAN connection of the device is failed.

1.6 Rear Panel

Rear Panel



The following table describes the interfaces of the device:

Items	Description
○	Power switch, power on or power off the device.
Power	Power interface, for connecting to the power adapter. The power adapter output is: 5 V DC 1A.
Ethernet	RJ-45 interface, for connecting to the Ethernet interface of PC or other Ethernet devices through the Ethernet cable.
Reset	Reset to the factory defaults. To reset to the factory defaults, keep the device powered on and push a paper clip in to the hole for over 5 seconds. Then release it, the configuration is reset to the factory defaults.
Line	RJ-11 interface, for connecting to the ADSL interface or a splitter through the telephone cable.

2 Hardware Installation

Step 1 Connect the **Line** interface of the device and the **Modem** interface of the splitter through a telephone cable. Connect the phone to the **Phone** interface of the splitter through a cable. Connect the incoming line to the **Line** interface of the splitter.

The splitter has three interfaces:

- **Line**: Connect to a wall phone jack (RJ-11 jack).
- **Modem**: Connect to the ADSL jack of the device.
- **Phone**: Connect to a telephone set.

Step 2 Connect the **Ethernet** interface of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:

Use twisted-pair cables to connect with the hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** interface of the device.

Connection 1

Figure 1 shows the application diagram for the connection of the router, PC, splitter and the telephone sets, when no telephone set is placed before the splitter.

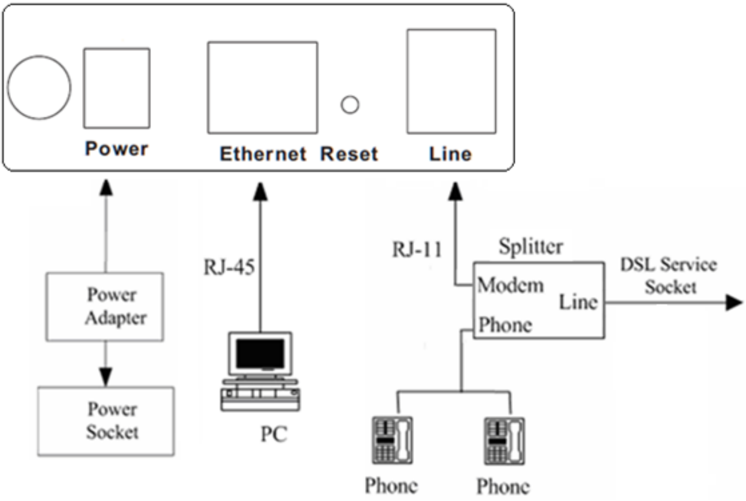


Figure 1 Connection diagram (Without connecting telephone sets before the splitter)

Connection 2

Figure 2 shows the connection when the splitter is installed close to the router.

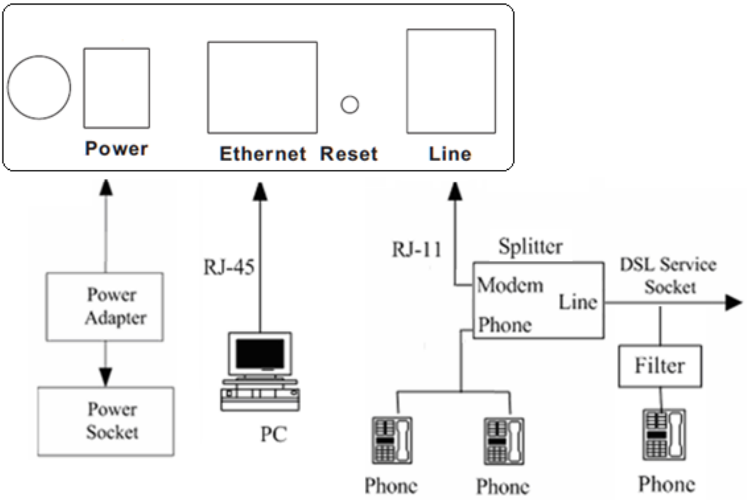


Figure 2 Connection diagram (Connecting a telephone set before the splitter)

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure2. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

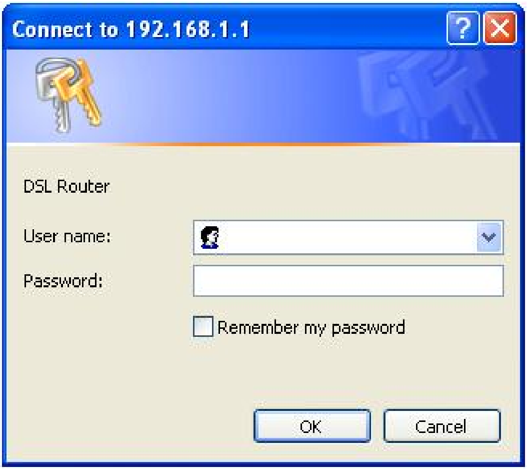
3 Web Configuration Management

3.1 Logging In to the Router

– Open the Internet Explorer or Netscape Web browser and enter **http://192.168.1.1** (default IP address).

(1) Connect the router. Enter the user name and password.

- The default user name and password of the super user are **admin** and **admin**.
- The default user name and password of the common user are **user** and **user**.



Connect to 192.168.1.1

DSL Router

User name:

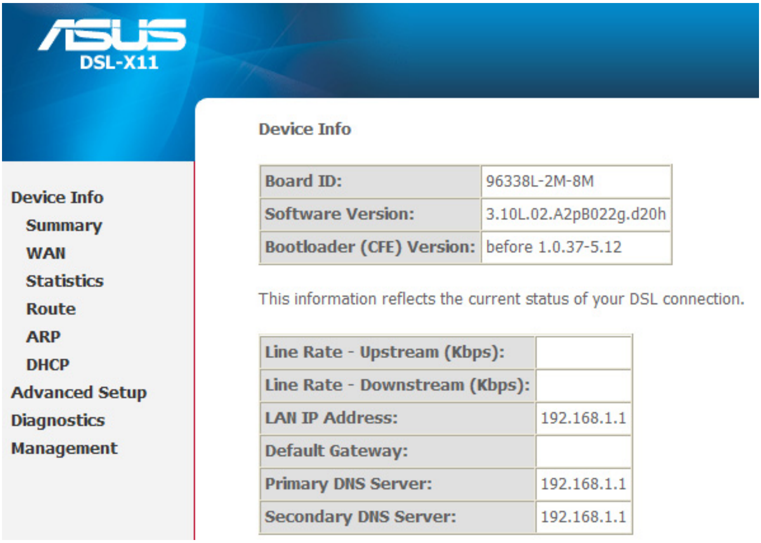
Password:

□ Remember my password

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

3.2 System Status

After finishing logging, “Device Info” interface appears. Four menus including Device Info, Advanced Setup, Diagnostics and Management are displayed on the left of the interface.



Device Info

Board ID:	96338L-2M-8M
Software Version:	3.10L.02.A2pB022g.d20h
Bootloader (CFE) Version:	before 1.0.37-5.12

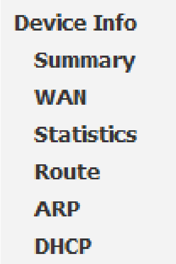
This information reflects the current status of your DSL connection.

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

- LAN IP Address: The management IP address
- Default Gateway: No gateway in a pure bridging mode such as PPPoE or PPPoA .It is the address of the uplink equipment.
- DNS Server address: In PPPoE/PPPoA mode, DNS Server address is obtained from the uplink equipment. In a pure bridging mode, there is no DNS Server address. In that case, user must enter them manually.

3.3 DSL Router Device Information

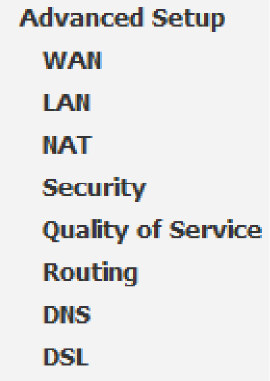
Choose **Device Info**, the following page appears. Choose items to view the corresponding information.



3.4 Advanced Setup

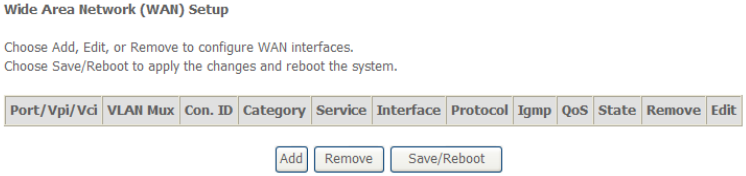
Click **Advanced Setup** and the **Advanced system setup** page appears. The information is as follows:

Advance Setup is key to DSL Router configuration.



3.4.1 WAN Configuration

Choose **Advance Setup** > **WAN**, if the modem is already configured, the following page appears.



Wide Area Network (WAN) Setup

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

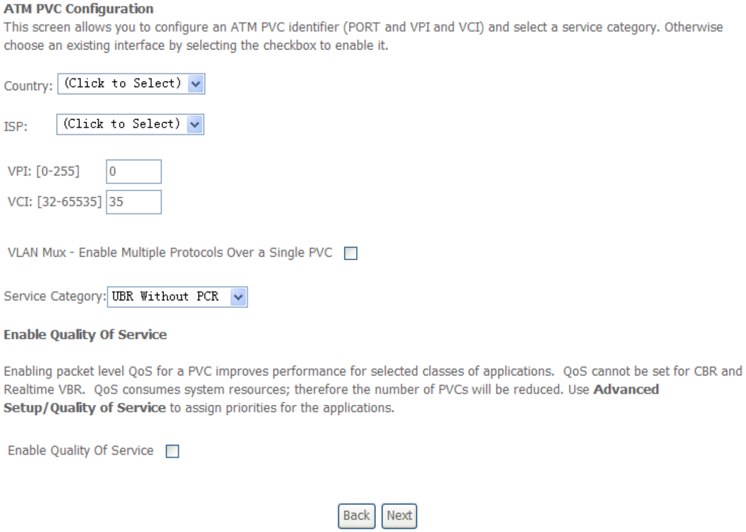
Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit

- To add an ATM PVC, click **Add**.
- To delete a PVC, select the **Remove** check box in the table and click **Remove**.
- Click **Save/Reboot** to apply the changes and reboot the modem.

Note:

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

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



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 35

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

Service Category: UBR Without PCR

Enable Quality Of Service

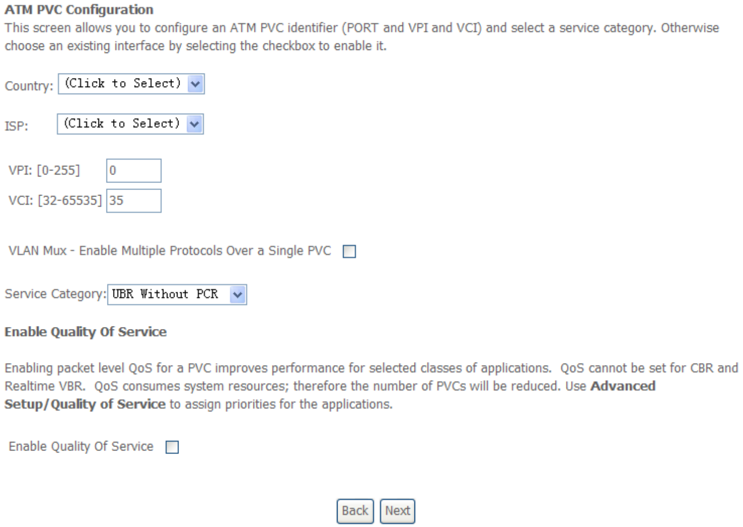
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service □

The procedure for adding a PVC is described as follows.

3.4.1.1 Adding a PPPoE PVC

This section describes the procedure for adding PVC 0/35 (PPPoE mode).
Click **Add** and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 35

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

Service Category: UBR Without PCR

Enable Quality Of Service

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

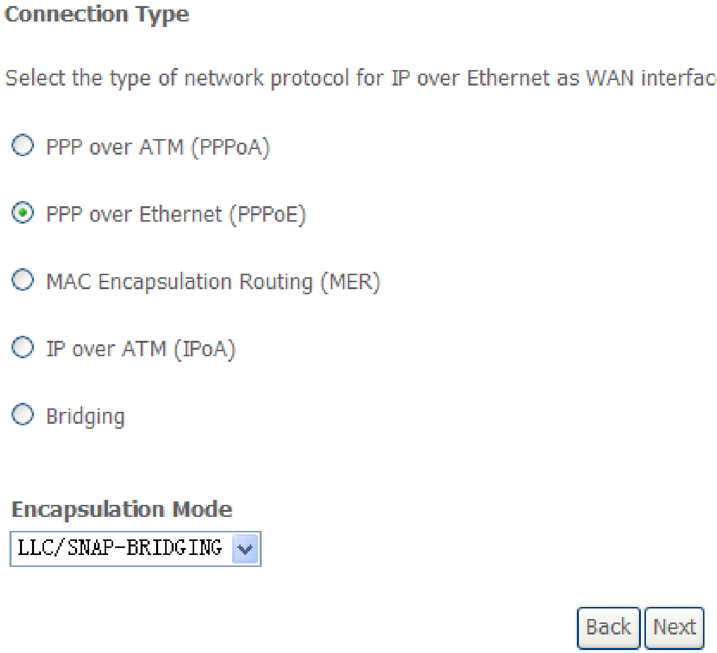
Enable Quality Of Service □

- **Country**: Select the **Country** from the drop-down list.
- **ISP**: Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category**: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service**: Enable or disable QoS.

In this example, PVC 0/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

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

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



Connection Type

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

○ PPP over ATM (PPPoA)

● PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

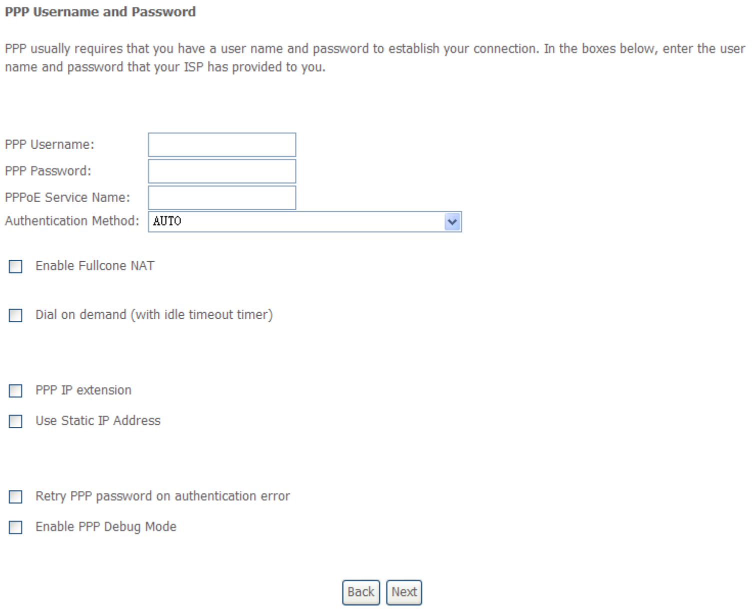
○ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

The connection type of PVC 0/35 is set to **PPP over Ethernet (PPPoE)** and the **Encapsulation Mode** is set to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

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



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:	
PPP Password:	
PPPoE Service Name:	
Authentication Method:	AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

□ Retry PPP password on authentication error

□ Enable PPP Debug Mode

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

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

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

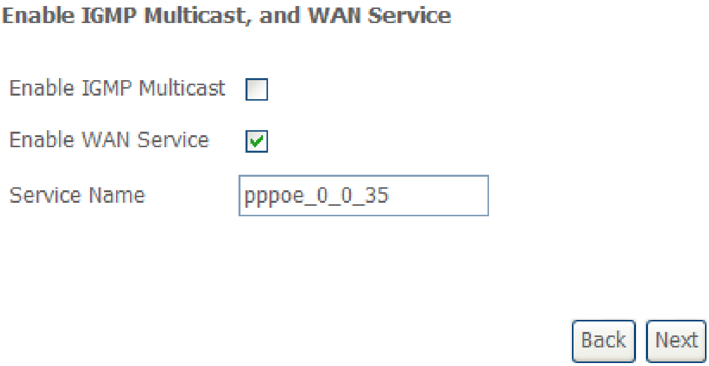
If this function is enabled, the modem uses this IP address as the WAN IP address.

Retry PPP password on authentication error:If this function is enabled, DSL will retry PPP password on authentication while authenticating with right password failure.

Enable PPP Debug Mode: The PPP Debug Mode enables connection debugging facilities. If this function is enabled, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

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

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



Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

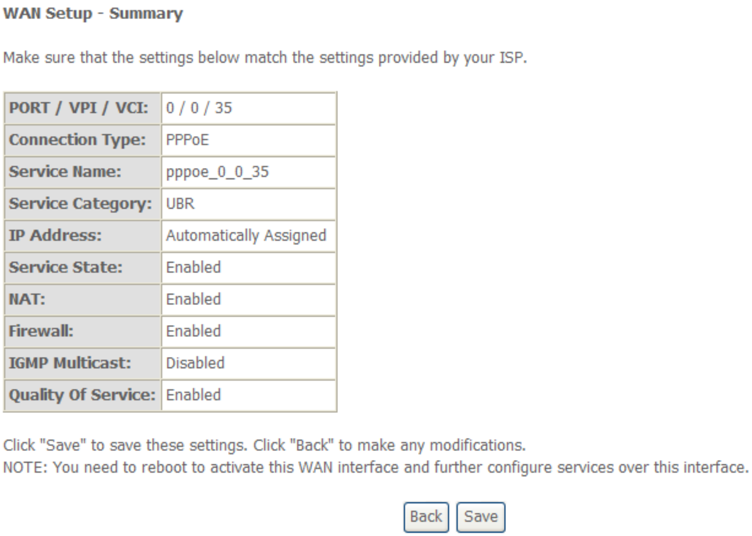
Service Name pppoe_0_0_35

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

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

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

This page shows all the configuration. You can view the default values of network address translation (NAT) enable and Firewall enable.



WAN Setup - Summary

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

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

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

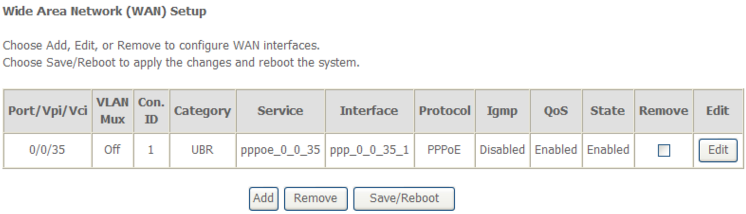
To save the settings, click **Save**. To make any modifications, click **Back**.

Note:

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

3.4.1.2 Adding a PPPoA PVC

This section describes the procedure for adding PVC 0/36(PPPoA mode).



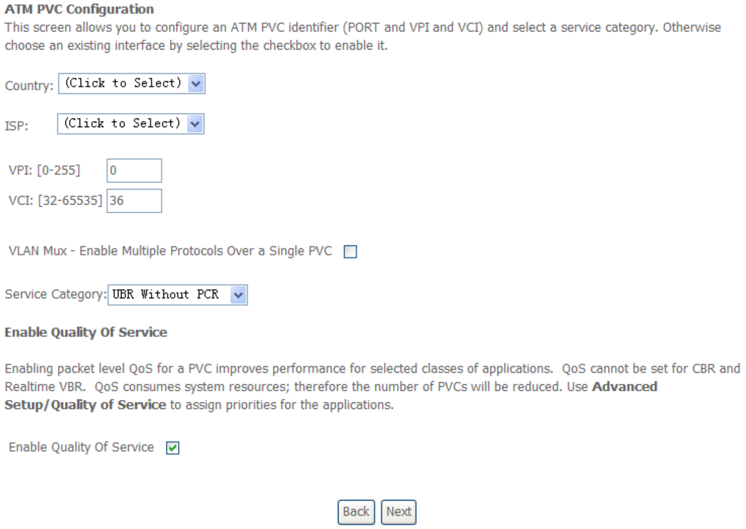
Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	□	Edit

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

In this page, you can modify VPI/VCI, service categories, and QoS.



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 36

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

Service Category: UBR Without PCR

Enable Quality Of Service

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

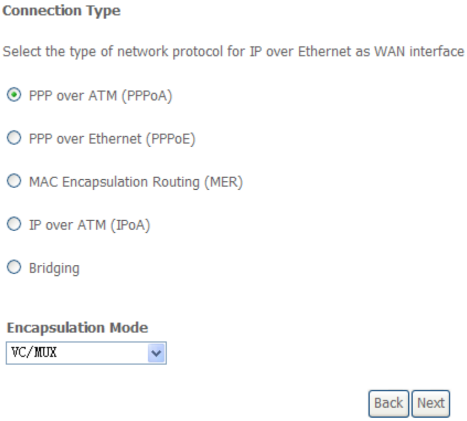
Enable Quality Of Service ☑

- **Country**: Select the **Country** from the drop-down list.
- **ISP**: Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 0/36 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

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

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



Connection Type

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

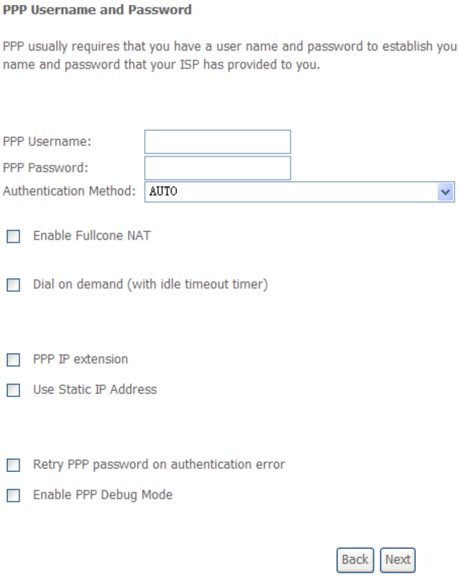
- ● PPP over ATM (PPPoA)
- ○ PPP over Ethernet (PPPoE)
- ○ MAC Encapsulation Routing (MER)
- ○ IP over ATM (IPoA)
- ○ Bridging

Encapsulation Mode

VC/MUX

The connection type is set to **PPP over ATM (PPPoA)** and the **Encapsulation Mode** is set to **VC/ MUX**.

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



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

□ Retry PPP password on authentication error

□ Enable PPP Debug Mode

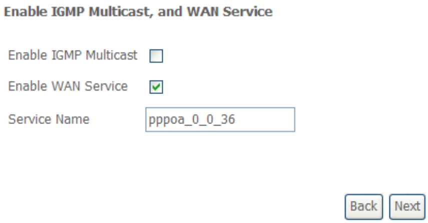
In this page, you need to enter the **PPP Username** and **PPP Password**.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you**.**
- **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.
- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached to the modem (at this time, the modem connects to only one PC).

- **Use Static IP Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Retry PPP password on authentication error**:If this function is enabled, DSL will retry PPP password on authentication while authenticating with right password failure.
- **Enable PPP Debug Mode:** The PPP Debug Mode enables connection debugging facilities. If this function is enabled, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

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

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



Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

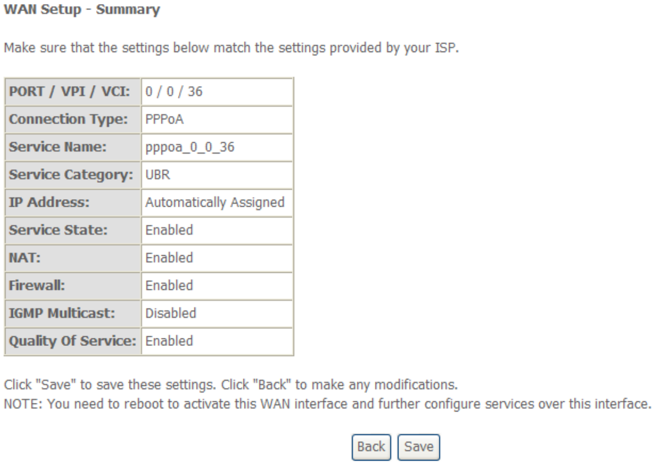
Service Name pppoa_0_0_36

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

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

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

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



WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 36
Connection Type:	PPPoA
Service Name:	pppoa_0_0_36
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

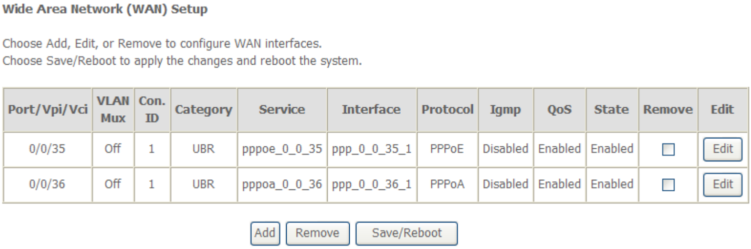
To save the settings, click **Save**. To make any modifications, click **Back**.

Note:

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

3.4.1.3 Adding an MER PVC

This section describes the procedure for adding PVC 0/37 (MER mode).



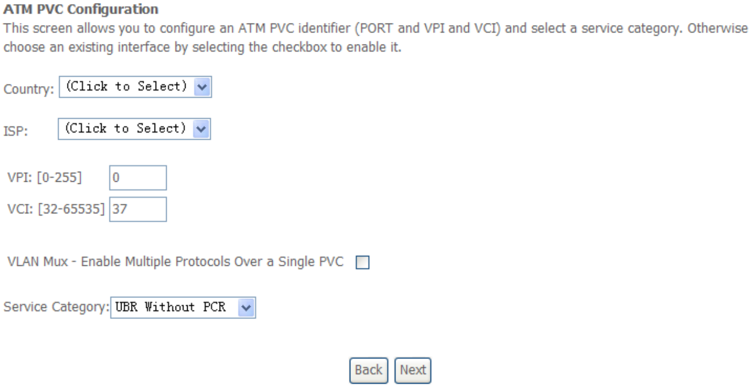
Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	□	Edit
0/0/36	Off	1	UBR	pppoa_0_0_36	ppp_0_0_36_1	PPPoA	Disabled	Enabled	Enabled	□	Edit

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

In this page, you can modify VPI/VCIs, service categories.



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 37

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

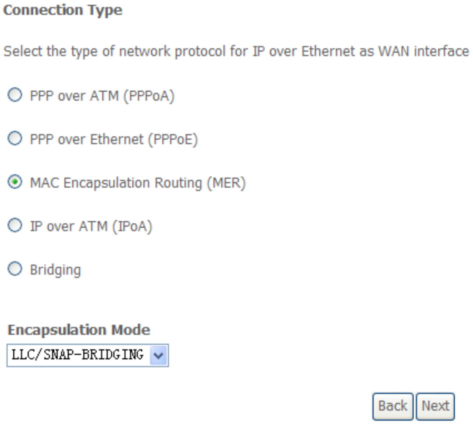
Service Category: UBR Without PCR

- **Country**: Select the **Country** from the drop-down list.
- **ISP**: Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
- **VPI**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

In this example, PVC 0/37 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

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

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



Connection Type

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

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

● MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

○ Bridging

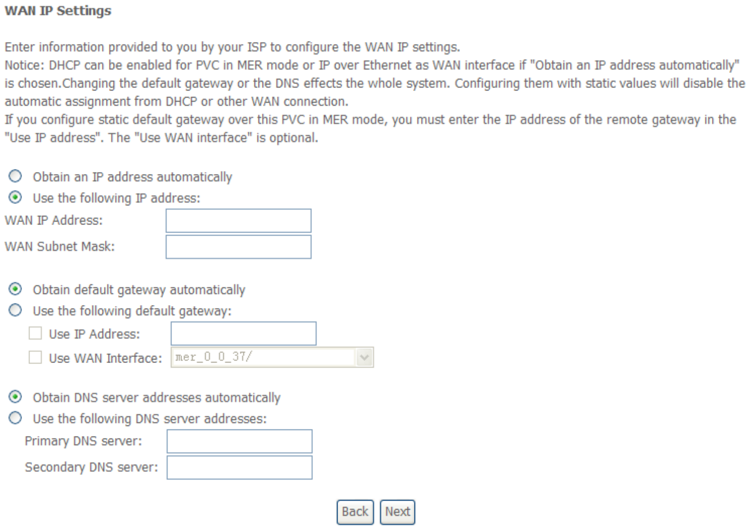
Encapsulation Mode

LLC/SNAP-BRIDGING

The connection type of PVC 0/37 is set to **MAC Encapsulation Routing (MER)** and the **Encapsulation Mode** is set to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

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

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



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

○ Obtain an IP address automatically
● Use the following IP address:
WAN IP Address:
WAN Subnet Mask:

● Obtain default gateway automatically
○ Use the following default gateway:
□ Use IP Address:
□ Use WAN Interface: mer_0_0_37/

● Obtain DNS server addresses automatically
○ Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

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

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

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

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

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

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

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

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

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

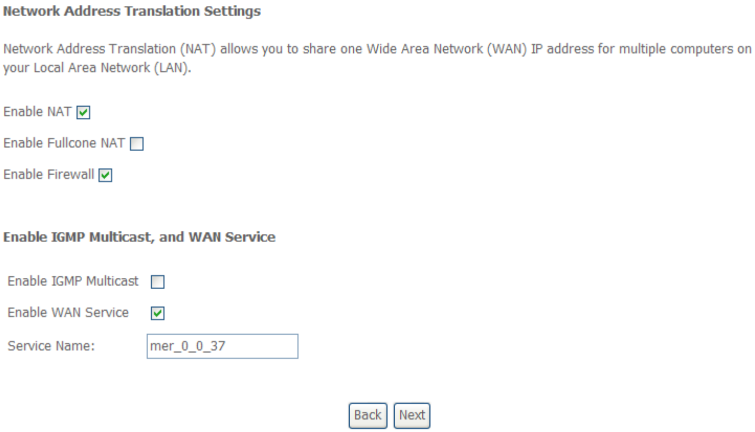
Use the following DNS server addresses: If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

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

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

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

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



Network Address Translation Settings

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

Enable NAT ☑

Enable Fullcone NAT □

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: mer_0_0_37

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

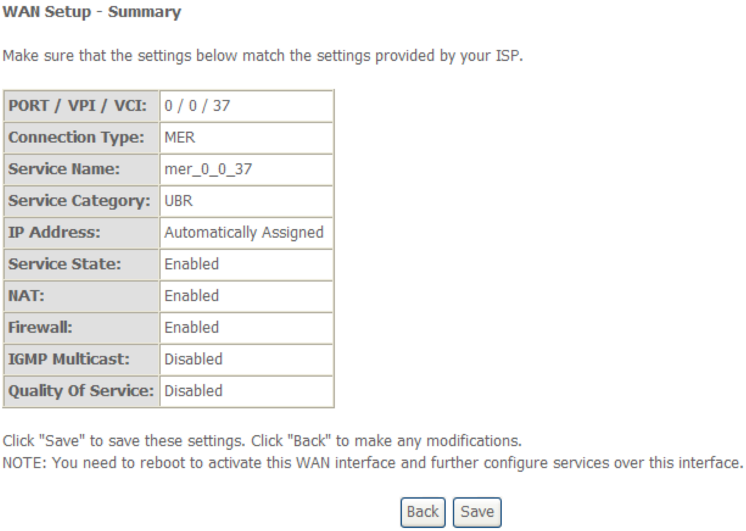
Enable Fullcone NAT: A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall: Enable or disable IP filtering.

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

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

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



WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 37
Connection Type:	MER
Service Name:	mer_0_0_37
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

To save the settings, click **Save**. To make any modifications, click **Back**.

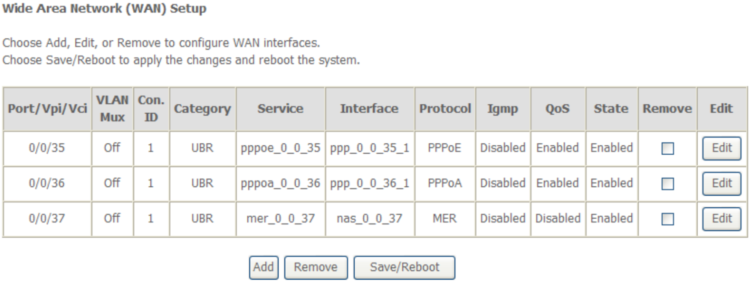
Note:

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

3.4.1.4 Adding an IPoA PVC

This section describes the procedure for adding PVC 0/38 (IPoA mode).

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

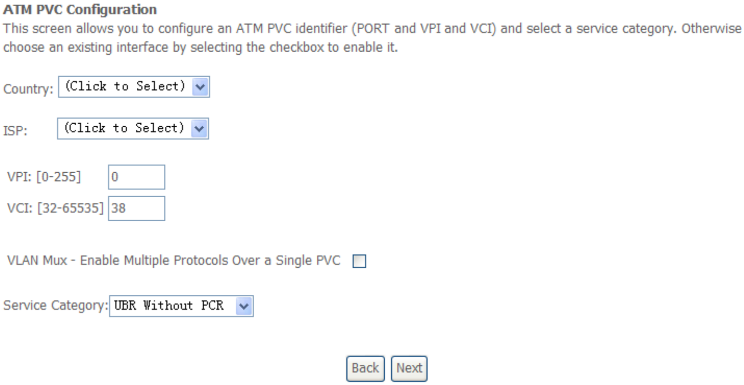


Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	□	Edit
0/0/36	Off	1	UBR	pppoa_0_0_36	ppp_0_0_36_1	PPPoA	Disabled	Enabled	Enabled	□	Edit
0/0/37	Off	1	UBR	mer_0_0_37	nas_0_0_37	MER	Disabled	Disabled	Enabled	□	Edit

In this page, you can modify VPI/VCIs, service categories.



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 38

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

Service Category: UBR Without PCR

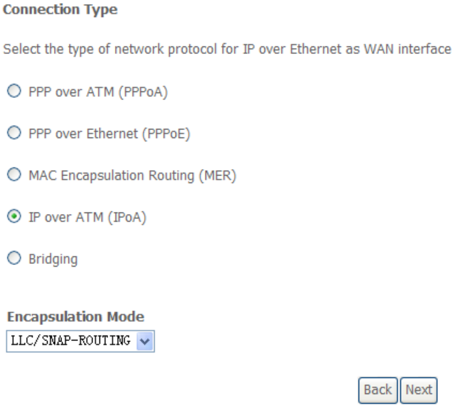
- **Country**: Select the **Country** from the drop-down list.
- **ISP**: Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

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

In this example, PVC 0/38 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

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

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



Connection Type

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

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

● IP over ATM (IPoA)

○ Bridging

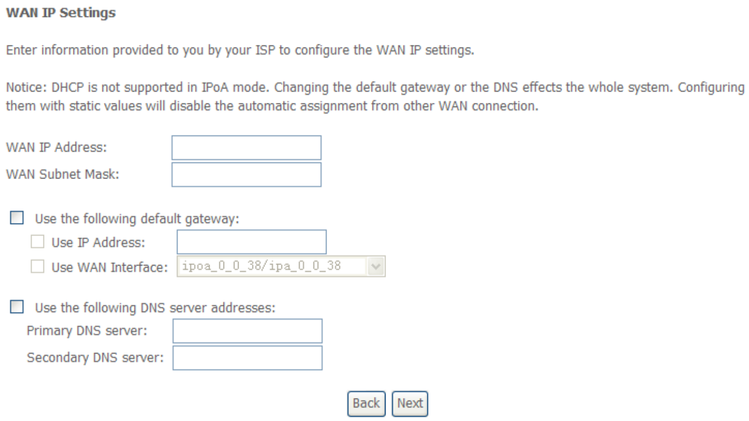
Encapsulation Mode

LLC/SNAP-ROUTING

The connection type of PVC 0/38 is set to **IP over ATM (IPoA)** and the **Encapsulation Mode** is set to **LLC/SNAP-ROUTING** (according to the uplink equipment).

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

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



WAN IP Settings

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

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

WAN IP Address:

WAN Subnet Mask:

□ Use the following default gateway:

□ Use IP Address:

□ Use WAN Interface: ipoa_0_0_38/ipa_0_0_38

□ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

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

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

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

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

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

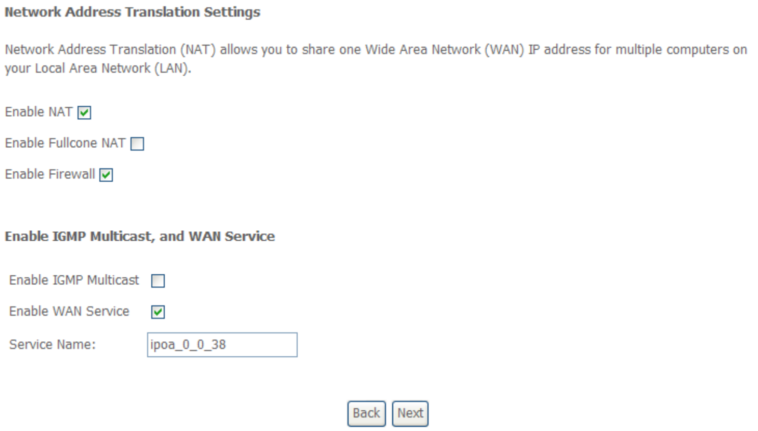
Use the following DNS server addesses: If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

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

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

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

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



Network Address Translation Settings

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

Enable NAT ☑

Enable Fullcone NAT □

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: ipoa_0_0_38

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

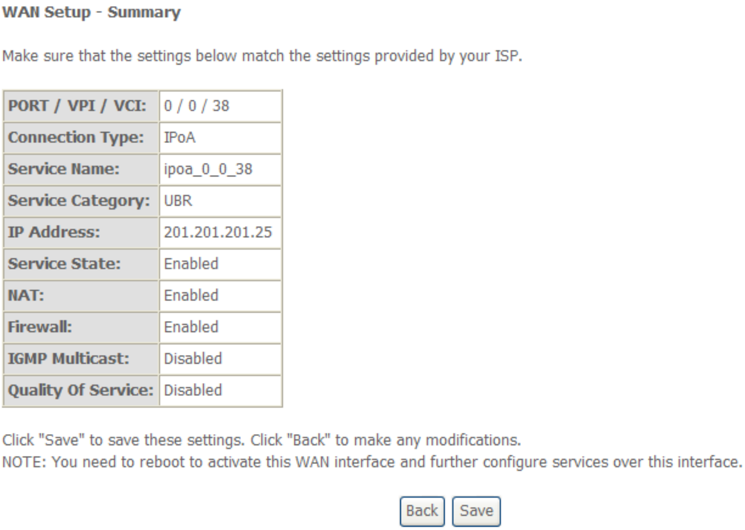
Enable Fullcone NAT: A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall: Enable or disable IP filtering.

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

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

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



WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 38
Connection Type:	IPoA
Service Name:	ipoa_0_0_38
Service Category:	UBR
IP Address:	201.201.201.25
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

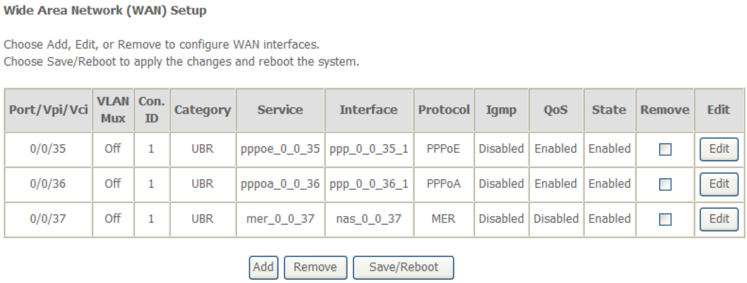
To save the settings, click **Save**. To make any modifications, click **Back**.

Note:

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

3.4.1.5 Adding a Bridge PVC

This section describes the procedure for adding PVC 0/39 (Bridge mode).



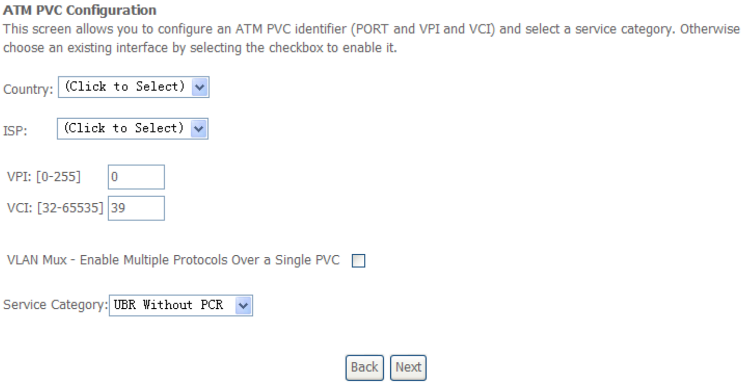
Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	□	Edit
0/0/36	Off	1	UBR	pppoa_0_0_36	ppp_0_0_36_1	PPPoA	Disabled	Enabled	Enabled	□	Edit
0/0/37	Off	1	UBR	mer_0_0_37	nas_0_0_37	MER	Disabled	Disabled	Enabled	□	Edit

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

In this page, you can modify VPI/VCIs, and service categories.



ATM PVC Configuration

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

Country: (Click to Select)

ISP: (Click to Select)

VPI: [0-255] 0

VCI: [32-65535] 39

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

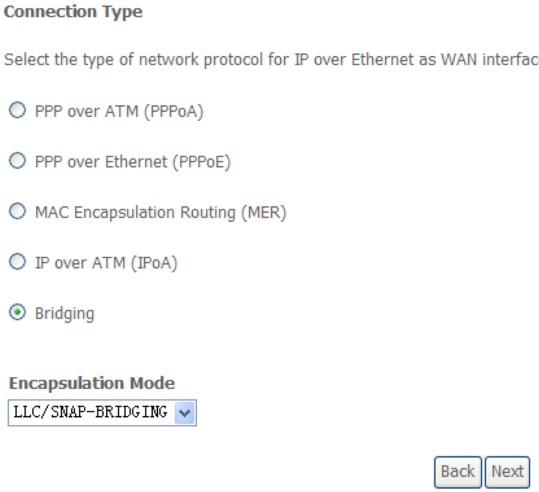
Service Category: UBR Without PCR

- **Country**: Select the **Country** from the drop-down list.
- **ISP**: Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
- **VPI (Virtual Path Identifier)**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

In this example, PVC 0/39 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

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

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



Connection Type

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

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

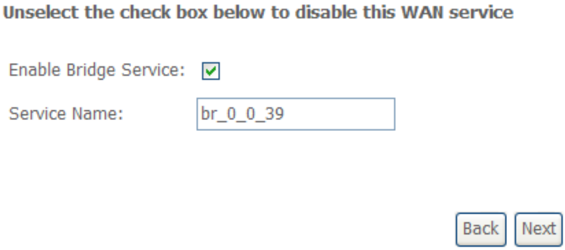
○ IP over ATM (IPoA)

● Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

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



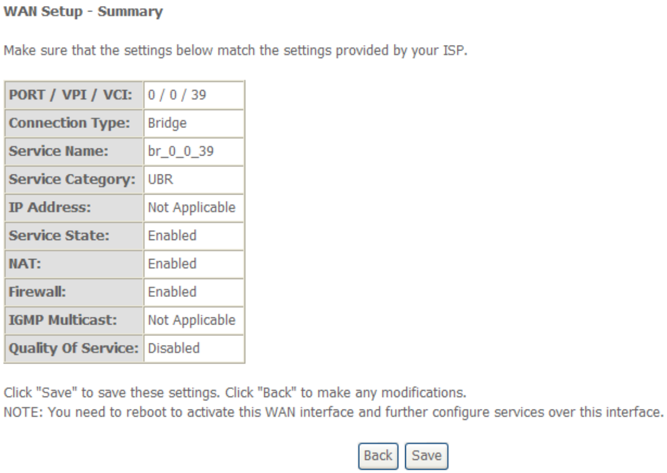
Unselect the check box below to disable this WAN service

Enable Bridge Service: ☑

Service Name: br_0_0_39

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

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



WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 39
Connection Type:	Bridge
Service Name:	br_0_0_39
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

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

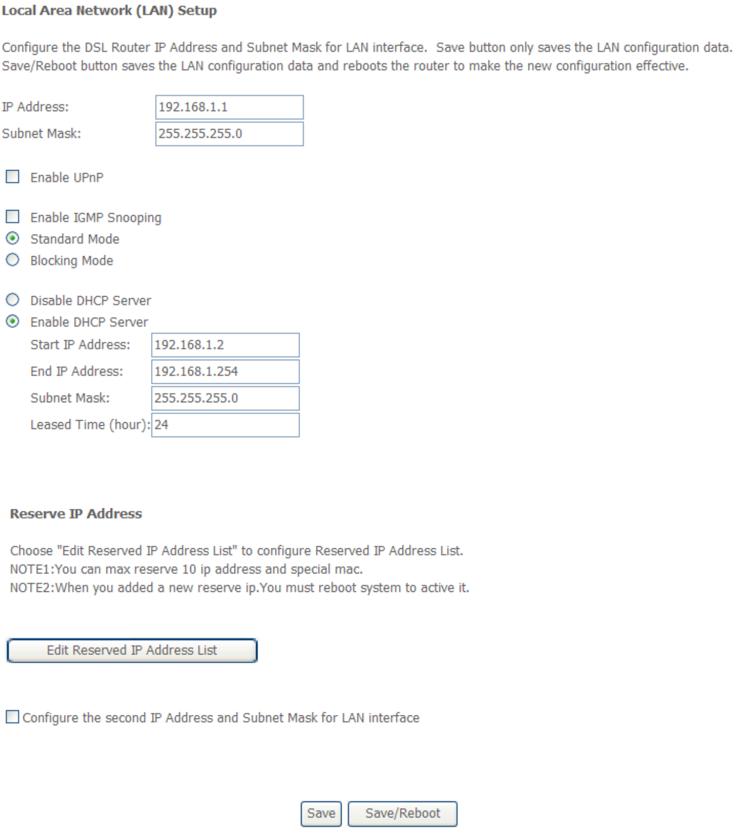
To save the settings, click **Save**. To make any modifications, click **Back**.

Note:

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

3.4.2 LAN Configuration

You can use the LAN configuration to define an IP address for the DSL Router and configure the DHCP server.



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

□ Enable UPnP

□ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

○ Disable DHCP Server
● Enable DHCP Server

Start IP Address:	192.168.1.2
End IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Leased Time (hour):	24

Reserve IP Address

Choose "Edit Reserved IP Address List" to configure Reserved IP Address List.
NOTE1:You can max reserve 10 ip address and special mac.
NOTE2:When you added a new reserve ip.You must reboot system to active it.

□ Configure the second IP Address and Subnet Mask for LAN interface

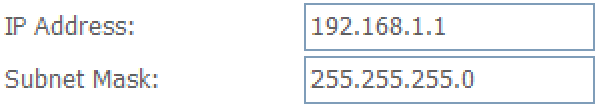
3.4.2.1 Defining the Private IP Address for the DSL Router

In this page, you can change 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.

- If you want to assign a different IP address to the DSL Router, enter it in the field next to IP address.
- Adjust the subnet mask if necessary.

It is recommended to use an address from a block that is reserved for private use.

The address block is 192.168.1.1~192.168.255.254.



IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

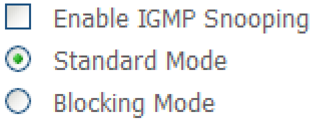
Note:

New settings can only be made after the DSL Router is rebooted. If necessary, reconfigure the IP address on your PC (including the one that is statically assigned) so that it matches the new configuration.

3.4.2.2 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. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the content of the first computer. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.



□ Enable IGMP Snooping

● Standard Mode

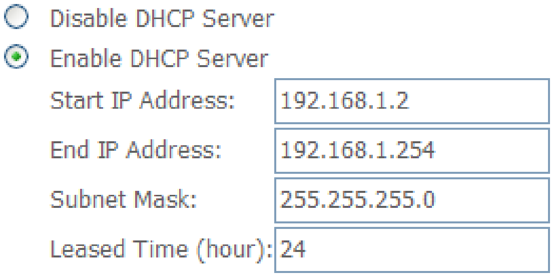
○ Blocking Mode

Note:

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

3.4.2.3 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.



○ Disable DHCP Server

● Enable DHCP Server

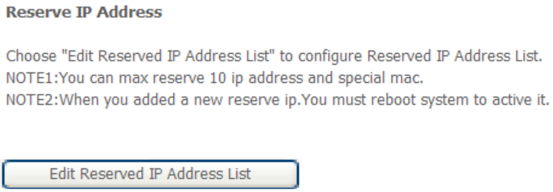
Start IP Address:	192.168.1.2
End IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Leased Time (hour):	24

Note:

- If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automatically is set up.
- If you deactivate the DHCP server, you need to assign a static IP address for the PCs that use the network settings.
- If the DHCP server is active, you can define a lease time. The lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.
- Define the range of IP addresses that the Router should use to automatically assign IP addresses to the PCs. Define the first issued IP address and the last issued IP address.

3.4.2.4 Reserve IP Address

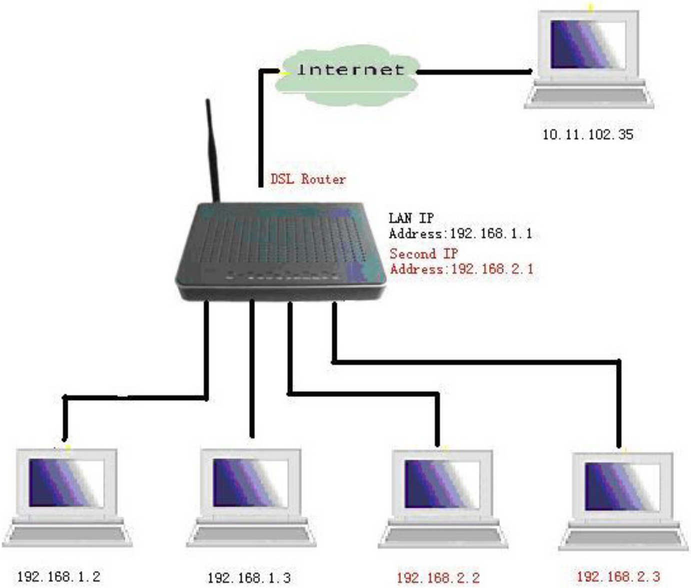
If you want to reserve one specific IP address for a certain PC by MAC address, edit the reserved IP Address List.



Reserve IP Address

Choose "Edit Reserved IP Address List" to configure Reserved IP Address List.
NOTE1:You can max reserve 10 ip address and special mac.
NOTE2:When you added a new reserve ip.You must reboot system to active it.

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



3.4.3 NAT

3.4.3.1 Overview

The DSL Router is equipped with the NAT function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses.

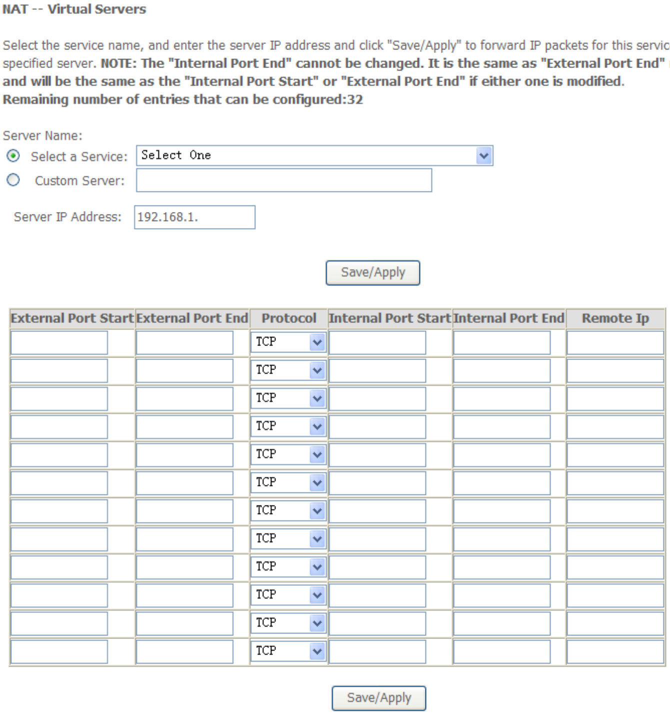
You can activate or deactivate the NAT function when you select these connection types of network protocol, for example, PPPoA, MER and IPoA. Once you add a WAN interface with PPPoE, the NAT function is activated by default. Otherwise, if selecting the type of Bridging, you could not configure NAT function.

3.4.3.2 Virtual Server Setup

The Virtual Server page is used to define applications that require special handling by DSL router. All you need to do is to select the application protocol and the local IP address of the computer that is using or providing the service. You can also add new protocols, besides the most common ones provided by DSL router.

Adding Virtual Servers

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**
Remaining number of entries that can be configured:32

Server Name:
● Select a Service: Select One
○ Custom Server:

Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Step 2 Select a service or enter a custom server.

Step 3 Set **Server IP Address**.

Step 4 Enter the Server IP address of the computer that provides the service (the server in the **Local Host** field).

Note:

Unless an additional external IP address is added, only one LAN computer can be assigned to provide a specific service or application.

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

Step 6 Select **Protocol**.

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

Step 8 Enter **Remote IP**.

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

If the application you require is not in the list, manually enter the information. Select the protocol for the service you are providing from the **Protocol** drop-down list. Under **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.

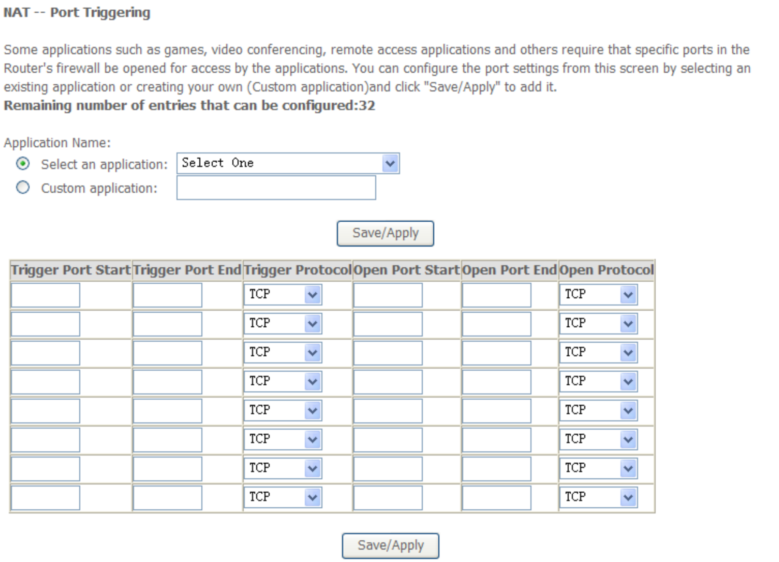
Step 2 Click **Remove** button to apply the settings.

3.4.3.3 Port Triggering

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

Adding Port Triggering

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



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Application Name:

● Select an application: Select One

○ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

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

- **Trigger Port Start and Trigger Port End**: Enter the port that is to be monitored for outgoing data traffic.
- **Trigger Protocol**: Select the protocol that is to be monitored for outgoing data traffic.
- **Open Protocol**: Select the protocol that is to be allowed for incoming data traffic
- **Open Port Start and Open Port End**: Enter the port that is to be opened for incoming traffic.

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

Removing Port Triggering

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

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

3.4.3.4 DMZ Host

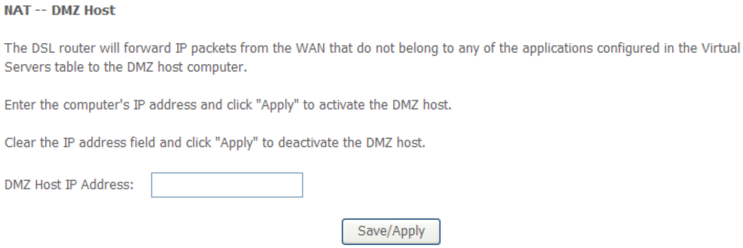
The DMZ host feature allows one local computer to be exposed to the Internet. You can set up a client in your local network to be the DMZ host. Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients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

Note:

Only one PC per public IP address can be set up as an Exposed Host.

Adding a DMZ Host

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



NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

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

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

Removing a DMZ Host

Step 1 Clear the DMZ Host Address.

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

3.4.4 Security

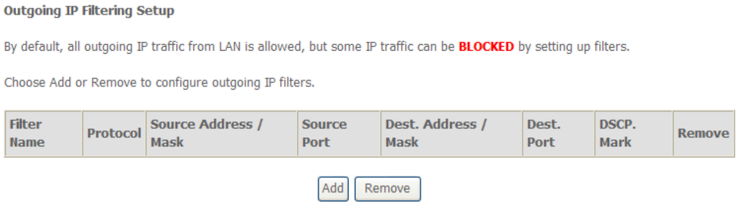
Security is an important function of DSL. It protects resources of a private network from users from other networks, and prevents unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet (that is, the local network to which you are connected) must pass through the security checks, which checks each message and blocks those that do not meet the specific security criteria.

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

Note:

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

If no PVC of Bridge mode is configured, MAC filtering is disabled and the MAC Filtering interface does not appear.



Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

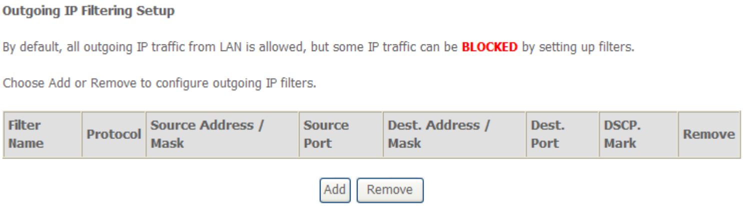
Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove

3.4.4.1 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. You can protect the network against hacker attacks and block access of individual PC to selected services or Internet websites.

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.



Outgoing IP Filtering Setup

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

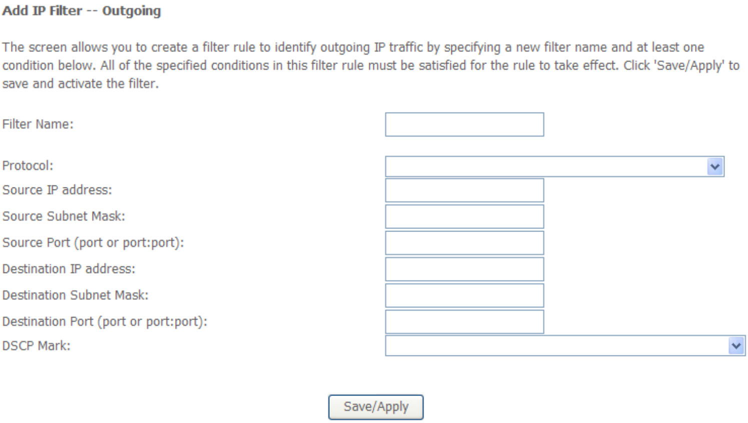
Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove

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

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

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



Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

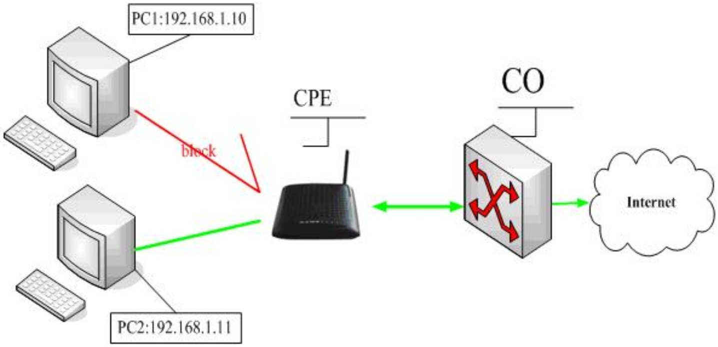
DSCP Mark:

- **Filter Name**: Enter the name of outgoing filter rule.
- **Protocol**: Select one from TCP/UDP, TCP, UDP, and ICMP protocols.

- **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 IP address**: IP address of the destination (default: null).
- **Destination port**: UPD/TCP destination port or a range of ports.
- **DSCP Mark**: Marking DSCP that outgoing packets.

The following is an example of configuring the outgoing IP filtering.

The topology is as follows:

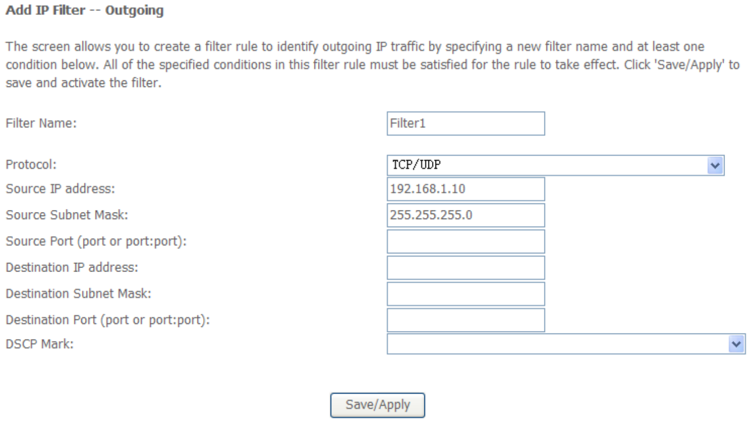


Request

- I need to block PC1 whose IP address is 192.168.1.10. All outgoing UDP/TCP packet from that PC1 (192.168.1.10) is not allowed.
- Allow all outgoing traffic packet from PC2 (192.168.1.11).

Configuration

Step 1 By default, all outgoing IP traffic from LAN is allowed. Hence, all outgoing IP packets from PC2 are allowed. The detailed configuration steps are as follows:

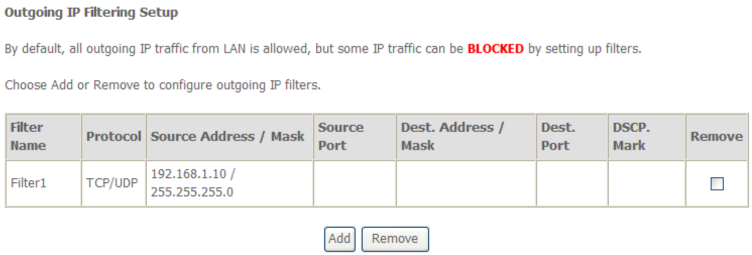


Add IP Filter -- Outgoing

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

Filter Name:	Filter1
Protocol:	TCP/UDP
Source IP address:	192.168.1.10
Source Subnet Mask:	255.255.255.0
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	
DSCP Mark:	

Step 2 Click **Save/Apply** and the following page appears:



Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

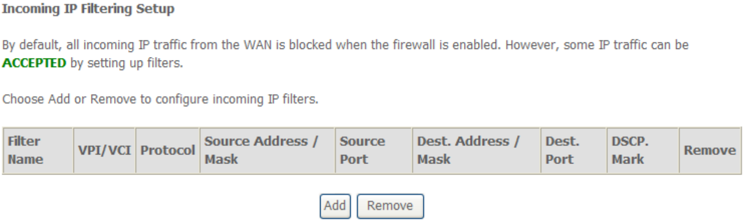
Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
Filter1	TCP/UDP	192.168.1.10 / 255.255.255.0					□

3.4.4.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmisstion from internet. By default incoming IP filter block all incoming packet from Internet. When incoming IP filtering rules setup being enable on the modem, you can permit remote individual PC to access various local network service.

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

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



Incoming IP Filtering Setup

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

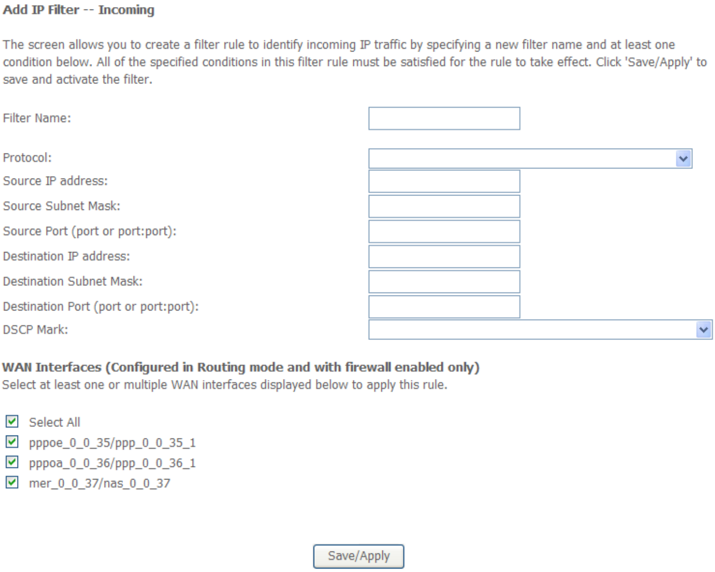
Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove

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.



Add IP Filter -- Incoming

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

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

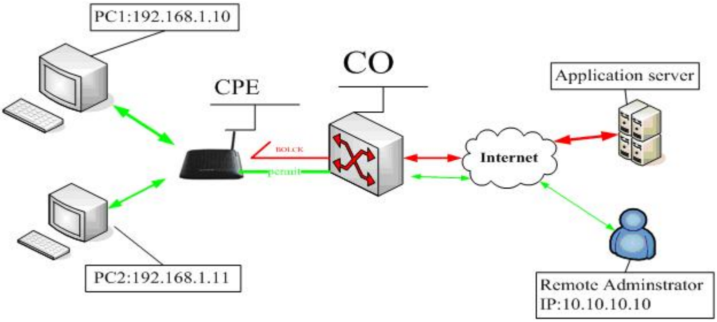
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All
☑ pppoe_0_0_35/ppp_0_0_35_1
☑ pppoa_0_0_36/ppp_0_0_36_1
☑ mer_0_0_37/nas_0_0_37

- **Filter Name**: Enter the name of incoming filter rule.
- **Protocol**: Select one from TCP/UDP, TCP, UDP, and ICMP protocols.

- **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.
- **DSCP Mark**: Marking DSCP that outgoing packets.
- **WAN interfaces**: You can select WAN interfaces and PVC.

The following is an example of configuring the incoming IP filtering:



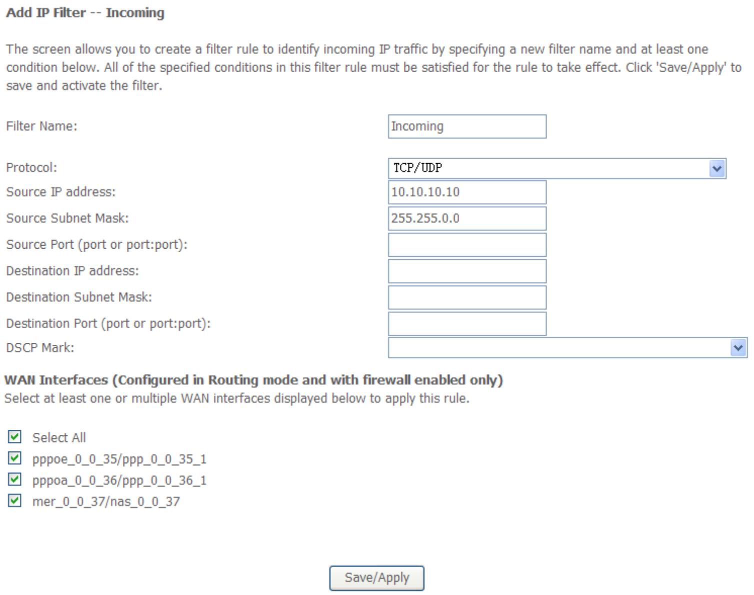
Request

- I need to permit a PC whose IP address is 10.10.10.10. All Incoming TCP/UDP packet traffic from that PC (10.10.10.10) is allowed.
- Block all IP traffic from other PCS.

Configuration

Step 1 By default, all incoming IP traffic from Internet is blocked. Hence, all incoming IP packets from other PCS except PC (10.10.10.10) are blocked.

Step 2 The detailed configuration steps are as follows:



Add IP Filter -- Incoming

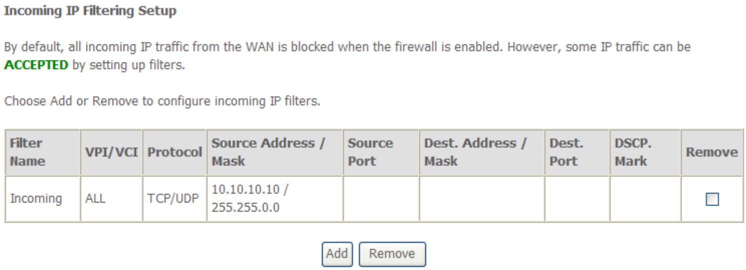
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:	Incoming
Protocol:	TCP/UDP
Source IP address:	10.10.10.10
Source Subnet Mask:	255.255.0.0
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	
DSCP Mark:	

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All
☑ pppoe_0_0_35/ppp_0_0_35_1
☑ pppoa_0_0_36/ppp_0_0_36_1
☑ mer_0_0_37/nas_0_0_37

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



Incoming IP Filtering Setup

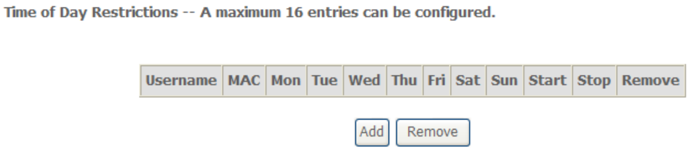
By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
Incoming	ALL	TCP/UDP	10.10.10.10 / 255.255.0.0					□

3.4.4.3 Parental Control

Choose **Content Filtering > Parental Control**, and the following page appears.

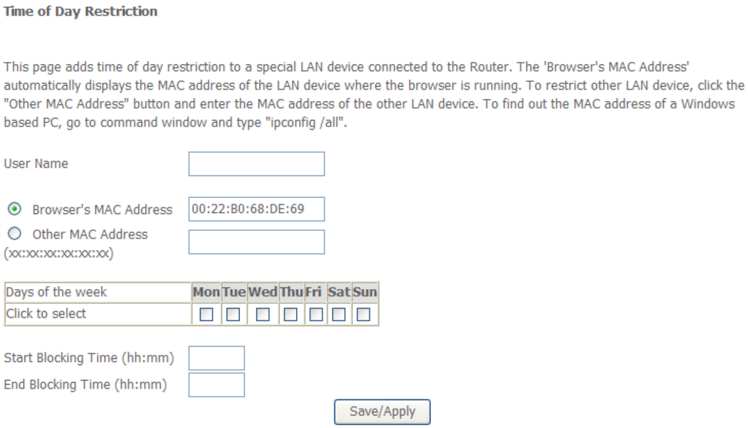


Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Figure 3 Time restriction setup

Click the **Add** button to display the following page.



Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

● Browser's MAC Address 00:22:B0:68:DE:69

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 4 Adding a time restriction rule

This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, se the user name and configure the time settings.

After finishing setting, click the click **Save**/**Apply** to save and apply the settings.

3.4.5 Quality of Service

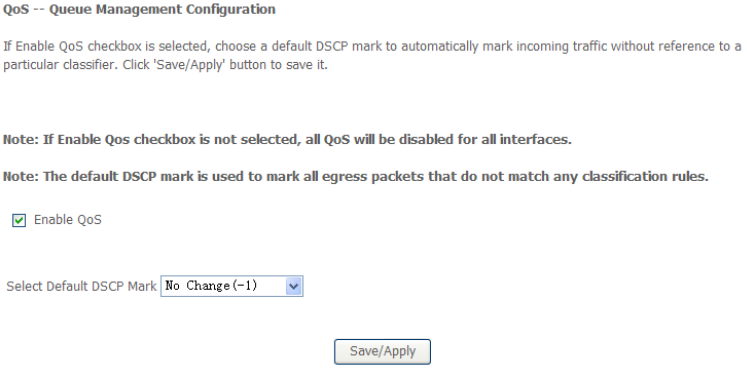
Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. QoS divides this capacity between the different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

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

3.4.5.1 Enabling QoS

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

Choose **Advance Setup** > **Quality of Service** and the following page appears:



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

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

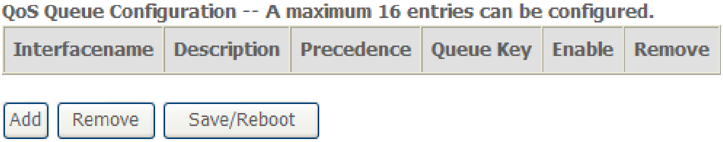
Click **Save/Apply** to active QoS.

3.4.5.2 QoS - Queue Configuration

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

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

QoS Queue Configuration can allocate three queues. Each of the queues can be configured for a precedence value. The queue entry configured is used by the classifier to place ingress packets appropriately.



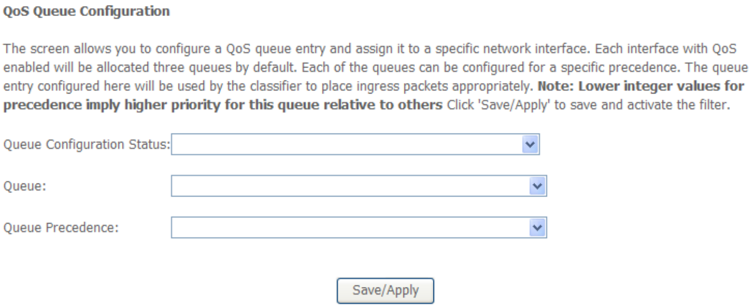
QoS Queue Configuration -- A maximum 16 entries can be configured.

Interfacename	Description	Precedence	Queue Key	Enable	Remove

Note:

Lower integer values for precedence indicate higher priority for this queue relative to others.

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



QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

Queue:

Queue Precedence:

Queue Configuration Status: Set to enable or disable a QoS queue.

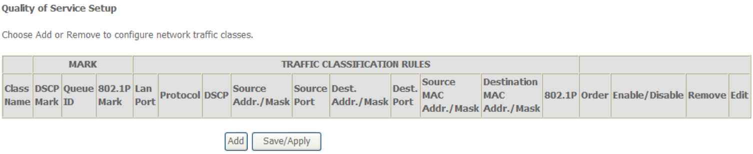
Queue: Select a specific network interface. The modem automatically allocates selected network interface to the queue.

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

3.4.5.3 QoS - QoS Classification

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

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

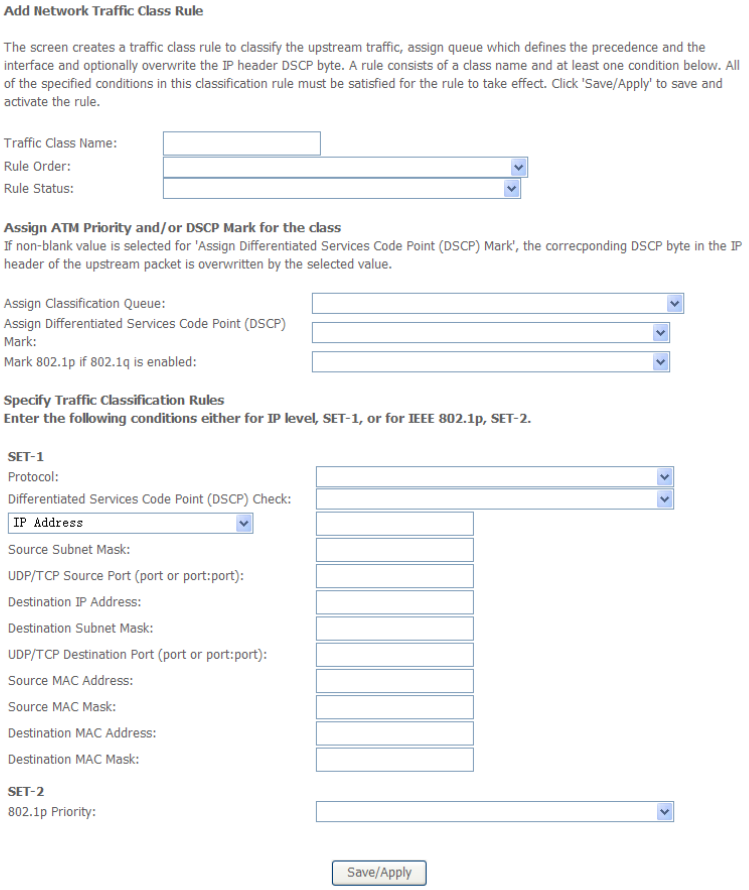


Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

	MARK			TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit

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



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:

Rule Order:

Rule Status:

Assign ATM Priority and/or DSCP Mark for the class

If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

Specify Traffic Classification Rules

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

SET-1

Protocol:

Differentiated Services Code Point (DSCP) Check:

IP Address

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

SET-2

802.1p Priority:

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

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

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

Set-1 Rules contain the following:

- **Protocol**: Select one among TCP/UDP TCP UDP or ICMP protocols.

Set-2 Rules contain the following:

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

3.4.6 Routing

3.4.6.1 Routing – Default Gateway

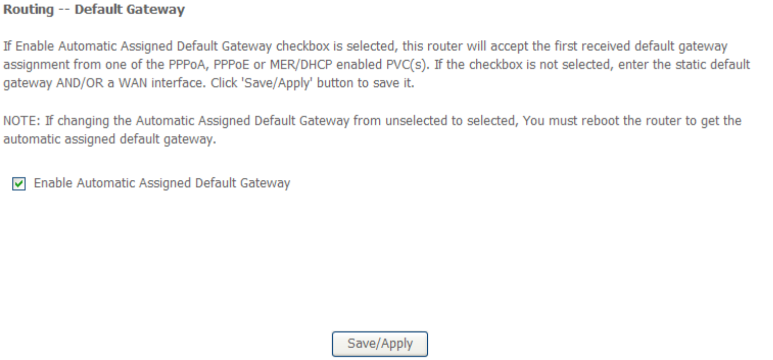
In this page, you can modify the Default Gateway settings.

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this router accepts the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or a WAN interface. Click **Save/Apply** to save it.

Note:

After changing the **Automatic Assigned Default Gateway** from unselected to selected, you must reboot the router to obtain the automatic assigned default gateway.

If you want to use a default gateway, select the **Enable Automatic Assigned Default Gateway** check box to show the following page:



Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

Use Default Gateway: Select the **Enable automatic Assigned Default Gateway** box.

Custom DSL router Default Gateway

- Enable Automatic Assigned Default Gateway
- Use Default Gateway IP Address
- Use Interface: interface that the packets pass through on the modem

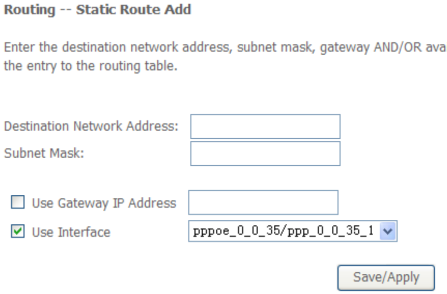
Click **Save/Apply** to apply the settings.

3.4.6.2 Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.



Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

□ Use Gateway IP Address

☑ Use Interface pppoe_0_0_35/ppp_0_0_35_1

Adding Static Route

Step 1 Enter destination network address.

Step 2 Enter subnet Mask.

Step 3 Enable **Use Gateway IP Address** and enter IP address.

Step 4 Select use interface.

Step 5 Click **Save/Apply** to apply the settings.

Remove static route

Select Remove box in the table, and click **Remove** to apply the settings.

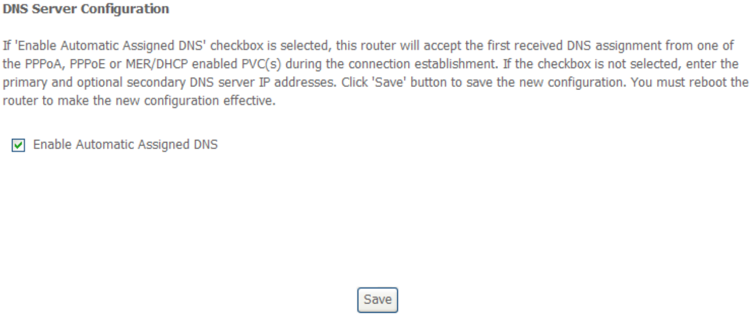
3.4.7 DNS

Domain Name System (or Service or Server) (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks other DNSs one by one, until the correct IP address is returned.

3.4.7.1 DNS Server

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



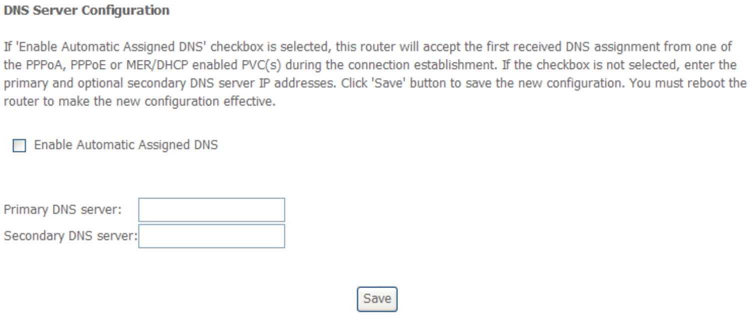
DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

☑ Enable Automatic Assigned DNS

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

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



DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

□ Enable Automatic Assigned DNS

Primary DNS server:

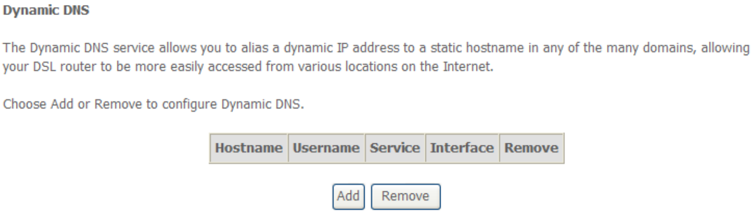
Secondary DNS server:

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

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

3.4.7.2 Dynamic DNS

Choose **Advanced > Dynamic DNS** and the following page appears.



Dynamic DNS

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

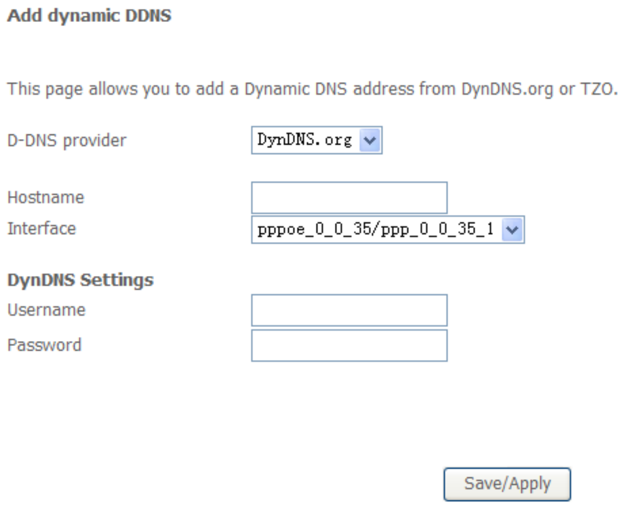
Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure 5 Dynamic DNS

- **Hostname**: The hostname of the server.
- **Username**: The access username of the DDNS service.
- **Service**: The service name of the selected WAN service.
- **Interface**: The selected WAN service.
- **Remove**: Enable the check-box to select the DDNS service to be removed.
- **Add**: Click to add a DDNS service. The Add Dynamic DNS window opens.
- **Remove**: Click to remove the selected DDNS service(s).

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



Add dynamic DDNS

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

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_0_35/ppp_0_0_35_1

DynDNS Settings

Username:

Password:

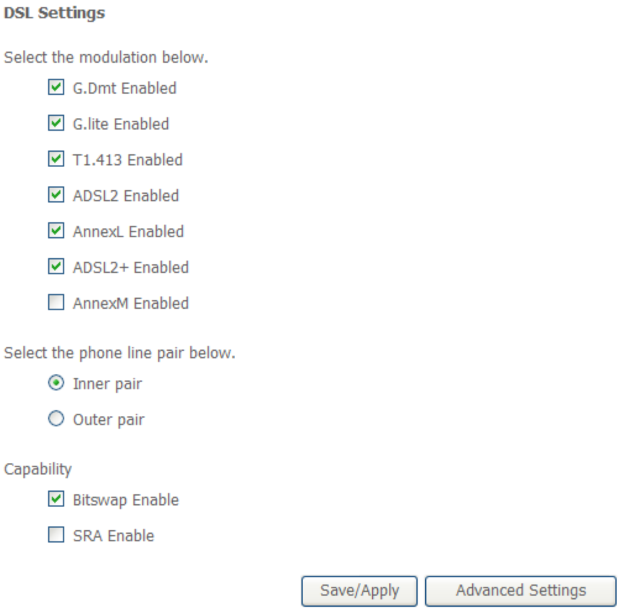
Figure 6 Adding a Dynamic DNS address

- **D-DNS provider**: Select a DDNS service provider. You can select **DynDNS.org** or **TZO.**
- **Hostname**: Enter the hostname of the server.
- **Interface**: Select a routing WAN service.
- **Username**: Enter the access username of the DDNS service.
- **Password**: Enter the password.

Click **Save/ Apply** to save and apply the settings.

3.4.8 DSL

Choose **Setup > DSL Settings** and the following page appears.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

□ AnnexM Enabled

Select the phone line pair below.

● Inner pair

○ Outer pair

Capability

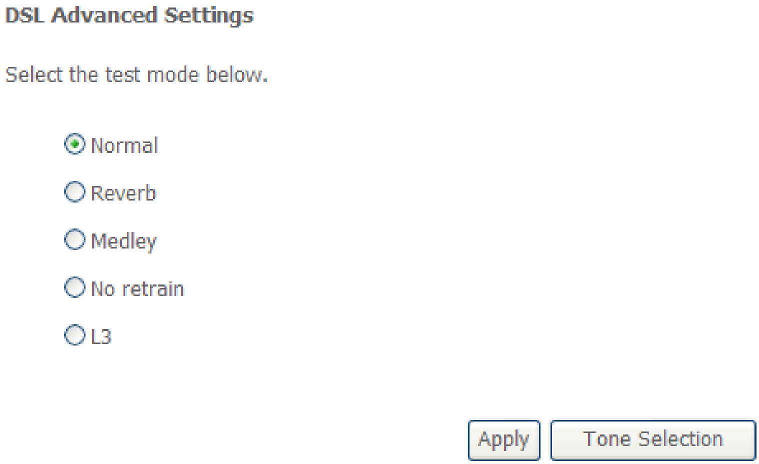
☑ Bitswap Enable

□ SRA Enable

Figure 7 DSL settings

In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

Click **Advanced Settings** and the following page appears.



DSL Advanced Settings

Select the test mode below.

● Normal

○ Reverb

○ Medley

○ No retrain

○ L3

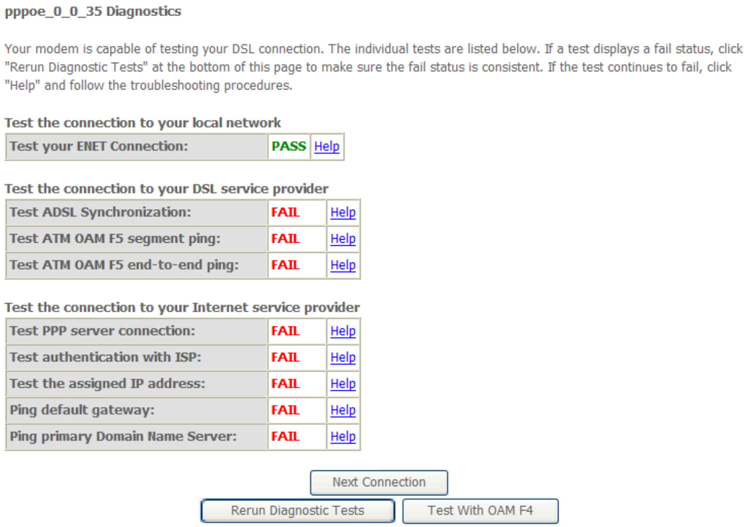
Figure 8 DSL Advanced Settings

Running tests in this page may make your DSL service inoperable. Do not change it unless your ISP asks you to. These tests are designed for use by an Internet Service Provider technician only. The DSL Advanced Settings page allows you to select a test mode, which you should only change when requested by your Internet Service Provider (ISP).

3.5 Diagnostics

Click **Diagnostics** to show the interface.

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



pppoe_0_0_35 Diagnostics

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

Test the connection to your local network

Test your ENET Connection:	PASS	Help

Test the connection to your DSL service provider

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

Test the connection to your Internet service provider

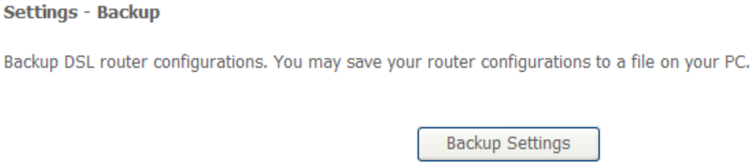
Test PPP server connection:	FAIL	Help
Test authentication with ISP:	FAIL	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

3.6 Management

3.6.1 Settings

Settings - Backup

Select the “Backup” to show the following interface. In the interface, you can backup the DSL router configurations.

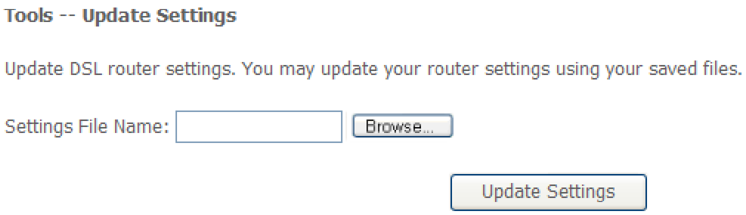


Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

Settings - Update

Select the “Update” to show the following interface. Click the “Browsing...” button to select the correct update configure settings file. Then click the “Update Settings” to update the router settings.



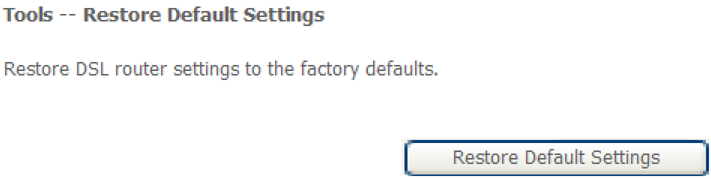
Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Settings – Restore Default

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

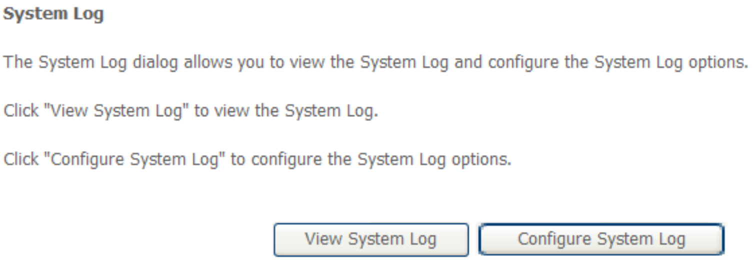


Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

3.6.2 System Log

Select “System Log” to show the following interface. The system log dialog allows you to view the system log and configure the system log options.



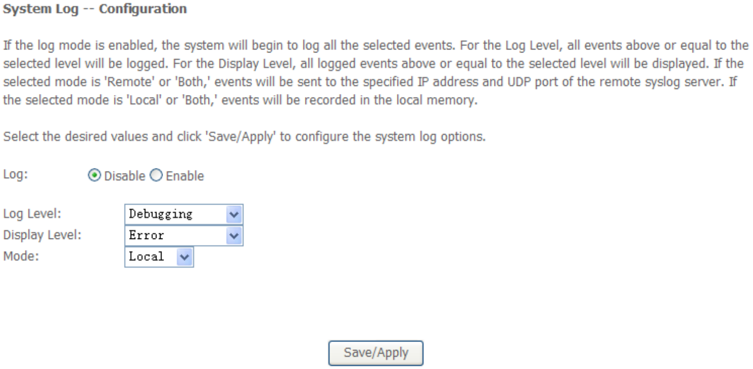
System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

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



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

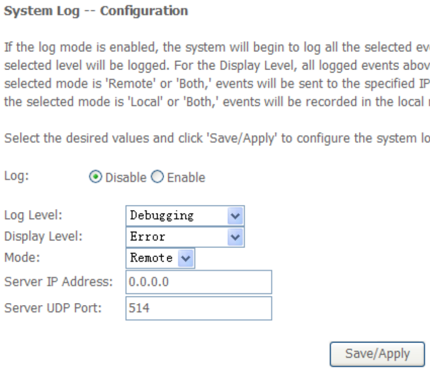
Log: ● Disable ○ Enable

Log Level: Debugging
Display Level: Error
Mode: Local

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

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

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



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

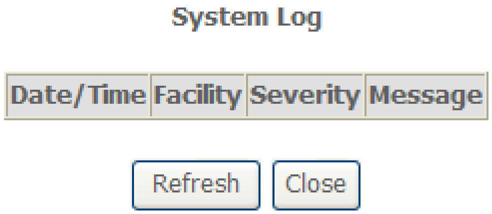
Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level:	Debugging
Display Level:	Error
Mode:	Remote
Server IP Address:	0.0.0.0
Server UDP Port:	514

After operations under “Configure System Log”, click “View System Log” to query the system logs.

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



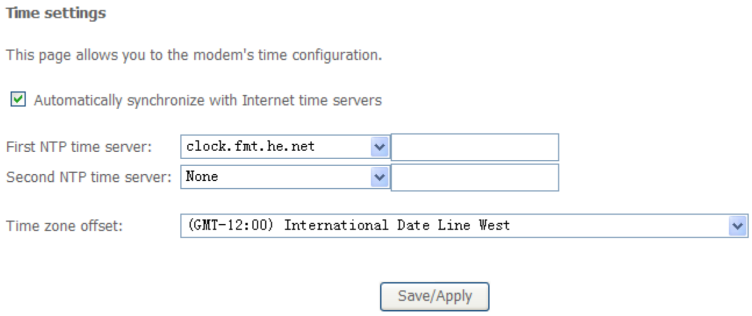
System Log

Date/Time	Facility	Severity	Message

Click “Refresh” to refresh the system event logs or “Close” to exit from this interface.

3.6.3 Internet Time

Choose **Management** > **Internet Time** and the following page appears. This page allows you to the modem's time configuration.



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: clock.fmt.he.net

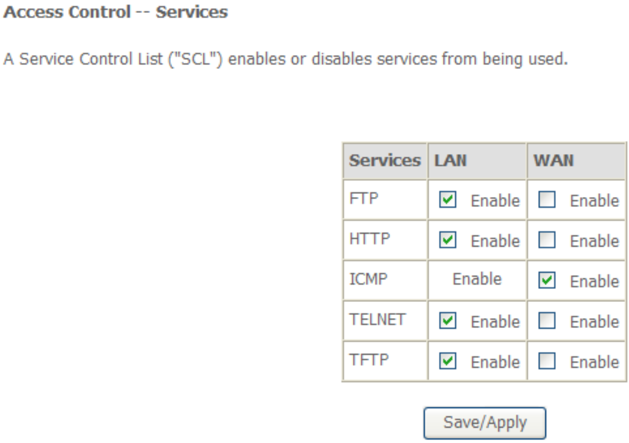
Second NTP time server: None

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

3.6.4 Access Control

Access Control – Services

Select "Access Control"-->"Services" to show the following interface. In the interface, you can enable/disable the FTP, HTTP, ICMP, TELNET and TFTP services. And the LAN side and WAN side show different configurations.



Access Control -- Services

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

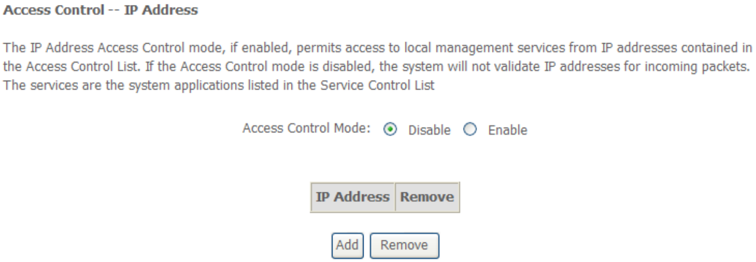
Services	LAN	WAN
FTP	☑ Enable	□ Enable
HTTP	☑ Enable	□ Enable
ICMP	Enable	☑ Enable
TELNET	☑ Enable	□ Enable
TFTP	☑ Enable	□ Enable

Note:

The WAN information is not displayed in the bridge mode.

Access Control – IP Addresses

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



Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

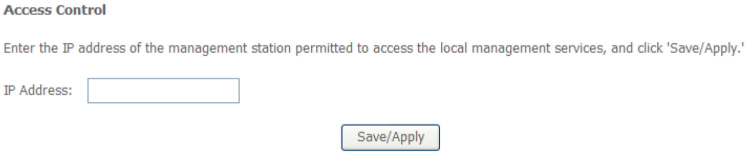
Access Control Mode: ● Disable ○ Enable

IP Address	Remove

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

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

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



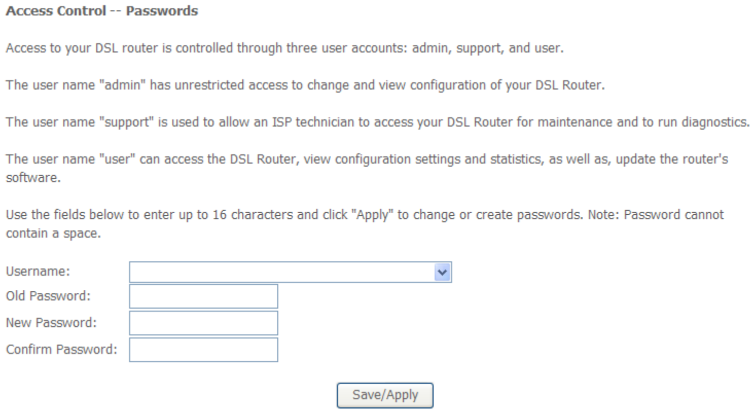
Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

Access Control – Passwords

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



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

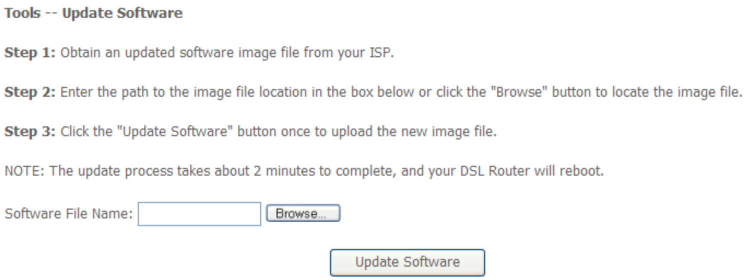
Old Password:

New Password:

Confirm Password:

3.6.5 Update Software

Click "Update Software" to show the following interface. In this interface, you can update the router software. Click the "Browse..." button to find the right version file and press "Update Software" to do the update.



Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

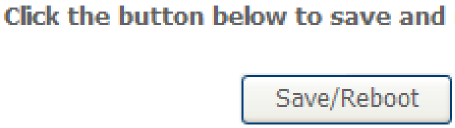
Software File Name:

Note: *Do not turn off your router during firmware updates. When the update is finished, the router reboots automatically. Do not turn off your router 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 router to the factory defaults and configure it again.

3.6.6 Save/Reboot

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



Click the button below to save and reboot the router.

4 Q&A

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

A: Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.

(2) **Q**: Why the **Ethernet** indicator is off?

A: Check the following

- The connection between the ADSL modem and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

(3) **Q**: Why the **Link** indicator is off?

A: Check the connection between the “Line” port of router and the wall jack.

(4) **Q**: Why Internet access fails while the **Link** indicator is on?

A: Check whether the VPI, VCI, user name, and password are correctly entered.

(5) **Q**: Why does the web configuration page of the modem fail to be accessed?

A: Choose **Start** > **Run** from the desktop, and ping ***192.168.1.1*** (IP address of the modem). If the modem cannot be reached, check the type of the network cable, the connection between the modem and the PC, and the TCP/IP configuration of the PC.

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

A: To restore the factory default, keep the device powered on; push a needle into the hole for about 5 seconds, and then release. The default IP address and subnet mask of the modem are **192.168.1.1** and **255.255.255.0** respectively.

- User/password of super user: **admin**/**admin**.
- User/password of common user: **user**/**user**