NWAR3650
User Manual

Contents

1 Introduction

The NWAR3650 is a highly ADSL2+ Integrated Access Device. The NWAR3650 can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet. And the wireless access supports IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

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

1.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Shared broadband internet access
- Audio and video streaming and transfer
- PC file and application sharing
- Wireless access

1.2 Environment Requirements

- Operating temperature: 0ºC~40ºC (32ºF to 104ºF)
- Storage temperature: -10ºC~55ºC (14ºF to 131ºF)
- Operating humidity: 10%~95%, non-condensing
- Storage humidity: 5%~95%, non-condensing
- Power adapter input: 100V~240V AC, 50/60Hz
- Power adapter output: 12V DC, 1A

1.3 System Requirements

Recommended system requirements are as follows:

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

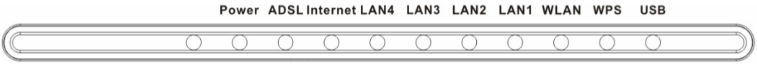
1.4 Safety Cautions

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

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat radiation is necessary to avoid any damage caused by overheating to the device. The holes are designed for heat radiation to ensure that the device works normally. Do not cover these heat radiant holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

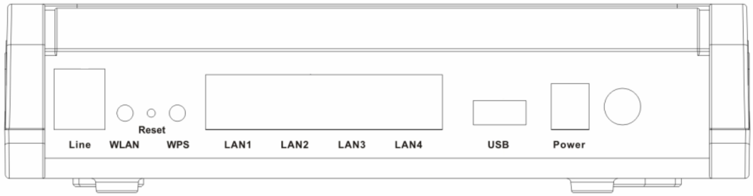
1.5 LED Status Description

1.5.1 Front Panel



Indicator	Color	Status	Description
Power	Green	Off	The power is off.
		On	The power is on and the device operates normally.
	Red	On	The power is self-testing.
		Blinks	Upgrading software.
ADSL	Green	Off	No signal is detected.
		Quick Blinks	The DSL line is training.
		Slow Blinks	The telephone cable is not connected to the device.
		On	The DSL line connection is established.
Internet	Green	Off	No internet connection.
		Blinks	The Internet data is passing through.
		On	The device has established the connection in route mode.
	Red	On	Device attempts to become Internet connected but fails.
LAN4/3/2/1	Green	Off	No Ethernet signal is detected.
		Blinks	The user data is passing through Ethernet port.
		On	Ethernet interface is ready to work
WLAN	Green	Off	No radio signal is detected.
		Blinks	The user data is passing through.
		On	WLAN interface is ready to work.
WPS	Green	Off	WPS service is not during using, or WPS service setup successfully.
		Blinks	The WPS service tries to establish.
		On	The WPS indicator is on for 5 seconds when the WPS service sets up successfully.
USB	Green	Off	No USB signal is detected.
		Blinks	The user data is passing through USB port.
		On	The USB interface is ready to work.

1.5.2 Rear panel



Interface	Description
Line	RJ-11 port: Connect the Modem to ADSL connector or splitter by telephone line.
WLAN	Enable or disable the WLAN. Press the button to enable WLAN.
Reset	To restore the factory default, keep the device powered on and push a long needle into the hole. Press down the button for 1 second and then release.
WPS	Enable or disable the WPS. Press the button to enable WPS.
LAN1/2/3/4	RJ-45 port: Conncet the Modem to a PC or other network device by network cable.
USB	USB host port, connect to another USB device to supply some value-added application.
Power	Power supplied port, plug in for power adapter that the power input is 12V DC, 1 A.
⏻	Power switch.

2 Hardware Installation

2.1 Choosing the Best Location for Wireless Operation

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

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

- Consider the direct line between access points and workstations:

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

- Building materials make difference:

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

- Position the antenna for best reception:

  Play around with the antenna position to see if signal strength improves. Some adapters or access points allow you to judge the strength of the signal.

- Keep your product away (at least 1~2 meters) from electrical devices:
- Keep wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

2.2 Connecting the ADSL Router

- See the following figure. Connect the Line port of the DSL Router with a telephone cable.
- Connect the LAN port of the DSL Router to the network card of the PC via an Ethernet cable.
- Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the DSL Router.

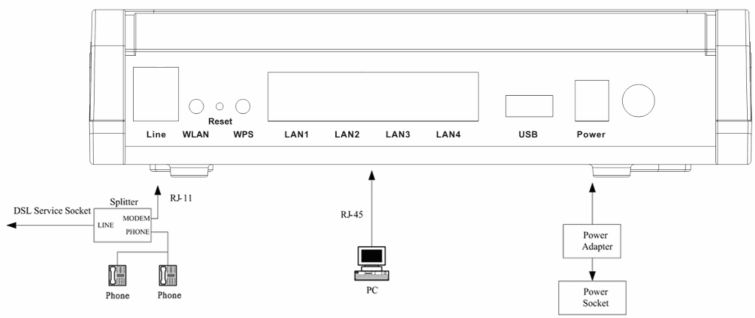


Figure 1 Without connecting telephone sets before the splitter

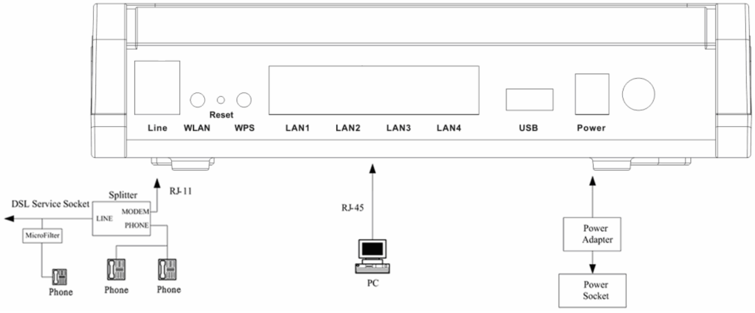


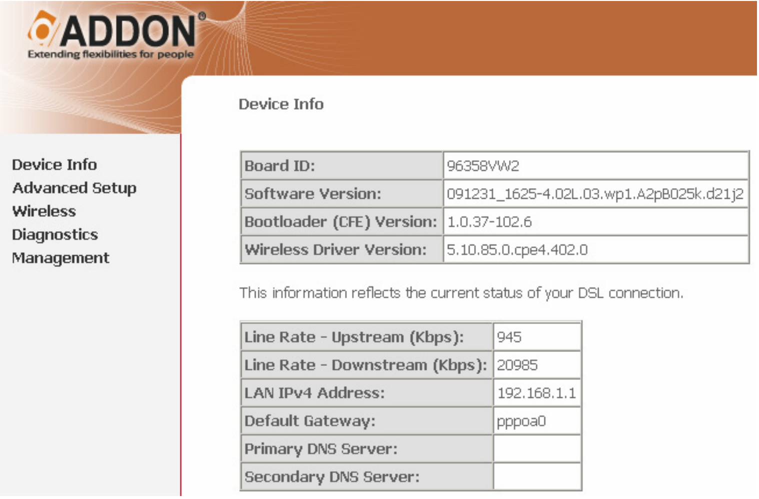
Figure 2 Connecting a telephone set before the splitter

3 Introduction to Web Configuration

Note:

The Web interface of software is for reference only.

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



Device Info

Board ID:	96358VW2
Software Version:	091231_1625-4.02L.03.wp1.A2pB025k.d21j2
Bootloader (CFE) Version:	1.0.37-102.6
Wireless Driver Version:	5.10.85.0.cpe4.402.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	945
Line Rate - Downstream (Kbps):	20985
LAN IPv4 Address:	192.168.1.1
Default Gateway:	pppoa0
Primary DNS Server:	
Secondary DNS Server:	

3.1 Logging In to the Modem

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

3.1.1 First-Time Login

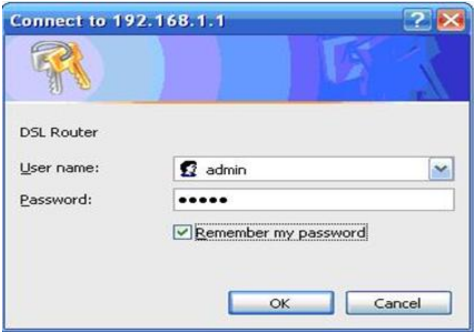
When you log in to the DSL Router for the first time, the login wizard appears.

Step 1 Open a Web browser on your computer.

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

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

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



Connect to 192.168.1.1

DSL Router

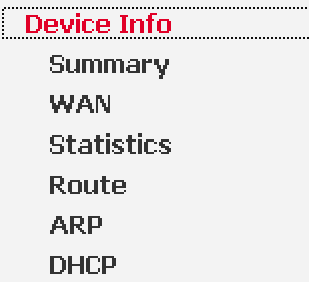
User name: admin

Password: •••••

☑ Remember my password

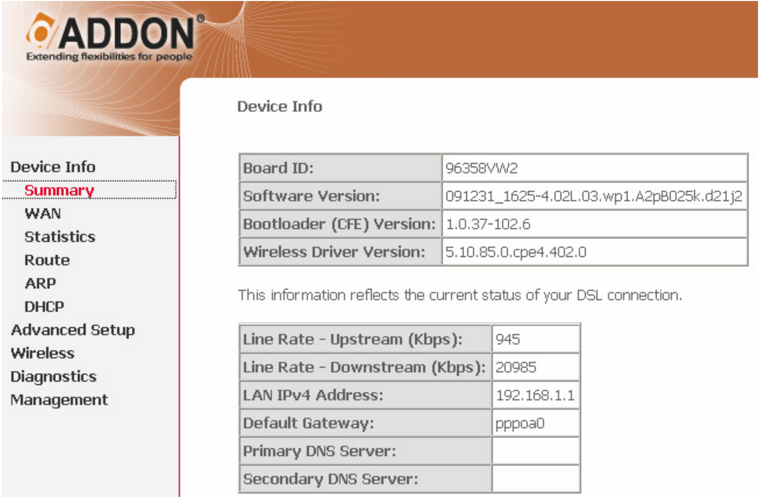
3.2 DSL Router Device Information

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



3.2.1 Summary of Device Information

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



Device Info

Board ID:	96358VW2
Software Version:	091231_1625-4.02L.03.wp1.A2pB025k.d21j2
Bootloader (CFE) Version:	1.0.37-102.6
Wireless Driver Version:	5.10.85.0.cpe4.402.0

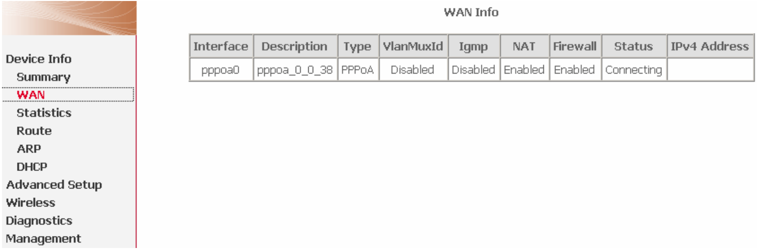
This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	945
Line Rate - Downstream (Kbps):	20985
LAN IPv4 Address:	192.168.1.1
Default Gateway:	pppoa0
Primary DNS Server:	
Secondary DNS Server:	

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

3.2.2 WAN Interface Information

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



WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
pppoa0	pppoa_0_0_38	PPPoA	Disabled	Disabled	Enabled	Enabled	Connecting	

- **Description:** Descripte this interface with protocol and PVC.

- **Type:** The connection type of WAN, such as PPPoE, PPPoA.

3.2.3 Statistics

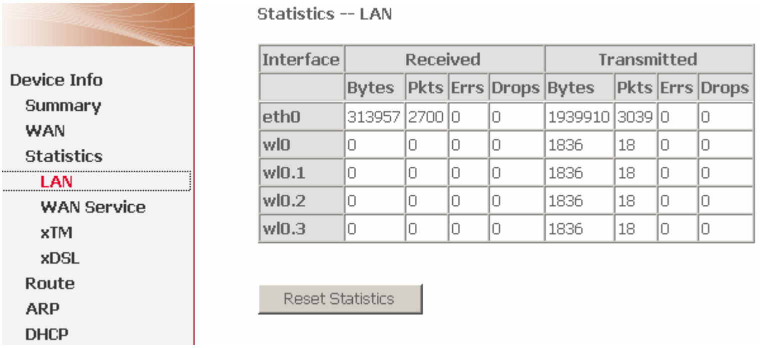
This page contains the following four parts:

- Statistics of LAN
- Statistics of WAN Service
- Statistics of xTM
- Statistics of xDSL

3.2.4 Statistics of LAN

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

The LAN side interface includes Ethernet USB and wireless device.

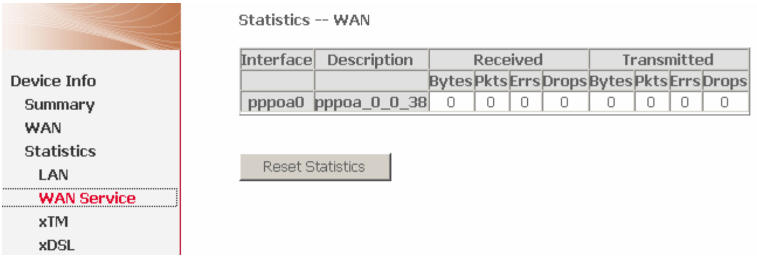


Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	313957	2700	0	0	1939910	3039	0	0
wl0	0	0	0	0	1836	18	0	0
wl0.1	0	0	0	0	1836	18	0	0
wl0.2	0	0	0	0	1836	18	0	0
wl0.3	0	0	0	0	1836	18	0	0

3.2.5 Statistics of WAN

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



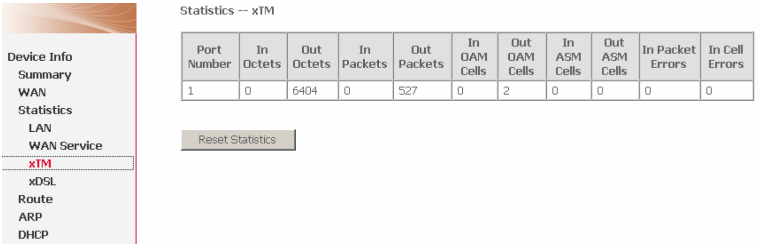
Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa0	pppoa_0_0_38	0	0	0	0	0	0	0	0

Figure 3 Statistics of WAN

3.2.6 Statistics of xTM

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

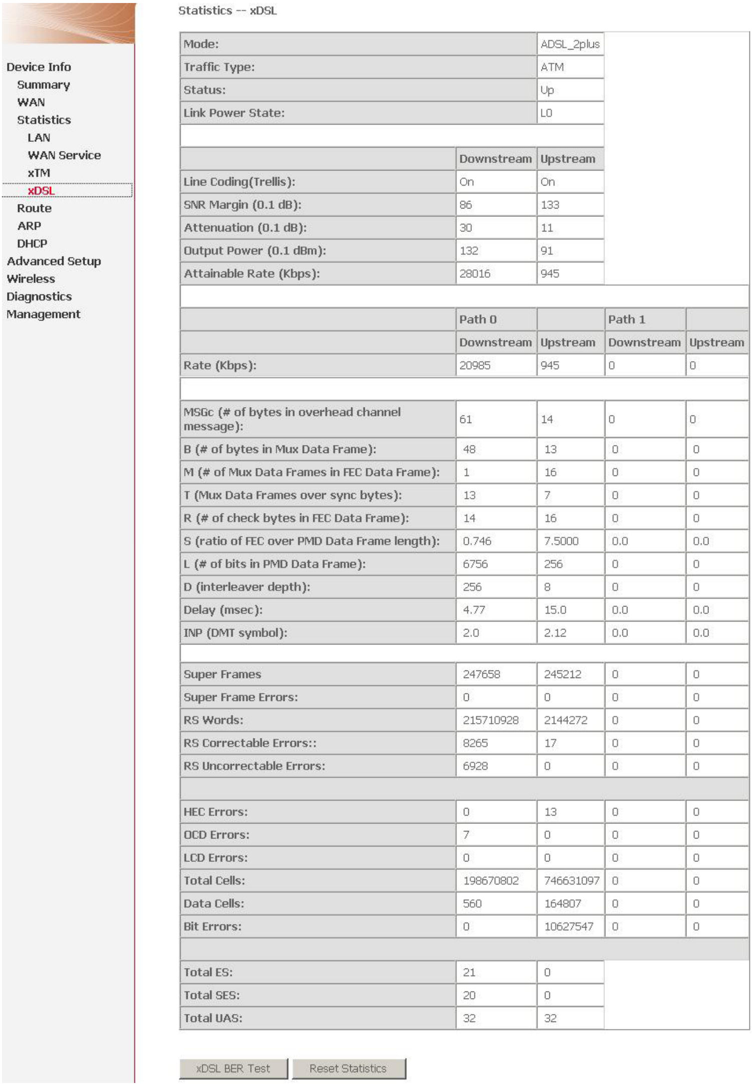


Statistics -- xTM

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	0	6404	0	527	0	2	0	0	0	0

3.2.7 Statistics of xDSL

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



Statistics -- xDSL

Mode:	ADSL_2plus
Traffic Type:	ATM
Status:	Up
Link Power State:	L0

	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	86	133
Attenuation (0.1 dB):	30	11
Output Power (0.1 dBm):	132	91
Attainable Rate (Kbps):	28016	945

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	20985	945	0	0
MSGc (# of bytes in overhead channel message):	61	14	0	0
B (# of bytes in Mux Data Frame):	48	13	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	16	0	0
T (Mux Data Frames over sync bytes):	13	7	0	0
R (# of check bytes in FEC Data Frame):	14	16	0	0
S (ratio of FEC over PMD Data Frame length):	0.746	7.5000	0.0	0.0
L (# of bits in PMD Data Frame):	6756	256	0	0
D (interleaver depth):	256	8	0	0
Delay (msec):	4.77	15.0	0.0	0.0
INP (DMT symbol):	2.0	2.12	0.0	0.0
Super Frames	247658	245212	0	0
Super Frame Errors:	0	0	0	0
RS Words:	215710928	2144272	0	0
RS Correctable Errors::	8265	17	0	0
RS Uncorrectable Errors:	6928	0	0	0
HEC Errors:	0	13	0	0
OCD Errors:	7	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	198670802	746631097	0	0
Data Cells:	560	164807	0	0
Bit Errors:	0	10627547	0	0
Total ES:	21	0		
Total SES:	20	0		
Total UAS:	32	32		

- **Traffic Type:** ATM, or PTM.
- **Status:** Up, NoSigal, Establishinglink
- **Link Power State:** L0, L1, L2

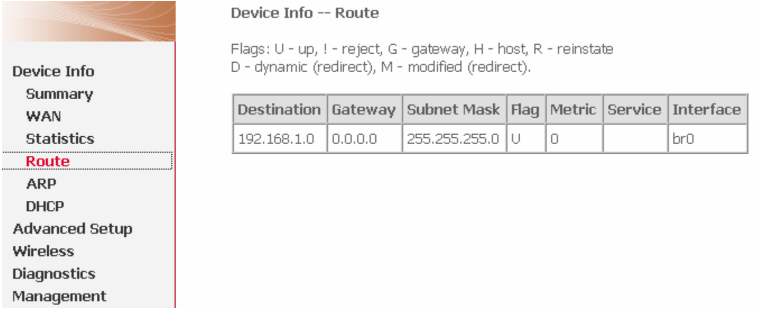
- **Line Coding:** Trallis on, etc.
- **Rate (Kbps):** Upstream Line Rate/Downstream Line Rate.

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

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

3.2.8 Route Table Information

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



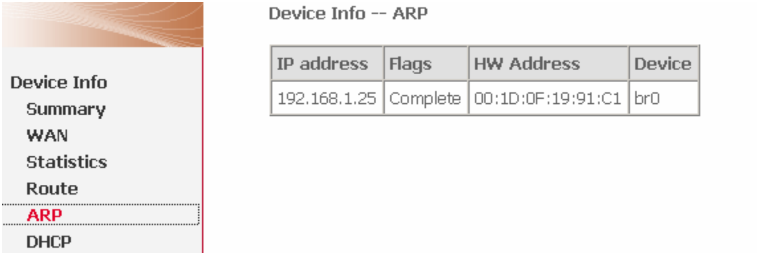
Device Info -- Route

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

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

3.2.9 ARP Table Information

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

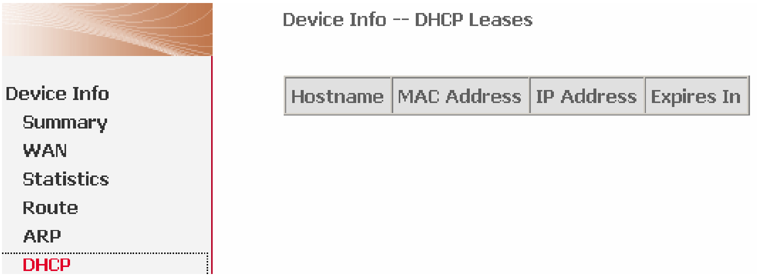


Device Info -- ARP

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

3.2.10 DHCP IP Lease Information

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



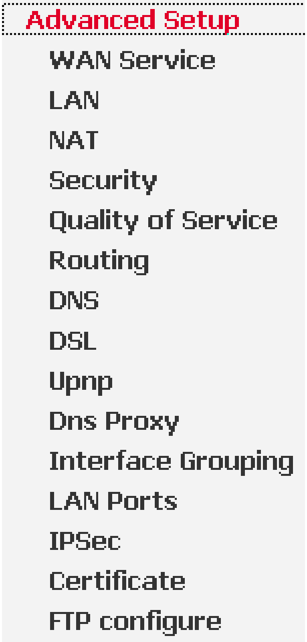
Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

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

3.3 Advanced Setup

Choose **Advanced Setup** and the following page appears.

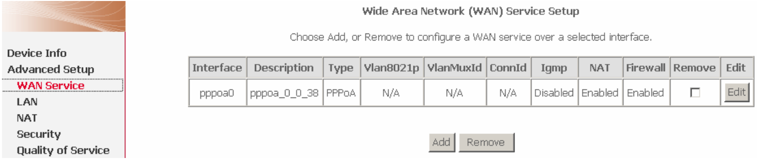


- **WAN Service:** wide area network service interface configuration
- **LAN:** local area network interface

Advanced Setup is key to DSL Router configuration.

3.3.1 WAN Configuration

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



Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
pppoa0	pppoa_0_0_38	PPPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	□	Edit

Figure 4 WAN configuration

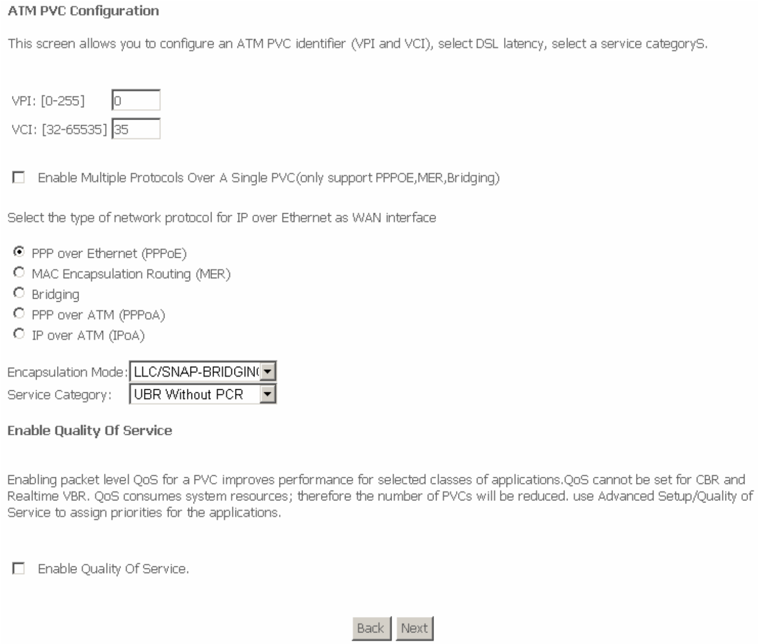
Click **Add** to configure PPPoE, MER, Bridging, PPPoA, and IPoA WAN configuration.

Choose **Remove** check box, click **Remove** to delete the WAN configuration.

3.3.1.1 PPPoE Configuration

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, QoS and select the Internet connection type, encapsulation mode and service category.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS.

VPI: [0-255] 0

VCI: [32-65535] 35

□ Enable Multiple Protocols Over A Single PVC(only support PPPOE,MER,Bridging)

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

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

Encapsulation Mode: LLC/SNAP-BRIDGING

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.

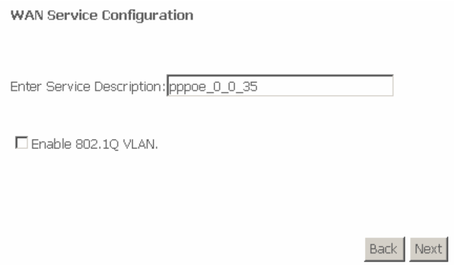
□ Enable Quality Of Service.

- **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 remain. In actual applications, you can modify them as required.

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

Click **Next** and the following page appears. In this page, you can modify the service description and enable the 802.1Q VLAN.

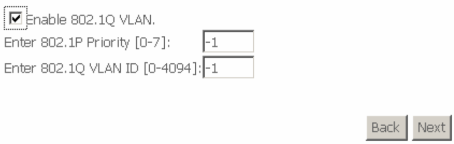


WAN Service Configuration

Enter Service Description: pppoe_0_0_35

☐ Enable 802.1Q VLAN.

Enable the 802.1Q VLAN and the following page appears.



☑ Enable 802.1Q VLAN.

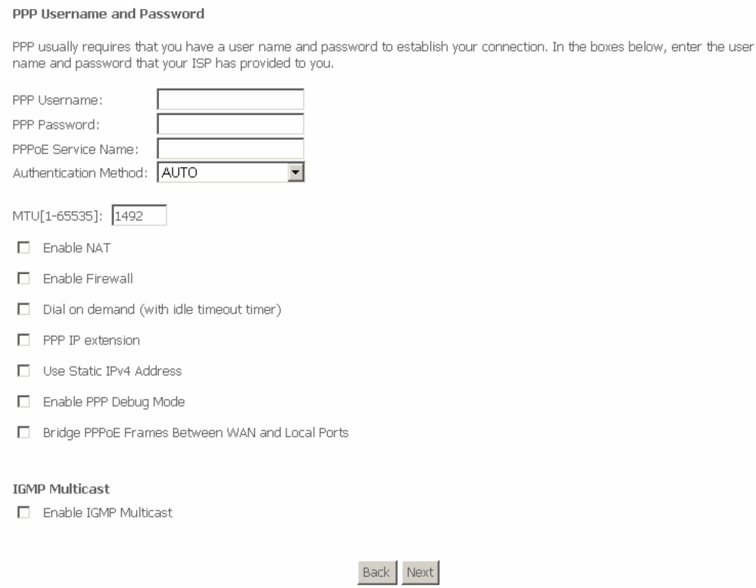
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Note:

The 802.1q VLAN tagging is only available for PPPoE, MER, and Bridge.

Click **Next** and the following page appears. In this page, you can modify the PPP user name, PPP password, and authentication method.



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

MTU[1-65535]: 1492

□ Enable NAT

□ Enable Firewall

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IPv4 Address

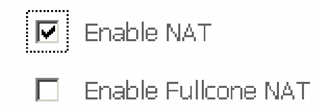
□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

□ Enable IGMP Multicast

- **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 NAT:** If you enable NAT, the **Enable Fullcone NAT** check box appears.

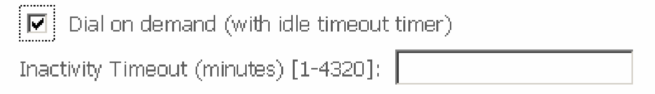


☑ Enable NAT

□ Enable Fullcone NAT

- **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,

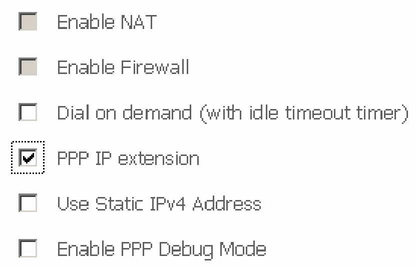
the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

- **PPP IP extension:** After **PPP IP extension** is enabled, the following page appears. The NAT and Firewall becom invalid, and the **Bridge PPPoE Frames Between WAN and Local Ports** check box disappears. And the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached with the modem (at this time, the modem has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the modem. If this function is disabled, the modem itself obtains the WAN IP address automatically.



□ Enable NAT

□ Enable Firewall

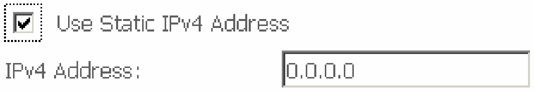
□ Dial on demand (with idle timeout timer)

☑ PPP IP extension

□ Use Static IPv4 Address

□ Enable PPP Debug Mode

- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.

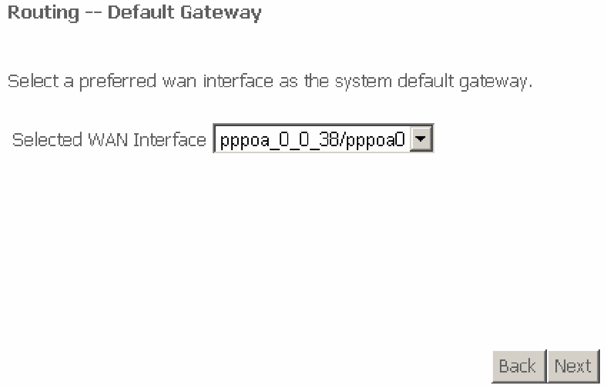


☑ Use Static IPv4 Address

IPv4 Address: 0.0.0.0

- **Enable PPP Debug Mode:** Enable or disable this mode of debug. This service is designed for the professional engineer.
- **Bridge PPPoE Frames Between WAN and Local Ports:** The PPPoE client can connect to router or PC.
- **IGMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

After proper configuration, click **Next** and the following page appears. In this page, select a preferred WAN interface as the system default gateway.

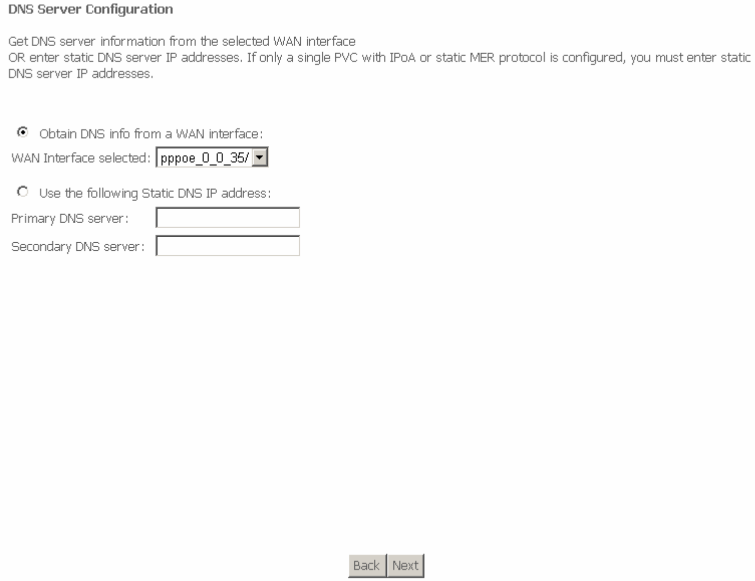


Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_38/pppoa0

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



DNS Server Configuration

Get DNS server information from the selected WAN interface
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_0_35/

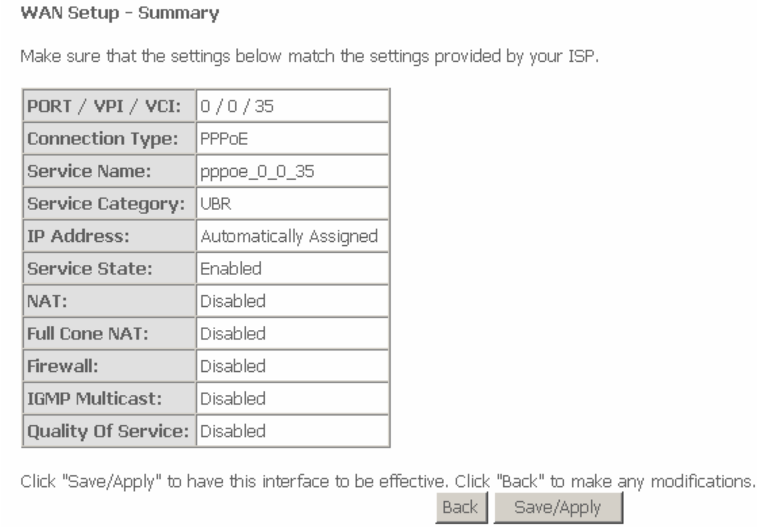
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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



WAN Setup - Summary

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

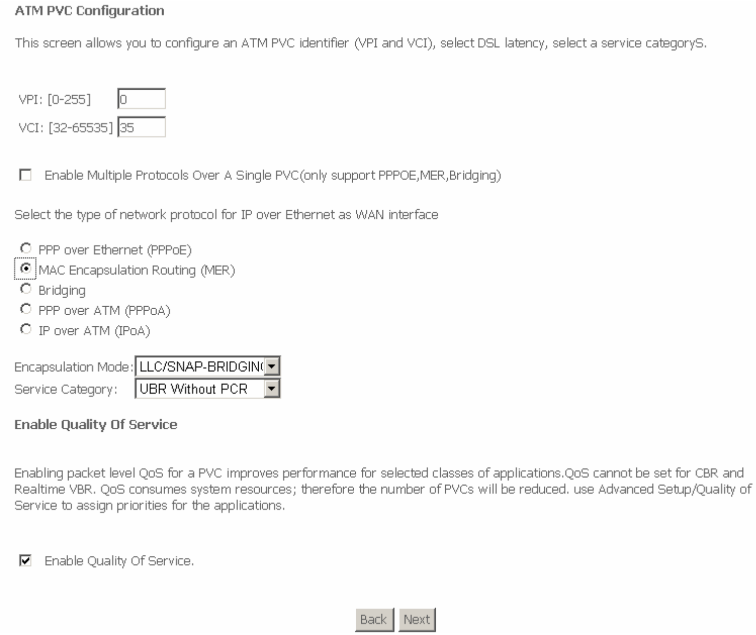
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

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

3.3.1.2 MER (IPoE) Configuration

Click **Add** and the following page appears. In this page, you can modify VPI/VCI, QoS and select the Internet connection type, encapsulation mode and service category.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS.

VPI: [0-255] 0

VCI: [32-65535] 35

□ Enable Multiple Protocols Over A Single PVC(only support PPPOE,MER,Bridging)

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

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

Encapsulation Mode: LLC/SNAP-BRIDGIN(

Service Category: UBR Without PCR

Enable Quality Of Service

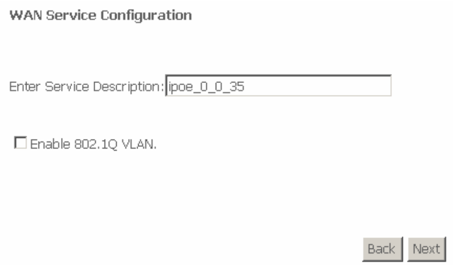
Enabling packet level QoS for a PVC improves performance for selected classes of applications.QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. use Advanced Setup/Quality of Service to assign priorities for the applications.

☑ Enable Quality Of Service.

- **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.

Change the connection type of PVC 0/35 to **MAC Encapsulation Routing (MER)** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

Click **Next** and the following page appears. In this page, you can modify the service description and enable the 802.1Q VLAN.

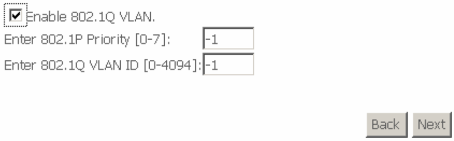


WAN Service Configuration

Enter Service Description: ipoe_0_0_35

☐ Enable 802.1Q VLAN.

Enable the 802.1Q VLAN and the following page appears.



☑ Enable 802.1Q VLAN.

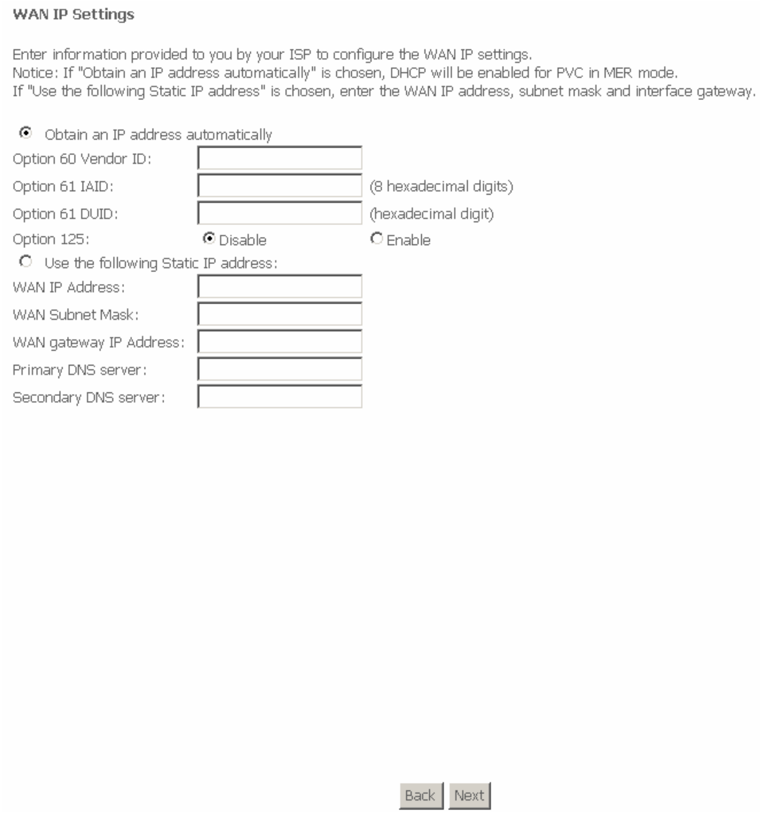
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Note:

The 802.1q VLAN tagging is only available for PPPoE, MER, and Bridge.

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



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

● Obtain an IP address automatically

Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(hexadecimal digit)
Option 125:	● Disable	○ Enable

○ Use the following Static IP address:

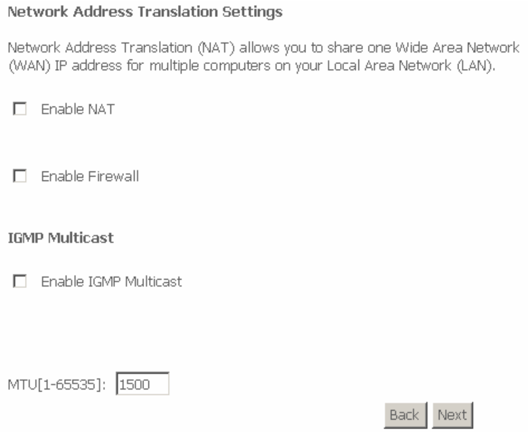
WAN IP Address:	
WAN Subnet Mask:	
WAN gateway IP Address:	
Primary DNS server:	
Secondary DNS server:	

In this page, you can modify the **IP Settings**. Enter information provided by your ISP to configure the WAN IP settings.

Note:

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

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



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

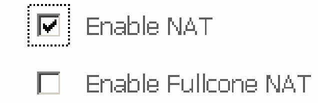
□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

MTU[1-65535]: 1500

In this page, you can modify the **Network Address Translation Settings.** If you enable NAT, the **Enable Fullcone NAT** check box appears.

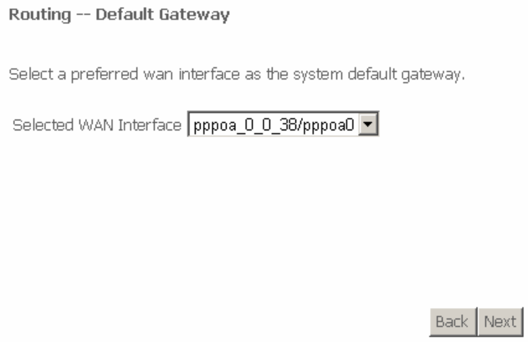


☑ Enable NAT

□ Enable Fullcone NAT

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.

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



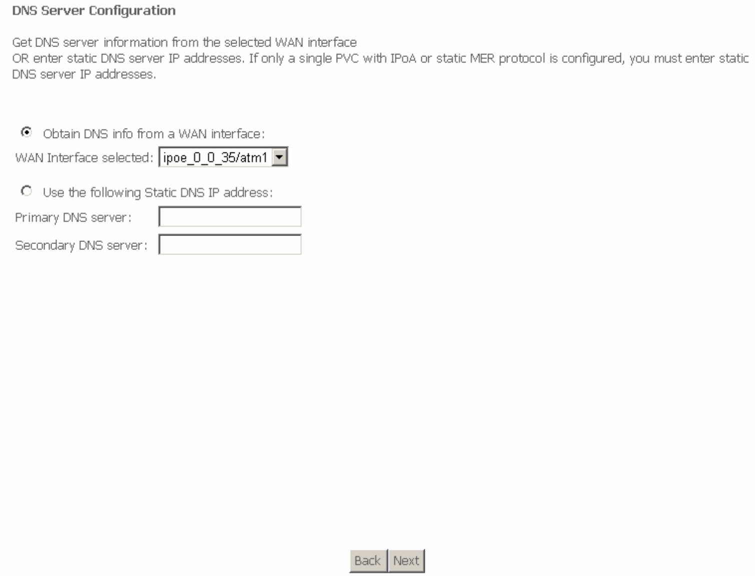
Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_38/pppoa0

In this page, select a preferred wan interface as the system default gateway.

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



DNS Server Configuration

Get DNS server information from the selected WAN interface
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: ipoe_0_0_35/atm1

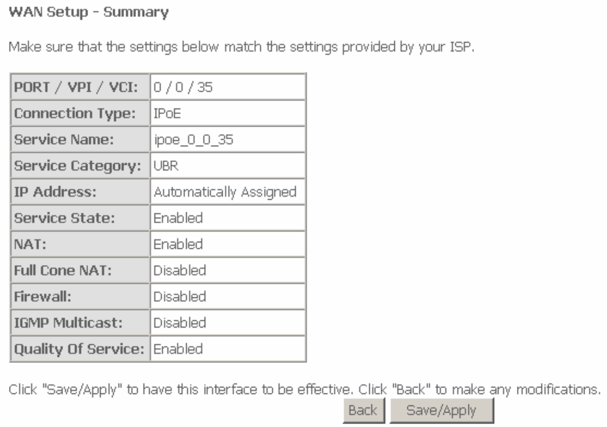
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

Click **Next** and the following page appears



WAN Setup - Summary

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

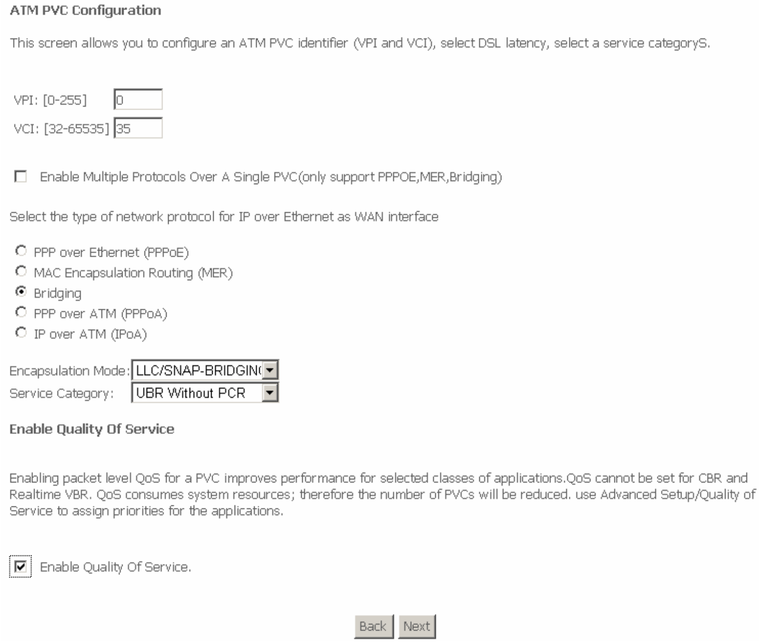
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoE
Service Name:	ipoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

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

3.3.1.3 Bridging Configuration

Click **Add** and the following page appears. In this page, you can modify VPI/VCI, QoS and select the Internet connection type, encapsulation mode and service category.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS.

VPI: [0-255] 0

VCI: [32-65535] 35

□ Enable Multiple Protocols Over A Single PVC(only support PPPOE,MER,Bridging)

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

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

Encapsulation Mode: LLC/SNAP-BRIDGIN(

Service Category: UBR Without PCR

Enable Quality Of Service

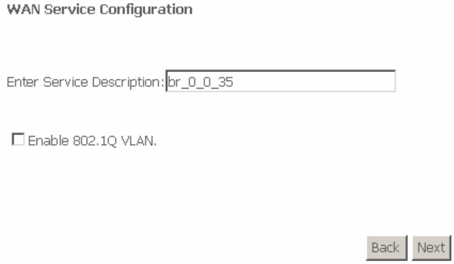
Enabling packet level QoS for a PVC improves performance for selected classes of applications.QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. use Advanced Setup/Quality of Service to assign priorities for the applications.

☑ Enable Quality Of Service.

- **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.

Change the connection type of PVC 0/35 to **Bridging** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

Click **Next** and the following page appears. In this page, you can modify the service description and enable the 802.1Q VLAN.

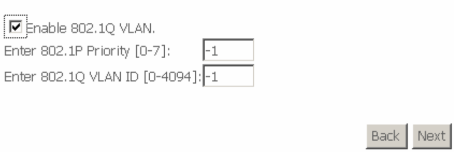


WAN Service Configuration

Enter Service Description: br_0_0_35

□ Enable 802.1Q VLAN.

Enable the 802.1Q VLAN and the following page appears.



☑ Enable 802.1Q VLAN.

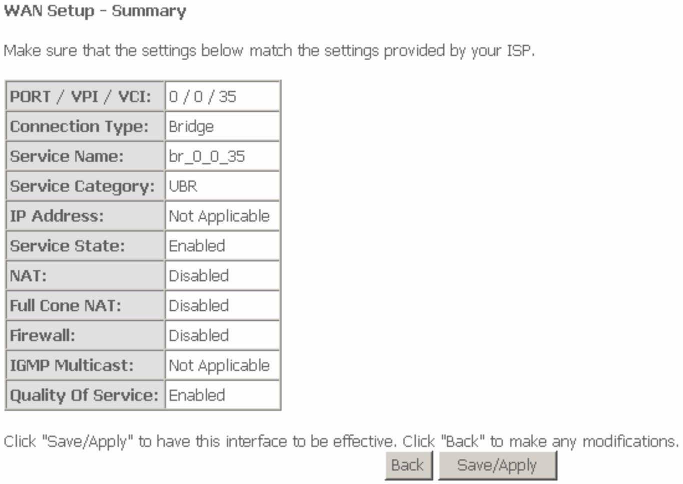
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Note:

The 802.1q VLAN tagging is only available for PPPoE, MER, and Bridge.

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



WAN Setup - Summary

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

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

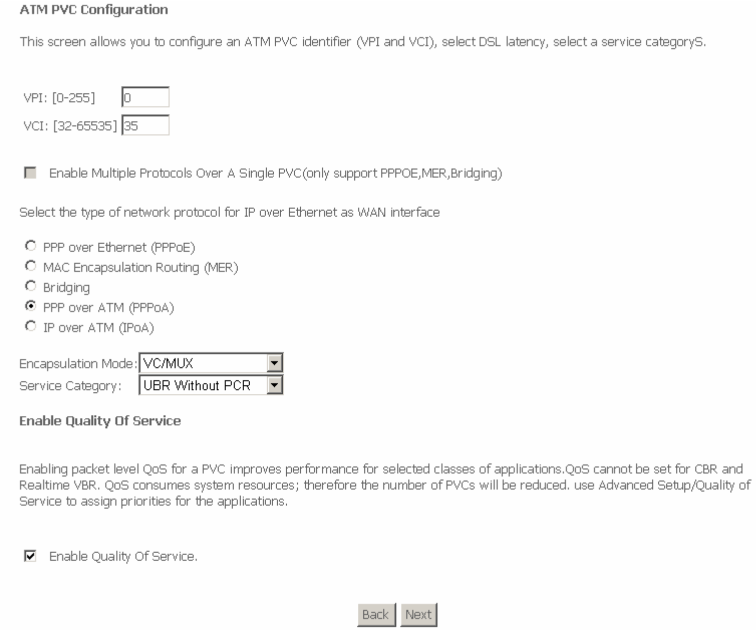
Click "Save/Apply" to have this interface to be effective. Click "Back" to make any modifications.

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

3.3.1.4 PPPoA Configuration

This section describes the procedure for adding PVC 0/35 (PPPoA mode).

Click **Add** and the following page appears. In this page, you can modify VPI/VCI, QoS and select the Internet connection type, encapsulation mode and service category.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS.

VPI: [0-255] 0

VCI: [32-65535] 35

□ Enable Multiple Protocols Over A Single PVC(only support PPPOE,MER,Bridging)

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

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

Encapsulation Mode: VC/MUX

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.

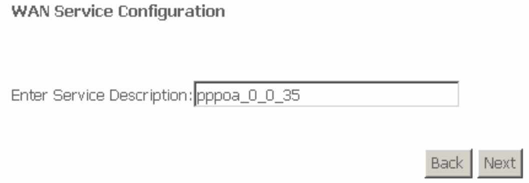
☑ Enable Quality Of Service.

- **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 remain. In actual applications, you can modify them as required.

Change the connection type of PVC 0/35 to PPPoA and set the Encapsulation Mode to VC/MUX (according to the uplink equipment).

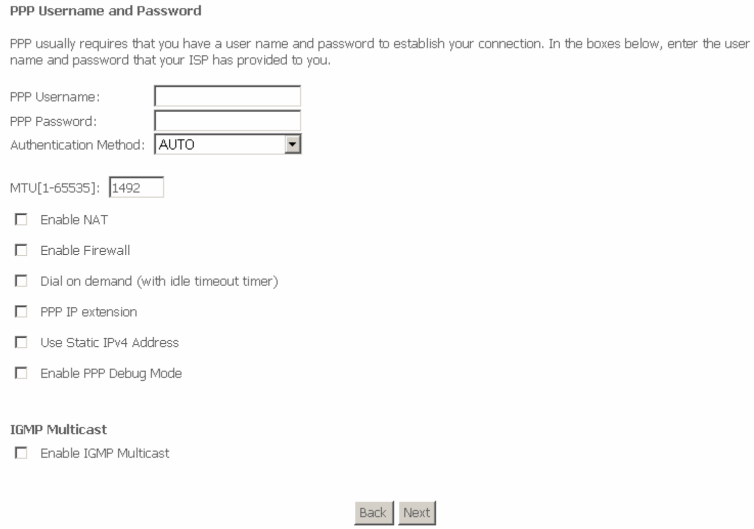
Click **Next** and the following page appears. In this page, you can modify the service description.



WAN Service Configuration

Enter Service Description: pppoa_0_0_35

Click **Next** and the following page appears. In this page, you can modify the PPP user name, PPP password, and authentication method.



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

MTU[1-65535]: 1492

□ Enable NAT

□ Enable Firewall

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

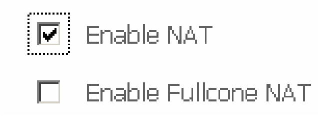
□ Use Static IPv4 Address

□ Enable PPP Debug Mode

IGMP Multicast

□ Enable IGMP Multicast

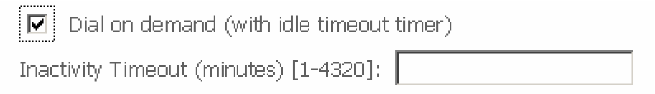
- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable NAT:** If you enable NAT, the **Enable Fullcone NAT** check box appears.



☑ Enable NAT

□ Enable Fullcone NAT

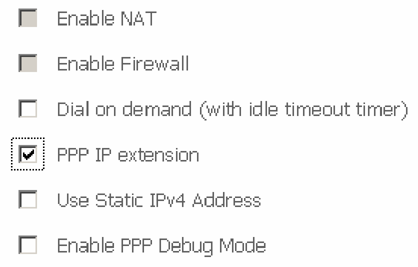
- **Enable Fullcone NAT:** A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand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



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

- **PPP IP extension:** After **PPP IP extension** is enabled, the following page appears. The NAT and Firewall becom invalid. And the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached with the modem (at this time, the modem has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the modem. If this function is disabled, the modem itself obtains the WAN IP address automatically.



□ Enable NAT

□ Enable Firewall

□ Dial on demand (with idle timeout timer)

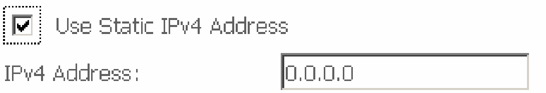
☑ PPP IP extension

□ Use Static IPv4 Address

□ Enable PPP Debug Mode

- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an

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

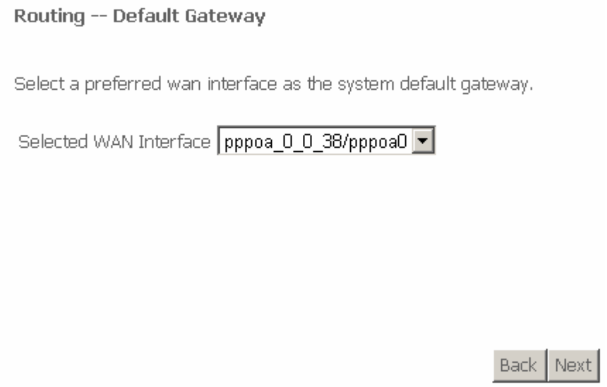


☑ Use Static IPv4 Address

IPv4 Address: 0.0.0.0

- **Enable PPP Debug Mode:** Enable or disable this mode of debug. This service is designed for the professional engineer.
- **IGMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

After proper configuration, click **Next** and the following page appears. In this page, select a preferred WAN interface as the system default gateway.

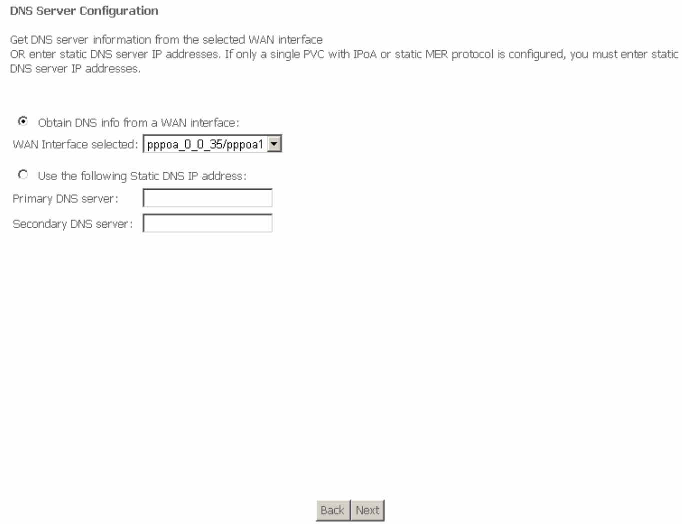


Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_38/pppoa0

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



DNS Server Configuration

Get DNS server information from the selected WAN interface
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_0_35/pppoa1

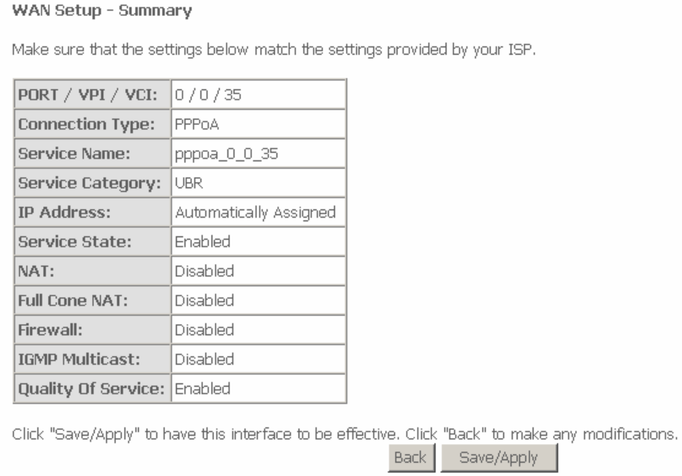
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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



WAN Setup - Summary

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

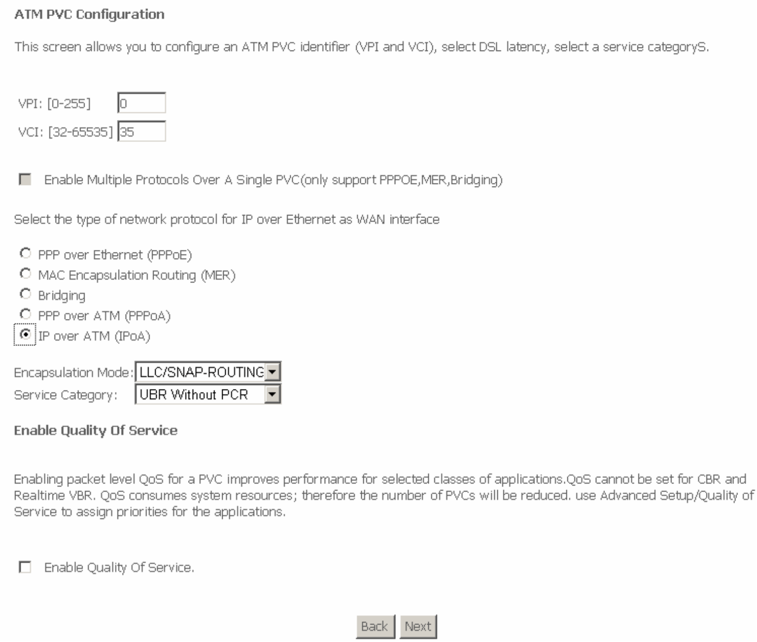
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

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

3.3.1.5 IPoA Configuration

Click **Add** and the following page appears. In this page, you can modify VPI/VCI, QoS and select the Internet connection type, encapsulation mode and service category.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS.

VPI: [0-255] 0

VCI: [32-65535] 35

□ Enable Multiple Protocols Over A Single PVC(only support PPPOE,MER,Bridging)

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

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

Encapsulation Mode: LLC/SNAP-ROUTING

Service Category: UBR Without PCR

Enable Quality Of Service

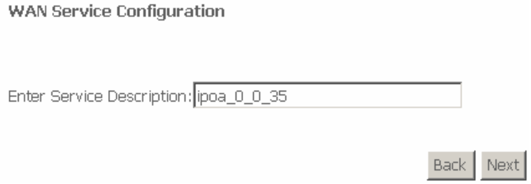
Enabling packet level QoS for a PVC improves performance for selected classes of applications.QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. use Advanced Setup/Quality of Service to assign priorities for the applications.

□ Enable Quality Of Service.

- **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.

Change the connection type of PVC 0/35 to **IP over ATM (IPoA)** and set the **Encapsulation Mode** to **LLC/SNAP-ROUTING** (according to the uplink equipment).

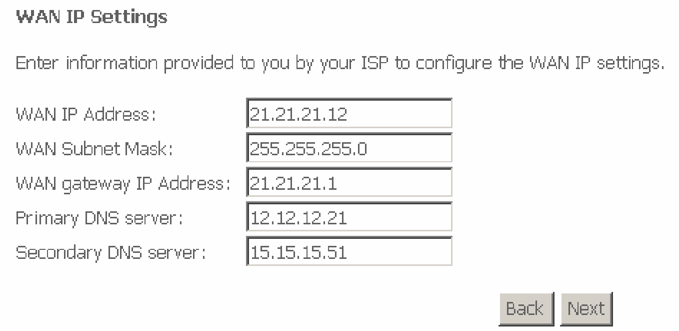
Click **Next** and the following page appears. In this page, you can modify the service description.



WAN Service Configuration

Enter Service Description: ipoa_0_0_35

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

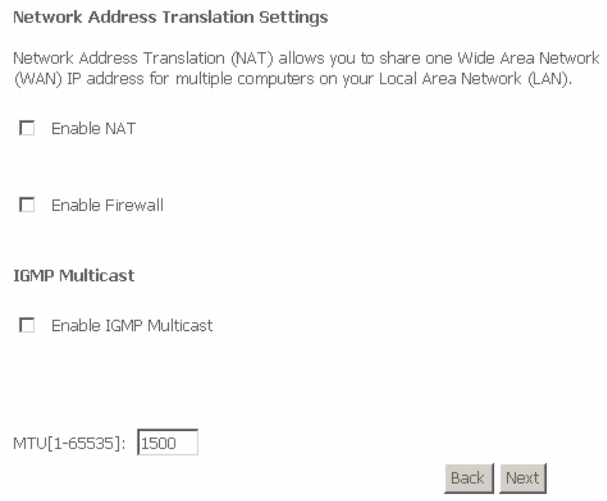


WAN IP Settings

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

WAN IP Address:	21.21.21.12
WAN Subnet Mask:	255.255.255.0
WAN gateway IP Address:	21.21.21.1
Primary DNS server:	12.12.12.21
Secondary DNS server:	15.15.15.51

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



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

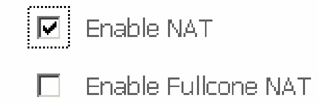
☐ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast

MTU[1-65535]: 1500

In this page, you can modify the **Network Address Translation Settings.** If you enable NAT, the **Enable Fullcone NAT** check box appears.

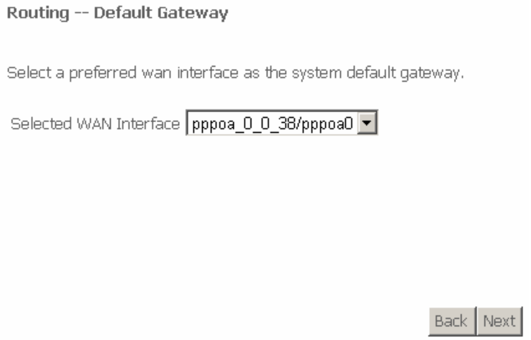


☑ Enable NAT

☐ Enable Fullcone NAT

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.

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



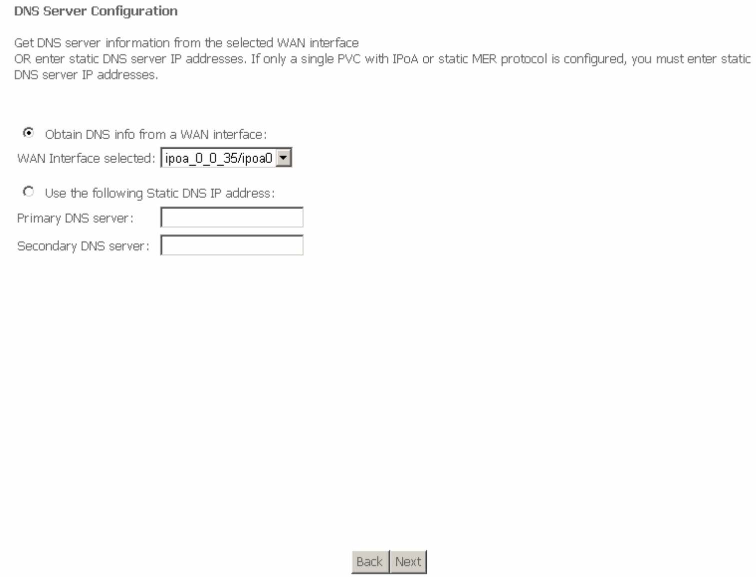
Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_38/pppoa0

In this page, select a preferred wan interface as the system default gateway.

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



DNS Server Configuration

Get DNS server information from the selected WAN interface
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: ipoa_0_0_35/ipoa0

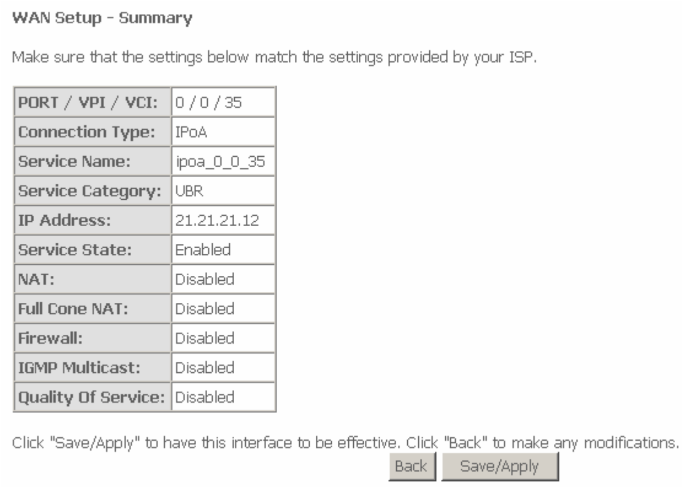
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

Click **Next** and the following page appears



WAN Setup - Summary

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

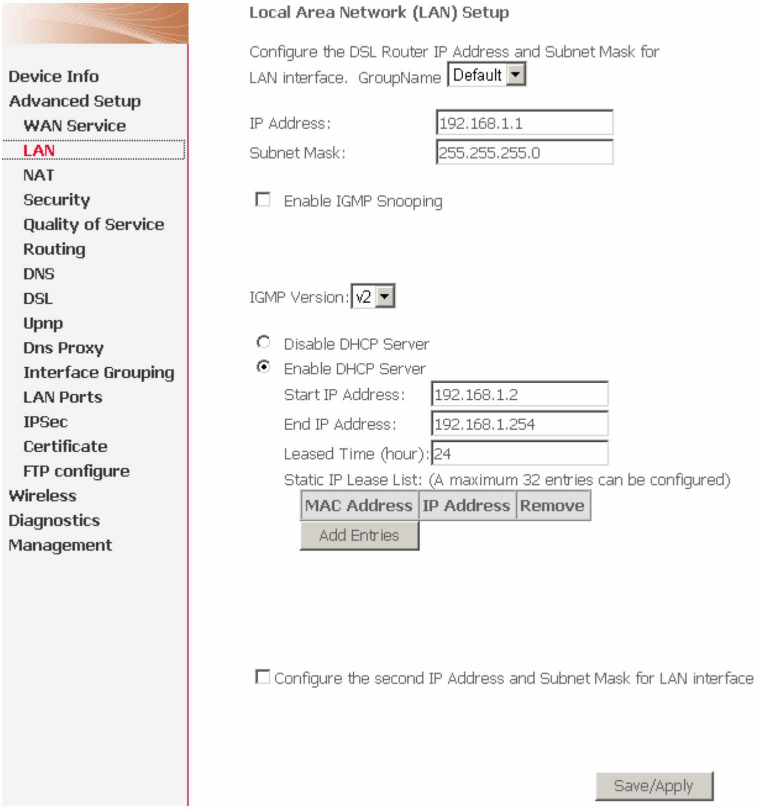
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	21.21.21.12
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

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

3.3.2 LAN Configuration

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



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

□ Enable IGMP Snooping

IGMP Version: v2

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

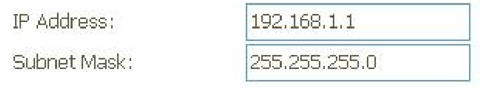
Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

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

3.3.2.1 Configuring the Private IP Address for the DSL Router

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

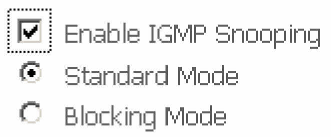


IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

3.3.2.2 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.



☑ Enable IGMP Snooping

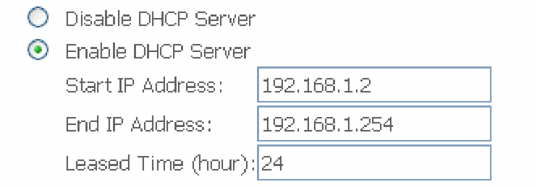
● Standard Mode

○ Blocking Mode

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

3.3.2.3 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.



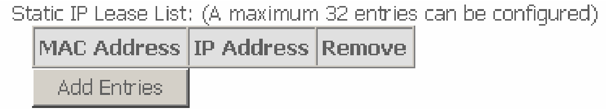
○ Disable DHCP Server

● Enable DHCP Server

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

3.3.2.4 Configuring DHCP Static IP Lease

View the following part for static IP Lease List.

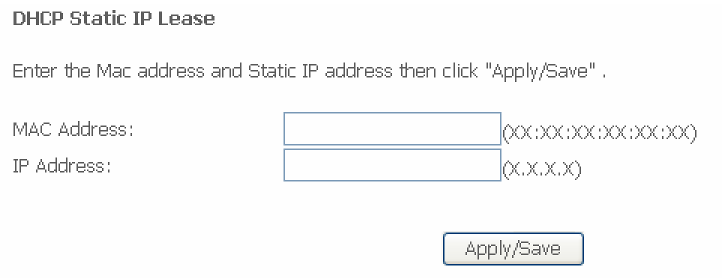


Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

Note: A maximum 32 entries can be configured.

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



DHCP Static IP Lease

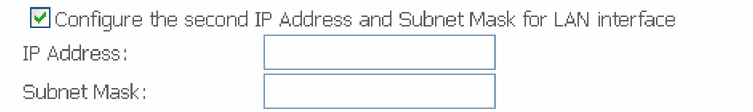
Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address: (XX:XX:XX:XX:XX:XX)

IP Address: (X.X.X.X)

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

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



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

IP Address:

Subnet Mask:

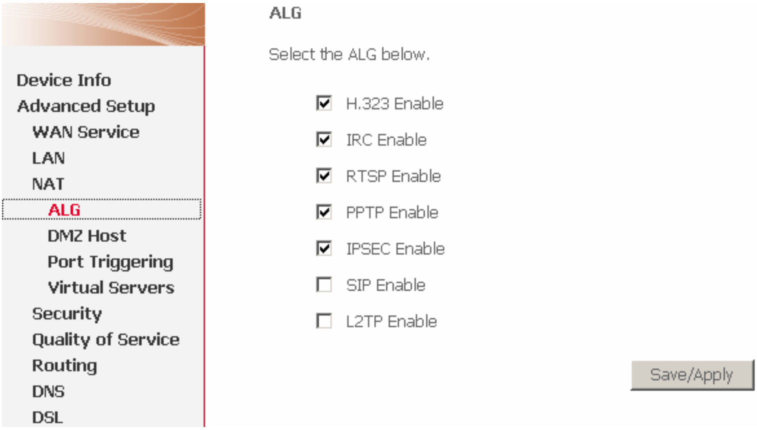
3.3.3 NAT

Note:

The NAT information is not displayed in the bridge mode.

3.3.3.1 ALG

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



ALG

Select the ALG below.

☑ H.323 Enable

☑ IRC Enable

☑ RTSP Enable

☑ PPTP Enable

☑ IPSEC Enable

☐ SIP Enable

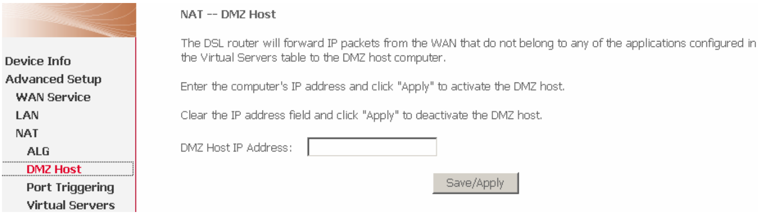
☐ L2TP Enable

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

3.3.3.2 DMZ 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 configurations.

Remove DMZ host

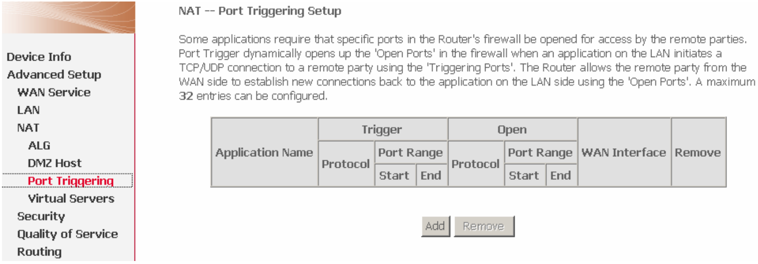
Clear the **DMZ Host Address**. Click **Save/Apply** to apply the setting.

3.3.3.3 Port Triggering

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

Adding Port Triggering

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

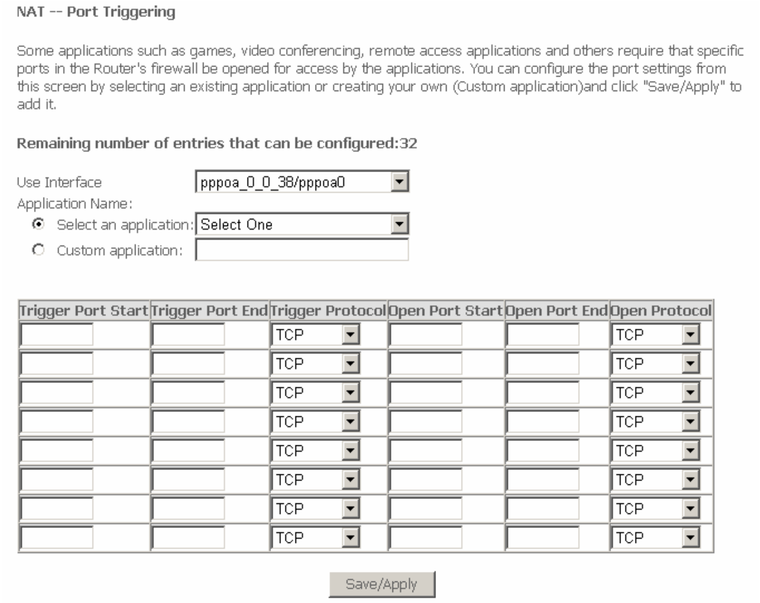


NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Step 1 To set up port triggering for a service, 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

Use Interface: pppoa_0_0_38/pppoa0

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

Step 2 Select the use Interface like that ipoa_0_0_35/ipoa0 and select the required application from the **Select an application** drop-down list, or manually enter the information in the **Custom application** field.

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

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

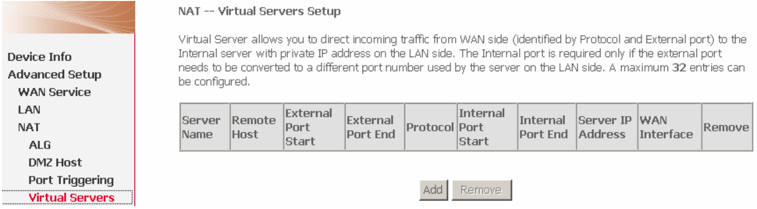
Step 3 Click **Save/Apply** to apply the settings.

Removing Port Triggering

Select the **Remove** check box. Click **Remove** to remove the settings.

3.3.3.4 NAT - Virtual Server Setup

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



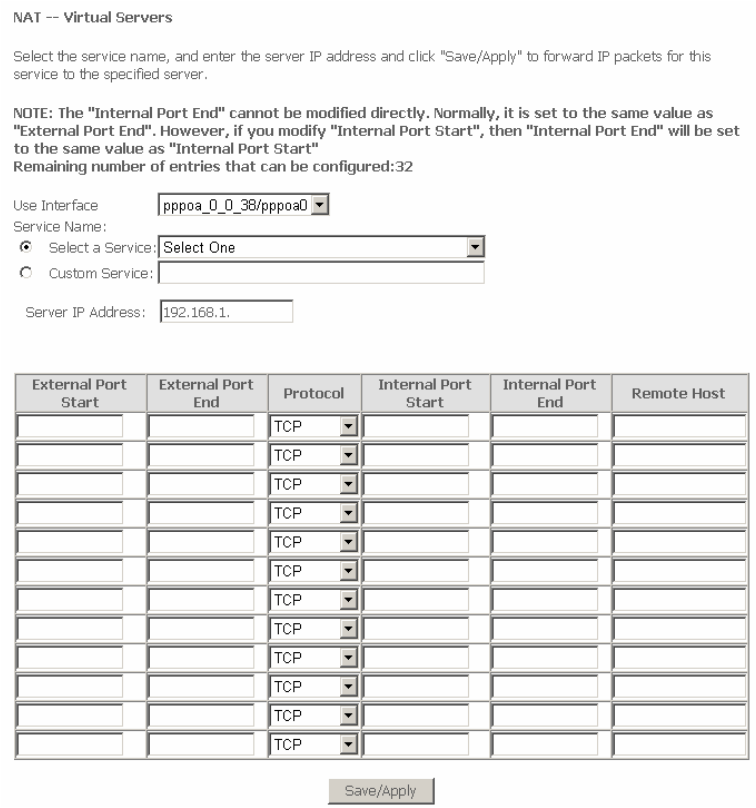
NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	Remote Host	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Adding Virtual Servers

Step 1 To set up virtual servers for a service, 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 modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start"
Remaining number of entries that can be configured:32

Use Interface: pppoa_0_0_38/pppoa0
Service Name:
● Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.1.

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

Step 2 Select the use Interface like that ipoa_0_0_35/ipoa0 and select a service or enter a custom server.

Step 3 Set **Server IP Address**.

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

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

Step 6 Select **Protocol**.

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

Step 8 Enter **Remote IP**.

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

If the application you require is not in the list, manually enter the information. Select the protocol for the service you are providing from the **Protocol** drop-down list. Under **Public Port**, enter the port number of the service you are providing. In the **Local Port** field, enter the internal port number to which service requests are to be forwarded. In the **Local IP Address** field, enter the IP address of the PC that provides the service.

Deleting Virtual Servers

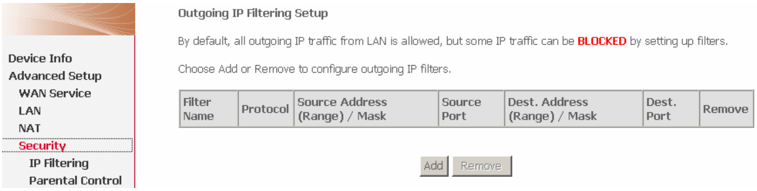
Select the **Remove** check box. Click **Remove** to remove the settings.

3.3.4 Security

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

Note:

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



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.

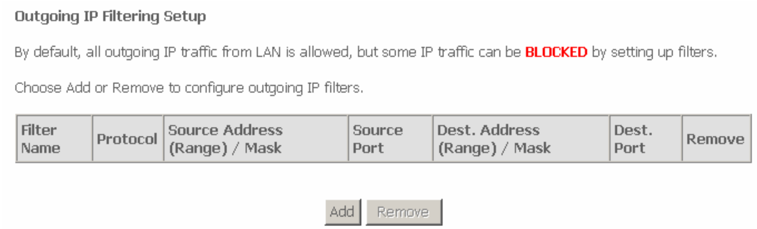
Filter Name	Protocol	Source Address (Range) / Mask	Source Port	Dest. Address (Range) / Mask	Dest. Port	Remove

3.3.4.1 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.

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.

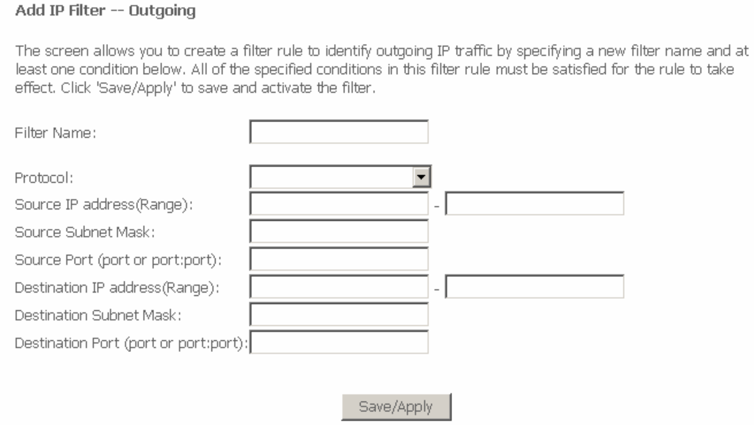
Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address (Range) / Mask	Source Port	Dest. Address (Range) / Mask	Dest. Port	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(Range): -

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address(Range): -

Destination Subnet Mask:

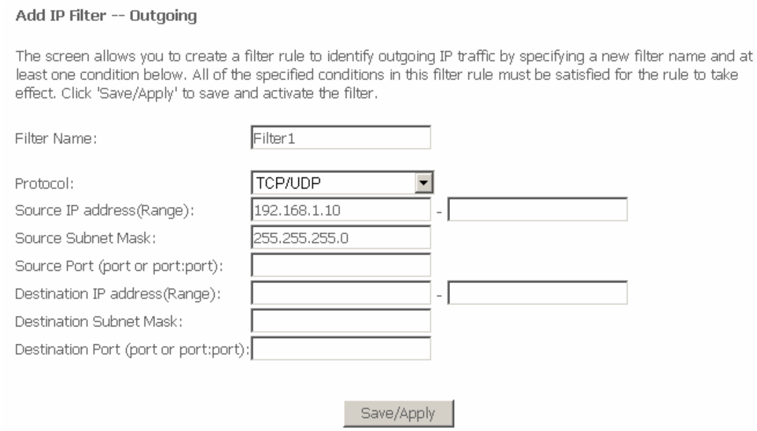
Destination Port (port or port:port):

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

Configuration

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

Step 2 The following page shows the detailed configuration.

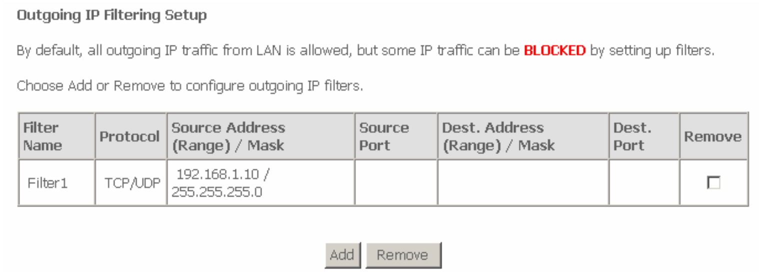


Add IP Filter -- Outgoing

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(Range):	192.168.1.10	-
Source Subnet Mask:	255.255.255.0	
Source Port (port or port:port):		
Destination IP address(Range):		-
Destination Subnet Mask:		
Destination Port (port or port:port):		

Step 3 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.

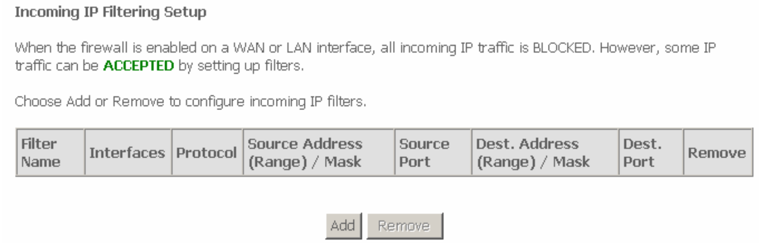
Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address (Range) / Mask	Source Port	Dest. Address (Range) / Mask	Dest. Port	Remove
Filter1	TCP/UDP	192.168.1.10 / 255.255.255.0				□

3.3.4.2 Incoming IP Filtering Setup

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

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



Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

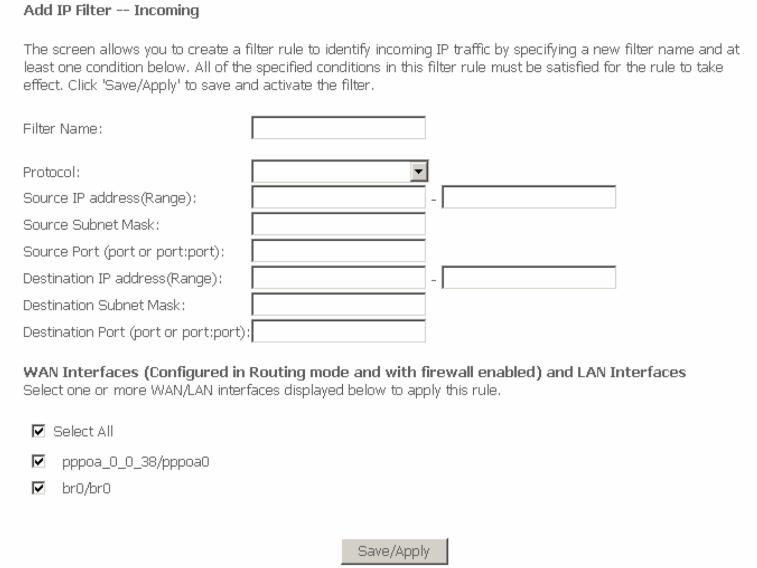
Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address (Range) / Mask	Source Port	Dest. Address (Range) / Mask	Dest. Port	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(Range): -

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address(Range): -

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All

☑ pppoa_0_0_38/pppoa0

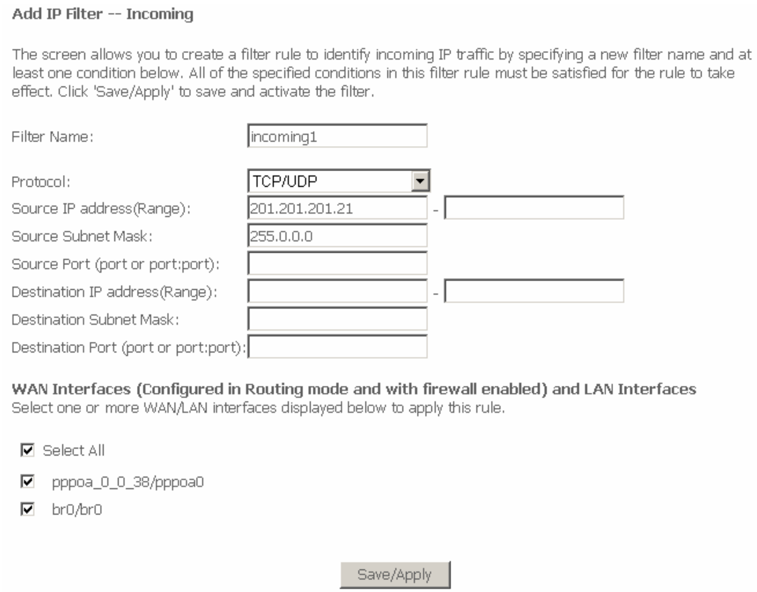
☑ br0/br0

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

Configuration

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

Step 2 The detailed configuration steps are as follows:



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:	incoming1
Protocol:	TCP/UDP
Source IP address(Range):	201.201.201.21 -
Source Subnet Mask:	255.0.0.0
Source Port (port or port:port):	
Destination IP address(Range):	-
Destination Subnet Mask:	
Destination Port (port or port:port):	

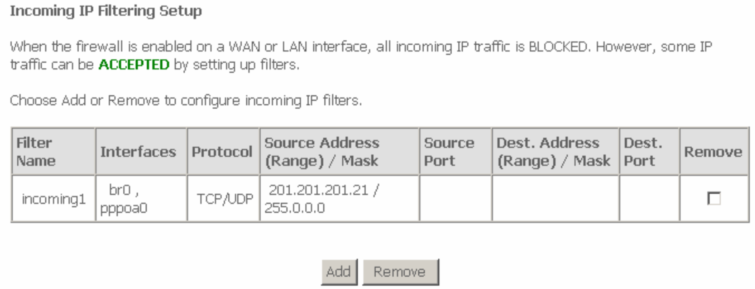
WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All

☑ pppoa_0_0_38/pppoa0

☑ br0/br0

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



Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters.

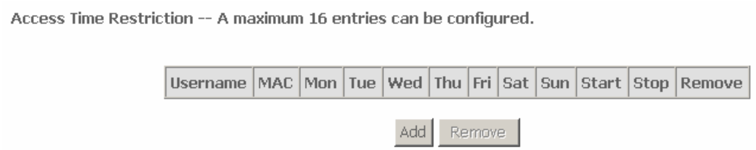
Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address (Range) / Mask	Source Port	Dest. Address (Range) / Mask	Dest. Port	Remove
incoming1	br0 , pppoa0	TCP/UDP	201.201.201.21 / 255.0.0.0				□

3.3.4.3 Parental Control - Time Restriction

Parental Control restricts a speciel LAN device with its MAC address by setting access time restriction.

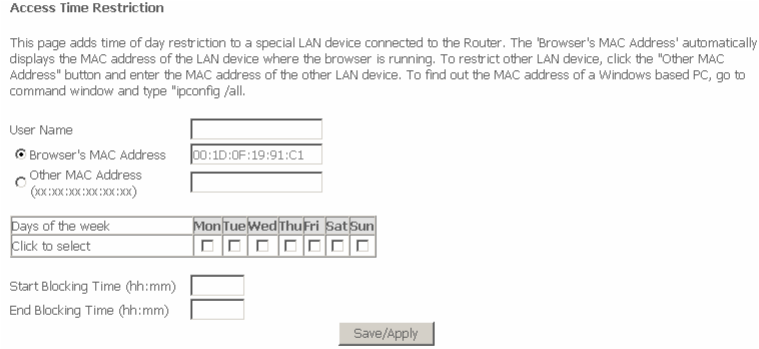
Step 1 Click **Advanced Setup**> **Security** > **Parental Control** > **Time Restriction**, and the following page appears.



Access Time Restriction -- A maximum 16 entries can be configured.

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

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



Access Time 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 00:1D:0F:19:91:C1

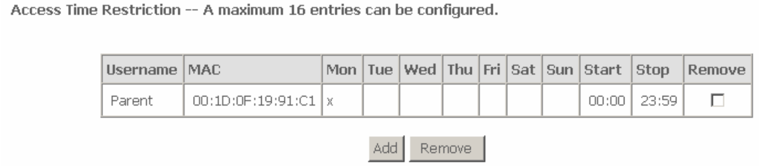
○ Other MAC Address (xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

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



Access Time Restriction -- A maximum 16 entries can be configured.

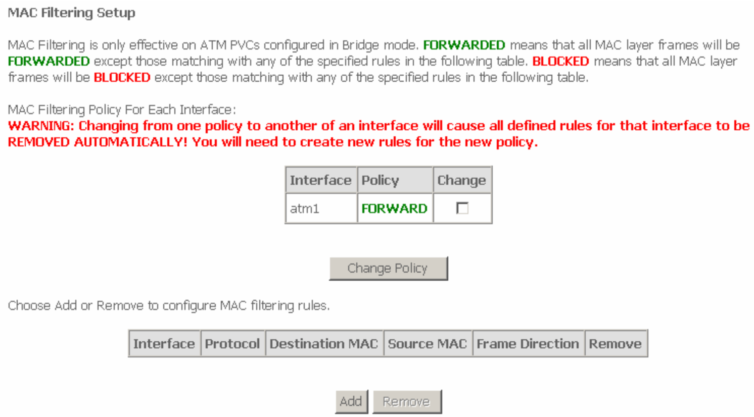
Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Parent	00:1D:0F:19:91:C1	x							00:00	23:59	□

3.3.4.4 MAC Filtering Configuration

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

Note:

MAC filtering is only effective on ATM PVCs configured in Bridge mode. If the ATM PVCs are configured in other routing modes (such as PPPoE mode), the MAC Filtering Setup page does not appear.



MAC Filtering Setup

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

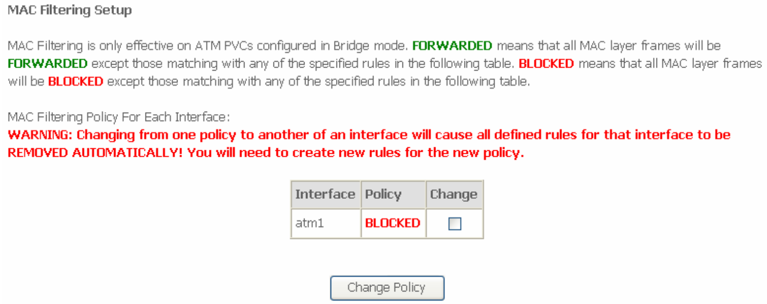
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm1	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

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



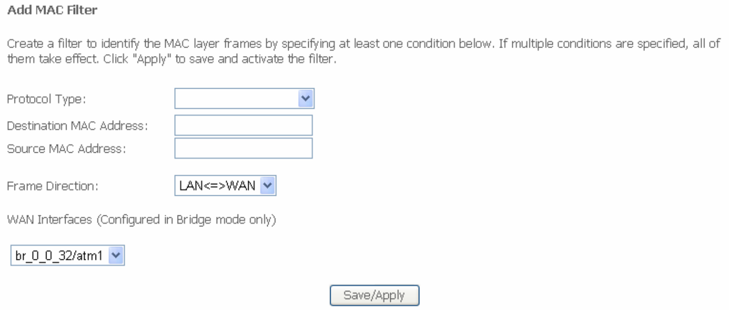
MAC Filtering Setup

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

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm1	BLOCKED	□

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



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:	
Destination MAC Address:	
Source MAC Address:	
Frame Direction:	LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

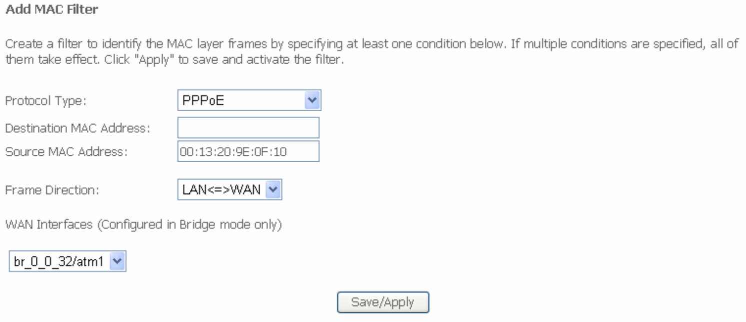
br_0_0_32/atm1

Frame Direction: Direction of transmission frame.

MAC Filtering - Global Policy FORWARDED

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

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



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type: PPPoE

Destination MAC Address:

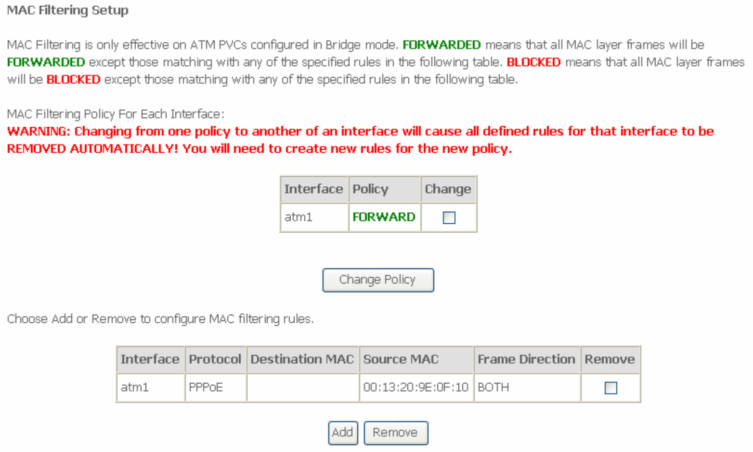
Source MAC Address: 00:13:20:9E:0F:10

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_32/atm1

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



MAC Filtering Setup

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

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm1	FORWARD	□

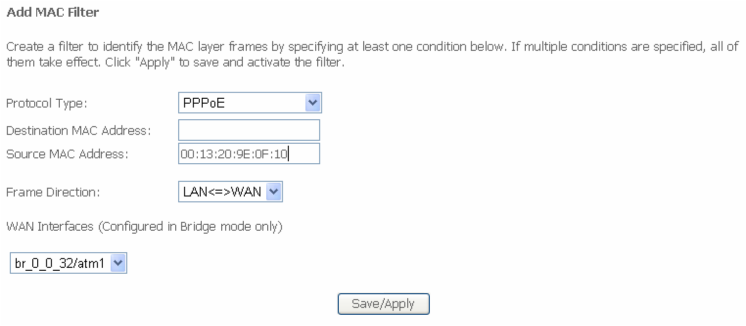
Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
atm1	PPPoE		00:13:20:9E:0F:10	BOTH	□

MAC Filtering - Global Policy BLOCKED

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

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



Add MAC Filter

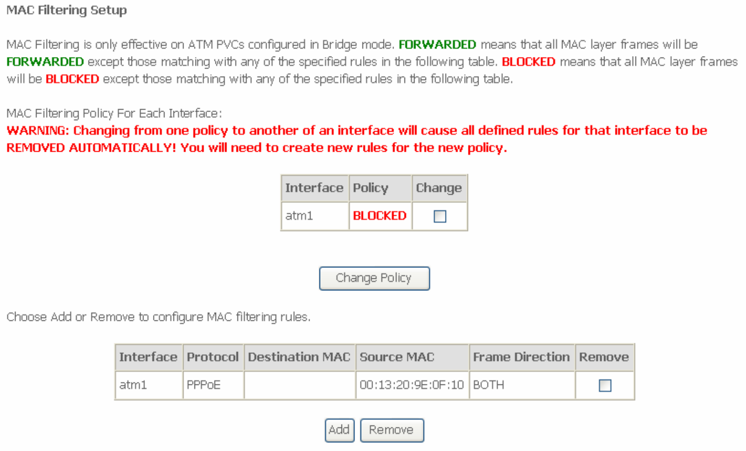
Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:	PPPoE
Destination MAC Address:	
Source MAC Address:	00:13:20:9E:0F:10
Frame Direction:	LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_32/atm1

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



MAC Filtering Setup

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

MAC Filtering Policy For Each Interface:

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

Interface	Policy	Change
atm1	BLOCKED	□

Choose Add or Remove to configure MAC filtering rules.

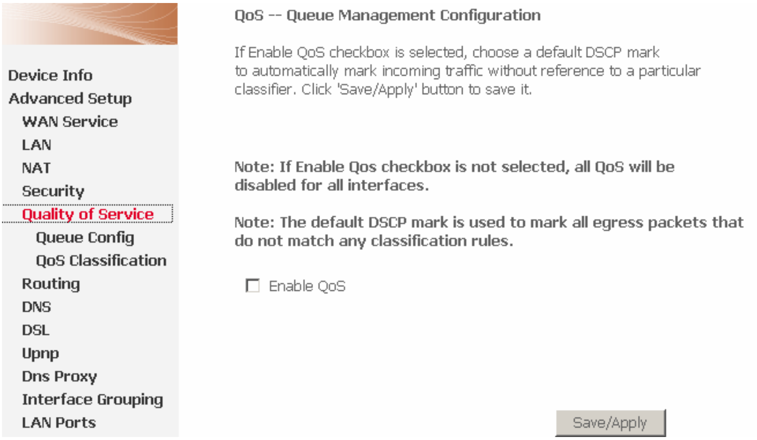
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
atm1	PPPoE		00:13:20:9E:0F:10	BOTH	□

3.3.5 Quality of Service

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

3.3.5.1 Enabling QoS

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



QoS -- Queue Management Configuration

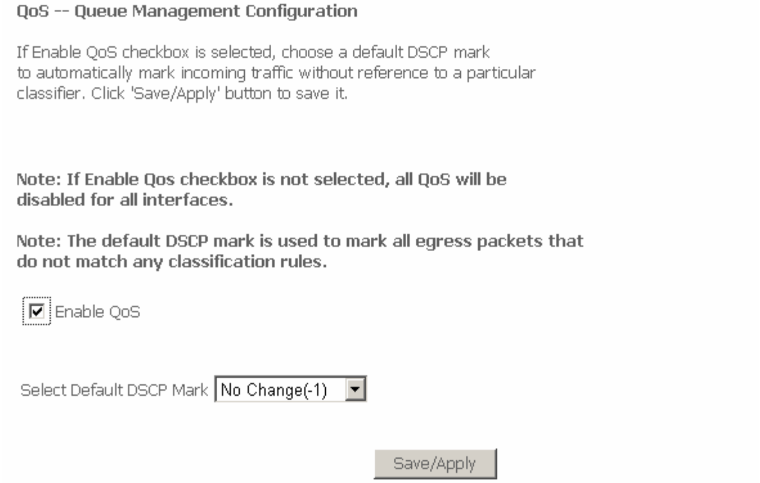
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

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



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)

Note:

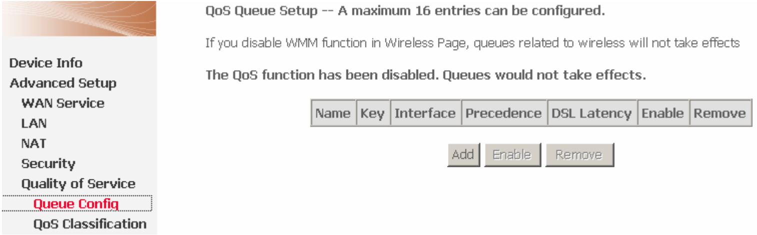
If Enable Qos checkbox is not selected, all QoS is disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

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

3.3.5.2 QOS - Queue Config

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

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



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

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

The QoS function has been disabled. Queues would not take effects.

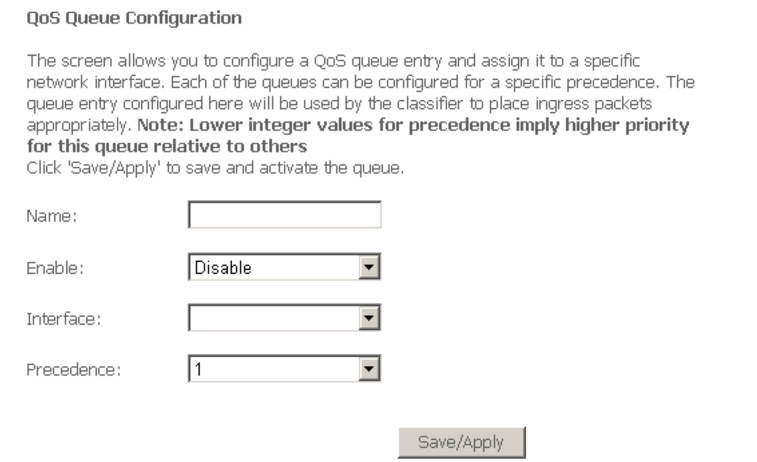
Name	Key	Interface	Precedence	DSL Latency	Enable	Remove

Note:

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

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

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 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 queue.

Name:

Enable: Disable

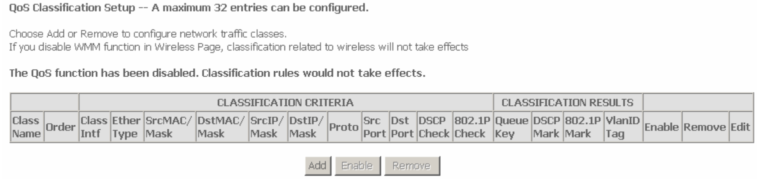
Interface:

Precedence: 1

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.

3.3.5.3 QoS--QoS Classification

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



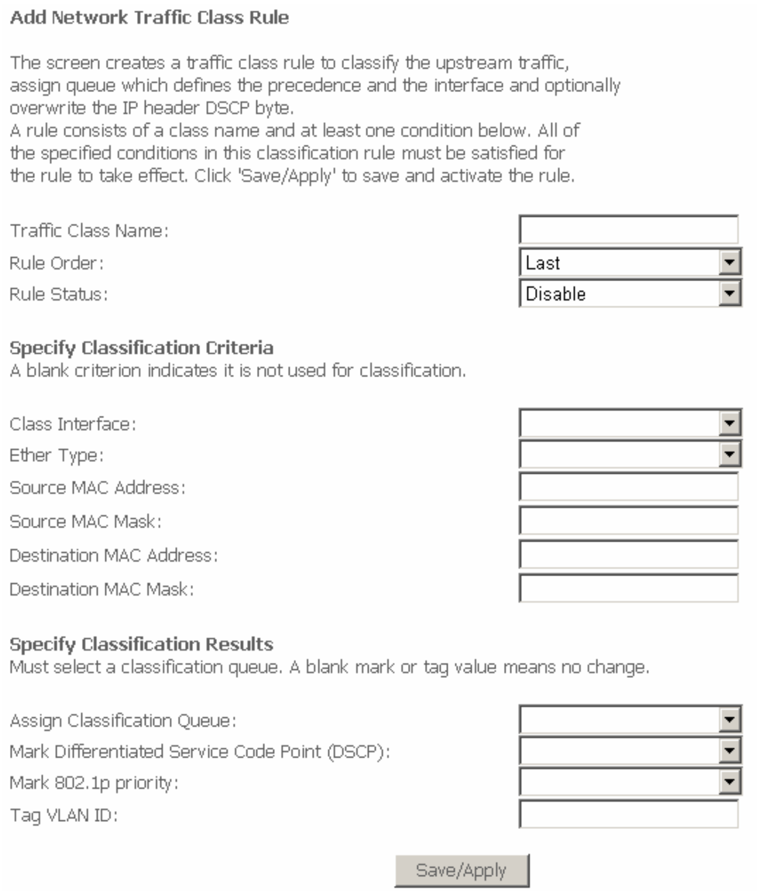
QoS Classification Setup -- A maximum 32 entries can be configured.

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

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	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:	Last
Rule Status:	Disable

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

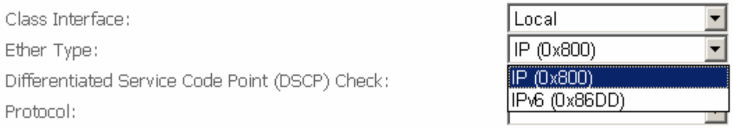
Class Interface:	
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

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

Assign Classification Queue:	
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID:	

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

  – **Class Interface:** If selected Local, this following page appears.



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

And there are just two ether types **IP** and **IPv6** to be selected.

– **Differentiated Service Code Point (DSCP) Check:** Select a mark service to match 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)

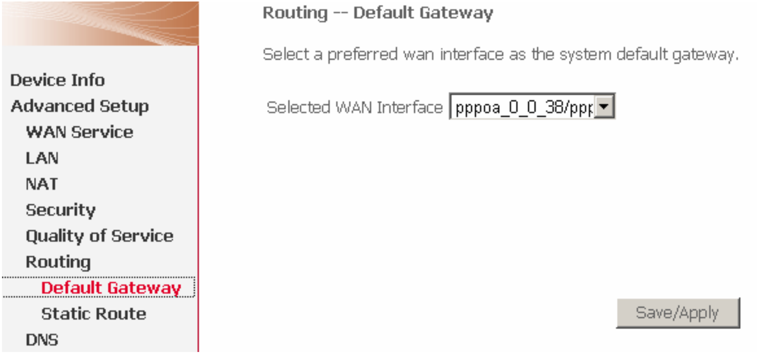
- **Specify Classification Results:** Must select a classification queue. A blank mark or tag value means no change.
  - **Mark Differentiated Service Code Point (DSCP):** Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS - Mark IP Precedence, AF - Assured Forwarding, EF - Expedited Forwarding)
  - **Mark 802.1p priority:** Select an 802.1p priority number that serves as the 802.1p value. The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

3.3.6 Routing

3.3.6.1 Routing – Default Gateway

Choose **Advanced Setup > Routing > Default Gateway,** and the following page appears. In this page, you can modify the default gateway settings.

If selected an interface by the **Selected WAN Interface** box, this router accepts the received default gateway assignment from this WAN interface. Click **Save/Apply** to save the configuration.



Routing -- Default Gateway

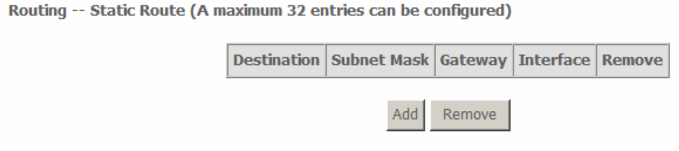
Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_38/ppp

3.3.6.2 Static Route

Adding Static Route

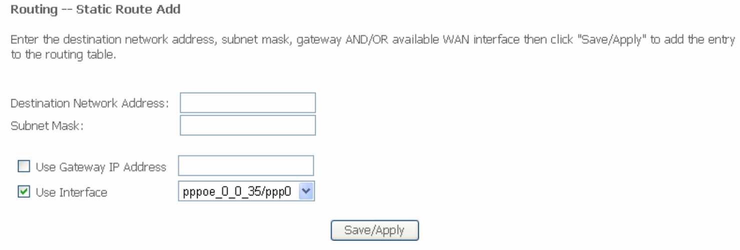
Step 1 Choose Advanced Setup > Routing > Static Route and the following page appears.



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

Destination	Subnet Mask	Gateway	Interface	Remove

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



Routing -- Static Route Add

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

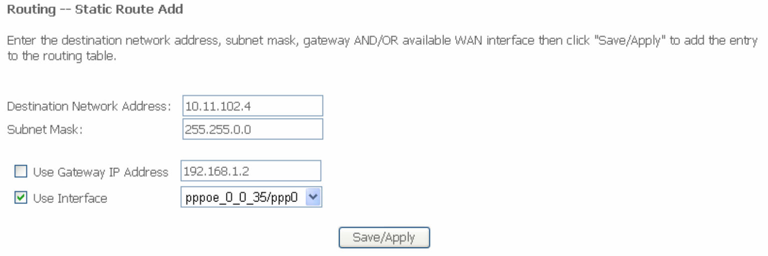
Destination Network Address:

Subnet Mask:

□ Use Gateway IP Address

☑ Use Interface pppoe_0_0_35/ppp0

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



Routing -- Static Route Add

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

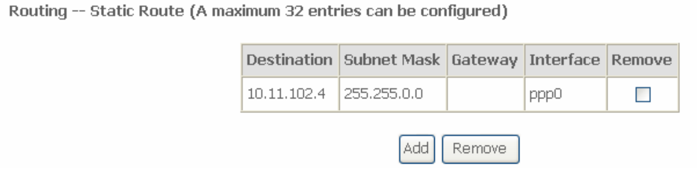
Destination Network Address: 10.11.102.4

Subnet Mask: 255.255.0.0

□ Use Gateway IP Address 192.168.1.2

☑ Use Interface pppoe_0_0_35/ppp0

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



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

Destination	Subnet Mask	Gateway	Interface	Remove
10.11.102.4	255.255.0.0		ppp0	□

Note:

A maximum 32 entries can be configured.

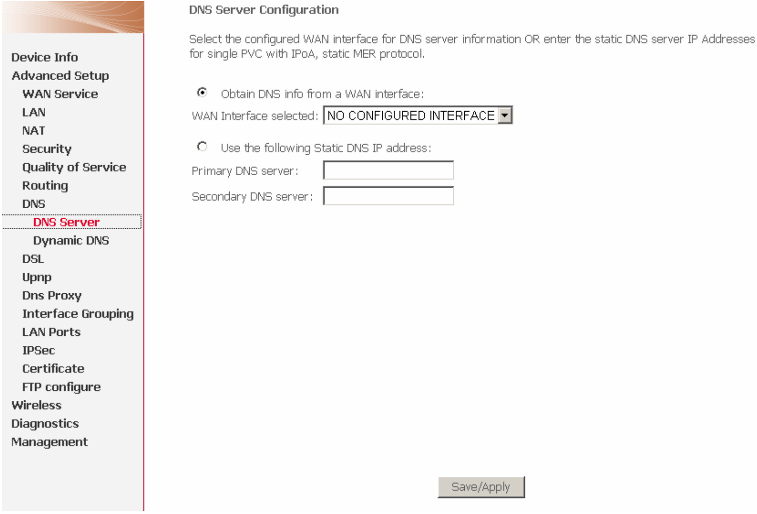
Remove Static Route

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

3.3.7 DNS

3.3.7.1 DNS Server

Choose **Advanced Setup** > **DNS** > **DNS Server** and the following page appears.



DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static MER protocol.

● Obtain DNS info from a WAN interface:

WAN Interface selected: NO CONFIGURED INTERFACE

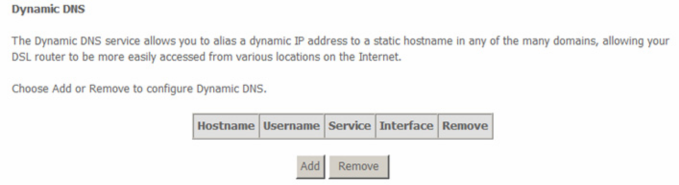
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

3.3.7.2 Dynamic Domain Name Service (DDNS)

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



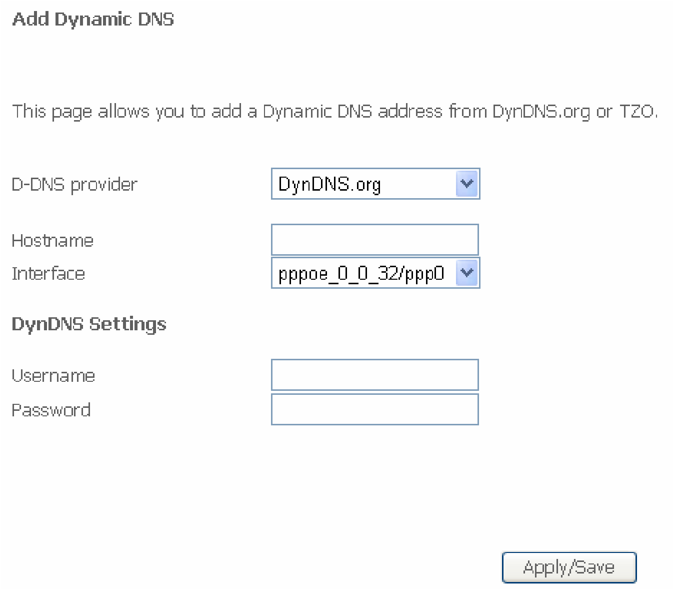
Dynamic DNS

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

Click **Add** to configure the information of a new host.



Add Dynamic DNS

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_32/ppp0

DynDNS Settings

Username:

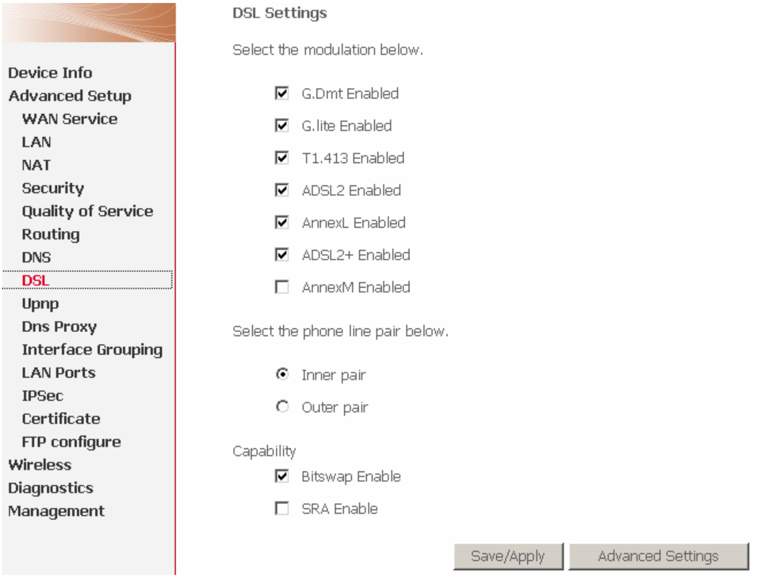
Password:

- **D-DNS provider**: Website of the dynamic DNS provider.
  - **DynDNS.org**: A free DNS service for hosts with dynamic IP addresses.
  - **TZO**: A service provider providing dynamic and static DNS services for a fee.
- **Hostname:** It is the domain name and it can be modified.
- **Interface**: The interface that the packets pass through on the modem.
- **Username:** This is the User name needed access the DDNS management interface.
- **Password:** This is the Password you will be prompted to enter when you access the DDNS management interface.

Select the service provider for the DDNS service, provide the hostname and the interface to use when sending the DDNS updates. Also enter the service provider specific registration information and click **Save/Apply** to use the feature.

3.3.8 DSL

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



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

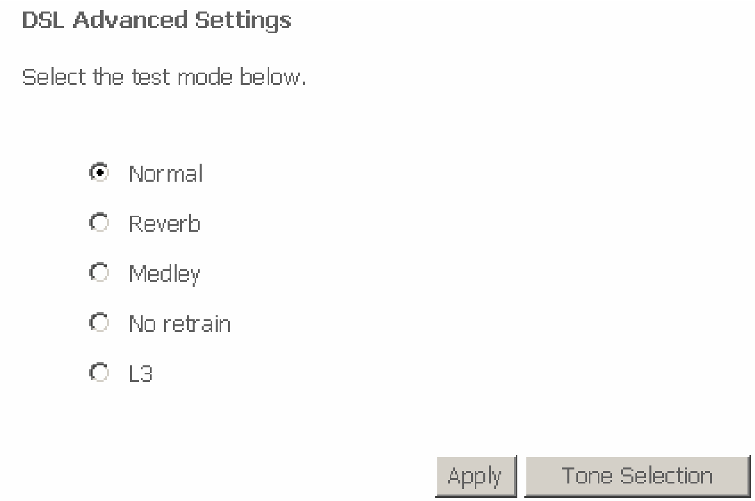
○ Outer pair

Capability

☑ Bitswap Enable

□ SRA Enable

Click **Advanced Settings** to select a DSL test mode.



DSL Advanced Settings

Select the test mode below.

● Normal

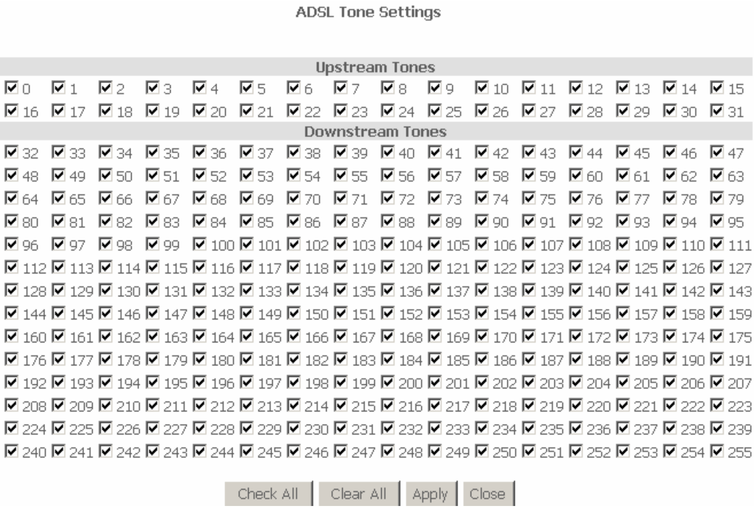
○ Reverb

○ Medley

○ No retrain

○ L3

Click **Tone Selection** to modify the upstream and downstream tones.



ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15
☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

Downstream Tones

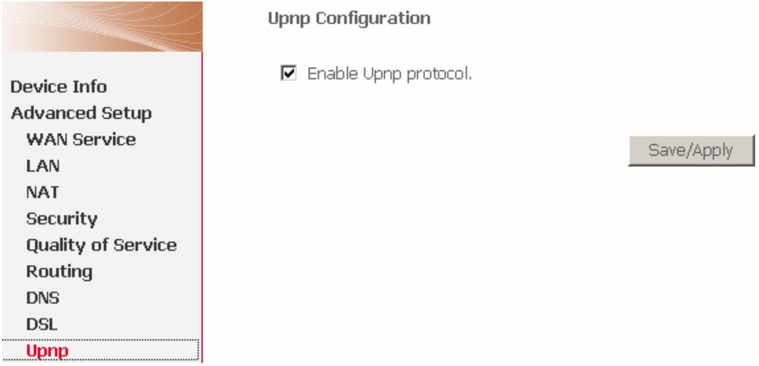
☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47
☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53 ☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63
☑ 64 ☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75 ☑ 76 ☑ 77 ☑ 78 ☑ 79
☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86 ☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95
☑ 96 ☑ 97 ☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108 ☑ 109 ☑ 110 ☑ 111
☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119 ☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 127
☑ 128 ☑ 129 ☑ 130 ☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141 ☑ 142 ☑ 143
☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152 ☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 159
☑ 160 ☑ 161 ☑ 162 ☑ 163 ☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174 ☑ 175
☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185 ☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191
☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196 ☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 207
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218 ☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 223
☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229 ☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 239
☑ 240 ☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251 ☑ 252 ☑ 253 ☑ 254 ☑ 255

Select the appropriate upstream and downstream tones for your ADSL connection. Click **Apply** to let your settings take effect.

3.3.9 UPNP

3.3.9.1 Enabling UPNP

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



Upnp Configuration

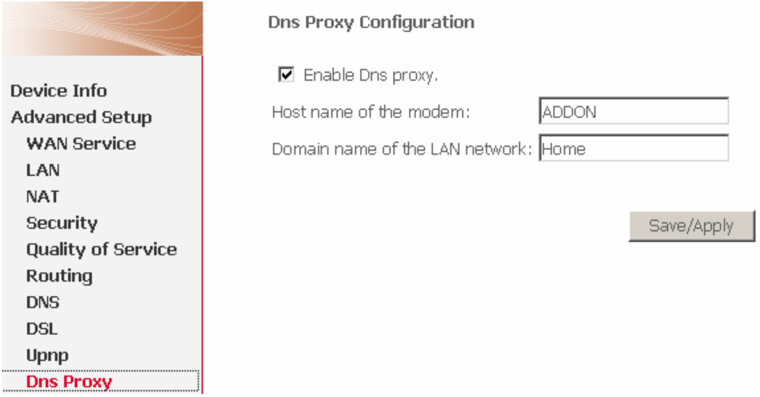
☑ Enable Upnp protocol.

Note:

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

3.3.10 DNS Proxy

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



Dns Proxy Configuration

☑ Enable Dns proxy.

Host name of the modem: ADDON

Domain name of the LAN network: Home

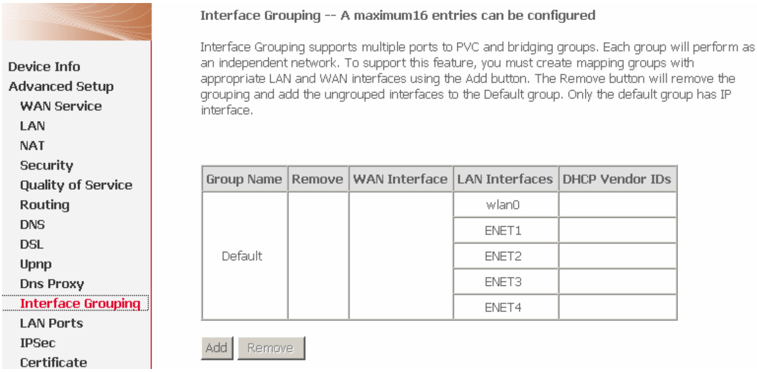
Enter Host name of the modem and domain name of the LAN network, click **Apply/Save** to save the configuration.

3.3.11 Interface Grouping

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

Note:

If you want to do Ethernet interface grouping, you need to enable the LAN ports first.

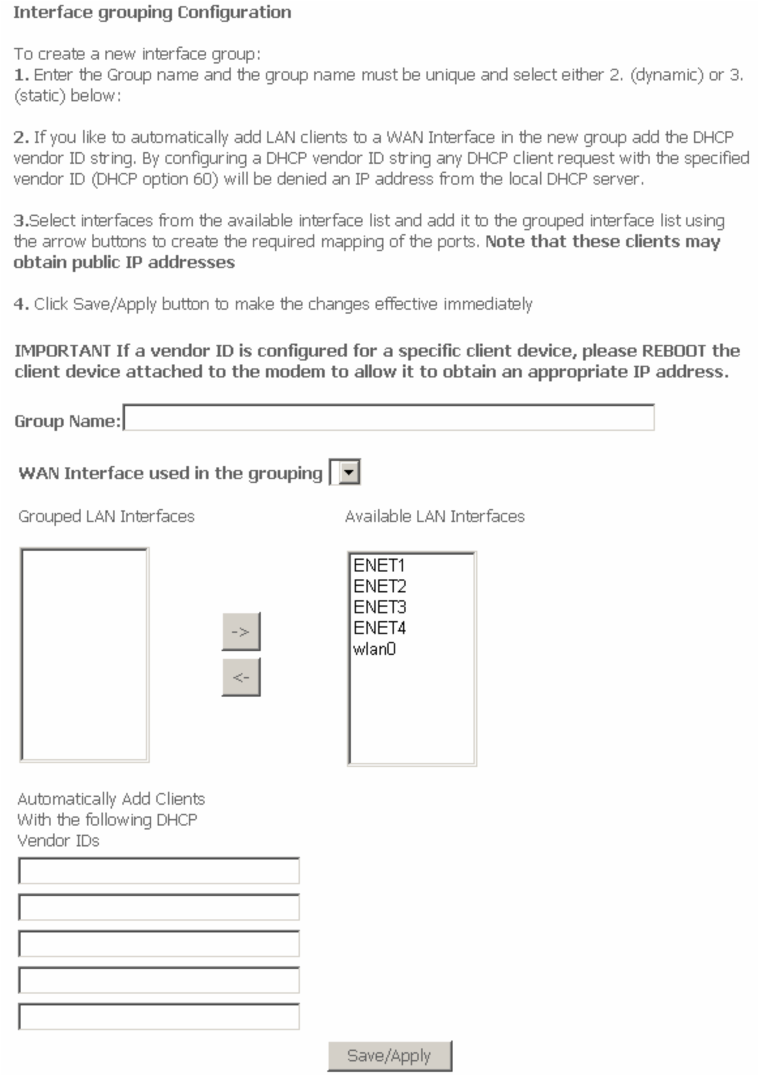


Interface Grouping -- A maximum16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			wlan0	
			ENET1	
			ENET2	
			ENET3	
			ENET4	

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



Interface grouping Configuration

To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

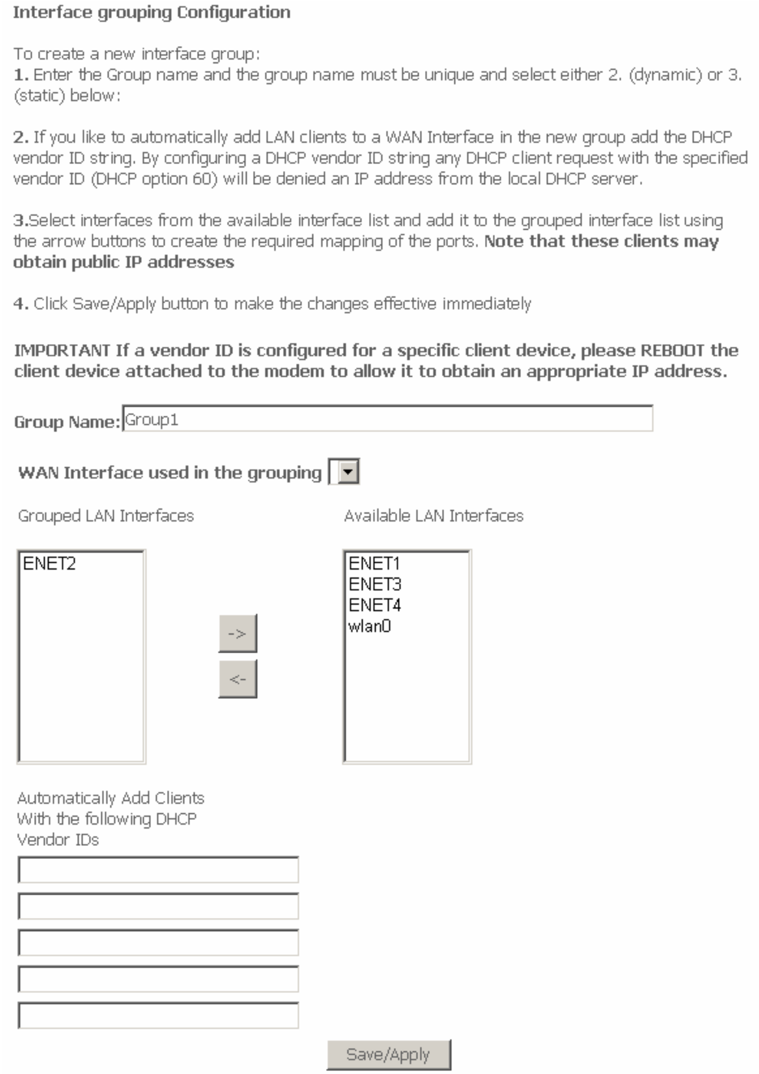
4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping

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



Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name: Group1

WAN Interface used in the grouping

Grouped LAN Interfaces: ENET2

Available LAN Interfaces: ENET1, ENET3, ENET4, wlan0

Automatically Add Clients With the following DHCP Vendor IDs

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

Note:

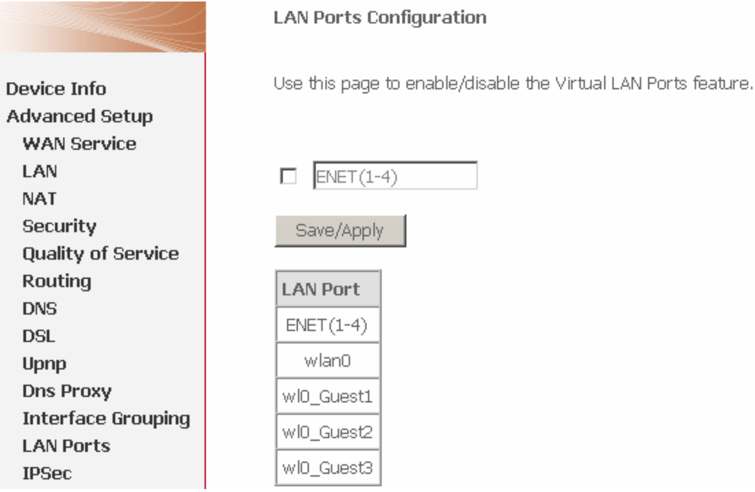
These clients may obtain public IP addresses.

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

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

3.3.12 LAN Ports

Choose **Advanced Setup > LAN Ports** and the following page appears. In this page, you can enable/disable the Virtual LAN Ports function.



LAN Ports Configuration

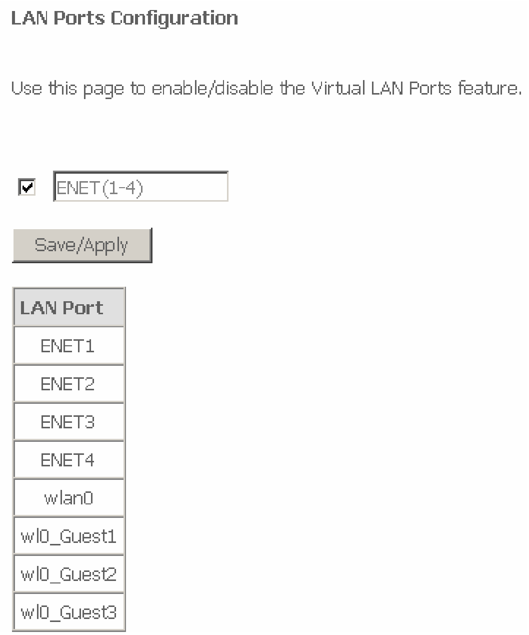
Use this page to enable/disable the Virtual LAN Ports feature.

□ ENET(1-4)

Save/Apply

LAN Port
ENET(1-4)
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

Select the checkbox, and the following page appears.



LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

☑ ENET(1-4)

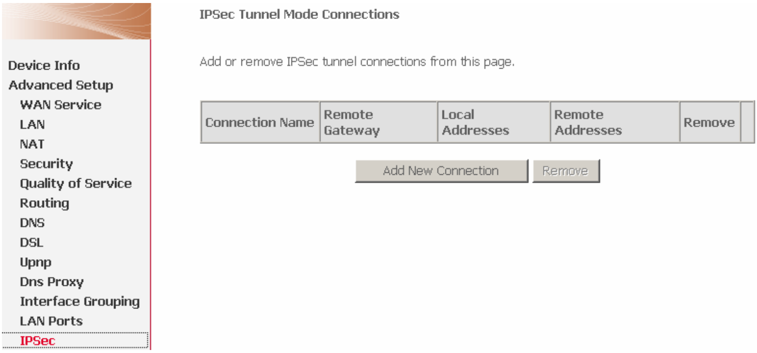
LAN Port
ENET1
ENET2
ENET3
ENET4
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

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

3.3.13 **IPsec**

3.3.13.1 How to Use and Configure the IPSec

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



IPSec Tunnel Mode Connections

Add or remove IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove

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

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

IPSec Setting Parameters

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

  If you select **subnet**, it allows more than one PC from local to connect remote hosts with IPSEC mode.

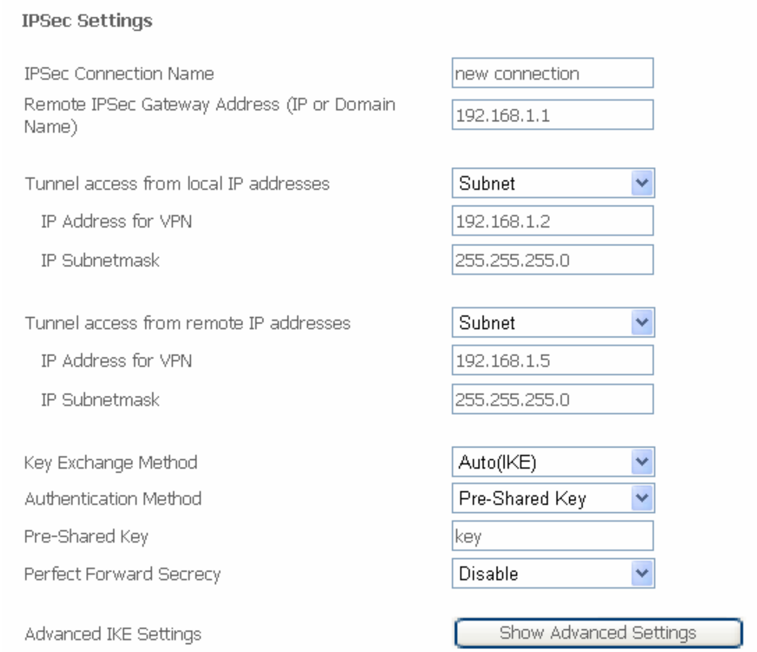
Note:

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

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

Example of Configuring IPSec

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

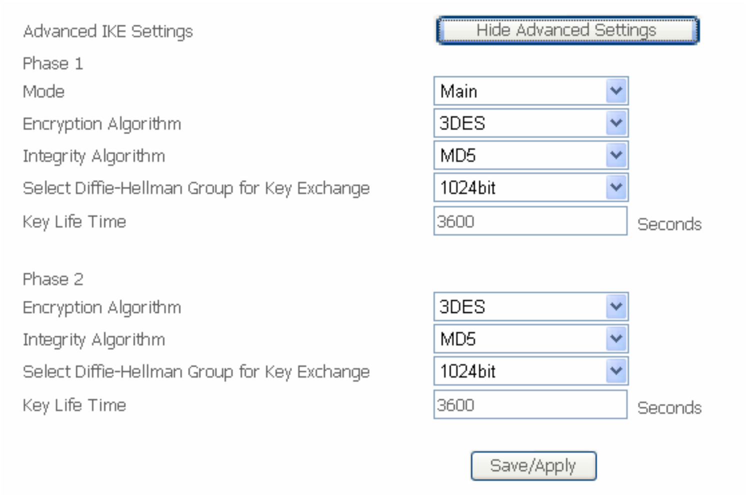


IPSec Settings

IPSec Connection Name	new connection
Remote IPSec Gateway Address (IP or Domain Name)	192.168.1.1
Tunnel access from local IP addresses	Subnet
IP Address for VPN	192.168.1.2
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	192.168.1.5
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

This is a dynamic page. The displays are different (some options are shown and hidden) when different types or connections are chosen. You can select automatic key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.

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



Advanced IKE Settings

Phase 1

Mode: Main

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Phase 2

Encryption Algorithm: 3DES

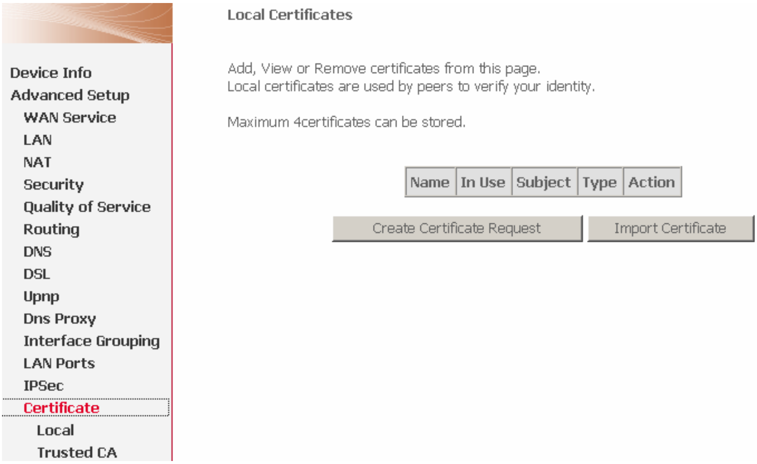
Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

3.3.14 Certificate

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



Local Certificates

Add, View or Remove certificates from this page.
Local certificates are used by peers to verify your identity.

Maximum 4certificates can be stored.

Name	In Use	Subject	Type	Action

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

Local certificates can be created by two ways:

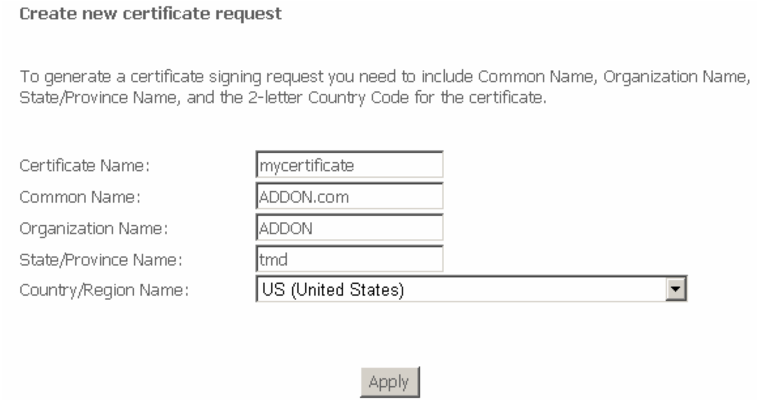
- Create a new certificate request, have it signed by a certificate authority and load the signed certificate.
- Import an existing signed certificate directly.

3.3.14.1 Create New Local Certificate

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

To create a new certificate, do as follows:

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

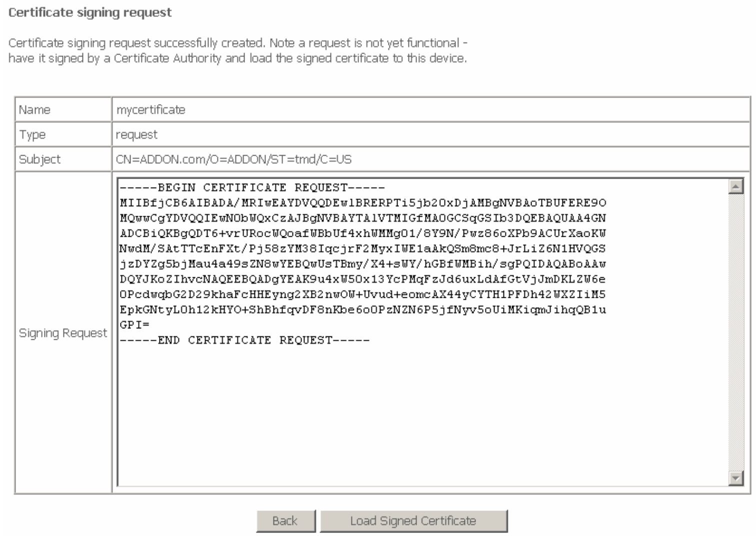


Create new certificate request

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

Certificate Name:	mycertificate
Common Name:	ADDON.com
Organization Name:	ADDON
State/Province Name:	tmd
Country/Region Name:	US (United States)

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



Certificate signing request

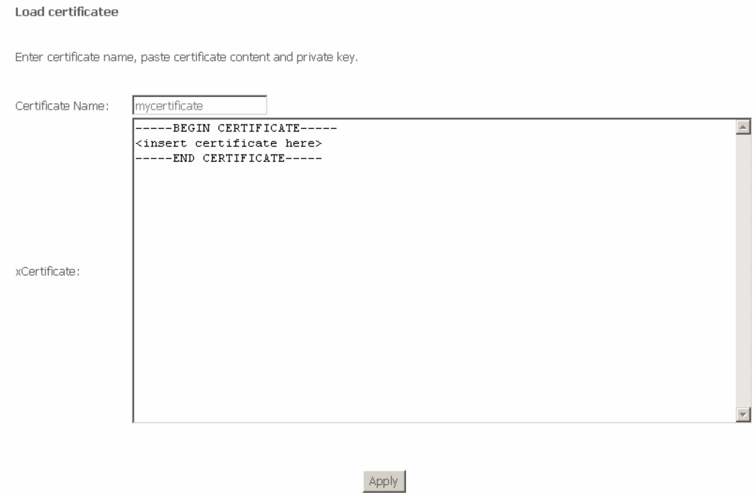
Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	mycertificate
Type	request
Subject	CN=ADDON.com/O=ADDON/ST=tmd/C=US

Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBfjCB6AIBADA/MRIwEAYDVQQDEwlBRERPTi5jb20xDjAMBgNVBAoTBUFERE9O
MQwwCgYDVQQIEwN0bWQxCzAJBgNVBAYTAlVTMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDT6+vrURocWQoafWBbUf4xhWMMg01/8Y9N/Pwz86oXPb9ACUrXaoKW
NwdM/SAtTTcEnFXt/Pj58zYM38IqcjrF2MyxIWE1aAkQSm8mc8+JrLiZ6N1HVQGS
jzDYZg5bjMau4a49sZN8wYEBQwUsTBmy/X4+sWY/hGBfWMBih/sgPQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAK9u4xW50x13YcPMqFzJd6uxLdAfGtVjJmDKLZW6e
0PcdwqbG2D29khaFcHHEyng2XB2nwOW+Uvud+eomcAX44yCYTH1PFDh42WXZIiM5
EpkGNtyL0h12kHYO+ShBhfqvDF8nKbe6o0PzNZN6P5jfNyv5oUiMKiqmJihqQB1u
GPI=
-----END CERTIFICATE REQUEST-----
```

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



Load certificatee

Enter certificate name, paste certificate content and private key.

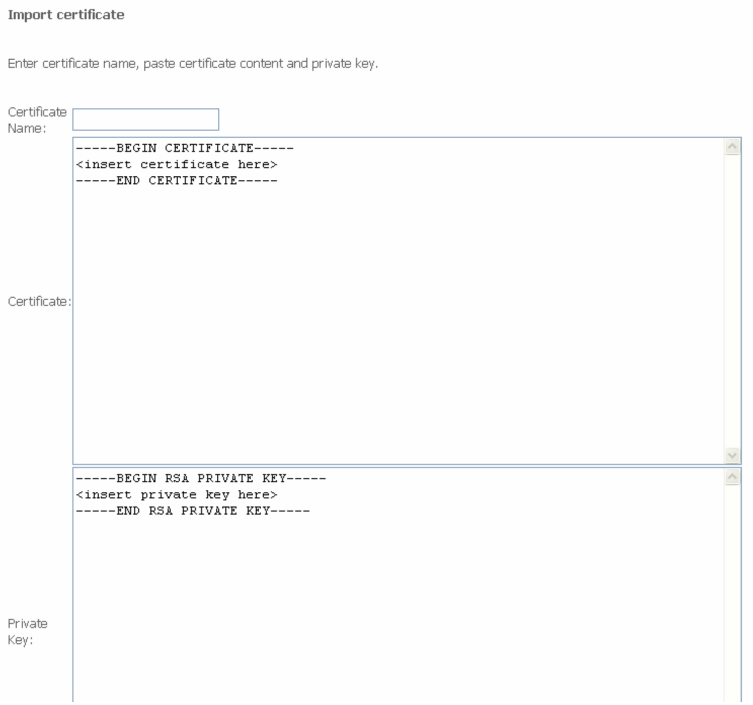
Certificate Name: mycertificate

xCertificate:

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

3.3.14.2 Importing an Existing Local Certificate

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


Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

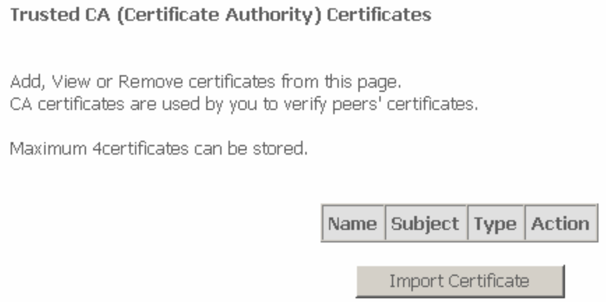
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

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

3.3.14.3 Trusted CA Certificates

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

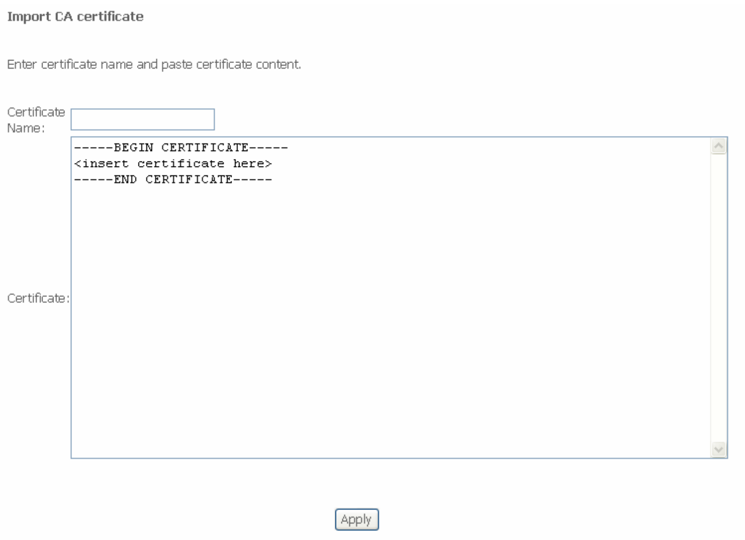

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page.
CA certificates are used by you to verify peers' certificates.

Maximum 4certificates can be stored.

Name	Subject	Type	Action

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



Import CA certificate

Enter certificate name and paste certificate content.

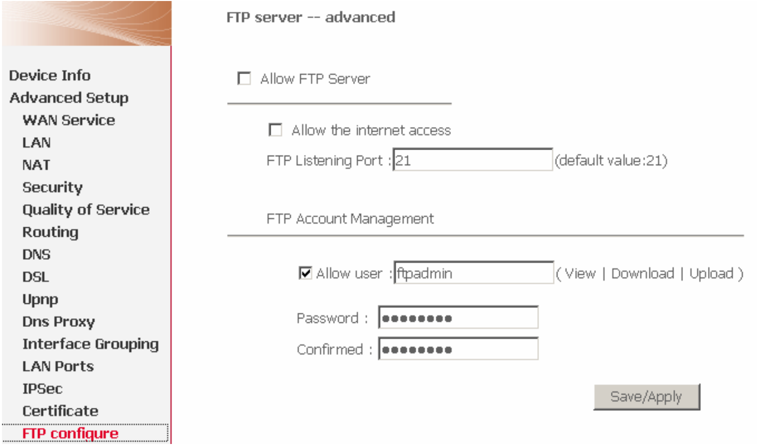
Certificate Name:

Certificate:

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

3.3.15 FTP Configuration

Choose **Advanced Setup** > **FTP Configure**, the following page appears.



FTP server -- advanced

□ Allow FTP Server

□ Allow the internet access

FTP Listening Port : 21 (default value:21)

FTP Account Management

☑ Allow user : ftpadmin (View | Download | Upload)

Password : ●●●●●●●●●

Confirmed : ●●●●●●●●●

- **Allow FTP Server**: If you allow users to access the FTP sever, please select this checkbox.

- **Allow the internet access**: If you allow the users of internet to access the FTP sever, please select this checkbox. Then configure the FTP listening port and maximum connections for the same IP.
- **FTP Account Management** If you allow the user of administrator to access the FTP sever, please select this checkbox. The user of administrator can view, download and upload the FTP file. Then configure the password.

3.4 Wireless

3.4.1 Wireless LAN Basics

3.4.1.1 Basic terms

- **AP:** Short for Access Point, a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.
- **STA:** Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).
- **SSID:** Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. You may disable SSID broadcasting in the web manager’s wireless menu.

3.4.1.2 Wireless Standard

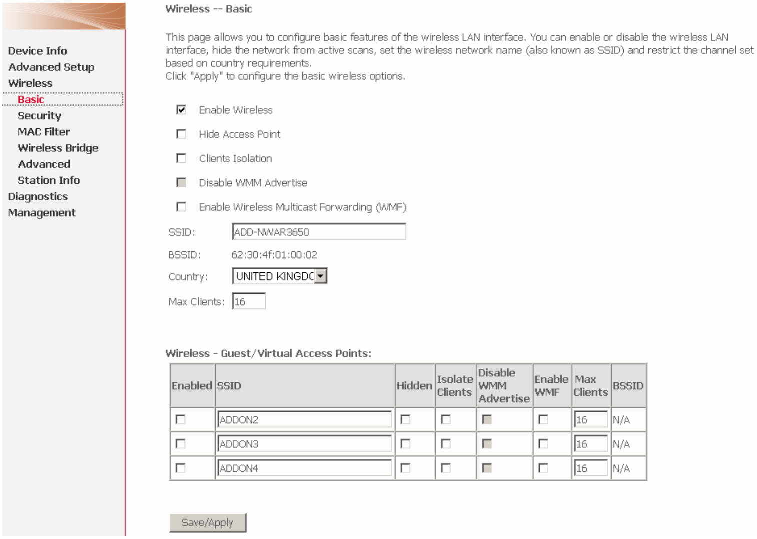
Wireless Standard includes **IEEE 802.11b**, **IEEE 802.11g** and **IEEE 802.11n.**

3.4.1.3 Wireless Security

Various security options are available on the DSL including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. Otherwise,you do not need to know the SSID and security keys or passphrases when connecting WPS-enabled devices.

3.4.2 Wireless – Basic

Choose **Wireless > Basic**, the following page appears.



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: ADD-NWAR3650

BSSID: 62:30:4f:01:00:02

Country: UNITED KINGDC

Max Clients: 16

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	ADDON2	□	□	□	□	16	N/A
□	ADDON3	□	□	□	□	16	N/A
□	ADDON4	□	□	□	□	16	N/A

- **Enable Wireless**: If you want to make wireless be available, you have to check this box first. Otherwise, the Hide Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID boxes are not displayed.
- **Hide Access Point**: Check this box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.
- **Clients Isolation**: When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can check this box.
- **Disable WMM Advertise**: WMM is short for wi-fi multimedia, which can provide high-performance multimedia voice and video data transfers.
- **Enable Wireless Multicast Forwarding (WMF):** The Wireless Multicast forwards to Wireless unicast.
- **SSID**: For added security, you should change the default SSID to a unique name.
- **Country**: The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specifies maximum wireless client stations to be enble to link with AP. Once the clients exceed the max vlaue, all other clients are refused.

The value of maximum clients is 16.

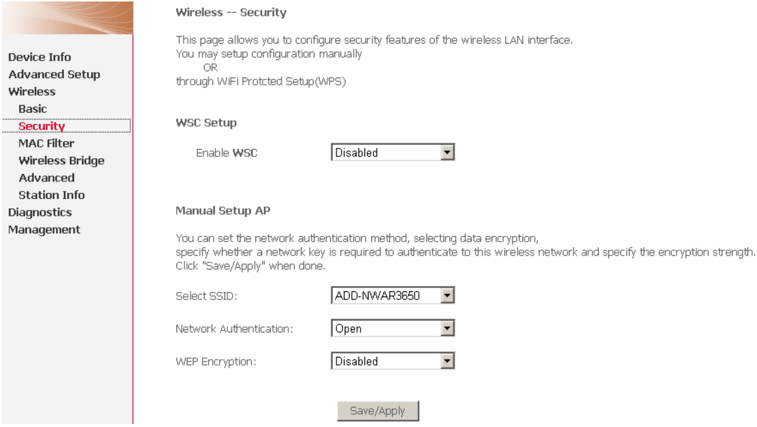
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After setting, click **Save/Apply** to save the basic wireless options and make the change take effect.

3.4.3 Wireless – Security

This page allows you can configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Another way, you can setup configuration through WiFi Protected Setup (WPS).

WSC Setup



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)

WSC Setup

Enable WSC: Disabled

Manual Setup AP

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

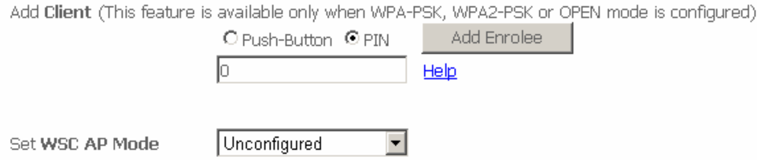
Select SSID: ADD-NWAR3650

Network Authentication: Open

WEP Encryption: Disabled

Enable WSC: If enable **Manual Setup AP**, you can not enable WSC.

Set WSC AP Mode: If selected Unconfigured, you need to add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured.)



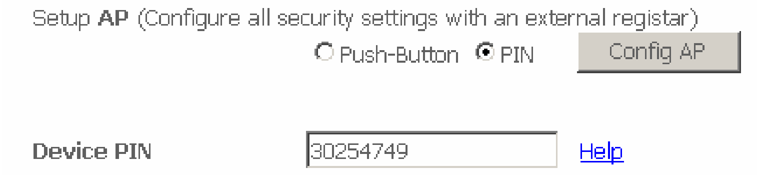
Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)

○ Push-Button ● PIN

0

Set WSC AP Mode: Unconfigured

and setup AP (Configure all security settings with an external registar).



Setup **AP** (Configure all security settings with an external registar)

○ Push-Button ● PIN

Device PIN 30254749

Device PIN: Device Pin is generated by AP.

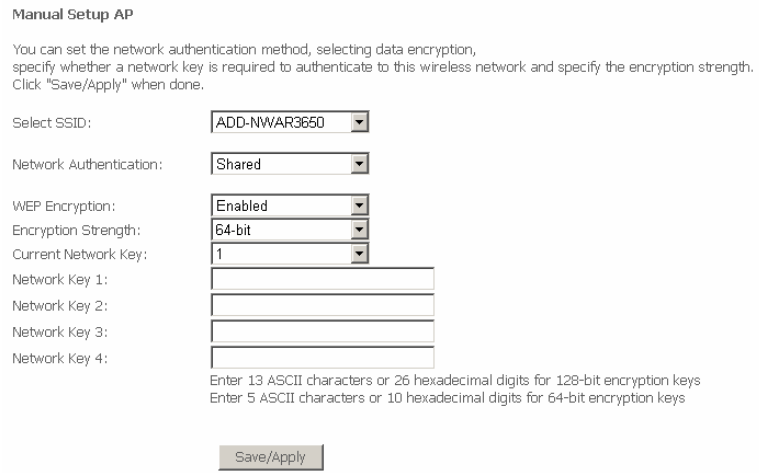
WSC Add External Registrar: If set WSC AP Mode to Configured, this part will show, and you can add external registrar.

Manual Setup AP

This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy).

Following is a description of the different options:

- **Select SSID:** Select the wireless LAN of SSID to configure security features.
- **No Encryption :** Please refer to below for details of configuration
- **Network Authentication:** Select the authentication mode for the selected wireless LAN of SSID to be open.
- **WEP Encryption:** Disable WEP Encryption.



Manual Setup AP

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

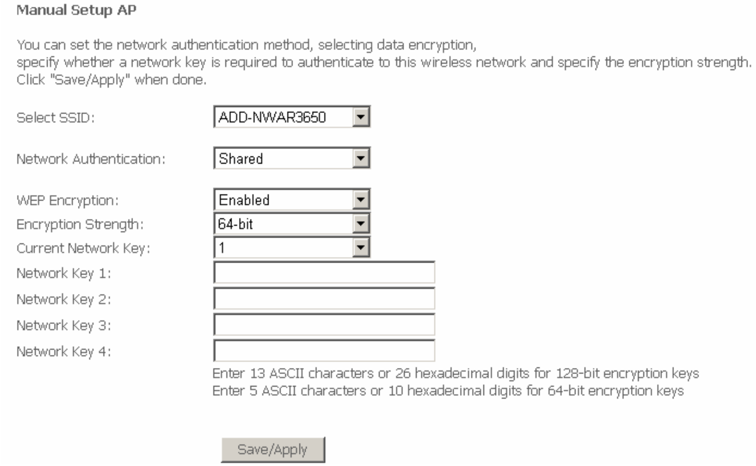
Select SSID:	ADD-NWAR3650
Network Authentication:	Shared
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	1
Network Key 1:	
Network Key 2:	
Network Key 3:	
Network Key 4:	

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

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

- **64-bit WEP**
  - – **Network Authentication:** Select the authentication mode for the selected wireless LAN of SSID to be open or shared.
  - – **WEP Encryption:** Enable WEP Encryption.
  - – **Encryption Strength:** click the desired Data Security level to be 64-bit.
  - – **Current Network Key:** Select one of network key that you set on the Key boxes as default one.
  - – **Network Key 1 to 4:** Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

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



Manual Setup AP

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

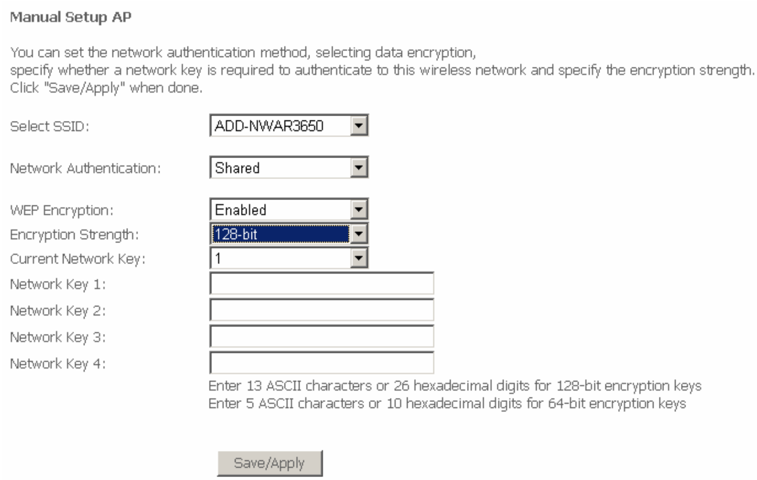
Select SSID:	ADD-NWAR3650
Network Authentication:	Shared
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	1
Network Key 1:	
Network Key 2:	
Network Key 3:	
Network Key 4:	

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

Figure 5 Wireless – security (64-bit WEP)

- **128-bit WEP**
  - – **Encryption Strength:** click the desired Data Security level to be 128-bit.
  - – **Network Key 1 to 4:** Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

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



Manual Setup AP

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

Select SSID: ADD-NWAR3650

Network Authentication: Shared

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1:

Network Key 2:

Network Key 3:

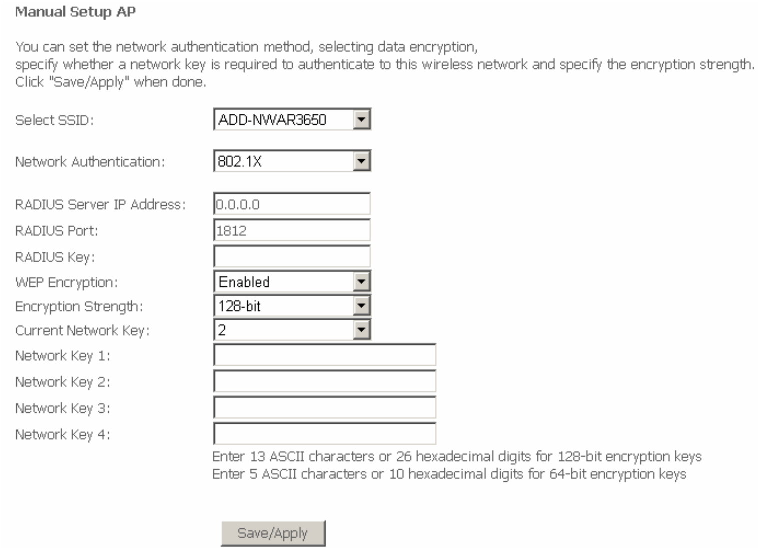
Network Key 4:

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

Figure 6 Wireless – security (128-bit WEP)

- **802.1x Authentication**
  - – **Radius Server IP Adress:** Enter the IP Address of the authentication server.
  - – **Radius Port:** Enter the port number of the authentication server. The default port number is 1812.
  - – **Radius Key:** Enter the same key as the Radius server’s.

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



Manual Setup AP

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

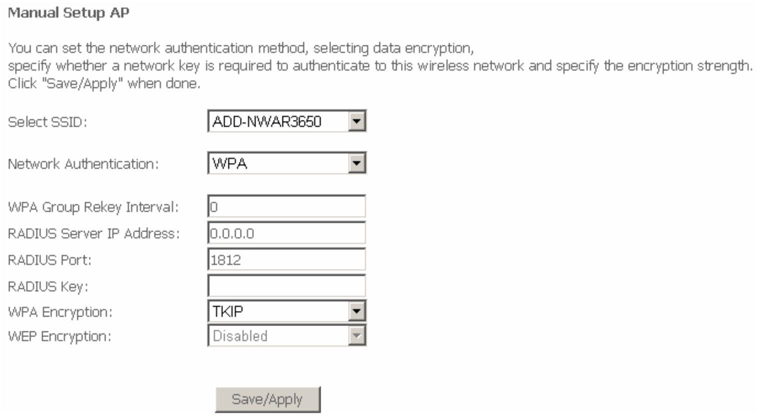
Select SSID:	ADD-NWAR3650
Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	2
Network Key 1:	
Network Key 2:	
Network Key 3:	
Network Key 4:	

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

Figure 7 Wireless – Security (802.1x Authentication**)**

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

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



Manual Setup AP

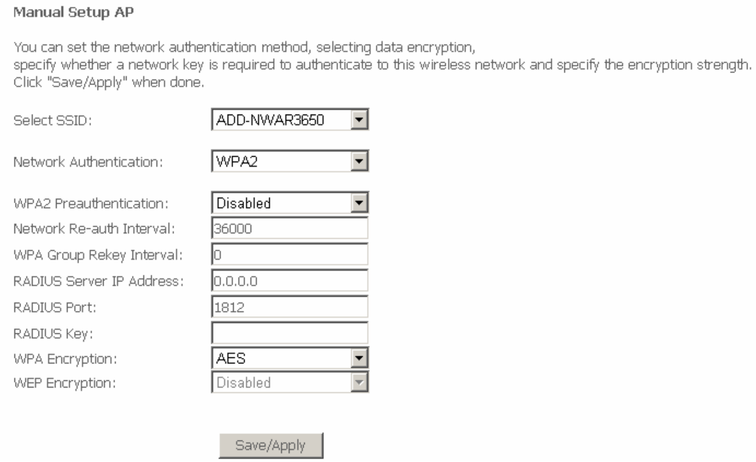
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID:	ADD-NWAR3650
Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Figure 8 Wireless – security (WPA authentication)

- **WPA2 Authentication**
  - –**WPA2 Preauthentication:** Selec Enable or Disenable.
  - –**Network Re-auth Interval:** Specifies the timer of re-authentication between the server and the client.

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



Manual Setup AP

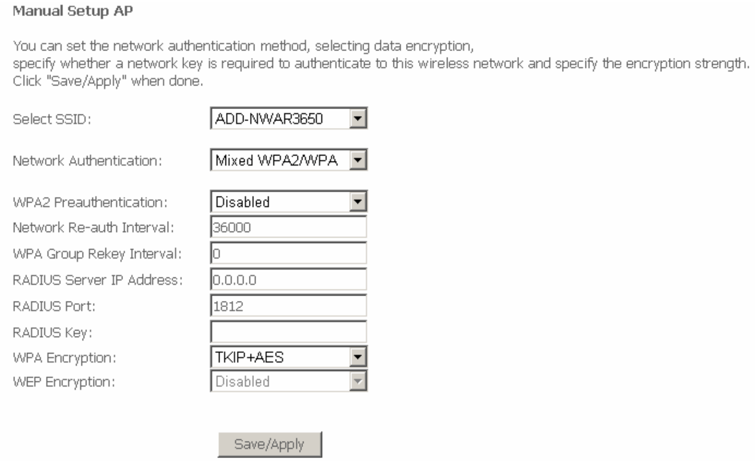
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID:	ADD-NWAR3650
Network Authentication:	WPA2
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	AES
WEP Encryption:	Disabled

Figure 9 Wireless – security (WPA2 authentication)

- **Mixed WPA2/WPA Authentication:** This authentication mode means AP auto adjust to use WPA2 or WPA according to wireless clients.

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



Manual Setup AP

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

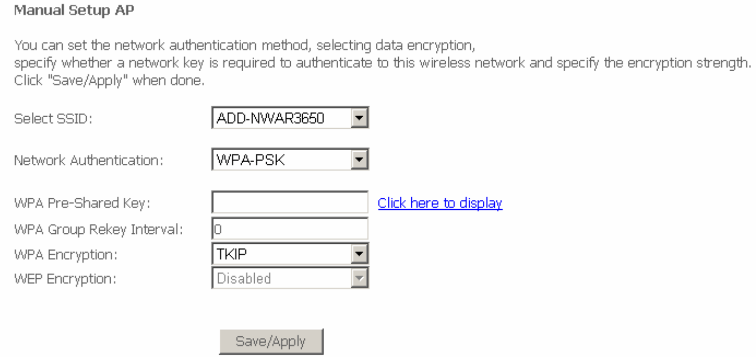
Select SSID:	ADD-NWAR3650
Network Authentication:	Mixed WPA2/WPA
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

Figure 10 Wireless – security (mixed WPA2/WPA authentication)

- **WPA-PSK Authentication**

  – **WPA Pre-Shared Key:** Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device.

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



Manual Setup AP

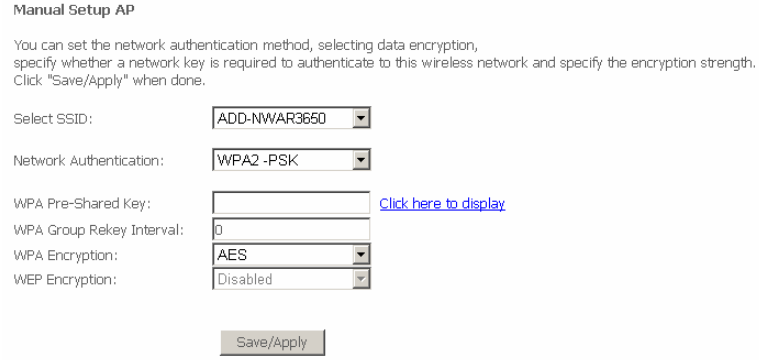
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Save/Apply" when done.

Select SSID:	ADD-NWAR3650
Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	Click here to display
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Figure 11 Wireless – security (WPA-PSK authentication**)**

- **WPA2-PSK Authentication**

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



Manual Setup AP

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

Select SSID: ADD-NWAR3650

Network Authentication: WPA2 -PSK

WPA Pre-Shared Key: Click here to display

WPA Group Rekey Interval: 0

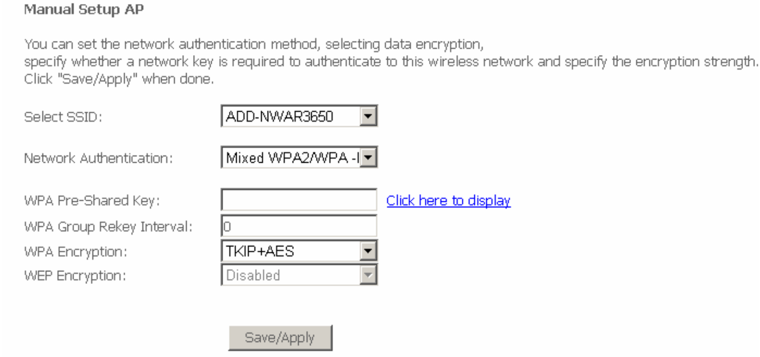
WPA Encryption: AES

WEP Encryption: Disabled

Figure 12 Wireless – security (WPA2-PSK authentication)

- **Mixed WPA2/WPA-PSK Authentication:** This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients.

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



Manual Setup AP

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

Select SSID: ADD-NWAR3650

Network Authentication: Mixed WPA2/WPA -I

WPA Pre-Shared Key: Click here to display

WPA Group Rekey Interval: 0

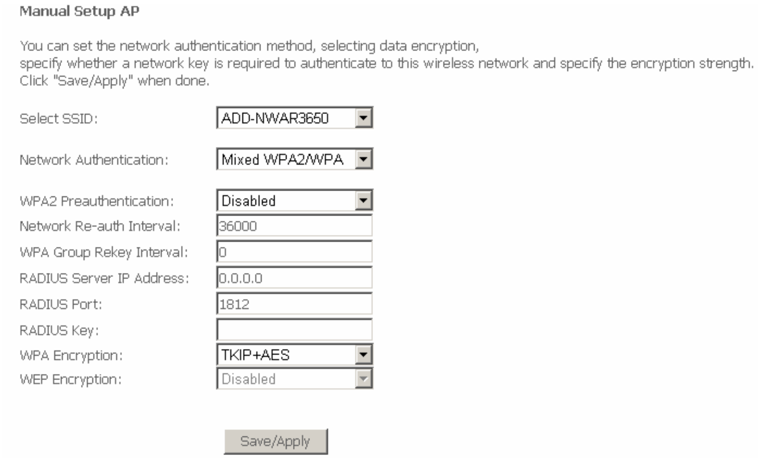
WPA Encryption: TKIP+AES

WEP Encryption: Disabled

Figure 13 Wireless – security (mixed WPA2/WPA-PSK authentication)

- **Mixed WPA2/WPA Authentication:** This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients.

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



Manual Setup AP

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

Select SSID:	ADD-NWAR3650
Network Authentication:	Mixed WPA2/WPA
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

Figure 14 Wireless – security (mixed WPA2/WPA authentication)

- **WPS Authentication:** There are 2 primary methods used in the Wi-Fi Protected Setup:
  – PIN entry, a mandatory method of setup for all WPS certified devices.
  – Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

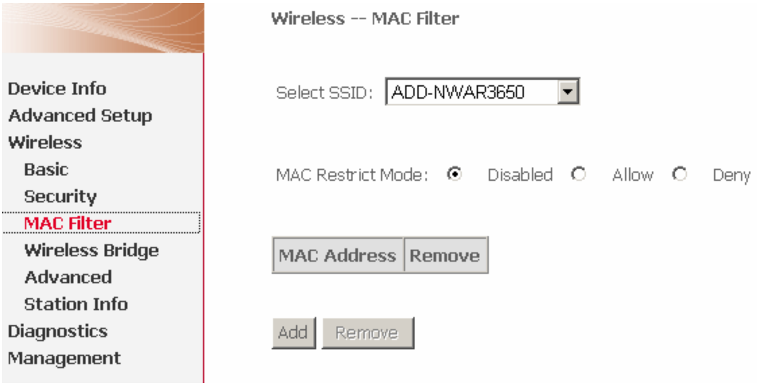
If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router. (Note: The PBC method may also need a Registrar when used in a special case where the PIN is all zeros)

In order to use wps authentication, you must ensure netcard support the function, if it support, you need not do any configuration. Only need to do is to press the wps button to enable the wps function.

3.4.4 Wireless-MAC Filter

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

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

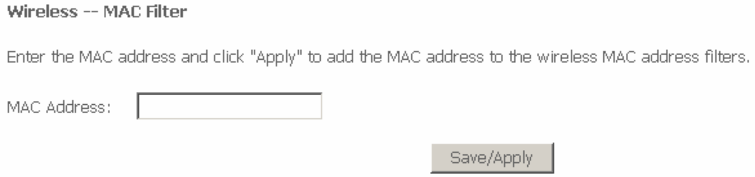

Wireless -- MAC Filter

Select SSID: ADD-NWAR3650

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

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


Wireless -- MAC Filter

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

MAC Address:

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

3.4.5 Wireless – Bridge

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

- **AP Mode:** Select Access Point's functionality to be Access Point or pure Wireless Bridge.
- **Bridge Restrict:** Wireless bridge restriction.

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

Step 1 In the Bridge Restrict list, click Enabled (Scan).

Step 2 Click Refresh to update the remote bridges.

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

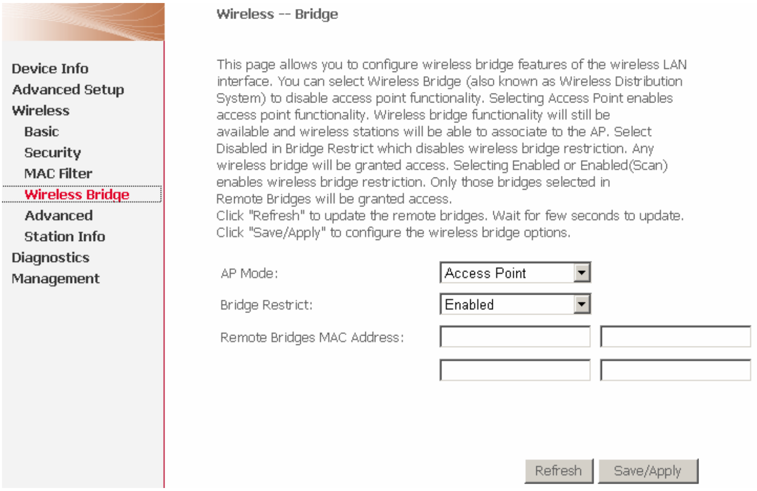
Step 3 Check on the box in the left column of the list for selecting the Access Point to which you want to establish a WDS connection.

Step 4 Click **Save/Apply**.

You must configure all Bridges Access Point with:

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

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



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

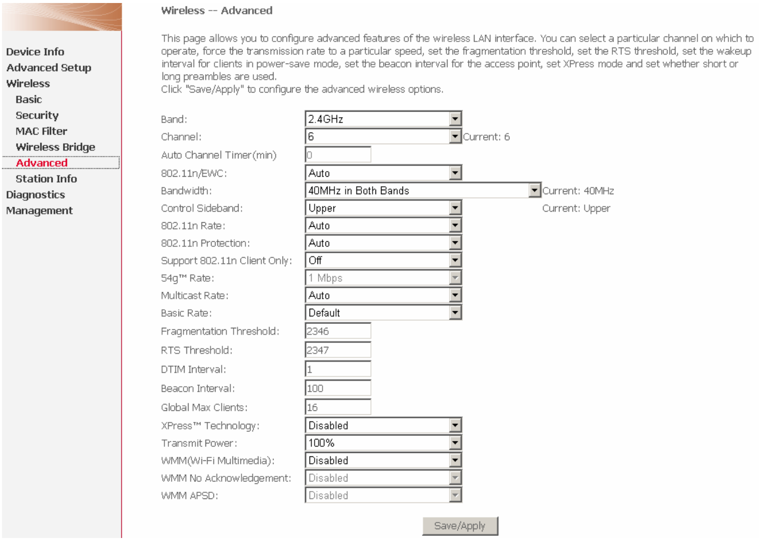
AP Mode: Access Point

Bridge Restrict: Enabled

Remote Bridges MAC Address:

3.4.6 Wireless – Advanced

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

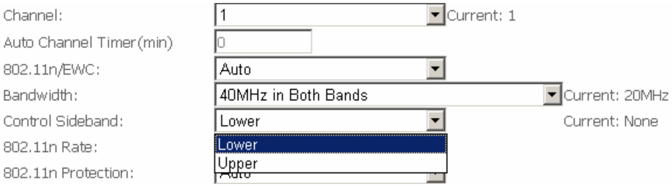


Wireless -- Advanced

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

Band:	2.4GHz	
Channel:	6	Current: 6
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	40MHz in Both Bands	Current: 40MHz
Control Sideband:	Upper	Current: Upper
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Disabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Disabled	

- **Band:** Select using wireless frequency band range. The radio frequency remains at 2.4GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer(min):** Specifies the timer of auto channelling.
- **802.11n/EWC:** Select **disable** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network.
- **Control Sideband:** If you select **20MHz in Both Bands** or **20MHz in 2.4G Band and 40MHz in 5G Band**, the service of control sideband does not work. When you select **40MHz in Both Bands** as the bandwidth, the following page appears. Then you can select **Lower** or **Upper** as the value of sideband. As the control sideband, when you select **Lower**, the channel is 1~7. When you select **Upper**, the channel is 5~11.



Channel:	1	Current: 1
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	40MHz in Both Bands	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:		
802.11n Protection:	Auto	

- **802.11n Rate/54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

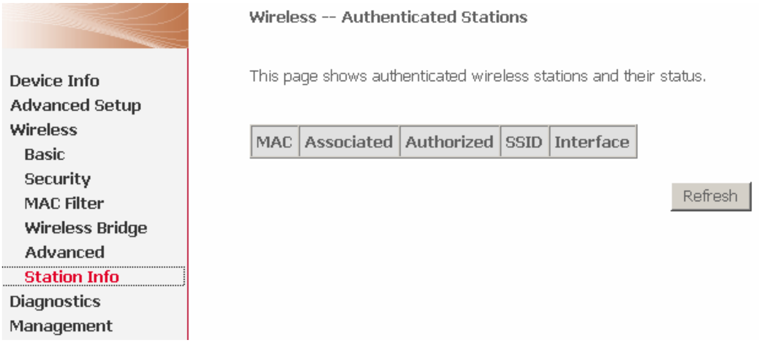
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without “speaking” at the same time.
- **Support 802.11n Client Only:** Only stations that are onfigured in 802.11n mode can associate.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.

- **WMM (Wi-Fi Multimedia):** Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
- **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
- **WMM APSD:** APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

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

3.4.7 Wireless -- Authenticated Stations

Choose **Wireless** > **Station Info**, the following page appears. This page shows authenticated wireless stations and their status about Association and authentication.



Wireless -- Authenticated Stations

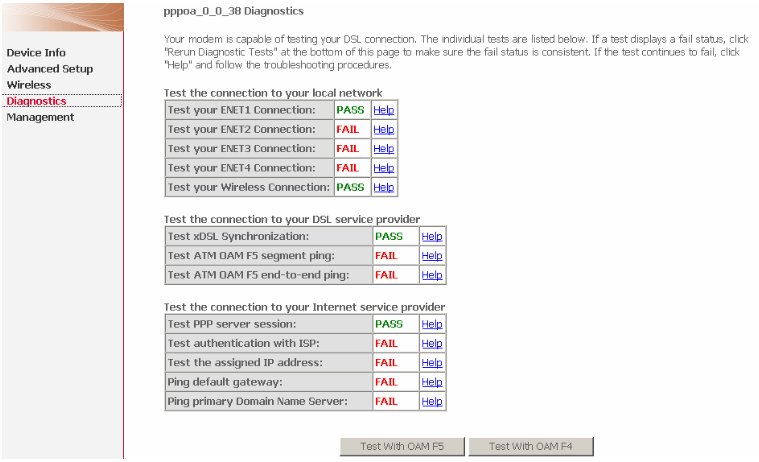
This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

3.5 Diagnostics

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

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



pppoa_0_0_38 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 ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	PASS	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

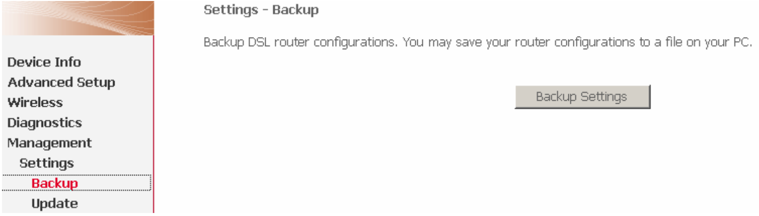
Test PPP server session:	PASS	Help
Test authentication with ISP:	FAIL	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

3.6 Management

3.6.1 Settings

3.6.1.1 Settings Backup

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

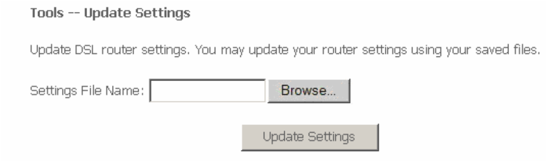


Settings - Backup

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

3.6.1.2 Settings Update

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



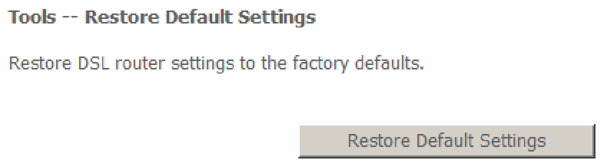
Tools -- Update Settings

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

Settings File Name:

3.6.1.3 Settings Restore Default

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

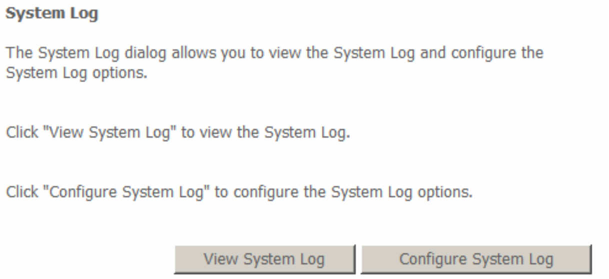


Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

3.6.2 System Log

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



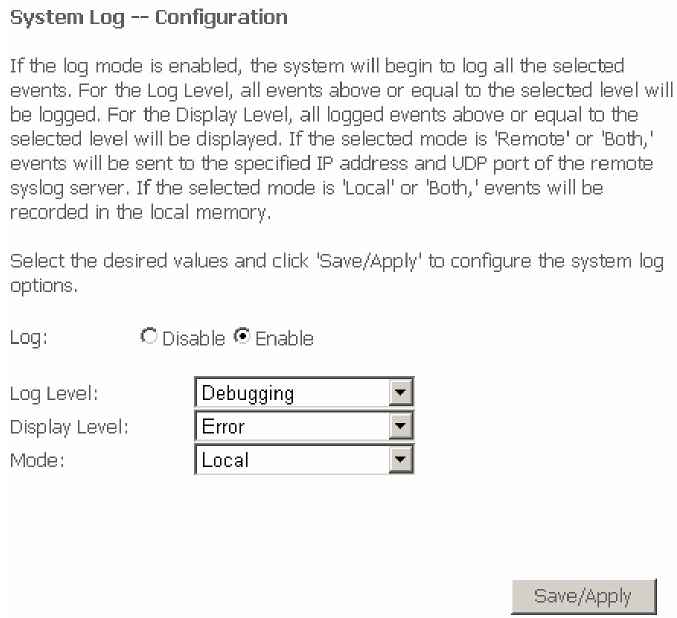
System Log

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

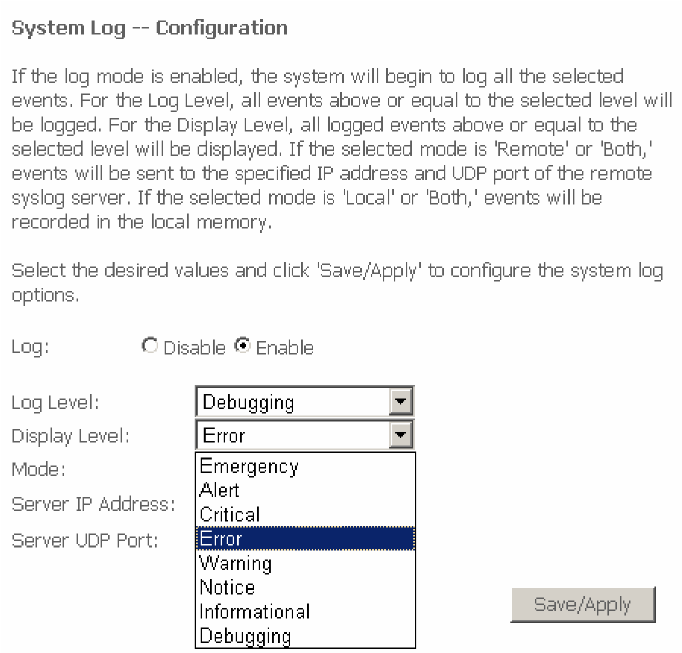
Log Level: Debugging

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 **Loca**l, **Remote**, and **Both**. The default is **Local**.



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

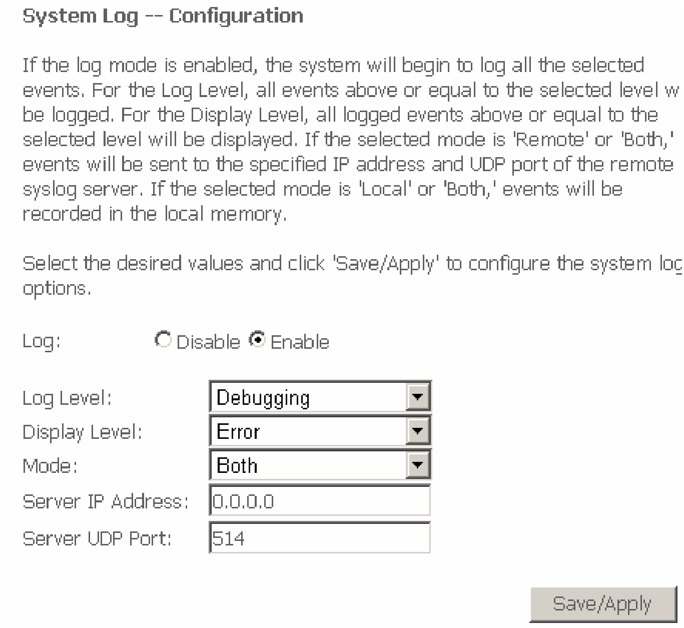
Mode:

Server IP Address:

Server UDP Port:

Figure 15 System log configuration (1)

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



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 w 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: Both

Server IP Address: 0.0.0.0

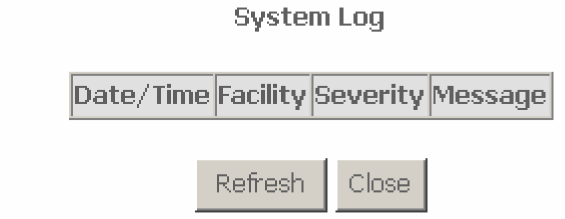
Server UDP Port: 514

Figure 16 System log configuration (2)

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

Note:

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



System Log

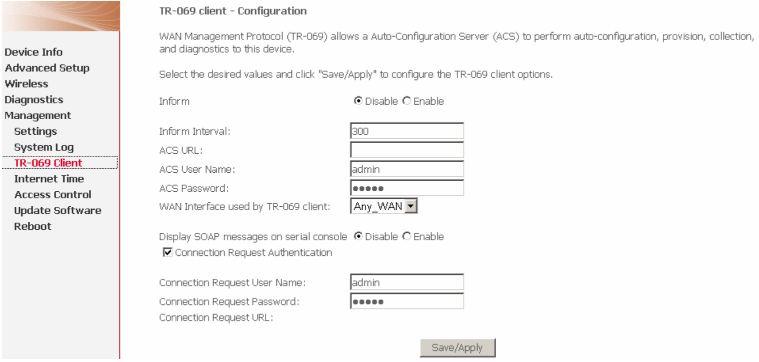
Date/Time	Facility	Severity	Message

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

3.6.3 TR-069 Client Management

3.6.3.1 Tr-069 Client-configuration

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



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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

Inform ● Disable ○ Enable

Inform Interval: 300
ACS URL:
ACS User Name: admin
ACS Password: ●●●●●
WAN Interface used by TR-069 client: Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable
☑ Connection Request Authentication

Connection Request User Name: admin
Connection Request Password: ●●●●●
Connection Request URL:

Figure 17 Tr-069 client -configuration

- **Inform:** If the **Enable** option is selected,the CPE accepts the commands from ACS, the CPE does not accept the commands from ACS when the

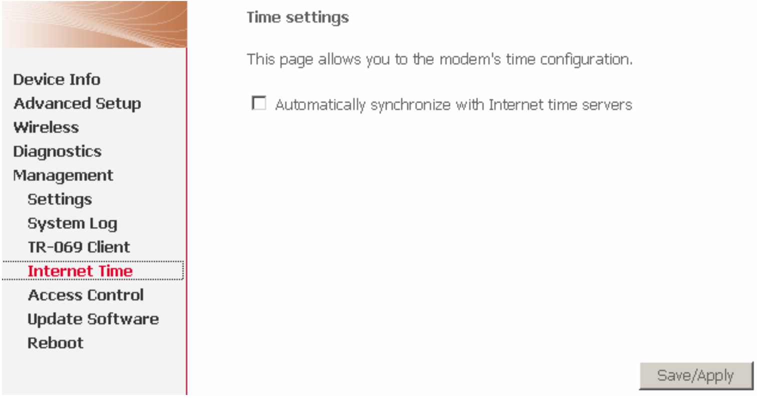
Disable option is selected.

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

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

3.6.4 Internet Time

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

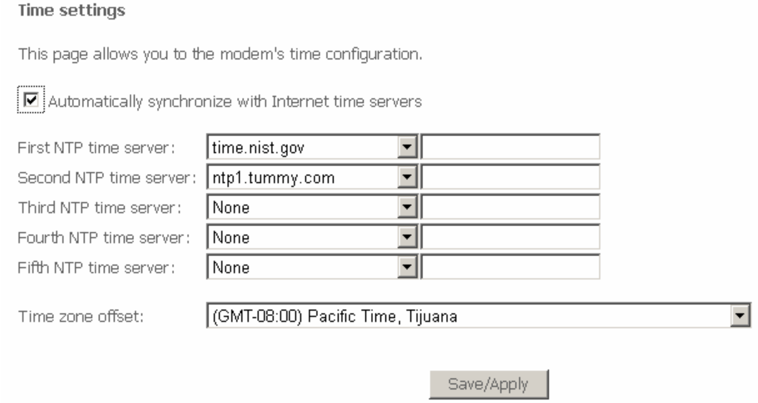


Time settings

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

☐ Automatically synchronize with Internet time servers

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



Time settings

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

☑ Automatically synchronize with Internet time servers

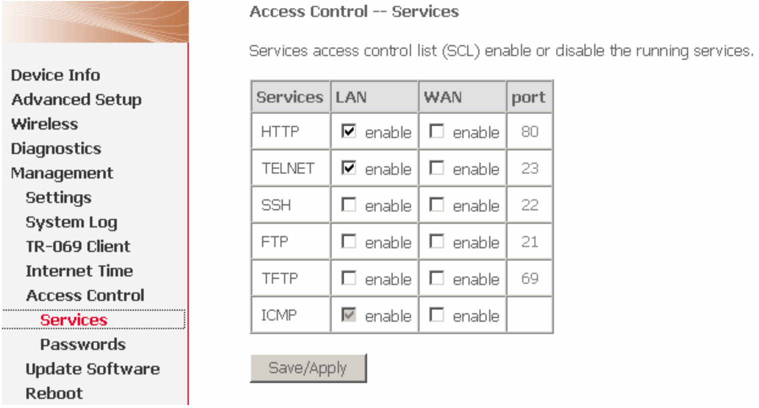
First NTP time server:	time.nist.gov	
Second NTP time server:	ntp1.tummy.com	
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

3.6.5 Access Control

3.6.5.1 Access Control – Services

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



Access Control -- Services

Services access control list (SCL) enable or disable the running services.

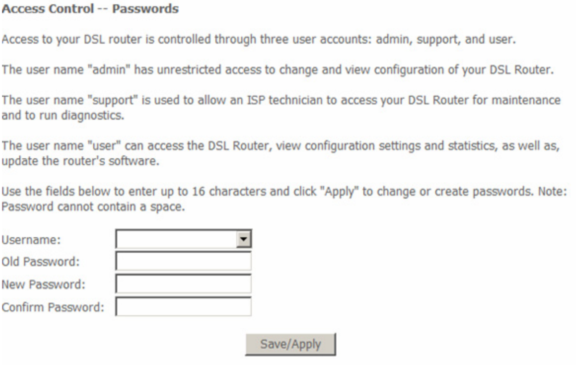
Services	LAN	WAN	port
HTTP	☑ enable	☐ enable	80
TELNET	☑ enable	☐ enable	23
SSH	☐ enable	☐ enable	22
FTP	☐ enable	☐ enable	21
TFTP	☐ enable	☐ enable	69
ICMP	☑ enable	☐ enable	

Note:

If the PVC connection is bridge mode, you can not view the information of WAN side.

3.6.5.2 Access Control – Passwords

Choose **Management > Access Control > Passwords,** and the following page appears. 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:

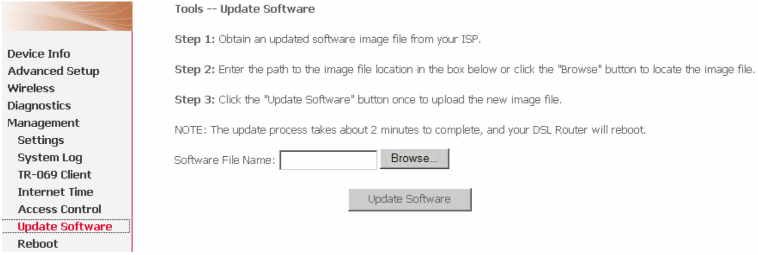
Old Password:

New Password:

Confirm Password:

3.6.6 Update Software

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



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:

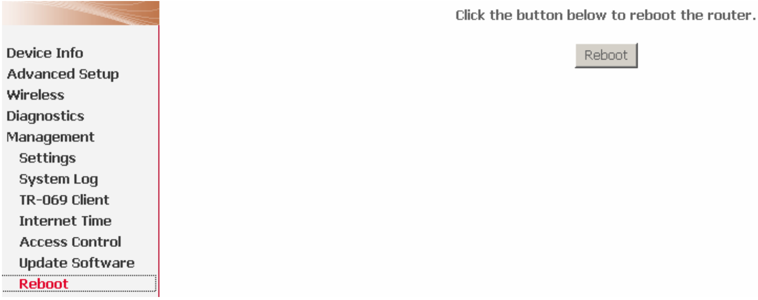
Note:

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

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

3.6.7 Reboot

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



Click the button below to reboot the router.

4 Q&A

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

A:

- Check the connection between the power adaptor and the power socket.
- Check the power switch is on or not.

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

A:

- Check the connection between the ADSL modem and your computer, hub, or switch.
- Check the running status of your PC, hub, or switch, and ensure that they are working normally.

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

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

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

A: Ensure that the following information is correctly entered.

- VPI/VCI
- Username/password.

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

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

- Choose **Start** > **Run** from the desktop, and ping ***192.168.1.1*** (the IP address of the modem).
- If the modem cannot be reached, please check following configuration:
  - Type of the network cable
  - Connection between the modem and computer
  - TCP/IP configuration of you computer

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

A:

- To restore the factory default, keep the device powered on and push a needle into the hole. Press down the button about one second 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**.