
NETGEAR JDGN1000

User Manual

Contents

1	Safety Precautions	2
2	Overview	2
2.1	Application	2
2.2	Features.....	2
2.3	Standards Compatibility and Compliance	2
3	Hardware Description and Hardware Installation	2
3.1	Hardware Description.....	2
3.1.1	Front Panel.....	2
3.1.2	Rear Panel	2
3.2	Hardware Installation.....	2
3.2.1	Choosing the Best Location for Wireless Operation	2
3.2.2	Connecting the Device.....	2
4	PC Network Configuration and Login.....	2
4.1	PC Network Configuration	2
4.2	Logging In to the DSL Router	2
5	Web-Based Management	2
5.1	Setup Wizard.....	2
5.2	Add WPS Client	2
5.3	Setup	2
5.3.1	Adsl Settings.....	2
5.3.2	Basic Settings.....	2
5.3.3	Interface Grouping.....	2
5.3.4	Wireless Settings.....	2
5.4	Content Filtering.....	2
5.4.1	Logs	2
5.4.2	Block sites	2
5.4.3	Block Services	2
5.5	Maintenance	2
5.5.1	Router Status.....	2
5.5.2	Attached Devices.....	2
5.5.3	Backup Settings.....	2
5.5.4	Set Password	2

5.5.5	Router Upgrade	2
5.5.6	Logout	2
5.6	Advanced	2
5.6.1	Wireless Settings	2
5.6.2	Wireless Repeating Function	2
5.6.3	Port Forwarding / Port Triggering	2
5.6.4	WAN Setup	2
5.6.5	LAN Setup	2
5.6.6	QoS Setup	2
5.6.7	Dynamic DNS	2
5.6.8	Static Routes	2
5.6.9	Remote Management	2
5.6.10	UPnP	2

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exists 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.

2 Overview

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

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

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

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration

- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- WLAN with high-speed data transfer rates of up to 130 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control
 - Web-based management (WBM)
 - Command line interface (CLI)
 - TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)

- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Hardware Installation

3.1 Hardware Description

3.1.1 Front Panel

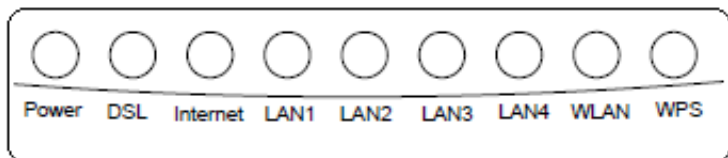


Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and the device operates normally.
		Blink	The software is upgrading.
		Off	The device is powered off.
	Red	On	The device is initiating.
		Blink	The software is upgrading.
DSL	Green	On	DSL link has established.
		Blink slowly	No DSL link is detected.
		Blink quickly	The DSL line is training.
		Off	Device is powered off.
Internet	Green	On	PPP/DHCP takes effect.
		Blink slowly	PPP/DHCP is negotiating.
		Blink quickly	Data is being transmitted.
	Red	On	The Internet authentication fails or the device is in the bridge mode.
LAN 1/2/3/4	Green	On	The Ethernet interface is connected.
		Blink	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet interface is disconnected.

Indicator	Color	Status	Description
WLAN	Green	On	WLAN is enabled.
		Blink	Data is being transmitted through the wireless interface.
		Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blink	Negotiation is in progress under Wi-Fi Protected Setup.
		Off	Wi-Fi Protected Setup is disabled.

3.1.2 Rear Panel

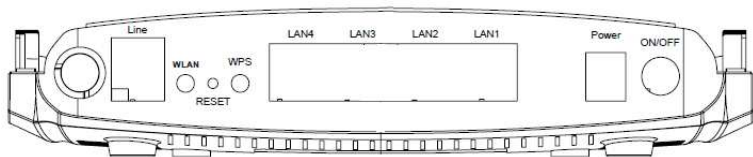


Figure 2 Rear panel

The following table describes the interfaces or the buttons on the rear panel.

Interface	Description
Line	RJ-11 port, for connecting the ADSL cable.
WLAN	WLAN switch, for enabling or disabling the WALN function.
RESET	Press the button for at least 1 second and then release it. System restores the factory default settings.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.
LAN 4~1	RJ-45 port, for connecting the router to a PC or another network device.
Power	Power interface, for connecting the power adapter.
ON/OFF	Power switch

 **Warning:**

Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 1 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

The power specification is 12V, 1A. If the power adapter does not match the specification, it may damage the device.

3.2 Hardware Installation

3.2.1 Choosing the Best Location for Wireless Operation

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

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting. Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business.

3.2.2 Connecting the Device

Please follow the steps below to connect the device.

- Step1** Connect the **Line** port of the DSL router with a telephone cable.
- Step2** Connect the **LAN** port of the DSL router to the network card of the PC via an Ethernet cable.
- Step3** Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** port of the DSL Router.

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

NETGEAR JDGN1000 User Manual

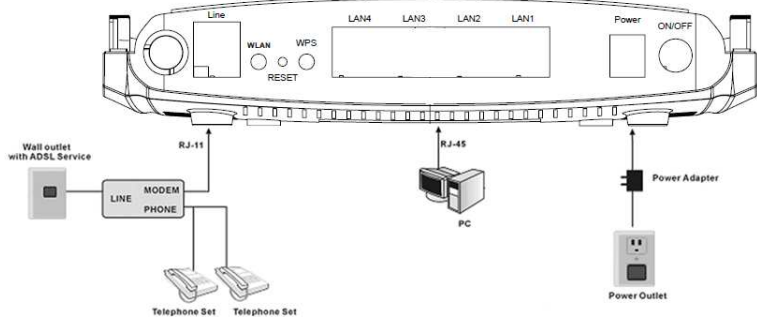


Figure 3 Connecting the DSL router

4 PC Network Configuration and Login

4.1 PC Network Configuration

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

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

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

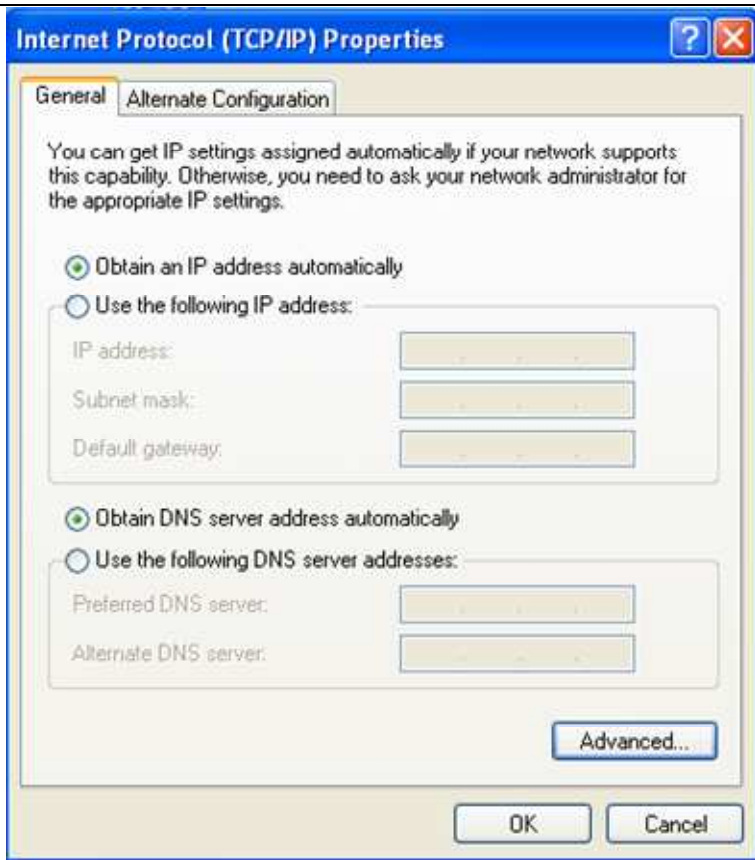


Figure 4 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

- Step1** Choose **Start > Control Panel > Network Connections**.
- Step2** Right-click the Ethernet connection icon and choose **Properties**.
- Step3** On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.
- Step4** The **Internet Protocol (TCP/IP) Properties** window appears.

- Step5** Select the **Obtain an IP address automatically** radio button.
- Step6** Select the **Obtain DNS server address automatically** radio button.
- Step7** Click **OK** to save the settings.

4.2 Logging In to the DSL Router

To log in to the DSL router, do as follows:

- Step1** Open a Web browser on your computer.
- Step2** Enter **http://192.168.1.1** (the default IP address of the DSL router) in the address bar. The login page appears.
- Step3** Enter the user name and the password. You need not enter the username and the 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.
- Step4** Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.



Figure 5 Login page

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

5 Web-Based Management

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.

5.1 Setup Wizard

Click **Setup Wizard**. The page shown in the following figure appears.

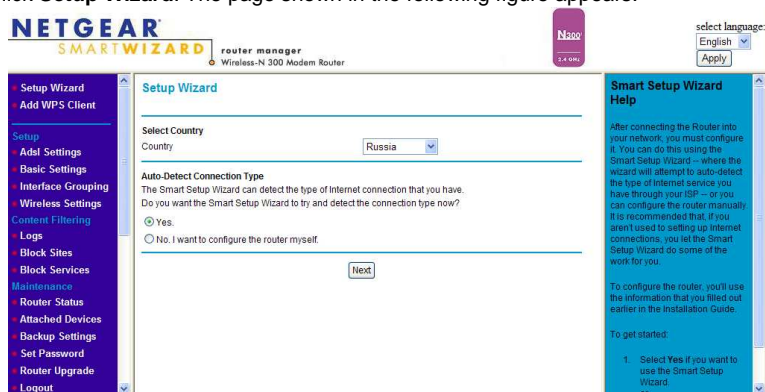


Figure 6 Setup Wizard page

Step1 Select the **country** where you are from the drop-down list and then select **Yes** if you want to use the Smart Setup Wizard.

Select **No. I want to configure the router myself** If you don't want to use the Smart Setup Wizard and want to configure the router manually

Step2 After PVC detection is selected, the following page appears if PVC detection fails.

No Internet Connection Detected

Please Check the Connections to the Internet WAN Port and Cable/DSL Modem.

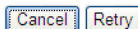


Figure 7 No Internet Connection Detected

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

For there is no ADSL synchronization, you can also refer to **Help** on the right to find out the causes in detail and then click **Retry**.

Step3 The following page appears when Internet connection detection is in process.

[Setup Wizard](#)

Detecting connection type on the Internet port



Please wait a moment..

Figure 8 Detection in process

Step4 The following page appears if no internet connection is detected.

[No Internet Connection Detected](#)

Please configure the router by myself.

Figure 9 No Internet Connection Detected

It means the PVC provided by your ISP is not among PVC automatic detection lists, and then click **Basic Setup** to configure manually.

Step5 If **Setup Wizard** detects that the internet service provided by your ISP is accessed through IPoA, the following page appears.

[Static \(Fixed\) IP Detected](#)

Figure 10 IPoA Detected

Click **Next** to configure IPoA connection. Here you can refer to the **Help** on the right to configure.

Static IP (Fixed) Addresses

Internet IP Address

IP Address

IP Subnet Mask

Domain Name Server (DNS) Address

Primary DNS

Secondary DNS

Figure 11 IPoA connection configuration

Step6 If Setup Wizard detects that the internet service provided by your ISP is accessed through PPPoE, the following page appears.

PPPoE Detected

Figure 12 PPPoE Detected

Click **Next** to configure your PPPoE connection. Here you can refer to **Help** on the right to configure.

PPPoE

Login

Password

Service Name(If Required)

Idle Timeout (In Minutes)

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Figure 13 PPPoE Configuration

Step7 Click **Apply** to save the settings. Then IPTV detecting dialog box appears.

IPTV Detecting

Do you want the Smart Setup Wizard to try and detect the IPTV connection type now?

Figure 14 IPTV detecting dialog box

- If your ISP provides IPTV service, you can click **Next** to start IPTV detection.
- If your ISP doesn't provide IPTV service, you can click **Skip** to complete the **Setup Wizard** configuration.

Step8 The following page shows that IPTV connection detection is in process.
Setup Wizard

Detecting IPTV connection on the Internet port-xxx

Please wait a moment..

Figure 15 IPTV Connection Detecting

Step9 If the detection fails, the following page appears.

No IPTV Connection Detected

Please configure the router by myself.

Figure 16 No IPTV Connection Detected

It indicates that the PVC provided by your ISP is not among the PVC automatic detection lists, and then you can click **Basic Setup** to configure manually.

Step10 If IPTV connection is successfully detected, the following page appears.

IPTV Connection Detected Successful

You can set up Interface Grouping with the IPTV Connection Detected.

Figure 17 IPTV Connection Detected Successful

It shows Setup Wizard has configured IPTV connection for you. Click **Setup** to enter **Interface Grouping** page, click **Cancel** to complete Setup Wizard configuration.

5.2 Add WPS Client

Click **Add WPS Client** and the page shown in the following figure appears.

Add WPS Client

New and easy way to connect to the Wireless Router via WiFi Protected setup (WPS)

A wireless client has to support WPS function in order to use this wizard to add the client to your WPS enabled Wireless Router.

Please check the user manual and giftbox of your wireless client to see whether it supports the WPS function.

If your wireless client does not support the WPS function, you have to configure your wireless client manually so it has the same SSID and wireless security settings as on this router.

Next

Figure 18 Add WPS Client

Click **Next** and the page shown in the following figure appears.

Add WPS Client

Enable WPS	Enabled ▾
Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)	
	<input type="radio"/> Push-Button <input checked="" type="radio"/> PIN <input type="button" value="Add Enrollee"/>
	<input type="text" value="0"/>
Set WPS AP Mode	Configured ▾
Setup AP (Configure all security settings with an external registrar)	
	<input type="radio"/> Push-Button <input checked="" type="radio"/> PIN <input type="button" value="Config AP"/>
Device PIN	<input type="text" value="18836486"/>

Figure 19 Add WPS Client

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 the push-button for WPS authentication, you must ensure that the network card support the function. if it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function

5.3 Setup

Choose **Setup** and the submenus of **Setup** are shown as below:

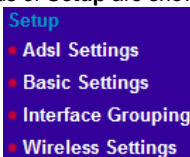


Figure 20 Submenus of Setup

5.3.1 Adsl Settings

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

[Adsl Settings](#)

DSL ATM Interface Configuration												
Interface	Vpl	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove	
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>	

Figure 21 DSL ATM interface configuration

In this page, you can add or remove the DSL ATM Interfaces. Click the **Add** button to display the following page.

ATM PVC Configuration

VPI: [0-255] VCI: [32-65535]

Select DSL Latency

 Path0 Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

 EoA PPPoA IPoA

Select Connection Mode

 Default Mode - Single service over one connection VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode:

 ▾

Service Category:

 ▾

Select IP QoS Scheduler Algorithm

 Strict Priority

Precedence of the default queue:

8 (lowest)

 Weighted Fair Queuing

Weight Value of the default queue: [1-63]

MPAAL Group Precedence:

 ▾

Figure 22 ATM interface configuration

In this page, you can set the VPI and VCI values, and select the DSL latency, link type (EoA is for PPPoE, IPoE, and Bridge.), connection mode, encapsulation mode, service category, and IP QoS scheduler algorithm.

- **VPI (Virtual Path Identifier):** The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

- **VCI (Virtual Channel Identifier):** The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Select DSL Latency:** You may select **Path0** and **Path1**.
- **Select DSL Link Type:** You may select **EoA** (it is for PPPoE, IPoE, and Bridge), **PPPoA**, or **IPoA**.
- **Select Connection Mode:** You may select the **Default Mode** or the **VLAN MUX Mode**.
- **Encapsulation Mode:** You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.
- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** in the drop-down list.
- **Select IP QoS Scheduler Algorithm:** You may select **Strict Priority** and **Weighted Fair Queuing**.

Note:

QoS cannot be set for CBR and Realtime VBR.

After finishing setting, click the **Apply/Save** button to make the settings take effect. See the following figure:

Adsl Settings

DSL ATM Interface Configuration												
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove	
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>	
atm1	0	36	Path1	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>	

Figure 23 Adding a DSL ATM interface

If you want to remove this Interface, please select the **Remove** check box that is corresponding to the selected interface and then click **Remove**.

5.3.2 Basic Settings

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

Basic Settings

Wide Area Network (WAN) Service Setup										
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

Figure 24 WAN service configuration

In this page, you are allowed to add, remove, or edit a WAN service.

Adding a PPPoE WAN Service

This section describes the steps for adding the PPPoE WAN service.

- Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.)

WAN Service Interface Configuration

atm1/(0_0_36) ▼

Figure 25 WAN service interface configuration (PPPoE)

- Step2** In this page, you can select a ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

WAN Service Configuration

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Figure 26 WAN service configuration (PPPoE)

Step3 In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to display the following page.

PPP Username and Password

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

- Config KeepAlive
- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)

- PPP IP extension
- Enable Firewall
- Use Static IPv4 Address

- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

- Enable IGMP Multicast Proxy

Back

Next

Figure 27 PPP username and password (PPPoE)

Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** 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 connection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it first.
- **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.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Bridge PPPoE Frames Between WAN and Local Ports:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.

Step5 After setting the parameters, click **Next** to display the following page.

Routing -- Default Gateway**Selected Default Gateway
Interfaces**

ppp0

**Available Routed WAN
Interfaces**

ppp1

[Back](#)[Next](#)

Figure 28 Routing-default gateway (PPPoE)

- Step6** In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

ppp0



Available WAN Interfaces

ppp1

[Back](#) [Next](#)

Figure 29 DNS server configuration(PPPoE)

Step7 In this page, you may obtain the DNS server addresses from the selected WAN interface. Click **Next**, and the following page appears.

WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

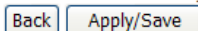


Figure 30 PPPoE summary

Step8 In this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** if necessary.

Basic Settings**Wide Area Network (WAN) Service Setup**

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	edit	Up
ppp1	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	edit	Up

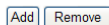


Figure 31 Completing the settings of PPPoE WAN service

Adding a MER (IPoE) WAN service

This section describes the steps for adding the MER WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM configuration for this WAN service.)

WAN Service Interface Configuration

atm2/(0_0_37) ▼

Back

Next

Figure 32 WAN service interface configuration (IPoE)

Step2 Select an ATM Interface, and then click **Next** to display the following page.

WAN Service Configuration

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description: ipoe_0_0_37

Back

Next

Figure 33 WAN service configuration (IPoE)

Step3 In this page, select the WAN service type to be IP over Ethernet. After finishing setting, click **Next** to display the following page.

WAN IP Settings

Obtain an IP address automatically

Option 55 Request List: (e.g.:1,3,6,12)

Option 58 Renewal Time: (hour)

Option 59 Rebinding Time: (hour)

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:

Figure 34 WAN IP settings (IPoE)

Step4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

Note:

If selecting **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.

If selecting **Use the following Static IP address**, please enter the WAN IP address, subnet mask and gateway IP address, primary DNS server and secondary DNS server.

Network Address Translation Settings

Enable NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast



Figure 35 Network address translation settings (IPoE)

Step5 In this page, you can set the network address translation settings, for example, enabling NAT, enabling firewall, and enabling IGMP multicast. After finishing setting, click **Next** and the following page appears.

Routing -- Default Gateway**Selected Default Gateway
Interfaces**

ppp0

**Available Routed WAN
Interfaces**

atm2
ppp1

[Back](#) [Next](#)

Figure 36 Routing-default gateway (IPoE)

Step6 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

ppp0



Available WAN Interfaces

atm2
ppp1

[Back](#) [Next](#)

Figure 37 DNS server configuration (IPoE)

- Step7** In this page, you may obtain the DNS server addresses from the selected WAN interface. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

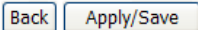


Figure 38 IPoE summary

Step8 In this page, it displays the information about the IPoE settings. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** if necessary.

Basic Settings

Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
atm2	ipoe_0_0_37	IPoE	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
ppp1	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

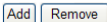


Figure 39 Completing the settings of IPoE WAN service

Adding a PPPoA WAN service

This section describes the steps for adding the PPPoA WAN service.

Step1 Choose **Setup > ADSL Settings >** to display the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for PPPoA mode. Click the **Add** in the **DSL ATM Interface Configuration** page to display the following page.

ATM PVC ConfigurationVPI: [0-255] VCI: [32-65535]

Select DSL Latency

 Path0 Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

 EoA PPPoA IPoAEncapsulation Mode: Service Category:

Select IP QoS Scheduler Algorithm

 Strict Priority

Precedence of the default queue: 8 (lowest)

 Weighted Fair QueuingWeight Value of the default queue: [1-63] MPAAL Group Precedence:

Figure 40 ATM PVC configuration (PPPoA)

- Step2** Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** to apply the settings, and the following page appears.

Adsl Settings

DSL ATM Interface Configuration											
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm1	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm2	0	37	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm3	0	38	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>

Figure 41 Adding a DSL ATM interface for PPPoA service

Step3 Choose **Setup > Basic Settings** and click **Add** to display the following page.

WAN Service Interface Configuration

atm3/(0_0_38) ▼

Figure 42 WAN service interface configuration (PPPoA)

Step4 Select the proper interface for the WAN service, and then click **Next** to display the following page.


WAN Service Configuration

Enter Service Description:

Figure 43 WAN service configuration (PPPoA)

Step5 Click **Next** to display the following page.

PPP Username and Password

PPP Username:
PPP Password:
Authentication Method: 

- Config KeepAlive
- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)

- Enable Firewall
- Use Static IPv4 Address

- Enable PPP Debug Mode

Multicast Proxy

- Enable IGMP Multicast Proxy

Figure 44 PPP username and password (PPPoA)

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** 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 PPPoA connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoA dialup. If this function is disabled, the modem performs PPPoA dial-up all the time. The PPPoA connection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoA mode to support IPTV, enable it.

Step6 In this page, you can enter the PPP username and PPP password provided by your ISP. Select the authentication method according to your requirement. After finishing setting, click **Next** to display the following page.

Routing -- Default Gateway**Selected Default Gateway
Interfaces**

ppp0

**Available Routed WAN
Interfaces**pppoa2
atm2
ppp1[Back](#) [Next](#)

Figure 45 Routing-default gateway (PPPoA)

- Step7** In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

ppp0



Available WAN Interfaces

pppoa2
atm2
ppp1

[Back](#) [Next](#)

Figure 46 DNS server configuration (PPPoA)

- Step8** In this page, you can obtain the DNS server addresses from the selected WAN interface. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	PPPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

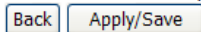


Figure 47 PPPoA summary

- Step9** In this page, it displays the information about the PPPoA settings. Click **Apply/Save** to apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** if necessary.

Basic Settings

Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	Vlanfluxid	Igmp	NAT	Firewall	Remove	Edit	Action
atm2	ipoe_0_0_37	IPoE	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
ppp1	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
ppp0a2	ppp0a_0_0_38	PPPoA	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

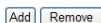


Figure 48 Completing the settings of PPPoA WAN service

Adding an IPoA WAN service

This section describes the steps for adding the IPoA WAN service.

- Step1** Choose **Setup > Adsl Settings** to display the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

ATM PVC Configuration

VPI: [0-255]
VCI: [32-65535]

Select DSL Latency

- Path0
 Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Select IP QoS Scheduler Algorithm

- Strict Priority
Precedence of the default queue: 8 (lowest)
- Weighted Fair Queuing
Weight Value of the default queue: [1-63]
MPAAL Group Precedence:

Figure 49 ATM PVC configuration (IPoA)

- Step2** Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to display the following page.

Adsl Settings

DSL ATM Interface Configuration											
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm1	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm2	0	37	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
atm3	0	38	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>
ipoa0	0	39	Path0	UBR	IPoA	DefaultMode	Enabled	SP	1	8	<input type="checkbox"/>

Figure 50 Adding a DSL ATM interface for IPoA service

Step3 Choose **Setup > Basic Settings** and click **Add** to display the following page.

WAN Service Interface Configuration

ipoa0/(0_0_39) ▼

Back

Next

Figure 51 WAN service interface configuration (IPoA)

Step4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.

WAN Service Configuration

Enter Service Description:

Figure 52 WAN service configuration (IPoA)

Step5 Click **Next** to display the following page.

WAN IP Settings

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

WAN IP Address:	<input type="text" value="0.0.0.0"/>
WAN Subnet Mask:	<input type="text" value="0.0.0.0"/>
Primary DNS server:	<input type="text" value="0.0.0.0"/>
Secondary DNS server:	<input type="text"/>

[Back](#)[Next](#)

Figure 53 WAN IP settings (IPoA)

Step6 In this page, enter the WAN IP address, the WAN subnet mask primary DNS server and secondary DNS server and then click **Next** to display the following page.

Network Address Translation Settings

Enable NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

[Back](#)[Next](#)

Figure 54 Network address translation settings (IPoA)

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

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

Step7 After finishing setting, click **Next** to display the following page.

Routing -- Default Gateway

Selected Default Gateway Interfaces

ppp0



Available Routed WAN Interfaces

ipoa0
atm2
ppp1
pppoa2

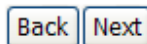


Figure 55 Routing-default gateway (IPoA)

Step8 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

ppp0



Available WAN Interfaces

ipoa0
atm2
ppp1
pppoa2

Back

Next

Figure 56 DNS server configuration (IPoA)

Step9 In this page, you can select DNS server interface from available WAN interfaces. Click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

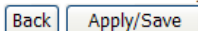


Figure 57 IPoA summary

Step10 In this page, it displays the information about the IPoA settings. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** if necessary.

Basic Settings

Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
atm2	ipoe_0_0_37	IPoE	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ipoa0	ipoa_0_0_39	IPoA	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
ppp1	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
pppoa2	pppoa_0_0_38	PPPoA	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

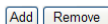


Figure 58 Completing the settings of IPoA WAN service

Adding a Bridge WAN service

This section describes the steps for adding the Bridge WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click **Add** to display the following page. (At first, you must add a proper ATM configuration for this WAN service.) Click **Add** to display the following page.

WAN Service Interface Configuration

atm4/(0_0_40) ▼

Back

Next

Figure 59 WAN service interface configuration (bridge)

Step2 Select the proper ATM Interface and then click **Next** to display the following page.

WAN Service Configuration

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description: br_0_0_40

Back

Next

Figure 60 WAN service configuration (bridge)

Step3 In this page, you can select the WAN service type, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

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

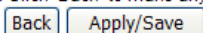


Figure 61 Bridge summary

Step4 In this page, it displays the information about the bridge settings. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking **Back** if necessary.

Basic Settings**Wide Area Network (WAN) Service Setup**

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
atm2	ipoe_0_0_37	IPoE	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ipoa0	ipoa_0_0_39	IPoA	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
atm4	br_0_0_40	Bridge	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
ppp1	pppoe_0_0_36	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>
pppoa2	pppoa_0_0_38	PPPoA	N/A	N/A	Disabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Up"/>

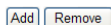


Figure 62 Completing the settings of bridge WAN service

5.3.3 Interface Grouping

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

Interface Grouping Settings

Interface Grouping -- A maximum 16 entries can be configured

Group Name	Remove	WAN Interface	LAN Interfaces
Default		ppp0	ENET1
		ppp1	ENET2
		atm2	ENET3
		atm4	ENET4
			wlan0
			wl0_Guest1
			wl0_Guest2
			wl0_Guest3

Figure 63 Interface grouping configuration

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 the 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.

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

Interface grouping Configuration

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:

Grouped Interfaces



Available Interfaces

atm2

atm4

ppp0

ppp1

ENET1

ENET2

ENET3

ENET4

wlan0

wl0_Guest1

Apply/Save

Figure 64 Adding a new interface group

In this page, please follow the configuration steps on the right of the screen to configure the parameters of the interface grouping.

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

5.3.4 Wireless Settings

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

Wireless Settings

Select the wireless network to configure

	Profile	SSID	Security	Enable	Broadcast SSID
<input checked="" type="radio"/>	Primary	wlan	WPA2-PSK	Yes	Yes
<input type="radio"/>	2	Broadcom2	None	No	Yes
<input type="radio"/>	3	Broadcom3	None	No	Yes
<input type="radio"/>	4	Broadcom4	None	No	Yes

Wireless Network

Name (SSID):

Region:

Channel:

802.11n Rate:

Enable this wireless Network

Enable SSID Broadcast

Wireless Isolation

Security Options

- None
- WEP
- WPA-PSK [TKIP]
- WPA2-PSK [AES]
- WPA-PSK [TKIP] + WPA2-PSK [AES]

WPA/WAPI passphrase: (8-63 characters or 64 hex digits)

Apply/Save

Figure 65 Wireless Settings

- **Name(SSID):** For the security reason, you should change the default SSID to a unique name.
- **Region:** Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our web site for more information on which channels to use.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

- **Channel:** You can select auto or 1~11 from the drop-down list
If you select **WEP** as Security Options, the following page appears.

Security Options

- None
 WEP
 WPA-PSK [TKIP]
 WPA2-PSK [AES]
 WPA-PSK [TKIP] + WPA2-PSK [AES]

Authentication Type:	Automatic ▾
Encryption Strength:	64-bit ▾
Current Network Key:	1 ▾
Network Key 1:	<input type="text" value="0987654321"/>
Network Key 2:	<input type="text" value="0987654321"/>
Network Key 3:	<input type="text" value="0987654321"/>
Network Key 4:	<input type="text" value="0987654321"/>

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 66 Wep Option

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys.

The router offers 64 or 128 bit encryption with four keys available.

Select **Encryption Strength** from the drop-down menu. (128 bit is stronger than 64 bit)

Enter the key into the Network Key field 1~4. (Key length is outlined at the bottom of the window.)

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

If you select **WPA-PSK**, **WPA2-PSK**, **WPA-PSK + WPA2-PSK** as security options, the following page appears.

Security Options

- None
 WEP
 WPA-PSK [TKIP]
 WPA2-PSK [AES]
 WPA-PSK [TKIP] + WPA2-PSK [AES]

WPA/WAPI passphrase:

(8-63 characters or 64 hex digits)

Figure 67 WPA-PSK Option

- WPA-PSK [TKIP] - Wi-Fi Protected Access with Pre-Shared Key, use WPA-PSK standard encryption with TKIP encryption type
- WPA2-PSK [AES] - Wi-Fi Protected Access version 2 with Pre-Shared Key, use WPA2-PSK standard encryption with the AES encryption type
- WPA-PSK [TKIP] + WPA2-PSK [AES] - Allow clients using either WPA-PSK [TKIP] or WPA2-PSK [AES].

Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters or 64 hex digits in length.

5.4 Content Filtering

Choose **Content Filtering** and the submenus of **Content Filtering** are shown as below:

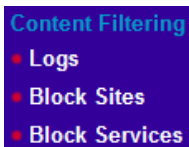


Figure 68 Submenus of content filtering

5.4.1 Logs

Choose **Content Filtering > Log** to display the following page.

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.



Figure 69 System log

In this page, you are allowed to view the system log and configure the system log.

- **View System Log**

Click the **View System Log** button to display the following page.

System Log

Date/Time	Facility	Severity	Message
-----------	----------	----------	---------

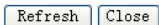


Figure 70 Viewing the system log

In this page, you can view the system log.

Click the **Refresh** button to refresh the system log. Click the **Close** button to exit.

- **Configuring the System Log**

Click the **Configure System Log** button to display the following page.

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 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level: ▾
Display Level: ▾
Mode: ▾
Local
Remote
Both

Apply/Save

Figure 71 Configuring the system log

In this page, you can set 3 types of system log modes, including **Local**, **Remote**, and **Both**.

- **Local:** When selecting **Local**, the events are recorded in the local memory.
- **Remote:** When selecting **Remote**, the events are sent to the specified IP address and UDP port of the remote system log server.
- **Both:** When selecting **Both**, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

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

Note:

*If you want to log all the events, you need to select the **Debugging** log level*

5.4.2 Block sites

Choose **Content Filtering > Block Sites** to display the following page.

Block Sites

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
---------	------	--------

Figure 72 URL filter setup

This page is used to prevent the LAN users from accessing some Websites in the WAN.

In this page, you may select the **Exclude** URL list type or the **Include** URL list type. If you select the **Exclude** URL list type, it means that the URLs in the list are not accessible. If you select the **Include** URL list type, you are allowed to access the the URLs in the list.

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

Parental Control -- URL Filter Add

Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:
Port Number: (Default 80 will be applied if leave blank.)

Figure 73 Adding a URL filter

In this page, enter the URL address and its corresponding port number. For example, enter the URL address **http://www.google.com** and the port number **80**, and then click the **Apply/Save** button. See the following figure:

Block Sites

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
http://www.google.com	80	<input type="checkbox"/>

Figure 74 Completing a URL filter

5.4.3 Block Services

When the outgoing IP filtering settings is enabled on the DSL router, the security functions for the local network are enabled at the same time.

Choose **Content Filtering > Block Services** and the following page appears.

Block Services

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	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Figure 75 Outgoing IP filtering setup

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

In this page, you can add or remove the outgoing IP filtering rules.

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

Block Services -- Add

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 'Apply/Save' to save and activate the filter.

Filter Name:	<input type="text"/>
IP Version:	<input type="text" value="IPv4"/>
Protocol:	<input type="text"/>
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address[/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>

Apply/Save

Figure 76 Adding an IP outgoing filtering rule

In this page, you can create a filter rule to identify the outgoing IP traffic by specifying a new filter name and at least one condition.

- **Filter Name:** Set the filter name.
- **IP Version:** Select the proper IP version in the drop-down list.
- **Protocol:** Select a protocol that needs to be filtered.
- **Source IP address [/prefix length]:** Set the range of local IP address.
- **Source Port (port or port: port):** Set the local port.
- **Destination IP address [/prefix length]:** Set the range of IP address of the exterior network.
- **Destination Port (port or port: port):** Set the port of the exterior network.

After finishing setting, click **Apply/Save** to save and activate the filtering rule.

5.5 Maintenance

Choose **Maintenance** and the submenus of **Maintenance** are shown as below:

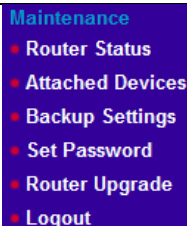


Figure 77 Submenus of maintenance

5.5.1 Router Status

Choose **Maintenance > Router Status**, and the following page appears.

Router Status

Hardware Version	tmp_hardware1.0
Firmware Version	V2.0.00.01_RU

Internet Port

Interface Name
IP Address
Default Gateway
DNS Servers

LAN Port

IP Address	192.168.1.1
DHCP	ON
IP Subnet Mask	255.255.255.0

Wireless Port

Name (SSID)	wlan
Region	US
Channel	1
Mode	b & g & n
Wme	ON
Wmf	OFF

Show Statistics

Figure 78 Router Status

In this page, you can check the current settings and statistics for your router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.

Interface	Received					Transmitted				
	Bytes	Pkts	Errs	Drops		Bytes	Pkts	Errs	Drops	
eth0	0	0	0	0	16005	228	0	0	0	
eth1	0	0	0	0	16005	228	0	0	0	
eth2	0	0	0	0	16005	228	0	0	0	
eth3	136886	1259	0	0	1613925	1771	0	0	0	
wlan	0	0	19	0	0	0	0	0	0	

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
slm2	ipoe_0_0_37	0	0	0	0	0	0	0	0
ipoa0	ipoa_0_0_39	0	0	0	0	0	0	0	0
alm4	br_0_0_40	0	0	0	0	0	0	0	0
ppp0	pppoe_0_0_35	0	0	0	0	0	0	0	0
ppp1	pppoe_0_0_36	0	0	0	0	0	0	0	0
pppa2	pppoa_0_0_38	0	0	0	0	0	0	0	0

Figure 79 statistical information

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

5.5.2 Attached Devices

Choose **Maintenance > Attached Devices**, and the following page appears.

Attached Devices

IP address	Flags	HW Address	Device
192.168.1.26	Complete	00:22:b0:68:de:69	br0

Figure 80 Attached Devices Information

This page shows the IP Address, Device Name and MAC (Media Access Control) Address for each computer attached to the router.

5.5.3 Backup Settings

Choose **Maintenance > Backup Settings**, and the following page appears.

Backup Settings

Save a Copy of Current Settings

Backup

Restore Saved Settings from a File

Browse

Restore

Revert to Factory Default Settings

Erase

Figure 81 Backup Settings

This page allows you to backup, restore and erase the router's current settings.

- **Backup:** Specify the path to back up the current configuration in a configuration file on your computer. You can rename the configuration file.
- **Restore:** Click **Browse**, locate and select the previously saved backup file, then Click **Restore** to restore settings from a backup file.
- **Erase:** Click **Erase** to erase the current settings and reset the router to the original factory default settings.



Caution:

Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.

5.5.4 Set Password

Choose **Maintenance > Set Password**, and the following page appears.

Set Password

User Name:	<input type="text"/>
New Username:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Figure 82 Modifying the password

In this page, you can change the password you use to access the *Settings* pages.

5.5.5 Router Upgrade

Choose **Management > Router Upgrade** and the following page appears.

Update Software

Software File Name:	<input type="text"/>	<input type="button" value="Browse..."/>
---------------------	----------------------	--

Figure 83 Updating software

If you want to upload the software, click the **Browse...** button to choose the new software, and then click the **Update Software** button.

Warning:

When uploading software to the wireless modem router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

Make sure that the new software for updating is correct, and do not use other software to update the router.

5.5.6 Logout

Choose **Management > Logout** and the following page appears.

Thank you for using the NETGEAR Web-based Router Configuration Utility.

GoodBye

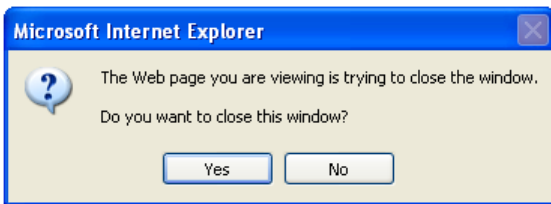


Figure 84 Logout page

Click **Yes** to log out of the configuration page.

5.6 Advanced

Choose **Advanced** and the submenus of **Advanced** are shown as below:



Figure 85 Submenus of advanced

5.6.1 Wireless Settings

Choose **Advanced > Wireless Settings** and the following page appears.

Wireless -- Advanced

Band:	2.4GHz	
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in 2.4G Band and 40MHz in 5G Band	Current Bandwidth:
Control Sideband:	Lower	Current Control Sideband:
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existence:	Disable	
RX Chain Power Save:	Enable	
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
Radio Power Save:	Disable	
Radio Power Save Quiet Time:	10	
Radio Power Save PPS:	10	
Radio Power Save On Time:	50	
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):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Wireless MAC Filter

Setup MAC Filter

Apply/Save

Figure 86 Wireless advanced settings

This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.

Note:

The advanced wireless setting is only for the advanced user. For the common user, do not change any settings in this page.

Click **Setup MAC Filter** to display the following page.

Wireless -- MAC Filter

Select SSID: wlan

MAC Restrict Mode: Disabled Allow Deny

Figure 87 MAC filter configuration

This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

In this page, you can add or remove the MAC filters.

The MAC restrict modes include **Disabled**, **Allow**, and **Deny**.

- **Disabled:** Disable the wireless MAC address filtering function.
- **Allow:** Allow the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.
- **Deny:** Reject the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

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

Wireless -- MAC Filter

Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.

MAC Address: Mac address in hexadecimal format: xx:xx:xx:xx:xx:xx, x range of 0 ~ F

Figure 88 Adding a MAC filter

In this page, enter the MAC address of the wireless client, and then click the **Apply/Save** button to add the MAC address to the MAC address list.

5.6.2 Wireless Repeating Function

Choose **Advanced > Wireless Repeating Function** and the following page appears.
[Wireless Repeating Function](#)

AP Mode: ▼

Bridge Restrict: ▼

Remote Bridges MAC Address:

Figure 89 Wireless Repeating Function

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

- **AP mode:** you may select Access Point or Wireless Bridge.
- **Bridge Restrict:** Enable or disable the bridge restrict function.
- **Remote Bridges MAC Address:** Enter the remote bridge MAC address.

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

5.6.3 Port Forwarding / Port Triggering

Choose **Advanced > Port Forwarding / Port Triggering** and the following page appears.

[Port Forwarding / Port Triggering](#)

Port Forwarding

Port Triggering

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

Figure 90 Port Forwarding/Port Triggering

In this page, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CUseeMe).

Port Forwarding

Select **Port Forwarding**, click **add** and the following page appears.

Ports - Custom Services

Select the service name, and enter the server IP address and click "Apply/Save" 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:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

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

Apply/Save

Figure 91 Port Forwarding Setup

Select a service for a preset application or enter the name in the **Custom Service** field.

Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.

The port table displays the ports that you want to open on the device. The **Protocol** indicates the type of protocol used by each port.

Click **Save/Apply** to save the settings. The page as shown in the following figure appears. A virtual server is added.

Port Forwarding / Port Triggering

Port Forwarding
 Port Triggering

Server Name	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
AUTH	TCP	113	113	192.168.1.4	<input type="checkbox"/>

Figure 92 Adding a virtual server

Port Triggering

Select **Port Triggering** and the following page appears.

Port Forwarding / Port Triggering

Port Forwarding
 Port Triggering

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

Figure 93 Port Triggering setup

In this page, you may add or delete an entry of port triggering.

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

Port Triggering - Services

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:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>

Figure 94 Adding an entry of port triggering

- **Use interface:** Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.
- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

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

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.

5.6.4 WAN Setup

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

WAN Setup

Default DMZ Server . . .

Respond to Ping on Internet Port

Figure 95 WAN setup

In this page, you can set up a Default DMZ Server and allow the router to respond to a 'ping' from the internet. Both of these options have security issues, so use them carefully.

Default DMZ Server

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you're willing to risk open access. If you do not assign a Default DMZ Server, the router discards any incoming service requests which are undefined.

To assign a computer or server to be a DMZ server:

1. Click the *Default DMZ Server* check box.
2. Type the IP address for that server.
3. Click **Apply**.

Note:

The router must enable the NAT. Otherwise, DMZ do not enable.

Respond to Ping on Internet Port

If you want the Router to respond to a 'Ping' from the Internet, click this check box. This can be used as a diagnostic tool. Again, like the DMZ server, this can be a security problem. You shouldn't check this box unless you have a specific reason to do so.

5.6.5 LAN Setup

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

LAN IP Setup

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

LAN TCP/IP Setup

IP Address:
 Subnet Mask:

Use Router As DHCP Server

Disable DHCP Server
 Enable DHCP Server
 Start IP Address:
 End IP Address:
 Leased Time (hour):

Address Reservation

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

MAC Address	IP Address	Remove

Figure 96 LAN setup

In this page, you can configure an IP address for the DSL router, enable or disable the DHCP server, and set the binding between a MAC address and an IP address.

Configuring the Private IP Address for the DSL Router

IP Address:
 Subnet Mask:

Figure 97 Configuring the IP address of the DSL router

In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1.

Configuring the DHCP Server

Disable DHCP Server
 Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Figure 98 Setting the DHCP server

If you enable the DHCP server, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.

Configuring the DHCP Static IP Lease List

The lease list of static IP address can reserve the static IP addresses for the hosts with the specific MAC addresses. When a host whose MAC address is in the lease list of static IP address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the host.

MAC Address	IP Address	Remove

Figure 99 DHCP static IP lease list

Click the **Add Entries** button in the **LAN Setup** page to display the **following** page.

Address Reservation

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

MAC Address:

IP Address:

Figure 100 Adding an entry of DHCP static IP lease list

In this page, enter the MAC address of the LAN host and the static IP address that is reserved for the host, and then click the **Apply/Save** button to apply the settings.

5.6.6 QoS Setup

Enabling QoS

Choose **Advanced > Queue Management Configuration** 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 'Apply/Save' 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

Apply/Save

Figure 101 QoS queue management configuration
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 'Apply/Save' 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

Apply/Save

Figure 102 Enabling QoS

In this page, enable the QoS function and select the default DSCP mark.
After finishing setting, click **Apply/Save** to save and apply the settings.

Note:

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

Queue Config

Choose **Advanced > Queue Config**, and the following page appears.

Queue Management Configuration **Queue Config** Classification Setup

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 4 queues can be configured.

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

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wi0	SP	1		Path1	High	Enabled	
WMM Voice Priority	2	wi0	SP	2		Path1	High	Enabled	
WMM Video Priority	3	wi0	SP	3		Path1	High	Enabled	
WMM Video Priority	4	wi0	SP	4		Path1	High	Enabled	
WMM Best Effort	5	wi0	SP	5		Path1	High	Enabled	
WMM Background	6	wi0	SP	6		Path1	High	Enabled	
WMM Background	7	wi0	SP	7		Path1	High	Enabled	
WMM Best Effort	8	wi0	SP	8		Path1	High	Enabled	
Default Queue	33	atm0	SP	8		Paht0	High	<input type="checkbox"/>	
Default Queue	38	atm1	SP	8		Paht0	High	<input type="checkbox"/>	
Default Queue	39	atm2	SP	8		Paht0	High	<input type="checkbox"/>	
Default Queue	41	atm3	SP	8		Paht0	High	<input type="checkbox"/>	
Default Queue	42	lpoa0	SP	8		Paht0	High	<input type="checkbox"/>	
Default Queue	43	atm4	SP	8		Paht0	High	<input type="checkbox"/>	

Add Enable Remove

Figure 103 QoS queue setup

In this page, you can enable, add or remove a QoS rule.

Note:

The lower integer value for precedence indicates the higher priority.

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

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others

Click 'Apply/Save' to save and activate the queue.

Name:

Enable: ▾

Interface: ▾

Figure 104 Adding a QoS queue

- **Name:** Enter the name of QoS queue.
- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

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

QoS Classification

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

[Queue Management Configuration](#) | [Queue Config](#) | [Classification Setup](#)

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/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TOS Check	802.1P Check	Queue Key	DSCP Mark	TOS Mark	802.1P Mark	VlanID Tag	Frame size	Enable	Remove	

Figure 105 QoS classification setup

In this page, you can enable, add or remove a QoS classification rule.

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

[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 'Apply/Save' to save and activate the rule.

Traffic Class Name:	<input type="text"/>
Rule Order:	Last ▾
Rule Status:	Enable ▾
Specify Classification Criteria	
A blank criterion indicates it is not used for classification.	
Class Interface:	LAN ▾
Ether Type:	<input type="text"/> ▾
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>
Frame size rage for Bridged interface(FROM:TO):	<input type="text"/>
Specify Classification Results	
Must select a classification queue. A blank mark or tag value means no change.	
Assign Classification Queue:	<input type="text"/> ▾
Mark Differentiated Service Code Point (DSCP): ▾	<input type="text"/> ▾
Mark 802.1p priority:	<input type="text"/> ▾
Tag VLAN ID [0-4094]:	<input type="text"/>

Apply/Save

Figure 106 Adding a QoS classification rule

In this page, enter the traffic name, select the rule order and the rule status, and specify the classification criteria and the classification results.

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

5.6.7 Dynamic DNS

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

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 Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
----------	----------	---------	-----------	--------

Figure 107 Dynamic DNS

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

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

Dynamic DNS -- Add

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

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text"/>
Interface	<input type="text" value="ipoe_0_0_37/atm2"/>
DynDNS Settings	
Username	<input type="text"/>
Password	<input type="text"/>

Figure 108 Adding a Dynamic DNS address

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

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

5.6.8 Static Routes

Choose **Advanced > Static Routes** and the following page appears.

Static Routes

Static Routes (A maximum 32 entries can be configured).

IP Version	DstIP/ PrefixLength	Gateway	Interface	Metric	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

Figure 109 Static route setup

In this page, you can add or remove a static routing rule of IPV4.

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

Static Routes -- Add

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

IP Version:	<input type="button" value="IPv4"/>
Destination IP address/prefix length:	<input type="text"/>
Interface:	<input type="button" value="v"/>
Gateway IP Address:	<input type="text"/>
(optional: metric number should be greater than or equal to zero)	
Metric:	<input type="text"/>
<input type="button" value="Apply/Save"/>	

Figure 110 Adding a static routing rule

- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

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

5.6.9 Remote Management

Choose **Advanced > Remote Management** and the following page appears.

Remote Management

Services	LAN	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="80"/>
TELNET	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="23"/>
FTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="21"/>
TFTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="69"/>
ICMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="0"/>

Apply/Save

Figure 111 Remote management

In this page, you can enable or disable the different types of services. After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.6.10 UPnP

Choose **Advanced > UPnP** and the following page appears.

UPnP

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

Apply/Save

Figure 112 UPnP

In this page, you can enable or disable the UPnP function. After finishing setting, click **Apply/Save** to save and apply the settings.