W3400

Four-port ADSL 2+ Wireless

Router

User manual

Contents

Introduction

The 4 ports wireless Modem is a router with wireless local area network (WLAN) function. It is a high integrated residential broadband access device, which provides one ADSL2+ RJ11 interface, four built-in Ethernet interfaces, and one wireless access point. The 4 ports wireless Modem is fully compliant with ADSL/2/2+ standards. The Ethernet interface complies with IEEE802.3/802.3u standards, and the WLAN interface complies with IEEE802.11b/g standards. This device provides high performance access to Internet, downstream up to 24Mbps and upstream up to 1Mbps. Computers on the LAN side can share the Internet access through the Ethernet interface or wireless access point. These local computers can communicate and share resources and files with each other when the Gaw9.5U6-4 is connected to the Internet with DSL line. This device can provide high access performance applications for individual users, SOHOs, and small enterprises.

- Support up to 8 permanent virtual circuits (PVCs)
- Provide one RJ11 interface and four built-in RJ45 interfaces
- IGMP Snooping and IGMP Proxy
- General IP: NAT, PAT, DHCP server, DHCP relay, and DNS relay
- Routing: Static routing, RIP V1 and V2

- Security: NAT, IP filtering, password authentication, and denial of service (DoS)
- Compatible with IEEE 802.11b and IEEE 802.11g

- Application
- Broadband Internet access sharing
- Higher data rate broadband sharing
- Audio, video streaming, and transfer
- PC file and application sharing
- Network and online gaming

Parameters and Specifications

Parameter	Specifications
System Spec	
Chipset	RTL8671BH 2lays
SDRAM	8 M
Serial Flash	2 M
Feature and Technical Spec	
Protocol Feature	RFC 1483 Bridge IEEE 802.1D transparent bridging Bridge Filtering RFC 1483 Router RIP 1 & 2 supported DHCP (RFC1541) Server, Relay Network Address Translation (NAT)/ Network Address Port Translation (NAPT) DNS relay IGMP v1 and v2
ADSL Feature	Support ANSI T1.413 Issue2 Support ITU G.992.1 (G.dmt) Annex A Support ITU G.992.2 (G.lite) Annex A Support ITU G.992.3 ADSL2 (G.dmt.bis) Annexs A, L, M Support ITU G.992.4 ADSL2 (G.lite.bis) Support ITU G.992.5 ADSL2 plus

Ethernet Feature	Fully compliant with IEEE802.3/802.3u auto-negotiation function Support 10 base-T and 100 base-TX Support half duplex and full duplex Support back pressure flow control for half duplex, IEEE02.3x flow control for full duplex Support MDI/MDIX auto cross
Wireless Feature	Standard: IEEE802.11b and IEEE 802.11g Frequency Band: 2.4 GHz (ISM frequency bands) Data Rate: 802.11b compliant: 11, 5.5, 2, 1 Mbps (DSSS/CCK); 802.11g compliant: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (OFDM) Operating Channel: 802.11b/g 11: (Ch. 1-11) – N. America (default) Frequency Range: 802.11 b/g 2.412~2.462 GHz – N. America (default) Transmit Output Power: 802.11b: 16.5+/- dBm @Normal Temp Range 802.11g: 14.5+/- dBm @ Normal Temp Range Transmission Distance: 300 meters outdoors, 100 meters indoors coverage area (varying depending on the actual environment.) Security: 64/128-bit WEP, AES, TKIP, WPA, WPA2, 802.1x Antenna Type: single external antenna,1.8dbi

1.1 LEDs and Interfaces

Front Panel

The page shown in the following figure shows the front panel of the device.

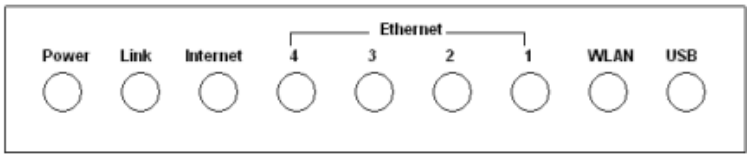


Figure 1 Front panel

The following table describes the LEDs of the device.

LEDs	Color	Status	Description
Power	Green	On	The device is powered on.
		Off	The device is powered off.
	Red	On	The device is initializing.
		Blinks	The firmware is upgrading.
Link	Green	On	The device is linked successfully to a DSLAM.
		Blinks	The device is initializing the DSL line.
		Off	The DSL link is down.
Internet	Green	On	The device has a PPP (PPPoA or PPPoE) connection.
		Blinks	The device is receiving or sending data on WAN.
		Off	The device does not have a PPP (PPPoA or PPPoE) connection.
	Red	On	PPPoA or PPPoE is failed.
Ethernet 1/2/3/4	Green	On	The device has successful Ethernet connections.
		Blinks	The device is receiving or sending data on LAN.
		Off	The LAN is not connected.
WLAN	Green	On	The wireless is actived.
		Blinks	The device is receiving or sending data on WLAN.

LEDs	Color	Status	Description
		Off	The wireless is not actived.

Rear Panel

The page shown in the following figure shows the rear panel of the device.

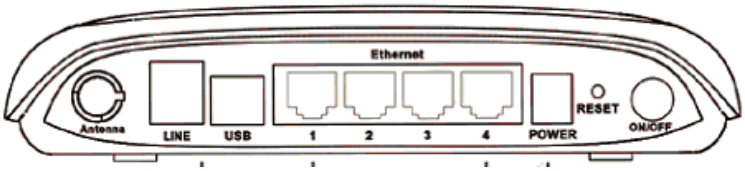


Figure 2 Rear panel

The following table describes the interfaces of the device.

Interface	F unction
ON/OFF	Power on or off.
RESET	Resets to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button over 5 seconds and then release.
POWER	Interface that connects to the power adapter. 12 V DC/ 1 A
Ethernet 1/2/3/4	Ethernet RJ-45 interfaces that connect to the Ethernet interface of the computer or Ethernet devices.
USB	Connect to the USB device interface of the PC for USB Ethernet connection.
LINE	RJ-11 interface that connects to the telephone set through the telephone cable.
Antenna	The button of the antenna.

1.2 System Requirements

Recommended system requirements are as follows:

- A 10/100 base-T Ethernet card is installed on your PC
- A hub or Switch. (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows 98SE, Windows 2000, Windows ME, Windows XP or Windows Vista
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or firefox 1.5 or higher.

1.3 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- Zero installation PPP bridge mode (ZIPB)
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade: Web, TFTP and FTP
- Reset to the factory defaults
- DNS relay
- Virtual server
- DMZ
- IP Address Mapping
- Two-level passwords and user names and six accounts (at most)

- Web user interface
- Telnet CLI
- System status display
- PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management (telnet and HTTP)
- Backup and restoration of configuration file
- Ethernet supports crossover detection, auto-correction and polarity correction.
- UPnP

2 Hardware Installation

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

The splitter has three ports.

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

Step 2 Connect the Ethernet port of the device to the network card of the PC through an Ethernet line (MDI/MDIX).

***Note**: Use twisted-pair cables to connect the Hub or Switch.*

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

Figure 3 displays the application diagram for the connection of the device, PC, splitter, and the telephone sets when no telephone set is placed before the splitter.

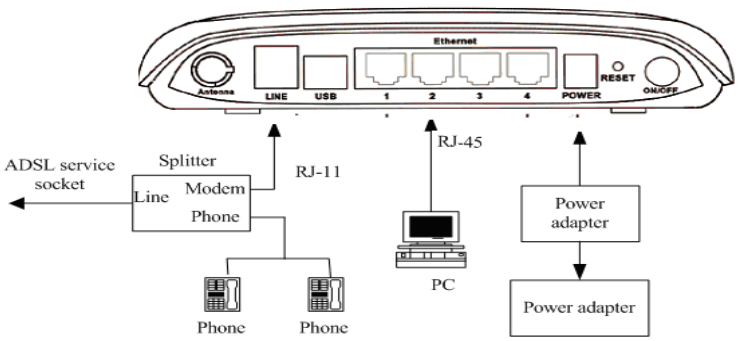


Figure 3 Connection diagram (without connecting telephone sets before the splitter)

Figure 4 displays the application diagram for the connection of the device, PC, splitter and the telephone sets when a telephone set is placed before the splitter.

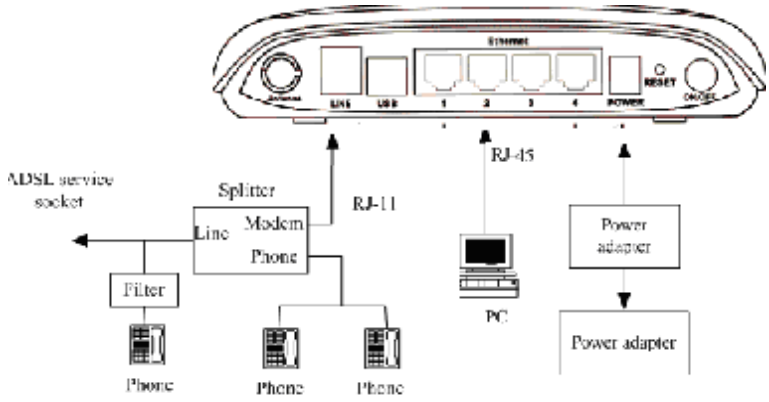


Figure 4 Connection diagram (connecting a telephone set before the splitter)

Connection 1 is recommended.

Note: *When connection of Figure 4 is used, the filter must be installed close to the telephone lines. Do not use the splitter instead of the filter.*

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

3 About the Web Configurator

This charpter describes how to configure the device by using the Web-based configuration utility.

3.1 Access the Router

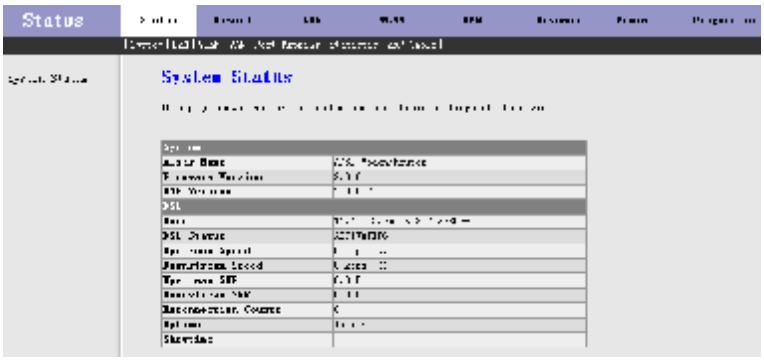
The following is the detailed description of accessing the device for the first time.

Step 1 Open the Internet Explore (IE) browser and enter **http://192.168.1.1**.

Step 2 In the **LOGIN** page shown in the following figure. Enter the user name and password.

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

If you log in as the super user successfully, the page shown in the following figure appears. You can check, configure and modify all the settings.



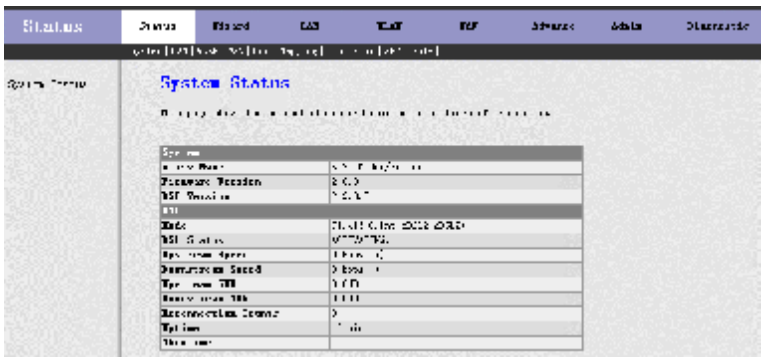
If you enter as a common user, you can check the status of the router, but can not change the most of the settings.

3.2 Status

In the navigation bar, choose **Status**. The **Status** page that is displayed contains: **System**, **LAN**, **WLAN**, **WAN, Port Mapping, Statistic** and **ARP Table**.

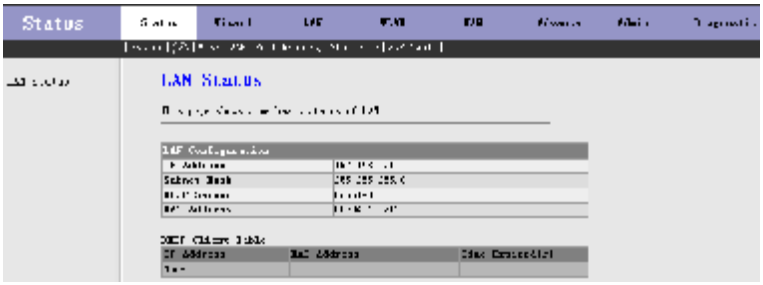
3.2.1 System

Choose **Status** > **System**. The page that is displayed shows the current status and some basic settings of the device.



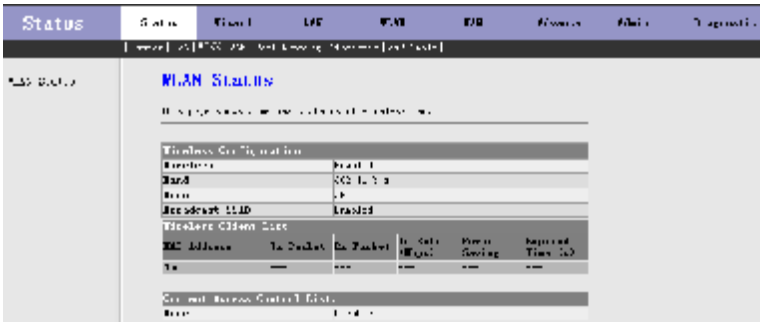
3.2.2 LAN

Choose **Status** > **LAN**. The page that is displayed shows some basic LAN settings of the device. In the **LAN** page, you can view the LAN IP address, subnet mask, DHCP server status, MAC address and DHCP client table. If you want to configure the LAN network, refer to the chapter 3.4.1 LAN Settings.



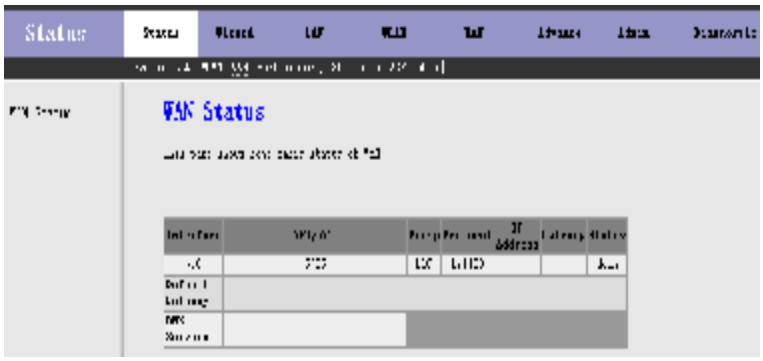
3.2.3 WLAN

Choose **Status** > **WLAN**. The page that is displayed shows some basic wirless LAN settings of the device.



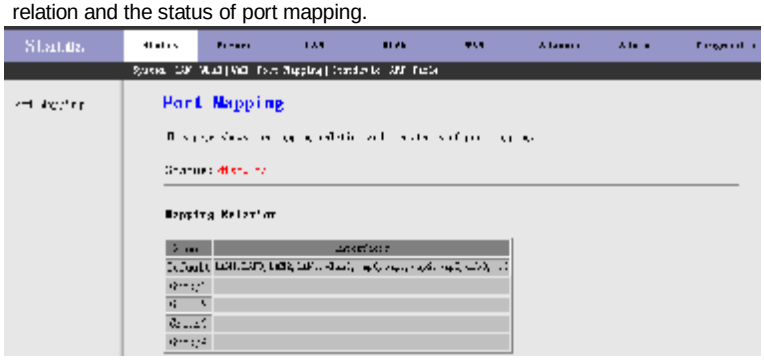
3.2.4 WAN

Choose **Status** > **WAN**. The page that is displayed shows some basic WAN settings of the device. In the **WAN** page, you can view basic status of WAN, default gateway, DNS server. If you want to configure the WAN network, refer to the chapter3.6.1 WAN Interface.



3.2.5 Port Mapping

Choose **Status** > **Port Mapping**. The page that is displayed shows the mapping relation and the status of port mapping.

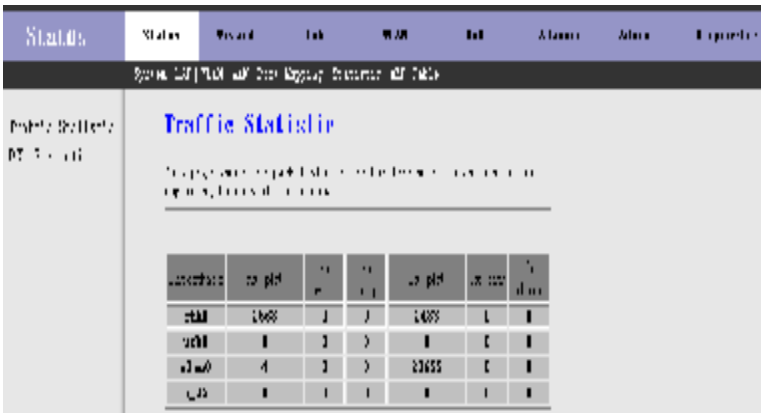


3.2.6 Statistic

Choose **Status** > **Statistic.** The **Statistic** page that is displayed contains **Traffic Statistic** and **DSL Statistic**.

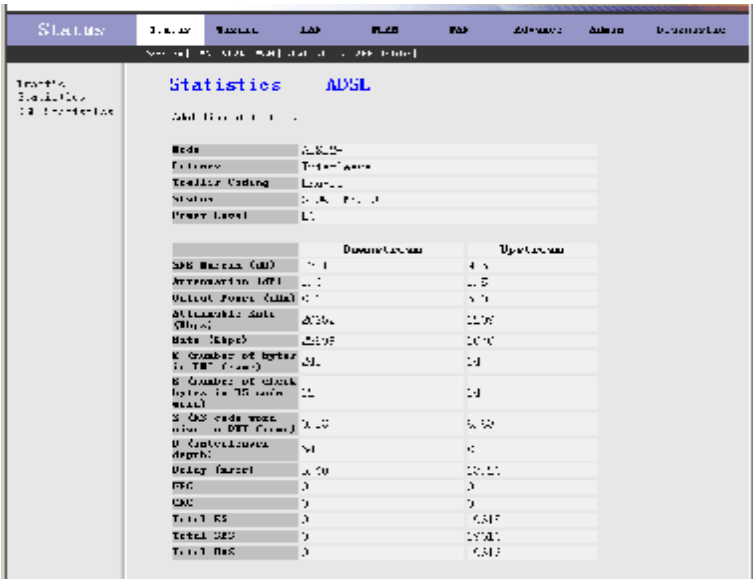
3.2.6.1 Traffic Statistic

Choose **Traffic Statistic.** In the **Traffic Statistic** page, you can view the statistics of each network port.



3.2.6.2 DSL Statistic

Choose DSL Statistic. In the Statistic-ADSL page, you can view the ADSL line statistics, downstream rate, upstream rate and other information.



3.2.7 ARP Table

Choose Status > ARP Table. In the ARP Table page, you can view the table which shows a list of learned MAC addresses.

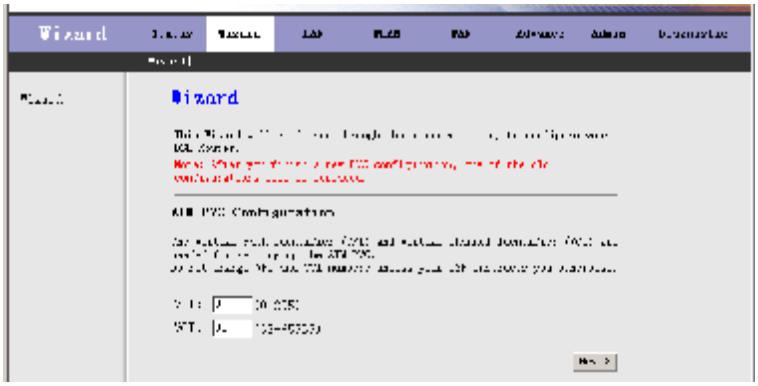
3.3 Wizard

3.3.1 Wizard

Wizard enables fast and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters.

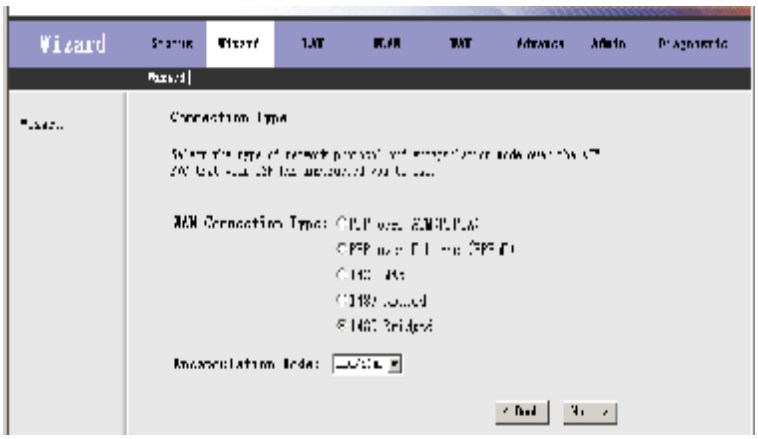
When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be either PPP, ADSL, or both. The technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol that you use to communicate on the Internet.

Choose **Wizard > Wizard.** In the **Wizard** page, you can configure the VPI/VCI number.



- 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 (0 to 31 is reserved for local management of ATM traffic).

Enter the correct VPI and VCI and Click **Next**. The page shown in the following figure appears. In the **Connection Type** page, you can select the WAN connection type and the encapsulation mode.



The following table describes the parameters in this page.

Field	Description
WAN Connection Type	Select the WAN connection type. You can select PPPoA, PPPoE, 1483 MER, 1483 Routed or 1483 Bridged.
Encapsulation Mode	Select the method of encapsulation provide by your ISP from the drop-down list box. You can choose LLC/SNAP or VC-Mux.
Back	Return to the previous page.
Next	Go to the next page.

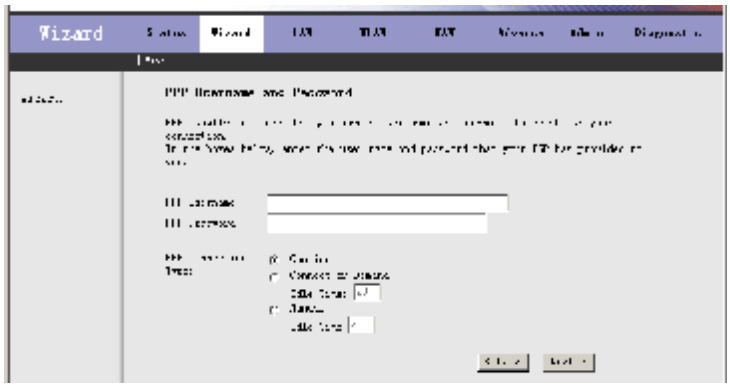
Select **PPPoA** or **PPPoE** in the **Connection Type** page and click **Next**. The page shown in the following figure appears.

The following table describes the parameters of this page.

Field	Description
Obtain an IP address automatically	The dynamic IP address is not fixed. Your ISP assigns the different one each time.
Use the following IP address	The static IP address provided by your ISP.
WAN IP Address	Enter the IP address of the WAN interface provided by your ISP.

Enable NAT	Select it to enable the NAT functionof the router. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise the access to the Internet fails. Normally, it is required to enable NAT.
Back	Return to the previous page.
Next	Go to the next page.

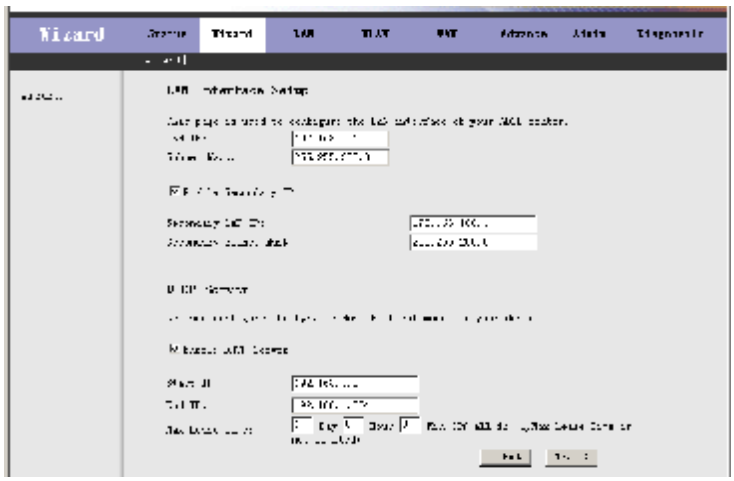
Click **Next**. The page shown in the following figure appears.



The following table describes the parameters of this page.

Field	Description
PPP Username	The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct username and password.
PPP Password	
PPP Connection Type	You can choose Continuous, Connect on Demand or Manual.
Back	Return to the previous page.
Next	Go to the next page.

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

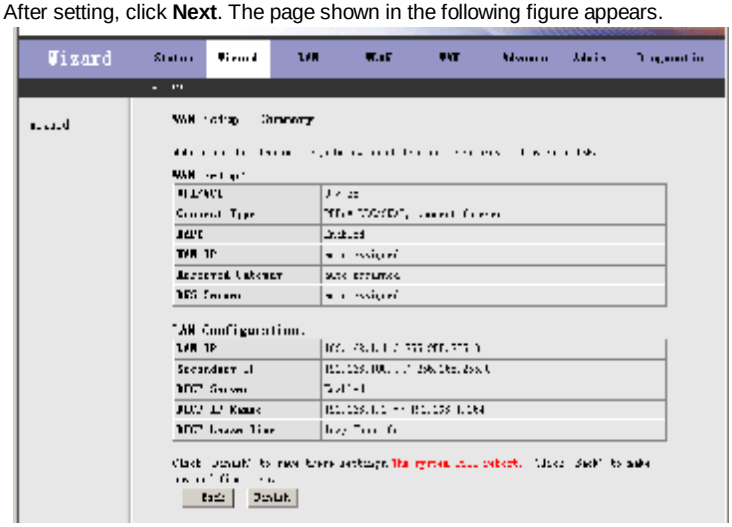


The following table describes the parameters of this page.

Field	Description
LAN IP	Enter the IP address of the router. For example, 192.168.1.1 (default IP address).
Subnet Mask	Enter the subnet mask of the LAN IP address.
Enable Secondary IP	Select it to enable the secondary LAN IP address.
Secondary LAN IP	Enter the secondary IP address of the router. For example, 192.168.100.1 (default IP address)
Secondary Subnet Mask	Enter the subnet mask of the secondary LAN IP address.
Enable DHCP Server	Select it to enable the DHCP server.
Start IP	It specifies the first of the contiguous addresses in the IP address pool.
End IP	It specifies the last of the contiguous addresses in the IP address pool.
Back	Return to the previous page.

Field	Description
Next	Go to the next page.

After setting, click **Next**. The page shown in the following figure appears.



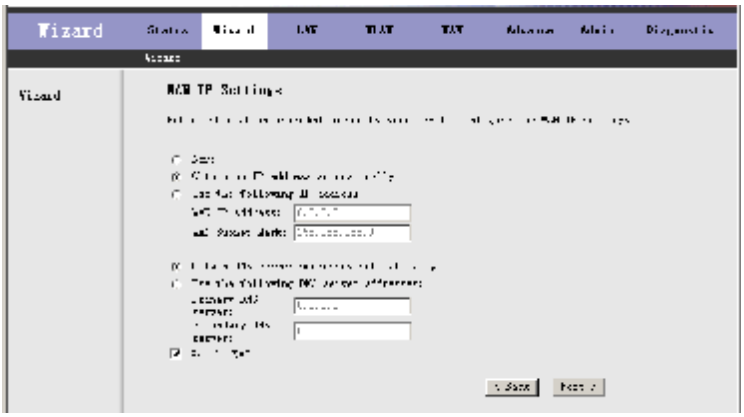
Select 1483 MER in the Connection Type page and click Next. The page shown in the following figure appears.

The following table describes the parameters of this page.

Field	Description
Obtain an IP address automatically	The router obtains a WAN IP address automatically and it enables DHCP client function. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP server function.
Use the following IP address	Select it to enter the WAN IP address by yourself.
WAN IP Address	Enter the IP address of the WAN interface

Field	Description
	provided by your ISP.
WAN Subnet Mask	Enter the subnet mask of the IP address of the WAN interface provided by your ISP.
Default Gateway	Enter the IP address of the default gateway.
Obtain DNS server addresses automatically	Obtain the IP address of the DNS server assigned by the uplink equipment, such as BAS.
Use the following DNS server addresses	If you want to enter the IP address of the DNS server by yourself, select it and enter the related data.
Primary DNS server	Enter the IP address of the primary DNS server.
Secondary DNS server	Enter the IP address of the secondary DNS server provided by your ISP.
Enable NAT	Select it to enable the NAT function of the router. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise the access to the Internet fails. Normally, it is required to enable NAT.
Back	Return to the previous page.
Next	Go to the next page.

Select **1483 Routed** in the **Connection Type** page and click **Next**. The page shown in the following figure appears.



The following table describes the parameters of this page.

Field	Description
None	
Obtain an IP address automatically	The dynamic IP address is not fixed. Your ISP assigns the different one each time.
Use the following IP address	The static IP address that your ISP provides.
WAN IP Address	Enter the IP address of the WAN interface provided by your ISP.
WAN Subnet Mask	Enter the subnet mask of the IP address of the WAN interface provided by your ISP.
Obtain DNS server addresses automatically	Obtain the IP address of the DNS server assigned by the uplink equipment, such as BAS.
Use the following DNS server addresses	If you want to enter the IP address of the DNS server by yourself, select it and enter the related data.
Primary DNS server	Enter the IP address of the primary DNS server here.
Secondary DNS server	Enter the IP address of the secondary DNS server provided by your ISP.

Field	Description
Enable NAT	Select it to enable the NAT function of the router. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise the access to the Internet fails. Normally, it is required to enable NAT.
Back	Return to the previous page.
Next	Go to the next page.

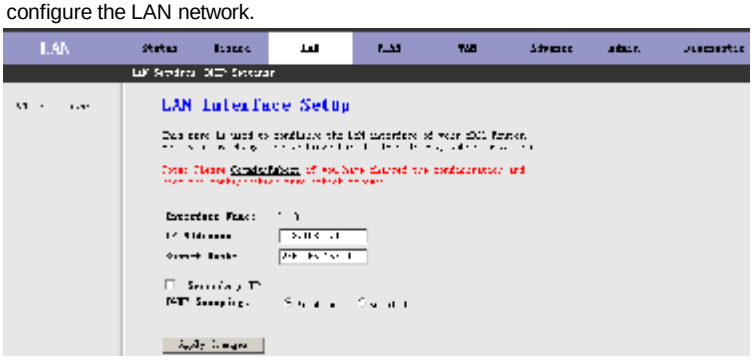
3.4 LAN

In the navigation bar, choose **LAN.** The **LAN** page that is displayed contains **LAN Settings** and **DHCP Settings.** You can use the LAN configuration to define an IP address for the DSL router and configure the DHCP server.

3.4.1 LAN Settings

In the **LAN Setting** page, you can change IP address of the router. The default IP address is 192.168.1.1. This is the private IP address of the DSL router. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses.

In the navigation bar, choose LAN Settings. In the LAN Settings page, you can configure the LAN network.



The following table describes the parameters of this page.

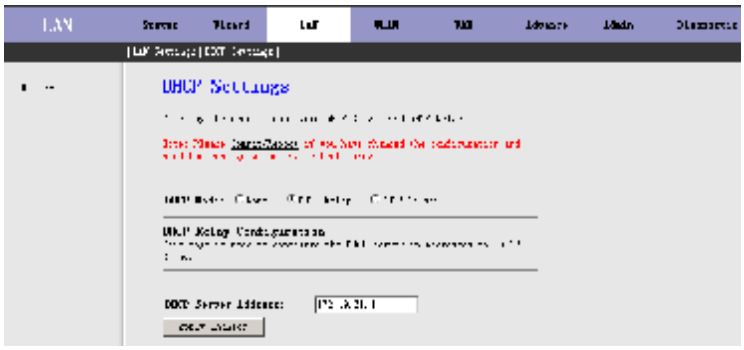
Field	Description
IP Address	Enter the IP of LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is 192.168.1.1- 192.168.255.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable the secondary LAN IP. The two LAN IP address must be in the different network.
IGMP Snooping	IGMP Snooping is the process of listening to IGMP traffic. It is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.
Apply Changes	Save the settings of this page.

3.4.2 DHCP Settings

Dynamic host configuration protocol (DHCP) allows the individual PC to obain the TCP/IP configuration from the centralized DHCP server. You can configure this router as a DHCP server or disable it. The DHCP server can assign IP address, IP default gateway and DNS server to DHCP clients. This router can also act as a surrogate DHCP server (DHCP relay) where it relays IP address assignment from an actual real DHCP server to clients. You can enable or disable DHCP server or DHCP proxy.

Select **None**. The page shown in the following figure appears.

Select **DHCP Relay** in the **DHCP Settngs** page. The page shown in the following figure appears.



The following table describes the parameters of this page.

Field	Description
DHCP Relay	Select it, the router acts a surrogate DHCP server. It relays the DHCP requests and reponses between the remote server and the client.
DHCP Server Address	Enter the IP address of the actual, remote DHCP server.
Apply Changes	Save the settings of this page.

Select **DHCP Server** in the **DHCP Server Setup** page, the page shown in the following figure appears.

The following table describes the parameters in this page.

Field	Description
DHCP Mode	If set to DHCP server, the router can assign IP addresses and IP default gateway. DNS servers can be Windows95, Windows NT and other systems that support the DHCP client.
IP Pool Range	It specifies the first and the last of contiguous IP address of the IP address pool.
Show Client	Click it, the **Active DHCP Client Table page** appears. It shows the assigned IP address of the clients.
Max Lease Time	The lease time determines the period that the PCs retain the assigned IP addresses before the IP addresses change.
Domain Name	Enter the domain name if you know. If you leave it blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual computer. The domain name can be assigned from the router through the DHCP server.
Gateway	Enter the IP default gateway of the IP address pool.

Field	Description
Address	
Apply Changes	Save the settings of this page.
MAC-Base Assignment	Click it, the **Static IP Assignment Table** page appears. It allows you to assign IP addresses on the LAN to specify individual computers based on their MAC address.

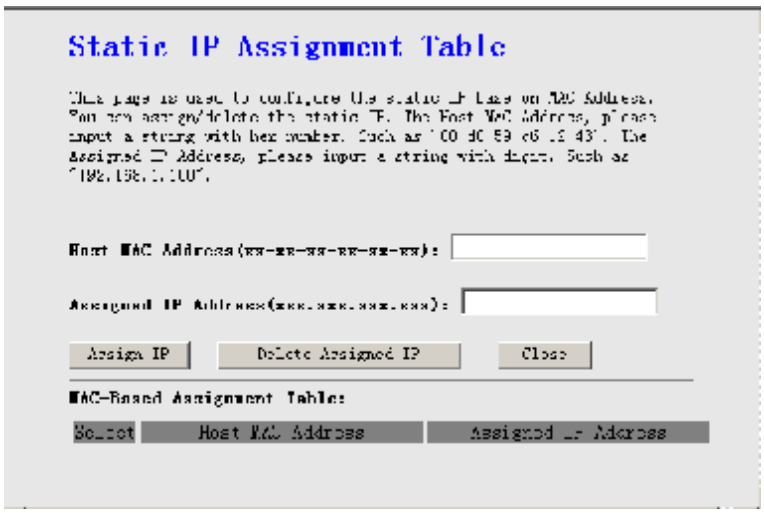
Click **Show Client** in the **DHCP Server Setup** page. The page shown in the following figure appears. In this page, you can view the IP address assigned to each DHCP client.

The following table describes the parameters in this page.

Field	Description
IP Address	It displays the IP address relative to the MAC address.
MAC Address	It displays the MAC address of the computer. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character. For example, 00-A0-C5-00-02-12.
Time Expired (s)	It shows the lease time. The lease time determines the period that the PCs retain the assigned IP addresses before the IP addresses change.

Refresh	Refresh the page.
Close	Close the page.

Click **MAC-Based Assignment** in the **DHCP Server Setup** page. The page shown in the following figure appears. In this page, you can assign the IP addresses on the LAN to the specific individual computers based on their MAC address.



The following table describes the parameters of this page.

Field	Description
Host MAC Address	Enter the MAC address of a computer on the LAN.
Assigned IP Address	It specifies the IP address of the IP address pool.
Assign IP	Click it after entering host MAC address and assigned IP address, a row will be added in MAC-base assignment table.
Delete Assigned IP	Select a row in MAC-base assignment table, then click it. The row is deleted.

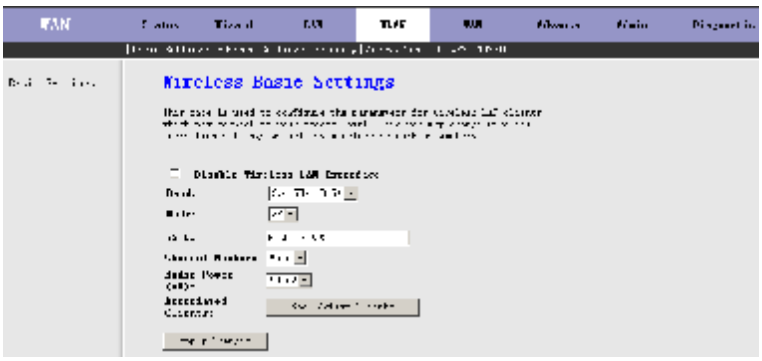
Close	Close the page.
MAC-Base Assignment Table	It shows the assigned IP address based on the MAC address.

3.5 WLAN

In the navigation bar, choose **WLAN.** The W**LAN** page that is displayed contains **Basic Settings**, **Security**, **Advance Settings**, **Access Control**, **WPS**, and **WDS Settings**. This page introduces the wireless LAN and some basic configurations. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a pear-to-pear network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

3.5.1 Basic Settings

Choose WLAN > Basic Settings. The page shown in the following figure appears. In this page, you can configure the parameters for wireless LAN clients that may connect to your access point.



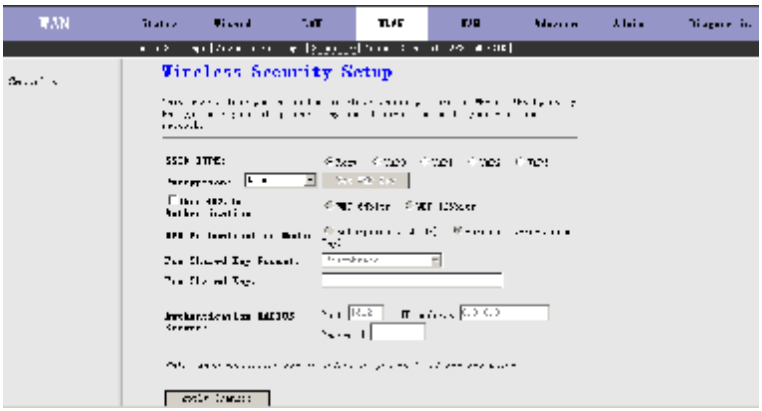
The following table describes the parameters of this page.

Field	Description
Disable Wireless LAN Interface	By default, the wireless LAN is enabled. Select it to disable the wireless LAN.
SSID	The service set identification (SSID) is a

Field	Description
	unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a desciptive name.
Channel Number	A channel is the radio frequency used by 802.11b/g wireless device. Channels available depend on your geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from diffirent APs overlap. Select a channel from the drop-down list box.
Apply Changes	Save the settings of this page.

3.5.2 Security

Choose **WLAN > Security**. The page shown in the following figure appears. Wireless security is vital to your network. It protects the wireless communication among the wireless stations, access points and the wireless network.



The following table describes the parameters of this page.

Field	Description
SSID Type	Select the SSID.
Encryption	You can choose None, WEP, WPA (TKIP), WPA2 (AES) and WPA2 Mixed. Wired equivalent privacy (WEP) entrypts data frames before transmitting over the wireless network. Wi-Fi protected access (WPE) is a subset of the IEEE802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.
Set WEP Key	It is available when you set to WEP. Click it, the wireless WEP key setup page appears.
Authentication RADIUS Server	RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is client and the server is RADIUS server. RADIUS is a simple package exchange in which your router acts as a message relay between the wireless station and the network RADIUS server.
Port	The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
IP Address	Enter the IP address of the RADIUS server.
Password	Enter a password as the key to be shared between the external authentication server and the access point. The key is not send over the network. This key must be the same on the external authentication server and your router.
Apply Changes	Save the the changes of this page.

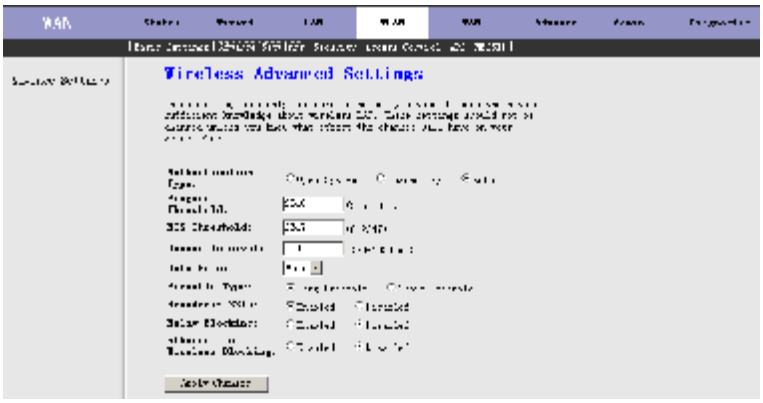
The following table describes the parameters of this page.

Field	Description
SSID TYPE	Select the SSID.
Key Length	Select 64-bit or 128-bit to use data encryption.
Key Format	If you chose 64-bit, you can choose ASCII (5 characters) or Hex (10 characters). If you chose 128-bit, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Select the default encryption key.
Encryption Key 1 to 4	The Encryption keys are used to encrypt the data. Both router and wireless stations must use the same encryption key for data transmission. If you chose 64-bit and ASCII (5 characters), then enter any 5 ASCII characters. If you chose 64-bit and Hex (10 characters), then enter any 10 hexadecimal characters. If you chose 128-bit and ASCII (13

Field	Description
	characters), then enter any 13 ASCII characters. If you chose 128-bit and Hex(26 characters), then enter any 26 hexadecimal characters.
Apply Changes	Save the changes of this page.
Close	Close the page.
Undo	Refresh the page.

3.5.3 Advance Settings

Choose **WLAN > Advance Settings**. The page shown in the following figure appears. These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know the effect of the changes on your AP.



The following table describes the parameters of this page.

Field	Description
Fragment Threshold	This is the maximum data fragment size (between 256 and 2346bytes) that can be sent in the wireless network before the router fragments the packet into smaller data frames.
RTS Threshold	Request to send (RTS) is designed to prevent

Field	Description
	collisions due to hidden node. A RTS defines the biggest size data frame you can send before a RTS handshake invoked. The RTS threshold value is between 0 and 2347. If the RTS threshold value is greater than the fragment threshold value, the RTS hankshake do not occur. Because the data frames are fragmented before they reach the RTS size.
Apply Changes	Save the changes of this page.

3.5.4 Access Control

Choose **WLAN > Access Control**. The page shown in the following figure appears. In this page, you can configure the wireless access control.

The following table describes the parameters of this page.

Field	Description
Wireless Access Control Mode	You can choose disable, allow listed and deny listed. Select allow listed, only the clients whose MAC address is listed can access the router. Select deny listed, the clients whose MAC address is listed are denied to access the router.

Field	Description
Apply Changes	Save the changes of select access control mode.
MAC Address	Enter the MAC address of the wireless station that are allowed or denied access to your router in this address field.
Add	The MAC address is added to current access control list.
Reset	Begin configuring the MAC address afresh.
Current Access Control List	The MAC address in this table is allowed or denied to access to the router.
Delete	Delete the row you select in the current access control list.
Delete All	Delete all rows in the current access control list.
Reset	Click it to begin configuring the current access control list afresh.

3.5.5 WPS

Choose **WLAN > WPS**. The page shown in the following figure appears. This page allows you to change the setting for Wi-Fi protected setup (WPS). WPS function helps your wireless client automically synchronize with its settings and connect to the access point in a minute without any hassle.

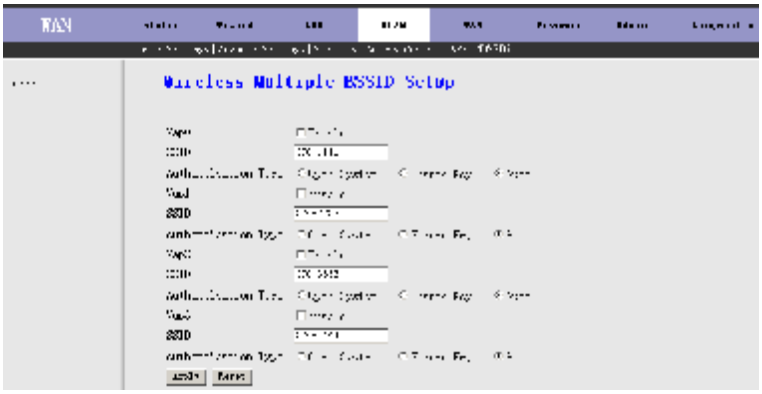
The following table describes the parameters of this page.

Field	Description
Self-PIN Number	The PIN number of access point use.

Start PBC	Use the PBC mode to connect to the access point.
Client PIN Number	The PIN number of client use.
Start PIN	Use the PIN mode to connect to the access point.

3.5.6 MBSSID

Choose **WLAN > MBSSID**. The page shown in the following figure appears. In this page, you can configure the vitual SSID.



The following table describes the parameters of this page.

Field	De cription
SSID	The SSID is a unique name to identify the router in the wireless LAN.
Apply	Save the settings of this page.
Reset	Refresh the page.

3.6 WAN

In the navigation bar, choose **WAN.** In the W**AN** page that is displayed contains **WAN Interface** and **ADSL Settings**.

3.6.1 WAN Interface

Choose **WAN > WAN Interface**. The page shown in the following figure appears. You can configure WAN Interface of the router.

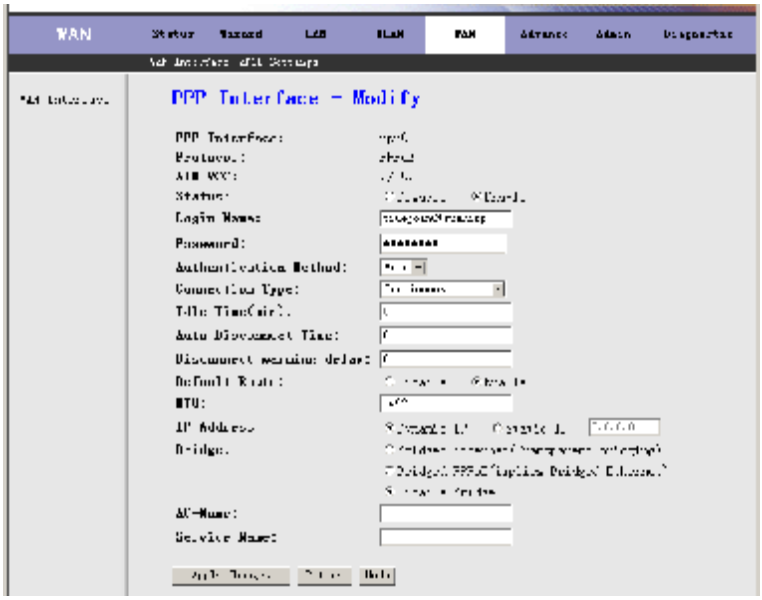
The following table describes the parameters of this page.

Field	Description
Current ATM VC Table	This table shows the existed PVCs. It shows the interface name, channel mode, VPI/VCI, encapsulation mode, local IP address, remote IP address, etc. The maximum item of this table is eight.
VPI	The virtual path between two points in an ATM network, ranging from 0 to 255.
VCI	The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols)

Field	Description
Encapsulation	You can choose LLC or VC-Mux.
Channel Mode	You can choose 1483 Bridged, 1483 MER, PPPoE, PPPoA and 1483 Routed.
Admin Status	Select Disable, this PVC is unusable.
Enable NAPT	Select it to enable the NAPT function of the router. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise the access to the Internet fails. Normally, it is required to enable NAPT.
User Name	The correct user name that your ISP has provided to you.
Password	The correct password that your ISP has provided to you.
Type	You can choose continuous, connect on demand and manual.
Idle Time(min)	If select connect on demand, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPOE connection.
WAN IP Settings	
Type	You can choose fixed IP and use DHCP. If select fixed IP, you should enter the local IP address, remote IP address and subnet mask. If set use DHCP, The router is a DHCP client, the WAN IP is assigned by the remote DHCP server.
Local IP Address	It is the IP address of WAN interface which is provided by your ISP.
Remote IP Address	This is the gateway IP address which is provided by your ISP.
Subnet Mask	It is the subnet mask of the local IP

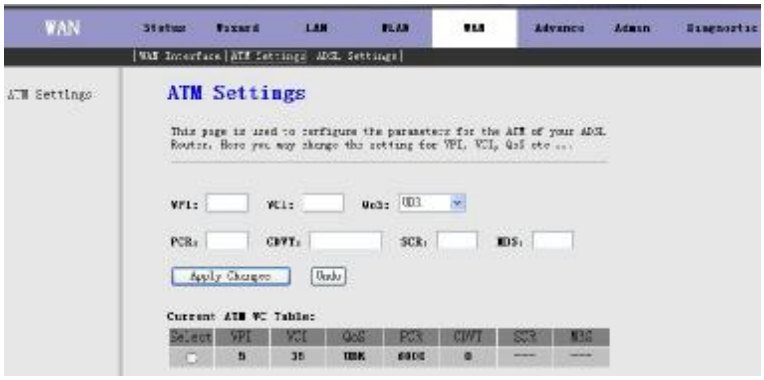
Field	Description
	address.
Unnumbered	Select it to enable IP unnumbered function.
Default Route	
Add	After configuring the parameters of this page, click it to add a new PVC into the current ATM VC table.
Modify	Select a PVC in the current ATM VC table, then modify the parameters of this PVC. When you finish, click it to apply the change of this PVC.
Delete	Select a PVC in the current ATM VC table, and click it to delete this PVC.
Undo	Click it to begin configuring this page afresh.
	Click it, the PPP Interface-Modify page appears. You can modify the PVCs' parameters.

Click  in the PPPoE mode. The page shown in the following figure appears. In this page, you can configure parameters of this
PPPoE PVC.



3.6.2 ATM Settings

Choose **WAN > ATM Settings**. The page shown in the following figure appears. In this page, you can configure the parameters of the ATM for your ADSL router, including QoS type, PCR, CDVT, SCR and MBS.



3.6.3 ADSL Settings

Choose **WAN > ADSL Settings**. The page shown in the following figure appears. You can select the DSL modulation. Normally, the user needs to remain this factory default settings. The router supports these modulations: G.Dmt, G.lite, T1.413, ADSL2, ADSL2+, AnnexL and AnnexM. The router negotiates the modulation mode with the DSLAM.

3.7 Advance

In the navigation bar, choose **Advance.** The **Advance** page that is displayed contains **DNS**, **Firewall**, **Virtual Server**, **Routing**, **IP QOS, Anti-dos, Port Mapping** and **Other**.

3.7.1 DNS

Choose **Advance > DNS.** The **DNS** page that is displayed contains **DNS Server** and **DDS.**

Domain name system (DNS) is an Internet service that translates the domain name into IP address. Because the domain name is alphabetic, it is easier to remember. The Internet however, is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system has its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

3.7.1.1 DNS Server

Choose DNS Server. The page shown in the following figure appears. You can configure the DNS server IP addresses for DNS relay.

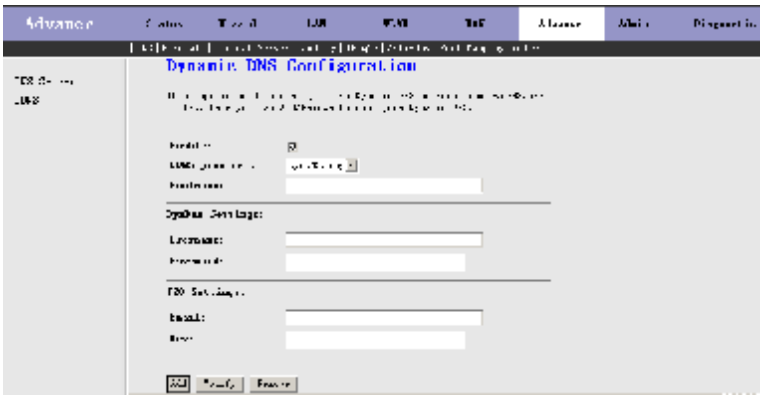
The following table describes the parameters of this page.

Field	escription
Attain DNS Automatically	Select it and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection

Field	escription
	establishment.
Set DNS Manually	Select it and enter the primary and optional secondary IP addresses of the DNS server.
Apply Changes	Save the settings of this page.
Reset Selected	Refresh this page.

3.7.1.2 DDNS

Choose **DDNS**. The page shown in the following figure appears. This page is used to configure the dynamic DNS address from DynDNS.org or TZO. You can add or remove to configure dynamic DNS.

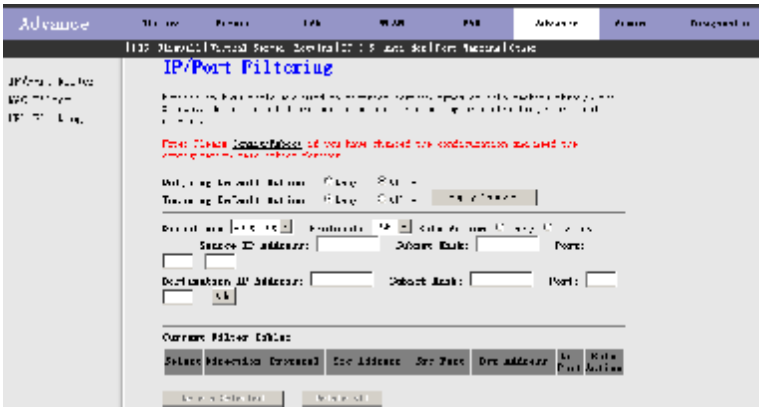


3.7.2 Firewall

Choose **Advance > Firewall**. The page shown in the following figure appears. The page that is displayed contains **IP/Port Fileter, MAC Filter** and **URL Blocking**.

3.7.2.1 IP/Port Filter

Choose **IP/Port Filter**. The page shown in the following figure appears. Entries in this table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



Click **Apply Changes** to save the settings of this page.
Click **Add** to add a new rule of the IP/port filter.

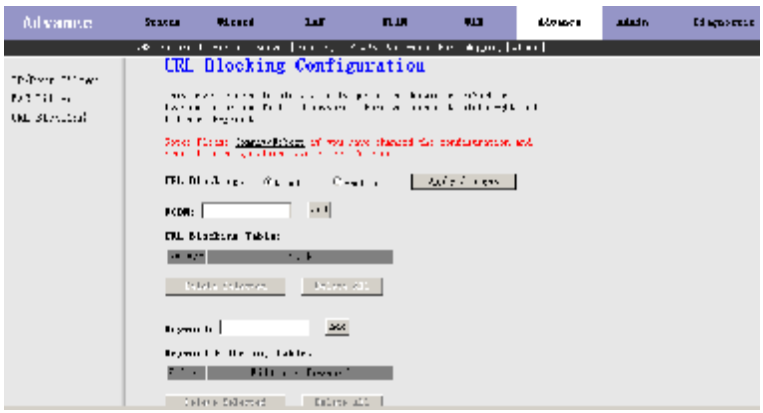
3.7.2.2 MAC Filter

Choose **MAC Filter**. The page shown in the following figure appears. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.

Click **Apply Changes** to save the settings of this page.
Click **Add** to add a new rule of the MAC filter.

3.7.2.3 URL Blocking

Choose **URL Blocking**. The page shown in the following figure appears. This page is used to block a fully qualified domain name and filtered keyword, such as www. yahoo.com. You can add or delete FQDN and filtered keyword.



3.7.3 Virtual Server

Choose **Advance > Virtual Server**. The page shown in the following figure appears. The page that is displayed contains **Services, DMZ Settings** and **IP Address Mapping**.

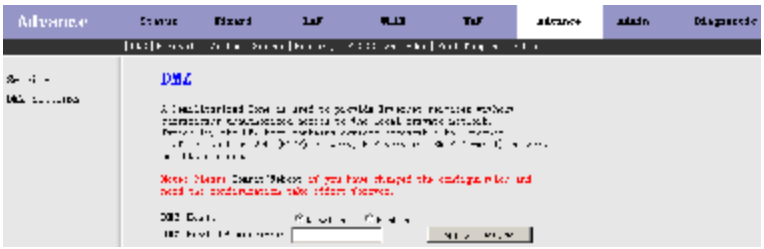
3.7.3.1 Services

Choose **Services**. The page shown in the following figure appears. This page is used to enable the servers in the local network.

Click **Add** to add a virtual server.

3.7.3.2 DMZ Settings

Choose **DMZ Settings**. The page shown in the following figure appears. A demilitarized zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



Step 1 Select **Enable DMZ** to enable this function.

Step 2 Enter an IP address of the DMZ host.

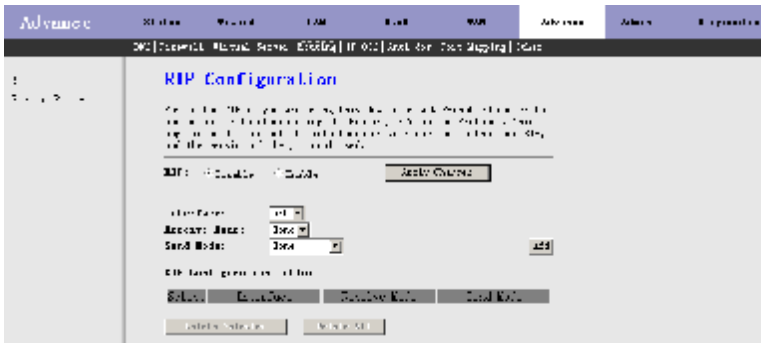
Step 3 Click **Apply Changes** to save the settings of this page.

3.7.4 Routing

Choose **Advance > Routing**. The page shown in the following figure appears. The page that is displayed contains **RIP** and **Static Route.**

3.7.4.1 RIP

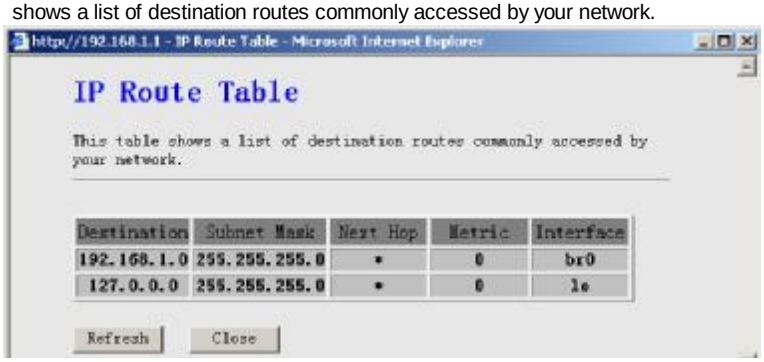
Choose **RIP**. The page shown in the following figure appears. Enable the RIP if you are using this device as a RIP-enabled router to communicate with others with the Routing Information Protocol (RIP). This page is used to select the interfaces on your router that use RIP, and the version of the protocol used.



3.7.4.2 Static Route

Choose **Static Route**. The page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.

Click **Show Routes**. The table shown in the following figure appears. The table shows a list of destination routes commonly accessed by your network.



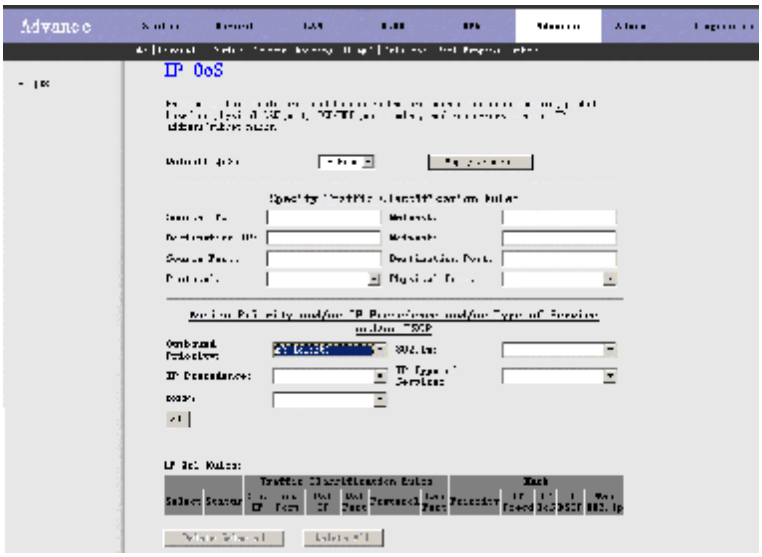
3.7.5 IP QOS

Choose **Advance > IP QOS**. The page shown in the following figure appears. Entries in this table are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, and source/destination IP address/subnet masks.

Step 1 Enable IP Qos

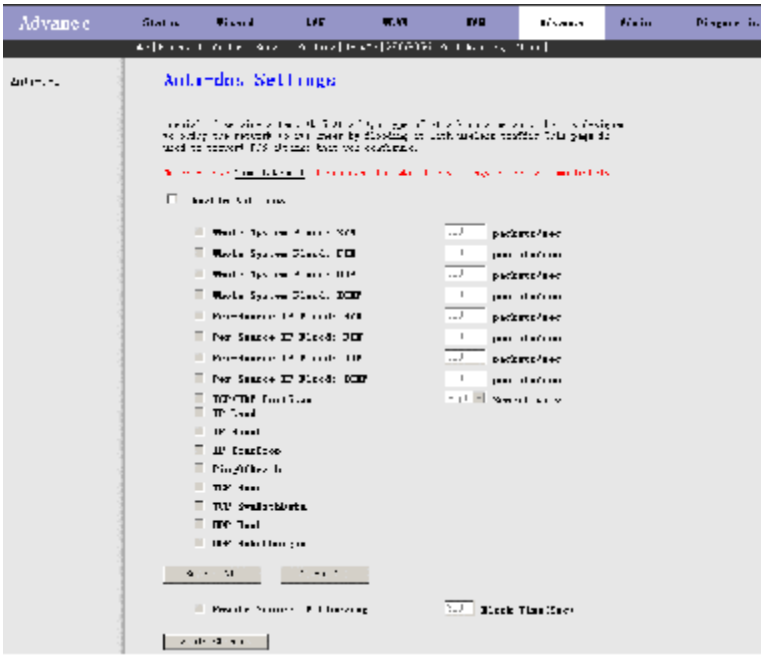
Step 2 Click **Configurate** to add a new IP Qos rule.

The page shown in the following figure appears.



3.7.6 Anti-dos

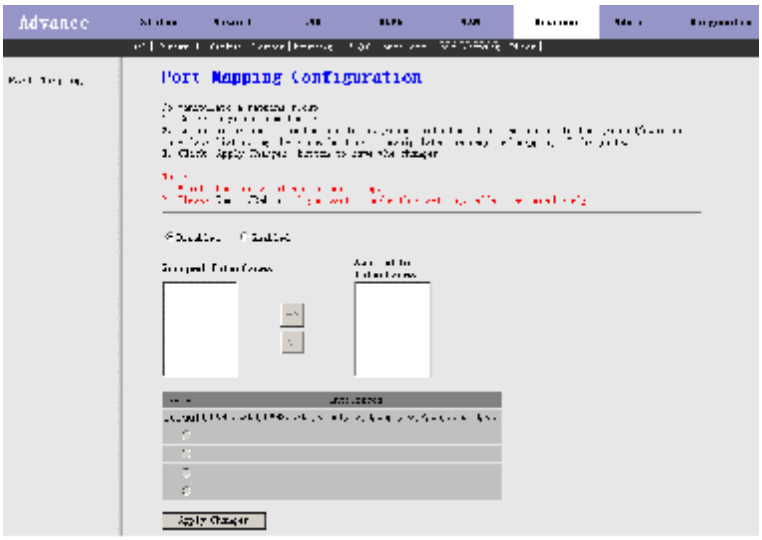
Choose **Advance > Anti-dos**. The page shown in the following figure appears. Denial-of-service attack (DoS Attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. In this page, you can configure to prevent DoS attacks.



Click **Apply Changes** to save the settings of this page.

3.7.7 Port Mapping

Choose **Advance > Port Mapping**. The page shown in the following figure appears.

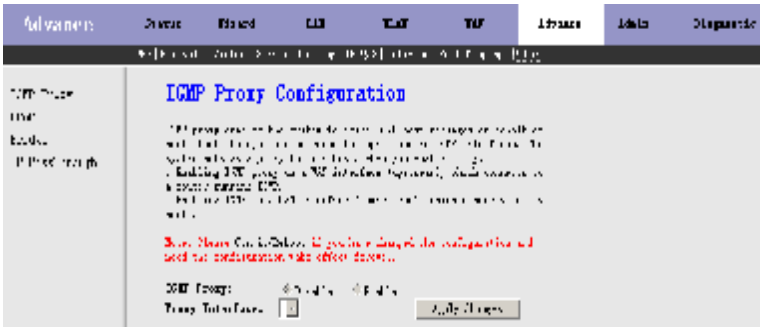


3.7.8 Other

Choose **Advance > Other**. The page shown in the following figure appears. The page that is displayed contains **IGMP Proxy, UPnP, Bridge** and **IP PassThrough**.

3.7.8.1 IGMP Proxy

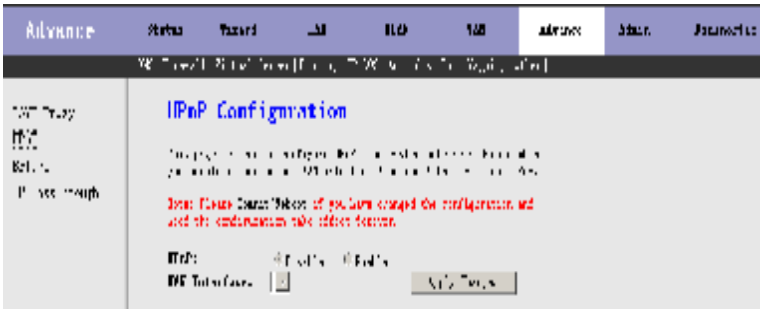
Choose **IGMP Proxy**. The page shown in the following figure appears. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovers through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.



Click **Apply Changes** to save the settings of this page.

3.7.8.2 UPNP

Choose **UPNP**. The page shown in the following figure appears. This page is used to configure UPnP. The system acts as a daemon after you enable it.



Click **Apply Changes** to save the settings of this page.

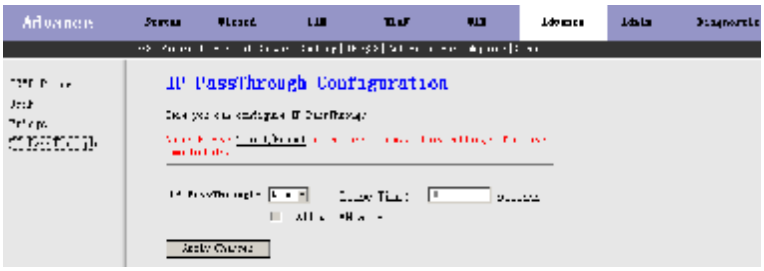
3.7.8.3 Bridge

Choose **Bridge**. The page shown in the following figure appears. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.

Click **Show MACs**. The page shown in the following figure appears. This table shows a list of learned MAC addresses for this bridge.

3.7.8.4 IP PassThrough

Choose **IP Pass Through**. The page shown in the following figure appears. In this page, you can enable and configure IP passthrough.



3.8 Admin

In the navigation bar, choose **Admin**. The page that is displayed contains **Access Control, Commit/Reboot, Password, Backup/Restore, Upgrade Fireware, Time Zone, System Log, SNMP, TR069 and ACL.**

3.8.1 Access Control

Choose **Admin > Access Control**. The page shown in the following page appears. You can enable or disable the services which are used by the remote host. For example, if TELNET service is enabled and the port is 23, the remote host can access this router by telnet through the port 23.

3.8.2 Commit/Reboot

Choose **Admin > Commit/Reboot**. The page shown in the following page appears. You can set the router reset to the default settings or set the router to commit the current settings.

The following table describes the parameters of this page.

Field	Description
Reset to Factory Default Settings	Select it to reset the router to the default settings.
Save Current Settings	Select it to save the current settings and reboot the router.
System Reboot	Reboot the router.

3.8.3 Password

Choose **Admin > Password**. The page shown in the following page appears. You can add user account to access the web server of the ADSL router or change the password of the selected user account. By default, the super user name and password are admin and admin. The common user name and password are user and user.

The following table describes the parameters of this page.

Field	Description
User Name	You can choose admin or user from the drop-down list box.
Old Password	Enter the old password of the user.
New Password	Enter the password to which you want to change the old password.
Confirmed Password	Enter the new password again.
Apply	Save the settings of the page.

Field	Description
Reset	Refresh the page.

3.8.4 Backup/Restore

Choose **Admin > Backup/Restore**. The page shown in the following page appears. You can back up the current settings to a file and restore the settings from the file which was saved previously.

***Notice**: Do not turn off your router or press the Reset button while these procedures are in progress.*

The following table describes the parameters of this page.

Field	Description
Save Settings to File	Click **Save** and select the path. Then you can save the configuration file of the router.
Load Settings from File	Click **Browse** to select the configuration file.
	Click **Upload** to upload the configuration file.

3.8.5 Upgrade Fireware

Choose **Admin >Upgrade Fireware**. The page shown in the following page appears. You can upgrade the fireware of the router.

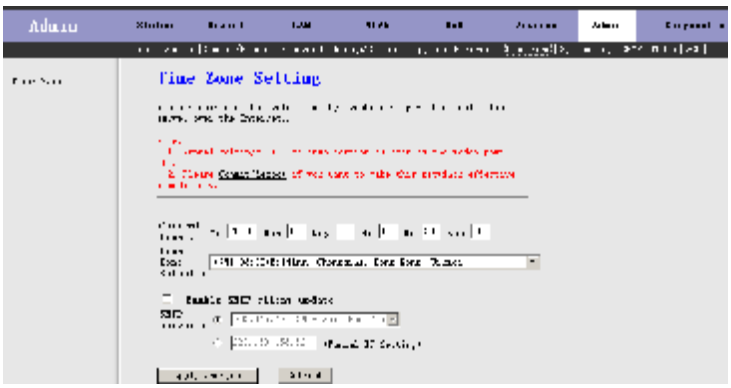
***Notice:** Do not turn off your router or press the Reset button while this procedure is in progress.*

The following table describes the parameters of this page.

Field	Description
Select File	Click **Browse** to select the fireware file.
Upload	Select the fireware file and click **Upload** to upgrade the fireware.
Reset	Click it to refresh the fireware file.

3.8.6 Time Zone

Choose **Admin > Time Zone**. The page shown in the following page appears. You can set the system time manually or get the system time from the time server.



The following table describes the parameters of this page.

Field	Description

Time Zone Select	Select the time zone in which area you are.
Enable SNTP Client Update	Select it, you can choose the correct SNTP server which you want.
SNTP server	Choose the SNTP server from the drop-down list box.
Apply Changes	Save the settings of this page.
Refresh	Refresh the page.

3.8.7 System Log

Choose **Admin > System Log**. The page shown in the following page appears. You can enable or disabled the system log function and view the system log.

The following table describes the parameters of this page.

Field	Description
System Log	You can enable or disable the system log function.
Apply Changes	Save the settings of this page.
Refresh	Refresh the system log shown in the textfield.

3.8.8 SNMP

Choose **Admin > SNMP**. The page shown in the following page appears. You can set the SNMP parameters.

The following table describes the parameters of this page.

Field	Description
Trap IP Address	Enter the IP address of trap IP. The trap information is sent to the host.
Community name (read-only)	The network administrators must use this password to read the information of this router.
Community name (write-only)	The network administrators must use this password to configure the information of the router.
Apply Changes	Save the settings of this page.
Reset	Click it to begin refreshing this page.

3.8.9 TR069

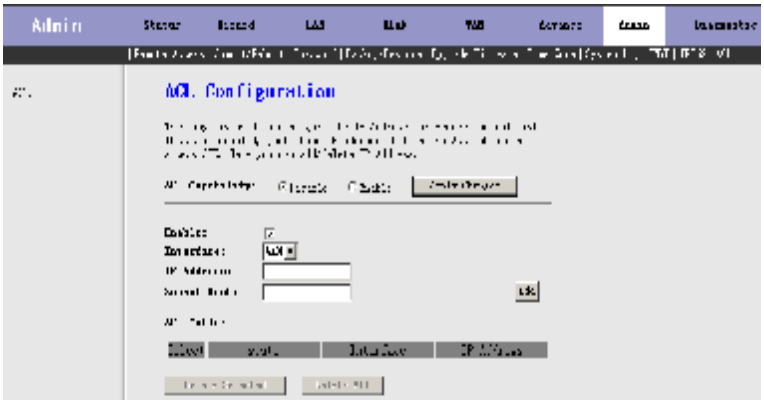
Choose **Admin > TR069**. The page shown in the following page appears. You can configure the TR-069 CPE.

3.8.10 ACL

Choose **Admin >ACL**. The page shown in the following page appears. In this page, you can configure the IP address for access control list. If ACL is enabled, only the effective IP address in ACL can access the ADSL router.

The procedure for configuring the IP address for access control list is as follows:

***Note**: If you select **Enable** in the **ACL Capability** field, make sure tha there is at least one IP address is in ACL list before it takes effect.*



The following table describes the parameters of this page.

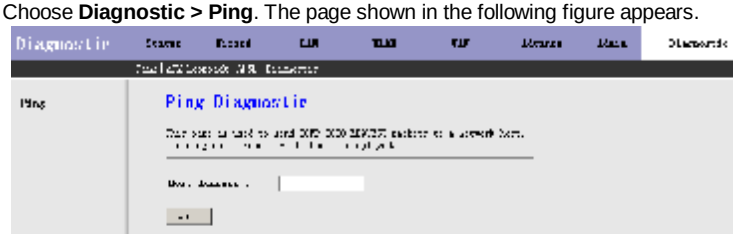
Field	Description
ACL Capability	Select the ACL rule, disable or enable.
Enable	Enable the ACL table.
Interface	Select the interface that becomes effective.
IP Address	Enter the IP address of ACL table.
Subnet Mask	Enter the subnet mask of IP address.

3.9 Diagnostic

In the navigation bar, choose **Diagnostic**. The page that is displayed contains **Ping**, **ATM Loopback**, **ADSL** and **Diagnostic**.

3.9.1 Ping

Choose **Diagnostic > Ping**. The page shown in the following figure appears.

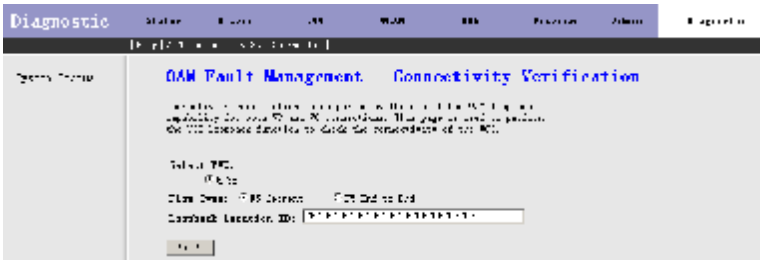


The following table describes the parameters in this page.

Field	Description
Host Address	Enter the IP Address.
Go!	Click it to begin to ping the host address.

3.9.2 ATM Loopback

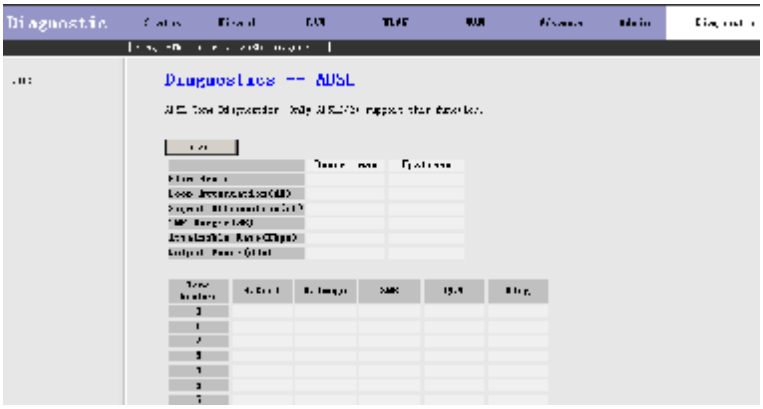
Choose **Diagnostic >ATM Loopback**. The page shown in the following figure appears. In this page, you can use VCC loopback function to check the connectivity of the VCC.



Click **Go!** to begin testing.

3.9.3 ADSL

Choose **Diagnostic > ADSL**. The page shown in the following figure appears. It is used for ADSL tone diagnostics.



Click **Start** to begin ADSL tone diagnostics.

3.9.4 Diagnostic

Choose **Diagnostic > Diagnostic**. The page shown in the following figure appears. You can test the DSL connection.

Click **Run Diagnostic Test** to begin testing.

FCC Information

FCC Information

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

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

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

Federal Communications Commission (FCC) Requirements, Part 15

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

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

---Reorient or relocate the receiving antenna.

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

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

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

Regulatory information / Disclaimers

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

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

MPE Statement (Safety Information)

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

Safety Information

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