LKW300-21A3

User Manual

V1.0

Contents

1 Introduction

The LKW300-21A3 is an ADSL access device that supports multiple line modes. The device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net cafes and office users. The device provides high performance access to the Internet, downlink up to 24 Mbps and uplink up to 1 Mbps. The device supports WLAN access. It can connect to the Internet through a WLAN AP or WLAN device. It complies with IEEE 802.11, 802.11b/g/n specifications, WEP, WPA, and WPA2 security specifications.

1.1 Packing List

- Wireless router x1
- Power adapter (DC) x1
- ADSL splitter x 1
- Quick installation guide x1
- RJ45 Cable x1
- RJ11 Cable x1
- CD (user manual) x1
- Warranty card X1

1.2 Safety Precautions

Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter 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 damage caused by overheating to the device. The long and thin 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 it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.3 LEDs and Interfaces

Front Panel

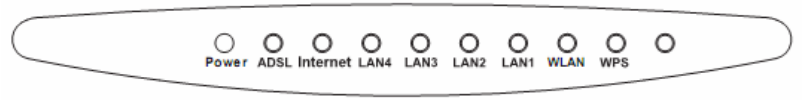


Figure 1 Front Panel

The following table describes the LEDs of the device.

LEDs	Color	Status	Description
Power	Green	On	The initialization of the device is successful.
		Off	The device is powered off.
ADSL	Green	On	Connection between the device and the physical layer of the office end is established.
		Blinks slowly	No signal is being detected.
		Blinks quickly	The device is handshaking with the physical layer of the office end.

LEDs	Color	Status	Description
Internet	Green	On	The Internet connection is normal in the routing mode (for example, PPP dial-up is successful), and no Internet data is being transmitted.
		Blinks	Internet data is being transmitted in the routing mode.
		Off	The device is in the bridge mode.
	Red	On	The Internet connection fails after successful synchronization in the routing mode (for example, PPP dial-up is failed).
LAN 4/3/2/1	Green	On	The LAN connection is normal and activated.
		Blinks	Data is being transmitted in the LAN or Internet data is being transmitted in the bridge mode.
		Off	The LAN interface is not connected.
WLAN	Green	On	The WLAN connection has been activated.
		Blinks	Data is being transmitted in the WLAN.
		Off	The WLAN connection is not activated.
WPS	Green	Blinks	WPS is enabled, and is waiting for client to negotiate.
		Off	WPS is disabled.

Rear Panel

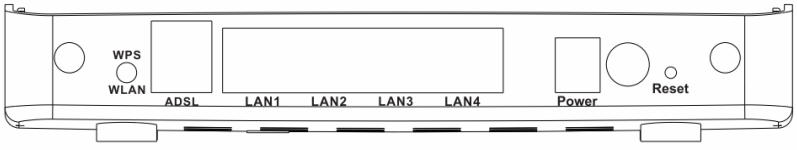


Figure 2 Rear panel

The following table describes the interfaces of the device.

Interface	Description
WPS/WLAN	Press the button and hold it for less than 1 second to enable WLAN. If WLAN is enabled, press the button for more than 3 seconds, to initialize WPS negotiation.
ADSL	RJ-11 interface, for connecting to the ADSL interface or a splitter through a telephone cable.
LAN1/2/3/4	RJ-45 interface, for connecting to the Ethernet interface of a computer or the Ethernet devices through an Ethernet cable.
Power	Power interface, for connecting to the power adapter
Reset	This button is used to restore the factory default settings of router. Keep the device powered on, and insert a needle into the hole for more than 3 seconds, then release it. The device restores the factory default settings of router.

1.4 System Requirements

Recommended system requirements are as follows:

- A 10/100 base-T Ethernet card is installed on your PC
- A hub or Switch. (connected to several PCs through one of Ethernet interfaces on the device)

- Operating system: Windows 98SE, Windows 2000, Windows ME, Windows XP
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.5 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483Briged/1483Routed/MER/IPoA access
- Multiple PVCs (up to eight) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- 802.1Q and 802.1P protocol
- DHCP server
- NAPT
- Static route
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- DNS
- Virtual server
- DMZ
- Two-level passwords and usernames
- Web interface
- Telnet CLI
- System status display
- PPP session PAP/CHAP
- IP filter
- IP quality of service (QoS)
- Remote access control
- Line connection status test
- Remote managing through Telnet or HTTP
- Backup and restoration of configuration file

- Ethernet interface supporting crossover detection, auto-correction, and polarity correction
- Universal plug and play (UPnP)

2 Hardware Installation

To connect the device, do as follows:

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

The splitter has three interfaces:

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

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

Note:

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

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

Connection 1

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

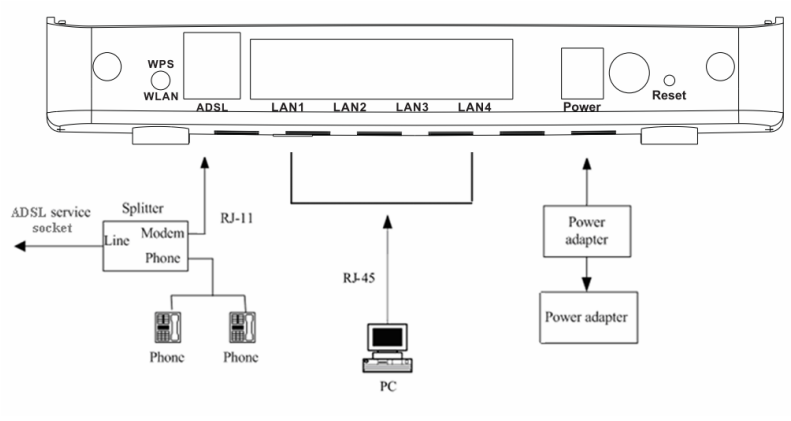


Figure 3 Connection diagram (Without connecting telephone sets before the splitter)

Connection 2

Figure 4 shows the connection when the splitter is installed close to the router.

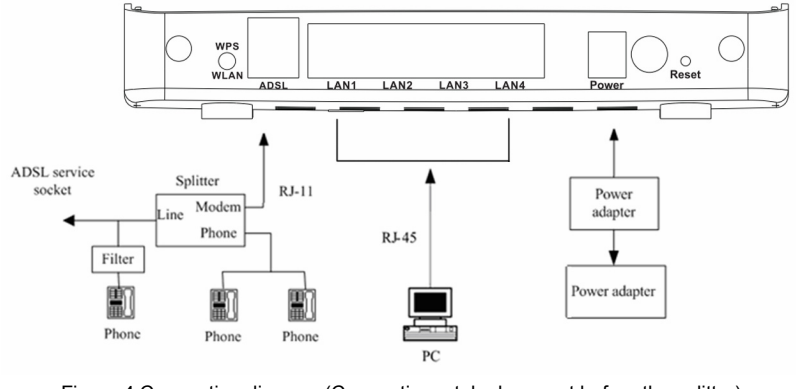


Figure 4 Connection diagram (Connecting a telephone set before the splitter)

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. Do not use the splitter to replace the filter.

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

3 About the Web Configuration

This chapter describes how to configure the router by using the Web-based configuration utility.

3.1 Access the Router

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

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

Step 2 In the **Login** page that is displayed, enter the username and password.

Figure 5 Login window

Note:

The username and password of the super user are **admin** and **admin**.

The username and password of the common user are **user** and **user**.

If you log in as a super user, you can check, configure and modify all the settings.

If you log in as a common user, you can check the status of the router, but can not configure the most of the settings.

Note:

In the Web configuration page, you can click **Apply Changes** to save the settings temporarily. If you want to save the settings of this page permanently, click **save** of **Attention** that appears on the left pane of the Web page after the configuration.

3.2 Wizard

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.

The **Wizard** page guides fast and accurate configuration of the Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **Next** to enable your Internet connection. In the navigation bar, choose **Wizard**. The page shown in the following figure appears.

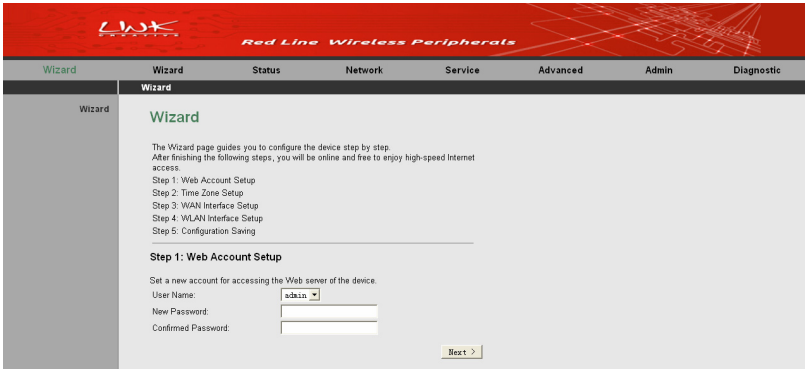


Figure 6 Web account setup

Enter the correct password and then click **Next**. The page shown in the following figure appears. In this page, you can set the system time and Network Time Protocol (NTP) server.

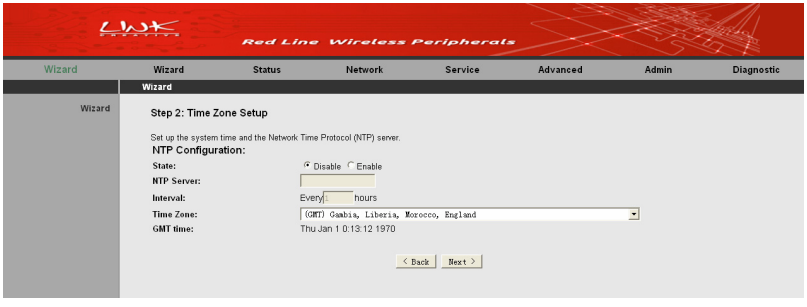


Figure 7 Time zone setup

The following table describes the parameters in this page.

Field	Description
State	You can disable or enable NTP function. You have to enable it if you want to configure the parameters in this page.
NTP Server	Enter the IP address of the specified time server manually.
Interval	Set the interval that the router obtains the time from the time server. That is, the interval that the router verifies the time with the server.
Time Zone	Choose the time zone of your country.
GMT time	Display the Greenwich mean time.

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

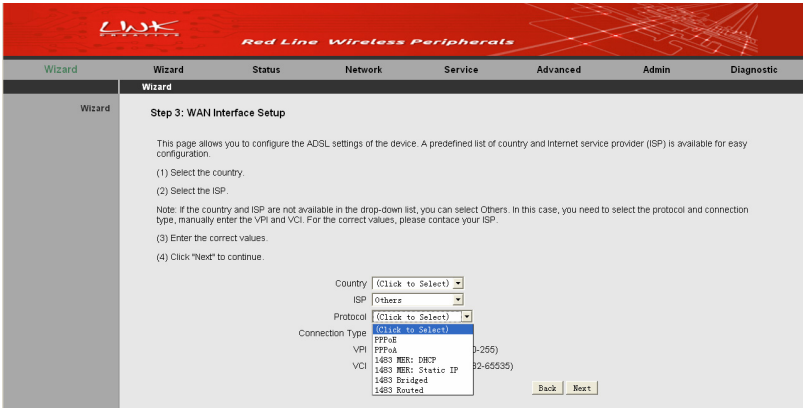


Figure 8 WAN interface setup

The router provides 6 types of WAN connection protocols. They are **PPPoE**, **PPPoA**, **1483 MER:DHCP**, **1483 MER:Static IP**, **1483 Bridged**, and.**1483 Routed**. The following wizard settings will vary depending on the protocol you select.

- **PPPoE/PPPoA**

If you select the **PPPOE** protocol, the page shown in the following figure appears.

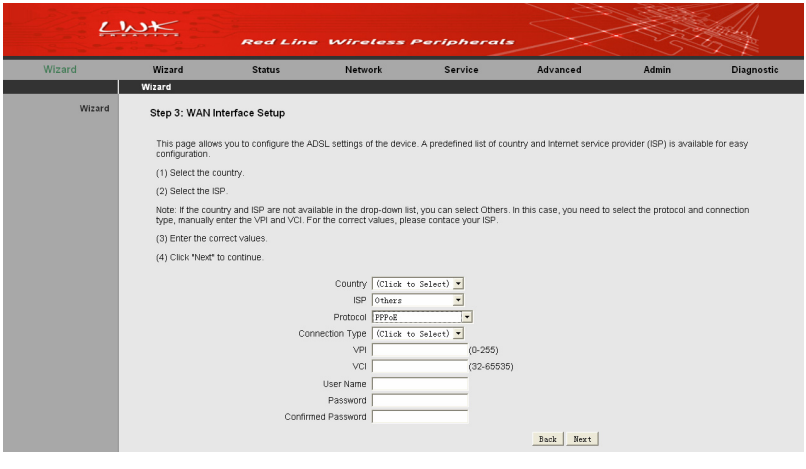


Figure 9 WAN interface setup (PPPoE)

The following table describes the parameters in this page:

Field	Description
Country	Select the country from the drop-down list of **Country**.
ISP	Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
Protocol	Select PPPoE.
Connection Type	You can select **VC-Mux** or **LLC**.
VPI	Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
VCI	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).
User name	The correct user name that your ISP provides to you.
Password	The correct password that your ISP provides to you.
Confirm Password	Enter the password again.

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

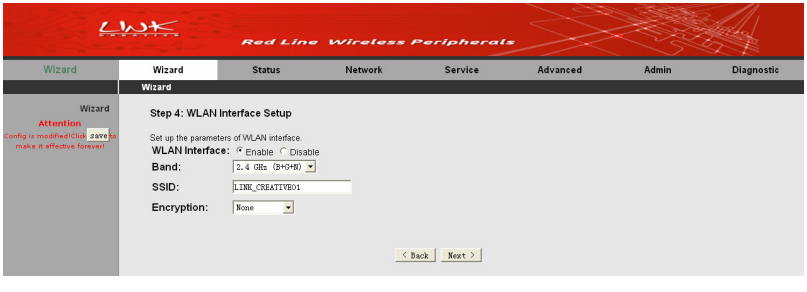


Figure 10 WLAN interface setup (PPPoE)

The following table describes the parameters in this page.

Field	Description
WLAN Interface	You can choose **Enable** or **Disable**. By default, WAN interface is enabled. You need to enable WAN interface, and then you can set the parameters in this page.
Band	Choose the working mode of the router.
SSID	The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the router.
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the router through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.

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

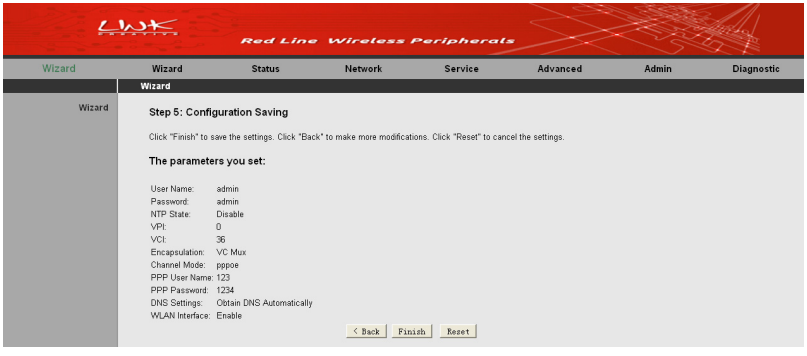


Figure 11 Configuration summary (PPPoE)

In this page, click **Finish** to complete the wizard configuration of PPPoE. You can modify the settings by clicking the **< Back** button if necessary. Click **Reset** to cancel the settings.

Note:

If the WAN connection protocol is set to **PPPoA**, the configuration steps are similar to that of **PPPoE**. For the parameters in these pages, refer to the parameter description of **PPPoE**.

- **1483 MER: DHCP**

If you select the **1483 MER: DHCP** protocol, the page shown in the following figure appears.

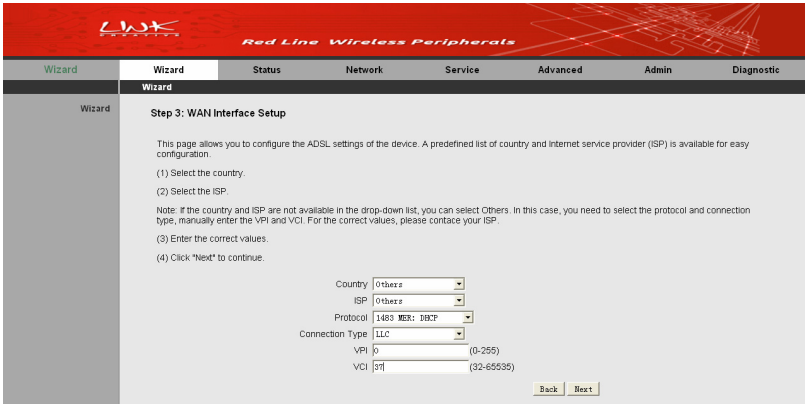


Figure 12 WAN interface setup (1483 MER:DHCP)

The following table describes the parameters in this page.

Field	Description
Country	Select the country from the drop-down list of **Country**.
ISP	Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
Protocol	Select **1483 MER: DHCP**.
Connection Type	You can select **LLC** or **VC-Mux**.
VPI	Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
VCI	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).

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

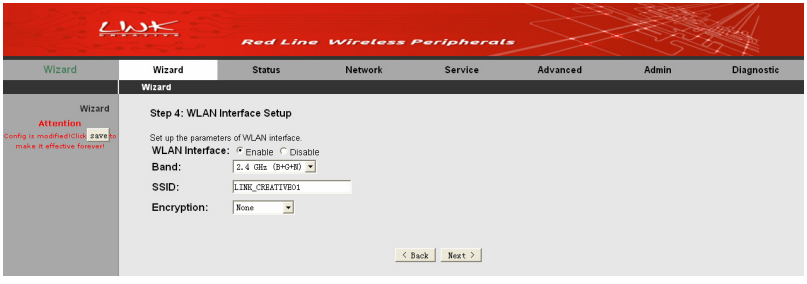


Figure 13 WLAN interface setup (1483 MER:DHCP)

The following table describes the parameters in this page.

Field	Description
WLAN Interface	You can choose **Enable** or **Disable**. By default, WAN interface is enabled. You need to enable WAN interface, and then you can set the parameters in this page.
Band	Choose the working mode of the router.
SSID	The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the router.
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the router through WPA or

Field	Description
	WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.

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

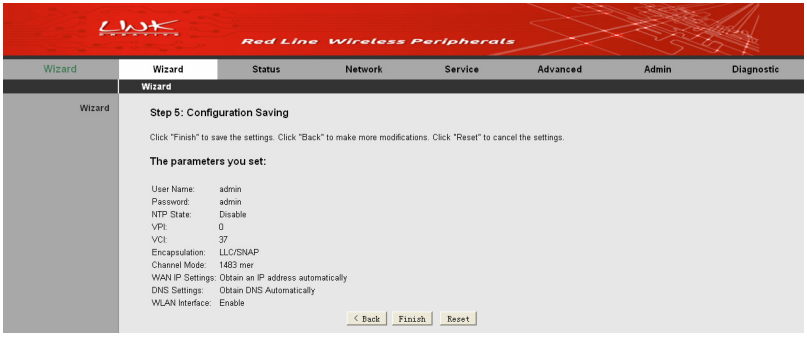


Figure 14 Configuration summary (1483 MER:DHCP)

In this page, click **Finish** to complete the wizard configuration of1**483 MER:DHCP**. You can modify the settings by clicking the **< Back** button if necessary. Click **Reset** to cancel the settings.

- **1483 MER: Static IP/1483 Routed**

If you select the **1483 MER: Static IP** protocol, the page shown in the following figure appears.

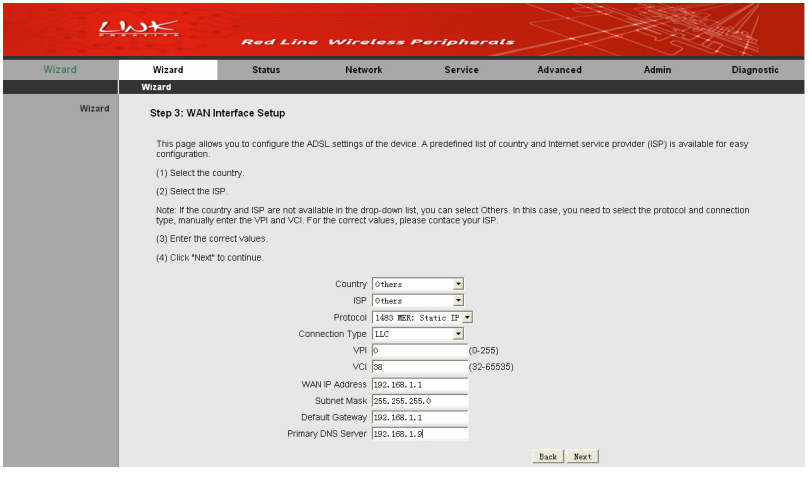


Figure 15 WAN interface setup (1483 MER: Static IP)

The following table describes the parameters in this page.

Field	Description
Country	Select the country from the drop-down list of **Country**.
ISP	Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
Protocol	Select **1483 MER: Static IP**.
Connection Type	You can select **LLC** or **VC-Mux**.
VPI	Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
VCI	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).
WAN IP Address	Enter the IP address of the WAN interface provided by your ISP.
Subnet Mask	Enter the subnet mask concerned to the IP address of

	the WAN interface provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server	Enter the primary DNS server provided by your ISP.

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

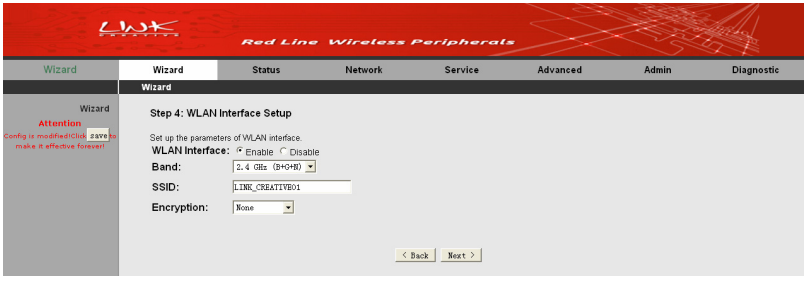


Figure 16 WLAN interface setup (1483 MER: Static IP)

The following table describes the parameters in this page.

Field	Description
WLAN Interface	You can choose **Enable** or **Disable**. By default, WAN interface is enabled. You need to enable WAN interface, and then you can set the parameters in this page.
Band	Choose the working mode of the router.
SSID	The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the router.
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**.

Field	Description
	● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the router through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.

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

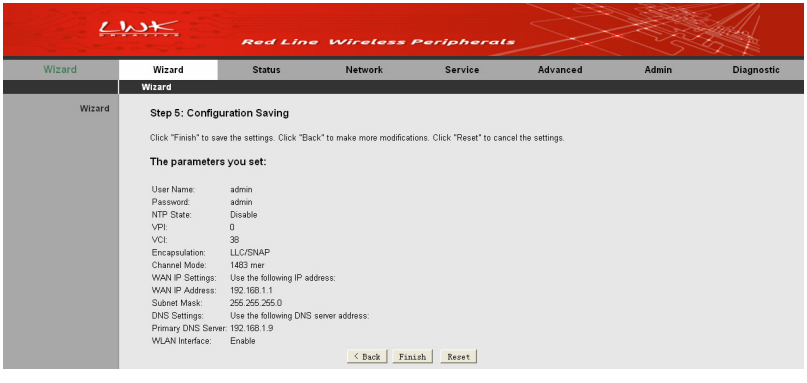


Figure 17 Configuration summary (1483 MER: Static IP)

In this page, click **Finish** to complete the wizard configuration of1**483 MER:Static IP**. You can modify the settings by clicking the **< Back** button if necessary. Click **Reset** to cancel the settings.

Note:

If the WAN connection protocol is set to **1483 Routed**, the configuration steps are similar to that of **1483 MER: Static IP**. For the parameters in these pages, refer to the parameter description of **1483 MER: Static IP**.

- **1483 Bridged**

If you select the **1483 Bridged** protocol, the page shown in the following figure appears.

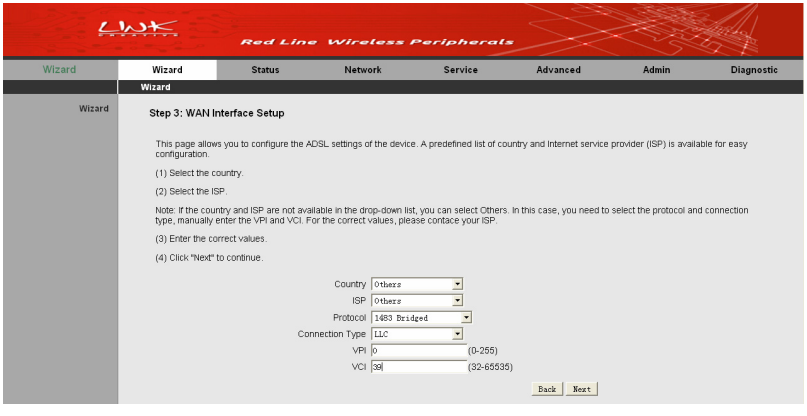


Figure 18 WAN interface setup (1483 Bridged)

The following table describes the parameters in this page.

Field	Description
Country	Select the country from the drop-down list of **Country**.
ISP	Select the ISP according to the country from the drop-down list. If you do not find the ISP that matches the country, you can select **Others**.
Protocol	Select **1483 Bridged**.
Connection Type	You can select **LLC** or **VC-Mux**.
VPI	Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
VCI	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).

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

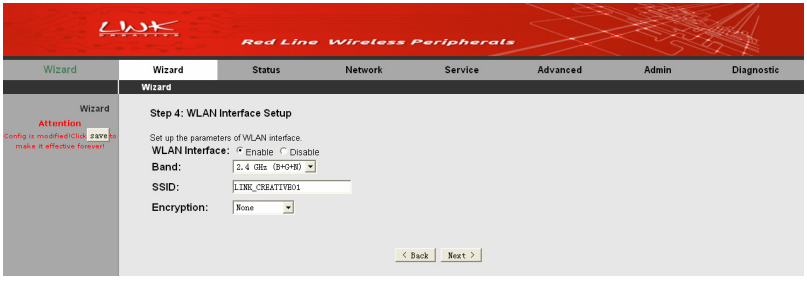


Figure 19 WLAN interface setup (1483 Bridged)

The following table describes the parameters in this page.

Field	Description
WLAN Interface	You can choose **Enable** or **Disable**. By default, WAN interface is enabled. You need to enable WAN interface, and then you can set the parameters in this page.
Band	Choose the working mode of the router.
SSID	The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the router.
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network.

Field	Description
	● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the router through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.

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

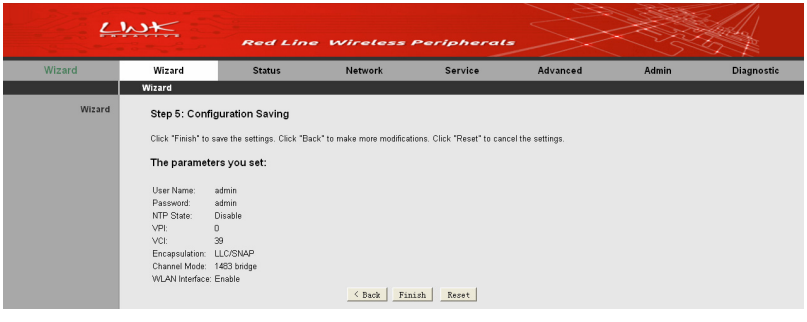


Figure 20 Configuration summary (1483 Bridged)

In this page, click **Finish** to complete the wizard configuration of **1483 Bridged**. You can modify the settings by clicking the **< Back** button if necessary. Click **Reset** to cancel the settings.

3.3 Status

In the navigation bar, choose **Status**. The submenus of **Status** contain **Device Info**, **LAN**, **WLAN**, **WAN**, **Port Mapping, Statistics**, and **ARP**.

3.3.1 System

Choose **Status** > **Device Info**. The page that is displayed shows the current status and some basic settings of the router, such as uptime, firmware version, upstream and downstream speed.

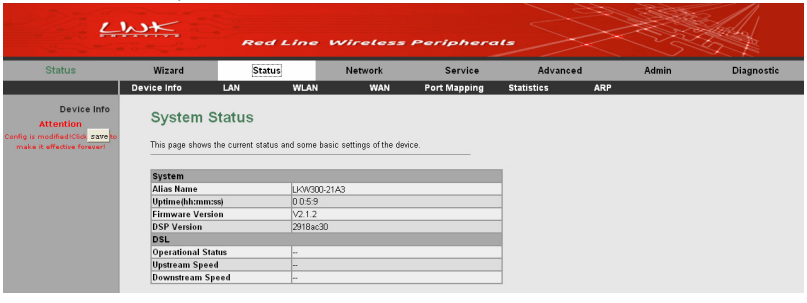


Figure 21 System status

3.3.2 LAN

Choose **Status** > **LAN**. The page that is displayed shows some basic LAN settings of the router. In this page, you can view the LAN IP address, DHCP server status, MAC address, and DHCP client table.

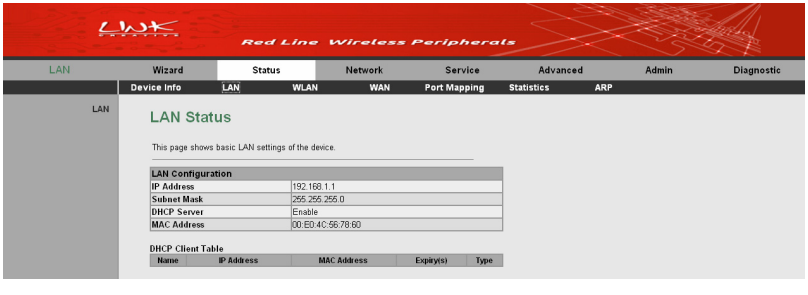


Figure 22 LAN status

3.3.3 WLAN

Choose **Status** > **WLAN**. The page that is displayed shows some basic settings of wireless LAN (WLAN).

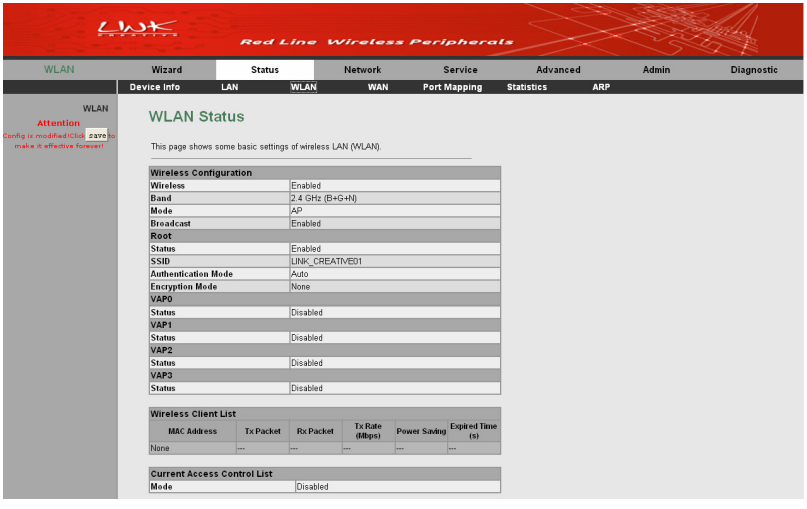


Figure 23 WLAN status

3.3.4 WAN

Choose **Status** > **WAN**. The page that is displayed shows some basic WAN settings of the router.

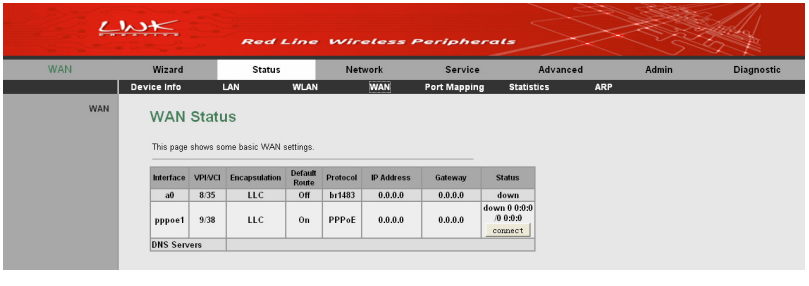


Figure 24 WAN status

3.3.5 Port Mapping

Choose **Status** > **Port Mapping**. In this page, you can view the mapping relation and the status of port mapping.

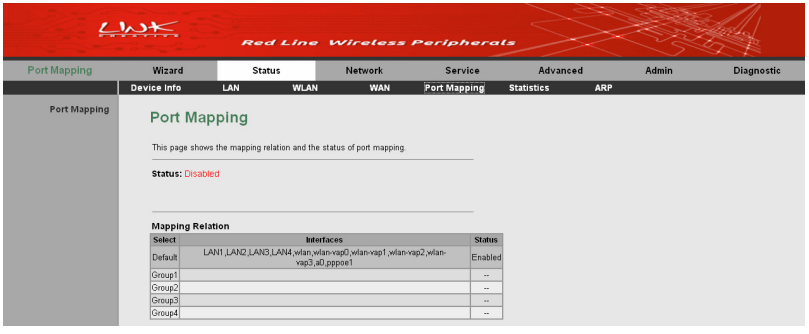


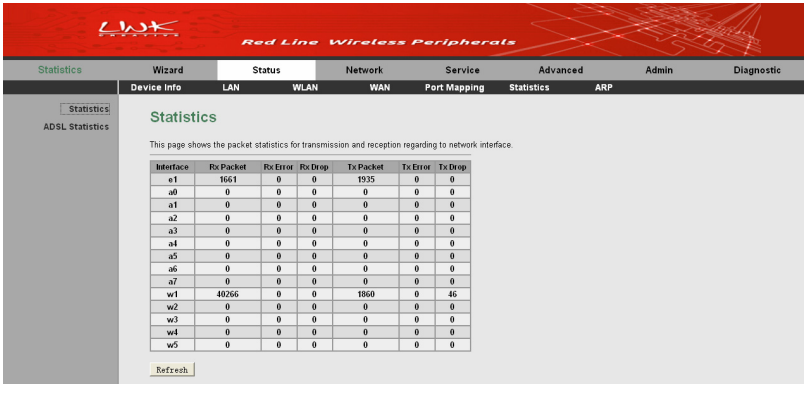
Figure 25 Port mapping

3.3.6 Statistics

Choose **Status** > **Statistics.** The submenus of **Statistics** contain **Statistics** and **ADSL Statistics**.

3.3.6.1 Statistics

Click **Statistics** on the left pane. The page shown in the following figure appears. In this page, you can view the statistics of each network port.



Interface	Rx Packet	Rx Error	Rx Drop	Tx Packet	Tx Error	Tx Drop
e1	1661	0	0	1935	0	0
a0	0	0	0	0	0	0
a1	0	0	0	0	0	0
a2	0	0	0	0	0	0
a3	0	0	0	0	0	0
a4	0	0	0	0	0	0
a5	0	0	0	0	0	0
a6	0	0	0	0	0	0
a7	0	0	0	0	0	0
w1	40266	0	0	1860	0	46
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0

Figure 26 Interface statistics

3.3.6.2 ADSL Statistics

Click **ADSL Statistics** on the left pane. The page shown in the following figure appears. In this page, you can view the ADSL line status, upstream rate, downstream rate, and other information.

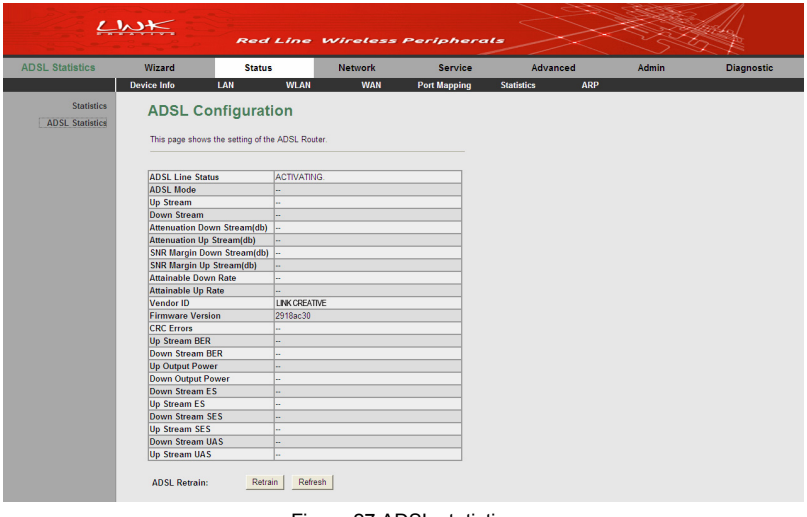


Figure 27 ADSL statistics

3.3.7 ARP

Choose **Status** > **ARP**. In the **ARP Table** page, you can view current ARP entries.

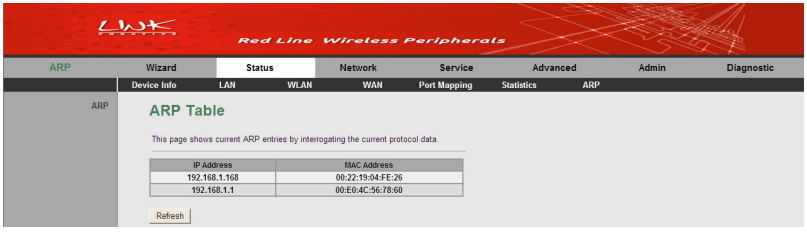


Figure 28 ARP information

3.4 Network

In the navigation bar, click **Network**. The submenus of **Network** contain **LAN**, **WAN**, and **WLAN.**

3.4.1 LAN

Choose **Network** > **LAN**. The **LAN** page that is displayed contains **LAN IP**, **DHCP**, and **DHCP Static IP**.

3.4.1.1 LAN IP

Click **LAN IP** on the left pane. The page shown in the following figure appears.
In this page, you can change IP address of the router. The default IP address is 192.168.1.1, which is the private IP address of the router.

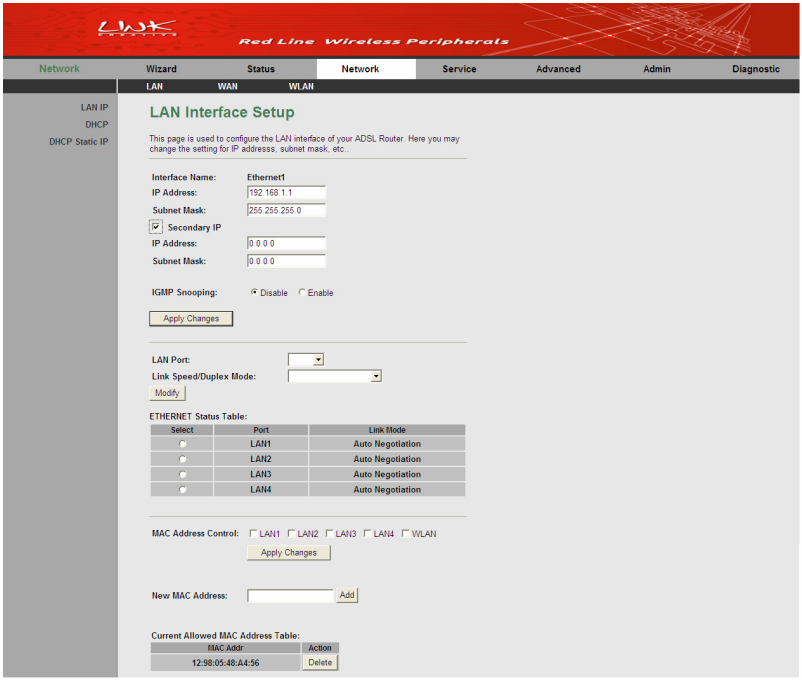


Figure 29 LAN interface setup

The following table describes the parameters in this page.

Field	Description
Interface Name	Display the interface name.
IP Address	Enter the IP address 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 the checkbox to enable the secondary LAN

Field	Description
	IP. The two LAN IP addresses must be in the different networks. After you select it, you need to enter the IP address and subnet mask.
IGMP Snooping	Enable or disable IGMP Snooping.
LAN Port	You can choose the LAN interface you want to configure.
Link Speed/Duplex Mode	You can select the proper mode from the drop-down list.
MAC Address Control	An access control function based on MAC addresses. When this function is enabled, hosts of the MAC addresses in the **Current Allowed MAC Address Table** can access the modem.
New MAC Address	Enter a MAC address, and then click **Add** to add a new MAC address.

After setting, click the **Apply Changes** button to save the settings.

3.4.1.2 DHCP

Dynamic Host Configuration Protocol (DHCP) allows the individual PC to obtain 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.
Click **DHCP** on the left pane and the page shown in the following figure appears.

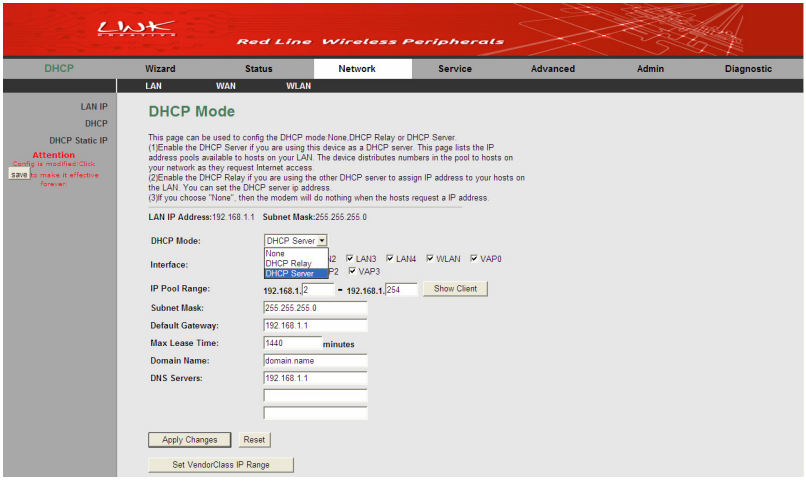


Figure 30 DHCP mode configuration

In this page, you can select different DHCP modes. You may select **None**, **DHCP Relay**, and **DHCP server**.

- **None**

Select **None** from the drop-down list of **DHCP Mode**, and the page as shown in the following figure appears.

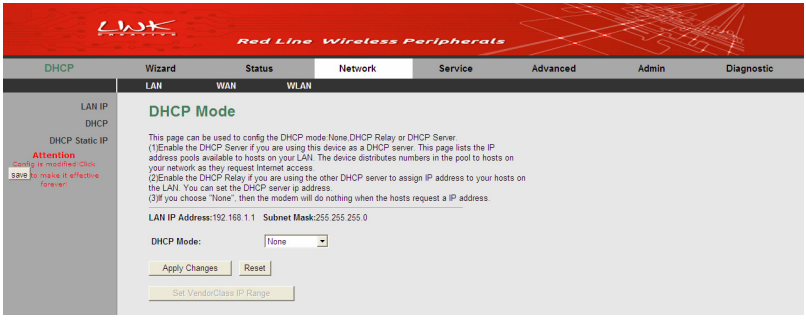


Figure 31 DHCP mode (None)

If you set the DHCP mode to be **None**, the router does not assign the IP address to the host when it requests an IP address.

- **DHCP Relay**

Select **DHCP Relay** from the drop-down list of **DHCP Mode**, and the page as shown in the following figure appears.

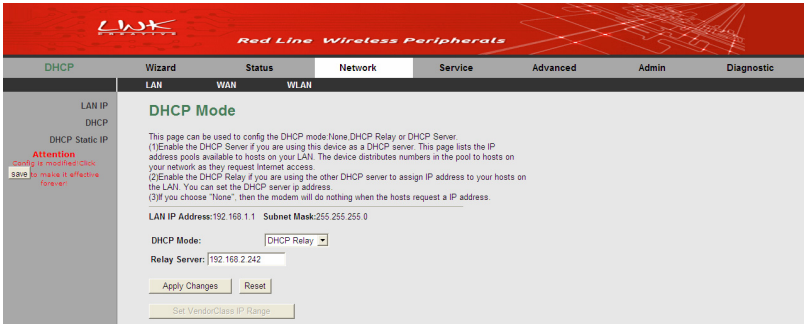


Figure 32 DHCP mode (DHCP relay)

Set the DHCP mode to be **DHCP Relay** if you are using another DHCP server to assign an IP address to your hosts on the LAN. You can set the IP address of the relay server.

The following table describes the parameters in this page:

Field	Description
DHCP Mode	If you select **DHCP Relay**, the router acts as a surrogate DHCP Server, and relays the DHCP requests and responses between the remote server and client.
Relay Server	Enter the relay server address provided by your ISP.

- **DHCP Server**

Select **DHCP Serer** from the drop-down list of **DHCP Mode**, and the page as shown in the following figure appears.

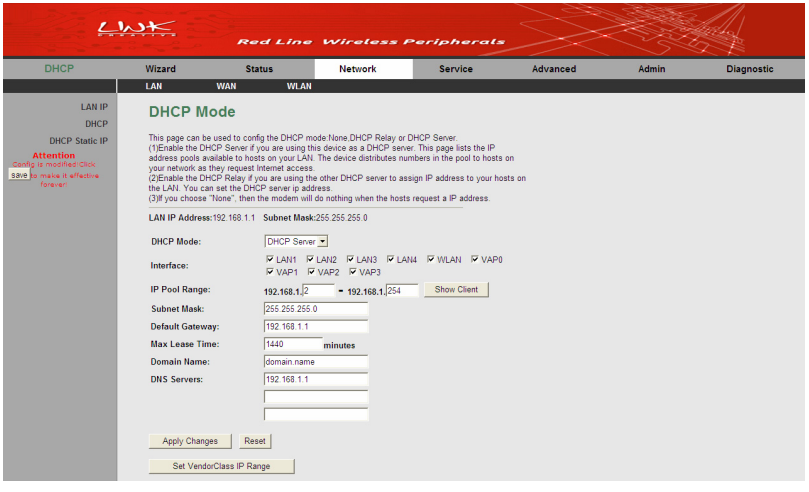


Figure 33 DHCP mode (DHCP server)

Set the DHCP mode to be **DHCP Server** if you are using this device as a DHCP server. This page lists an IP address pool available to the hosts on your LAN. The router assigns IP addresses in the pool to the hosts on your network when they request Internet access.

The following table describes the parameters and buttons in this page:

Field	Description
DHCP Mode	If you select **DHCP Server**, the router can assign IP addresses, IP default gateway and DNS servers to the hosts that are on Windows95, Windows NT and other systems that support the DHCP client.
Interface	Select the network interfaces. DHCP only assigns IP addresses to the selected interfaces.
IP Pool Range	It specifies the first and the last of contiguous IP

Field	Description
	address in the IP address pool.
Show Client	Click this button to display the **Active DHCP Client Table** page. It shows the assigned IP addresses of the clients.
Subnet Mask	Enter the subnet mask of IP address pool.
Default Gateway	Enter the IP default gateway of the IP address pool.
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 this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
DNS Servers	Enter the DNS server addresses.
Set Vendor Class IP Range	Click this button to display the **Device IP Range Table** page. You can configure the IP address range based on the device type.

- **Active DHCP Client List**

Click **Show Client** in the **DHCP Mode** page, and the page as shown in the following figure appears.

Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

Name	IP Address	MAC Address	Expiry(s)	Type

Refresh Close

Figure 34 Active DHCP client table

In this page, you can view the IP addresses assigned to the DHCP clients.

- **Device IP Range Table**

Click **Set VendorClass IP Range** (DHCP server mode) in the **DHCP Mode** page, and the page as shown in the following figure appears.

Device IP Range Table

This page is used to configure the IP address range based on device type.

device name:
start address: 192.168.1.
end address: 192.168.1.
router address:
option60

add delete modify Close

IP Range Table:

Select	device name	start address	end address	default gateway	option60

Figure 35 Device IP range table

In this page, you can configure the IP address range based on the device type. The following table describes the parameters and buttons in this page.

Field	Description
device name	Enter the name of device that needs an IP address assigned by DHCP.
Start address	Enter the start IP address assigned by DHCP.
end address	Enter the end IP address assigned by DHCP.
router address	Enter the routing gateway address of assigned IP.
Option 60	Enter the string identifier of the assigned device.
add	Click this button to add a new rule.
delete	Click this button to delete a rule.
modify	Click this button to modify the rule.
Close	Click this button to close current window.

3.4.1.3 DHCP Static IP

Click **DHCP Static IP** on the left pane and the page shown in the following figure appears. You can assign the IP addresses on the LAN to the specific individual PCs based on their MAC address.

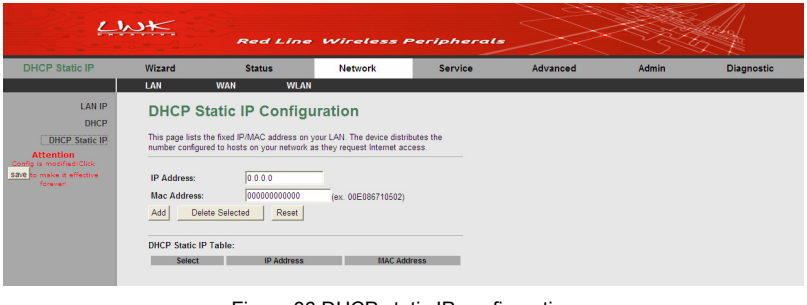


Figure 36 DHCP static IP configuration

The following table describes the parameters and buttons in this page.

Field	Description
IP Address	It specifies the IP address of the IP address pool.
MAC Address	Enter the MAC address of a PC in the LAN.
Add	After entering the IP address and MAC address, click this button to add an entry to the **DHCP Static IP Table**.
Delete Selected	Select an entry in the **DHCP Static IP Table**, and then click this button to delete the selected entry.
Reset	Click this button to reset the values in this page.
DHCP Static IP Table	It shows the assigned IP addresses based on the MAC addresses.

3.4.2 WAN

Choose **Network** > **WAN**. The submenus of **WAN** contain **WAN**, **Auto PVC**, **ATM Settings**, and **ADSL Settings**.

3.4.2.1 WAN

Click **WAN** on the left pane and the page shown in the following figure appears.

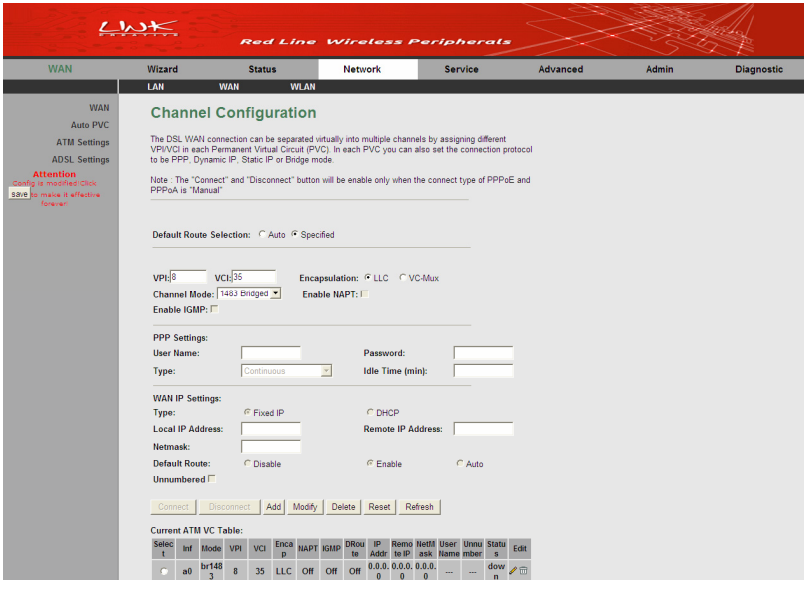


Figure 37 Channel configuration

In this page, you can configure the WAN interface of your router. You can add, delete, or modify a PVC entry. This page provides 6 types of channel modes, including **1483 Bridged**, **1483 MER**, **PPPoE**, **PPPoA**, **1483 Routed** and **IPoA**.

The following table describes the parameters and buttons in this page:

Field	Description
Default Route Selection	You can choose **Auto** or **Specified**.
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)
Encapsulation	You can choose **LLC** and **VC-Mux**.
Channel Mode	You can choose **1483 Bridged**, **1483 MER**, **PPPoE**, **PPPoA**, **1483 Routed** or **IPoA**.
Enable NAPT	Select it to enable the NAPT function of the

Field	Description
	router. If you do not select it and you want to access the Internet normally, you must add a route on the uplink device. Otherwise, the access to the Internet fails. Normally, it is required to enable NAPT.
Enable IGMP	You can enable or disable IGMP function.
PPP Settings	
User Name	Enter the correct user name provided by your ISP.
Password	Enter the correct password provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand**, or **Manual** if the channel mode is set to PPPoE or PPPoA.
Idle Time (min)	When selecting **Connect on Demand**, you need to enter the time of idle timeout. Within the preset time, if the router does not detect the flow from the user end continuously, the router automatically disconnects the PPPoE or PPPoA connection.
WAN IP Settings	
Type	You can choose **Fixed IP** or **DHCP**. ● If you select Fixed IP, you should enter the local IP address, remote IP address and subnet mask. ● If you select DHCP, the router serves as a DHCP client, and the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of the WAN interface provided by your ISP.
Remote IP Address	Enter the gateway IP address that is provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.

Field	Description
Default Route	You may select **Disable**, **Enable**, or **Auto**.
Unnumbered	Select this checkbox to enable the IP Unnumbered function.

You can edit the parameters of an entry in the **Current ATM VC Table** by clicking the icon . If you click the icon of an entry, this entry can be deleted.

The following describes how to configure a PPPoE (0/32) connection.

Note:

The figures and the configuration steps below are illustrated as an example. The figures and configuration description may vary according to the channel mode that you select.

Step 1 Set the VPI to **0**, VCI to **32**.

Step 2 Select **PPPoE** as the channel mode.

Step 3 Enter the user name and password provided by your ISP for PPPoE dial-up.

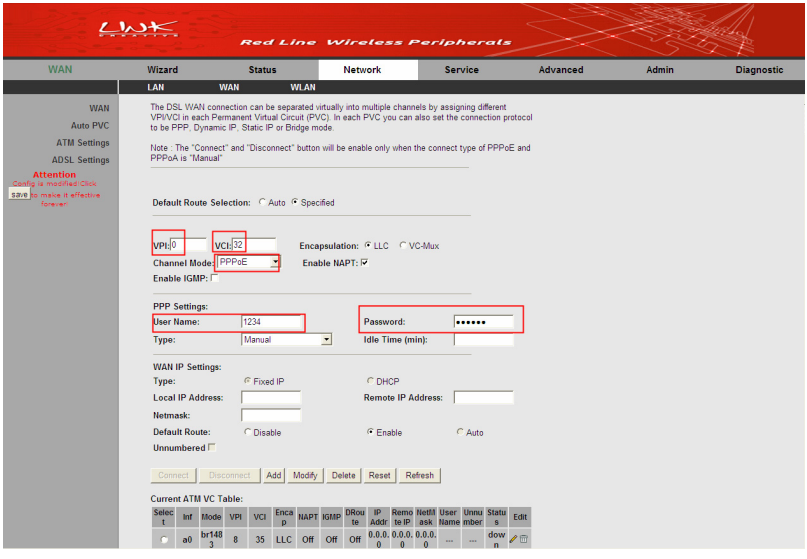


Figure 38 Configuring the parameters of PPPoE connection

Step 4 Click **Add** to add the PVC to the **Current ATM VC Table**.

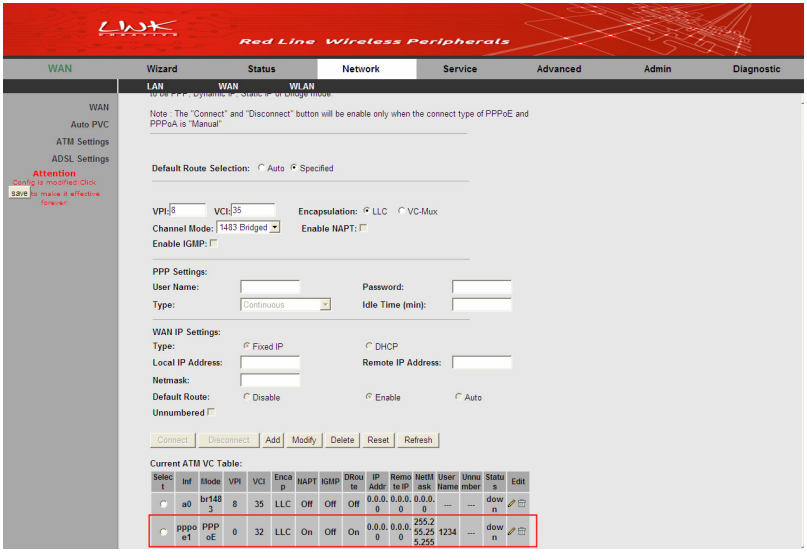


Figure 39 Adding a PPPoE connection

3.4.2.2 Auto PVC

Click **Auto PVC** on the left pane and the page shown in the following figure appears.

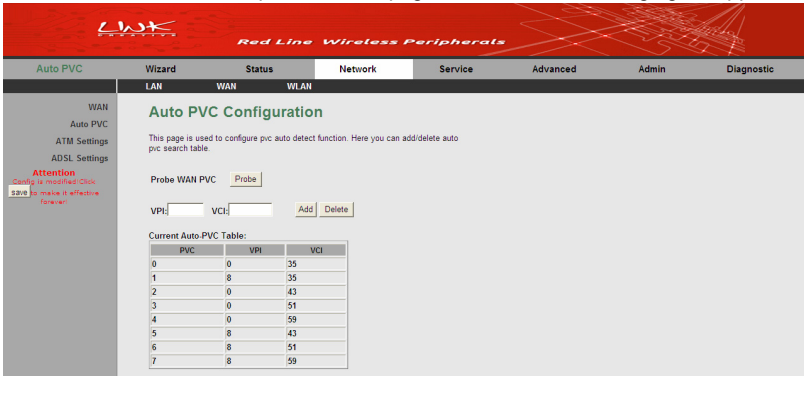


Figure 40 Auto PVC configuration

In this page, you can add or delete an entry of auto PVC.
The following table describes the parameters and buttons in this page.

Field	Description
Probe WAN PVC	Click the **Probe** button and system automatically detects current PVCs supported by the office end.
VPI	Enter the VPI value.
VCI	Enter the VCI value.

After setting, click the **Add** button to an entry of auto PVC to the **Current Auto-PVC** table.

3.4.2.3 ATM Settings

Click **ATM Setting** on the left pane. The page shown in the following figure appears. In this page, you can configure the parameters of the ATM, such as QoS, PCR, CDVT, and SCR.

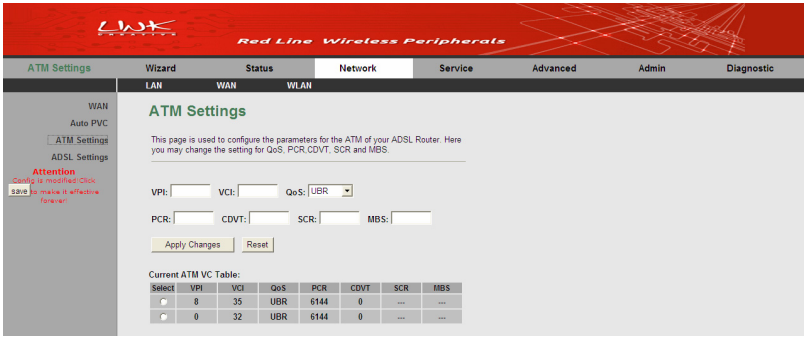


Figure 41 ATM settings

The following table describes the parameters of this page:

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose **UBR**, **CBR**, **nrt-VBR**, or **rt-VBR**.
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to 4294967295.
SCR	Subtain cell rate (SCR) is the maximum rate that traffic can pass over a PVC without the risk of cell loss. Its value ranges from 0 to 65535.
MBS	Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR. Its value ranges from 0 to 65535.

After finishing setting, click **Apply Changes** to save the settings.

3.4.2.4 ADSL Settings

Click **ADSL Settings** on the left pane. The page shown in the following figure appears.

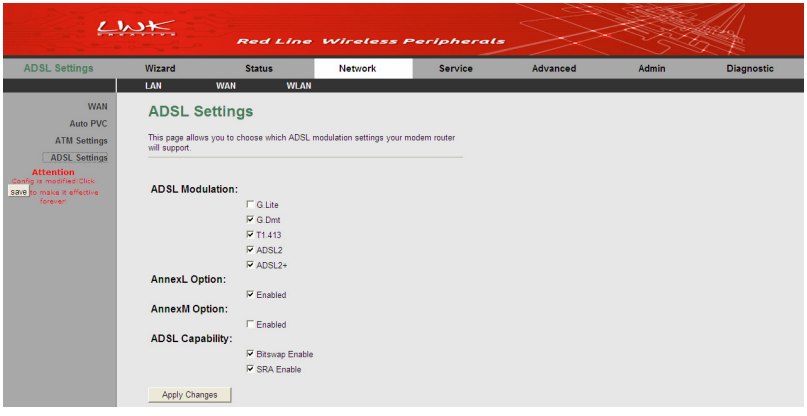


Figure 42 ADSL settings

In this page, you can select the DSL modulation schemes. Usually, you do not need to change the factory default settings. The ADSL modulation schemes that router supports contain **G.lite**, **G.Dmt**, **T1.413**, **ADSL2**, and **ADSL2+**. The router negotiates the modulation modes with the DSLAM. You can also enable or disable the **AnnexL Option**, **AnnexM Option**, and **ADSL Capability**.

3.4.3 WLAN

3.4.3.1 Basic Settings

Choose **WLAN** > **Basic** and the following page appears. In this page, you can configure the parameters for wireless LAN clients that may connect to the modem.

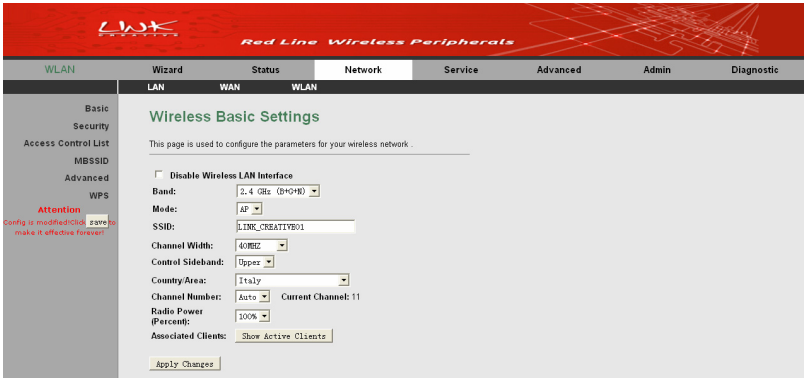


Figure 43 Wireless basic settings

The following table describes the parameters in this page:

Field	Description
Disable Wireless LAN Interface	Enable or disable the wireless LAN interface.
Band	Choose the working mode of the modem.
Mode	Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is **AP**.
SSID	The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.
Channel Width	Choose a proper channel width from the drop-down list.
Control Sideband	You may select **Upper** or **Lower**.
Country/Area	Select the country from the drop-down list.
Channel Number	A channel is the radio frequency used by 802.11b/g/n wireless devices. There are 13

Field	Description
	channels (from 1 to 13) available depending on the 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 different APs overlap. Choose a channel from the drop-down list.
Radio Power	You can choose the transmission power of the radio signal. The default one is **100%**. It is recommended to choose the default value**100%**.
Associated Clients	Click **Show Active Clients** to view the information of the wireless clients that are connected to the modem.

After setting, click **Apply Changes** to save the settings of this page.

3.4.3.2 Security

Choose **WLAN** > **Security** and the following page appears.

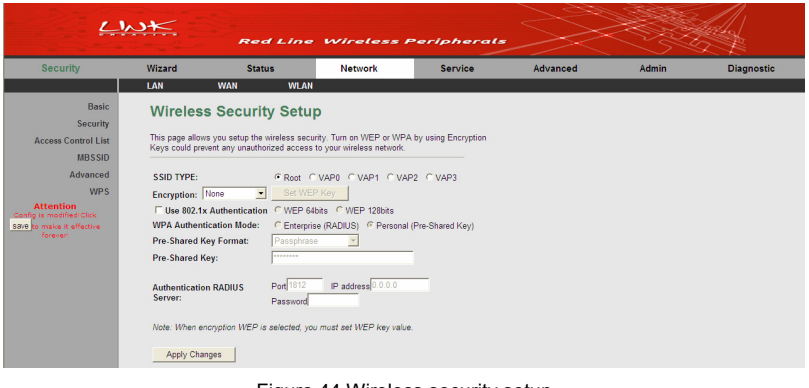


Figure 44 Wireless security setup

The following table describes the parameters in this page:

Field	Description
SSID TYPE	Select the proper SSID type.
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
Set WEP Key	It is available when you set the encryption mode to **WEP**. Click it, and the **Wireless WEP Key Setup** page appears.
Use 802.1x Authentication	Enable or disable 802.1x authentication.
WEP 64bits/WEP 128bits	If the encryption mode is set to **WEP**, you can set the WEP key length.
WPA Authentication Mode	● If you select **Enterprise (RADIUS)**, enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem. ● If you select **Personal (Pre-Shared Key)**, enter the pre-shared key in the **Pre-Shared Key** field. If the encryption is set to **WEP**, the modem uses

Field	Description
	802.1 X authentication, which is Radius authentication.
Pre-Shared Key Format	The WPA key format contains **Passphrase** or **Hex (64 characters)**.
Pre-Shared Key	Set the WPA pre-shared key according to the key format.
Authentication RADIUS Server	Enter the port, IP address, and password of the Radius server.

Click **Set WEP Key**, and the following page appears.

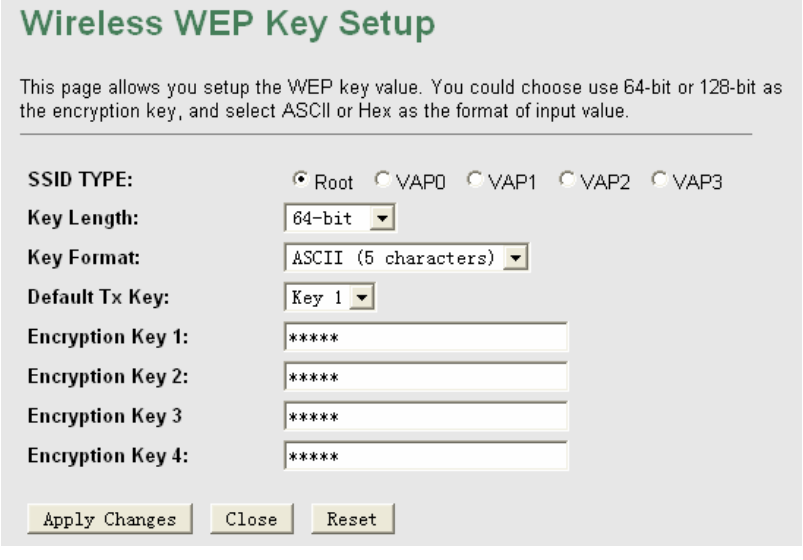


Figure 45 Wireless WEP key setup

In this page, you can set the WEP key.

The following describes the parameters in this page:

Field	Description
SSID TYPE	Select the proper SSID type.
Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Key Format	● If you choose **64-bit**, you can choose ASCII (5 characters) or Hex (10 characters). ● If you choose **128-bit**, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Choose the index of WEP Key. You can choose **Key 1**, **Key 2**, **Key 3**, or **Key 4**.
Encryption Key 1 ~ 4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. ● If you choose **64-bit** and **ASCII (5 characters)**, enter any 5 ASCII characters. ● If you choose **64-bit** and **Hex (10 characters)**, enter any 10 hexadecimal characters. ● If you choose **128-bit** and **ASCII (13 characters)**, enter any 13 ASCII characters. ● If you choose **128-bit** and **Hex (26 characters)**, enter any 26 hexadecimal characters.

After setting, click **Apply Changes** to save the settings of this page.

3.4.3.3 Access Control List

Choose **WLAN** > **Access Control List** and the following page appears.

Figure 46 Wireless access control

In this page, you can configure the access control of the wireless clients.

Select **Allow Listed** in the **Wireless Access Control Mode** field to enable the white list function. Only the devices whose MAC addresses are listed in the **Current Access Control List** can access the router.

Select **Deny Listed** in the **Wireless Access Control Mode** field to enable the black list function. The devices whose MAC addresses are listed in the **Current Access Control List** are denied to access the router.

Select a proper access control mode, and then enter a MAC address. Click the **Add** button to add a MAC entry to the **Current Access Control List**. You may also delete an entry or all entries form this list.

3.4.3.4 MBSSID

Choose **WLAN** > **MBSSID** and the following page appears.

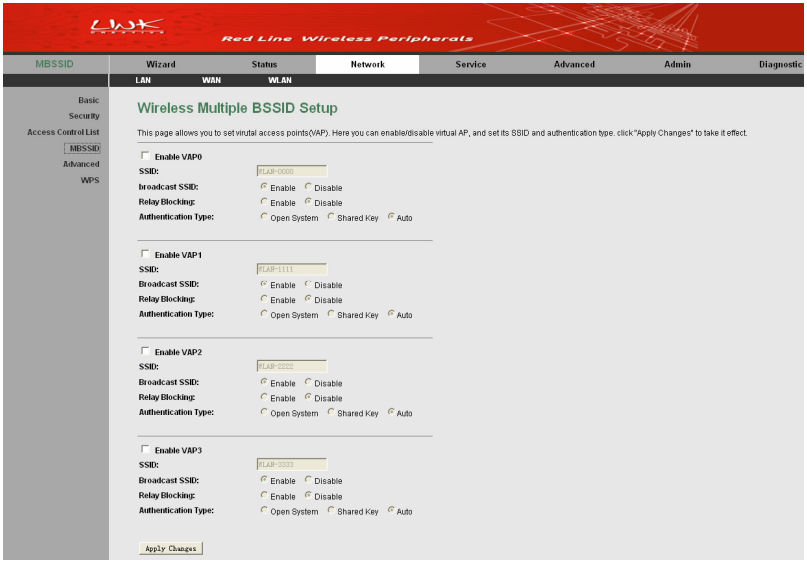


Figure 47 Wireless multiple BSSID setup

In this page, you can configure multiple VAPs (Virtual Access Points).
The following table describes the parameters in this page.

Field	Description
Enable VAP0/1/2/3	Enable or disable the selected VAP.
SSID	The service set identification (SSID) is a unique name to identify the router in the wireless LAN.
Relay Blocking	Enable or disable relay blocking.
Broadcast SSID	Enable this function if you want to hide any access point, so a station cannot obtain the SSID through passive scanning.
Authentication Type	You may select **Open System**, **Shared key** or **Auto**.

After finishing the settings, click the **Apply Changes** button to apply the settings.

3.4.3.5 Advanced Settings

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

Note:

The parameters in the **Wireless Advanced Settings** page can only be modified by the professional personnel. It is recommended that you keep the default values.

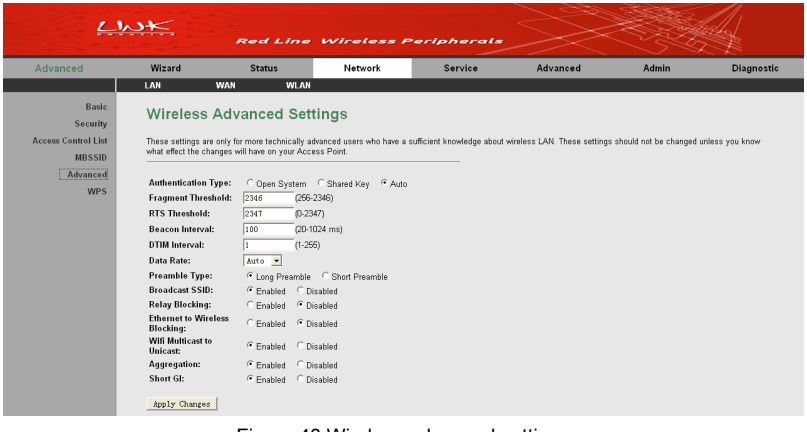


Figure 48 Wireless advanced settings

In this page, you can configure the wireless advanced parameters.
The following table describes the parameters in this page.

Field	Description
Authentication Type	You can choose **Open System**, **Shared Key**, or **Auto**. In the open system mode, the wireless client can directly connect to the device In the encryption authentication mode, the wireless client connects to the router through the shared

Field	Description
	key.
Fragment Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
RTS Threshold	If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
Beacon Interval	Beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). The default value is recommended.
DTIM Interval	Set the proper DTM value. The DTIM Interval determines the number of AP beacons between each Delivery Traffic Indication Message (DTIM). This informs clients of the next window for listening to broadcast and multicast messages.
Data Rate	Choose the proper transmission rate in the drop-down list.
Preamble Type	Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems

Field	Description
	like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble only if the 54g mode is set to 802.11b.
Broadcast SSID	Select whether the router broadcasts SSID or not. You can select **Enable** or **Disable**. ● Select **Enable**, and the wireless client searches the router through broadcasting SSID. ● Select **Disable** to hide SSID, and the wireless clients can not search the SSID.
Relay Blocking	If you select **Enable**, the wireless clients that are connected to the router can not intercommunicate.
Ethernet to Wireless Blocking	Whether the wireless network can communicate with the Ethernet network or not.
Wifi Multicast to Unicast	After enabling this function, the transmission quality of wireless multicast stream can be improved.
Aggregation	It is applied when the destination end of all MPDU are for one STA.
Short GI	It is not recommended to enable GI in obvious environment of Multi-path effect.

After finishing the settings, click **Apply Changes** to save the settings.

3.4.3.6 WPS

Choose **WLAN** > **WPS** and the following page appears.

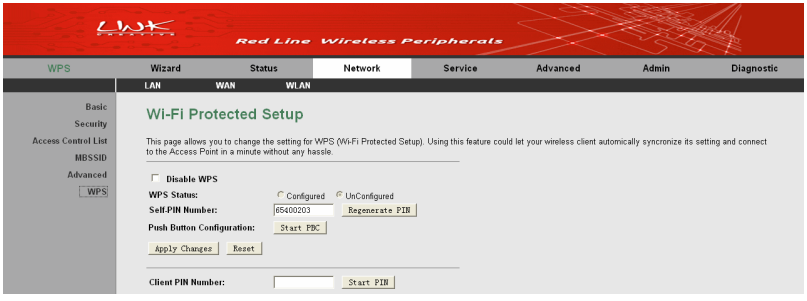


Figure 49 Wi-Fi protected setup

By default, the WPS service is enabled.

This page provides two WPS modes, including PIN and PBC modes.

At present, WPS supports three types of operation modes, including Enrollee mode, Registrar mode, and PBC mode. Enrollee and Registrar modes need to apply PIN code negotiation.

- **Enrollee Mode**

Step1 Select the enrollee mode on the wireless client and the configuration utility of the wireless client will generate a random PIN code, for example, 12345678.

Step2 In the **Wi-Fi Protected Setup** page, enter the PIN code of the wireless client to the **Client PIN Number** field on the wireless router, and then click the **Start PIN** button within 2 minutes. After you click the **Start PIN** button, the wireless router will automatically connect to the wireless client.

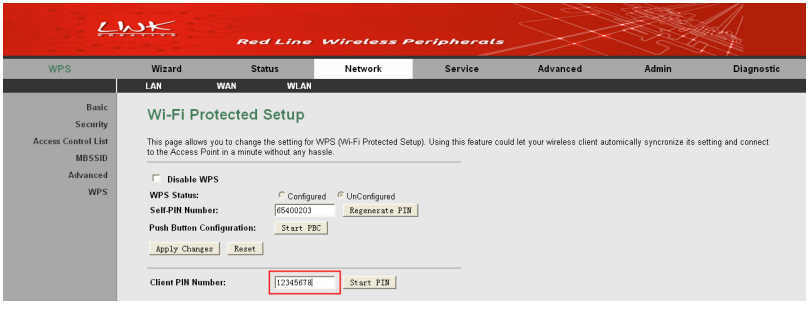


Figure 50 Enrollee mode setup

- **Registrar Mode**

Step1 View the PIN code of the ADSL router in the **Wi-Fi Protected Setup** page, for example, 31668729.

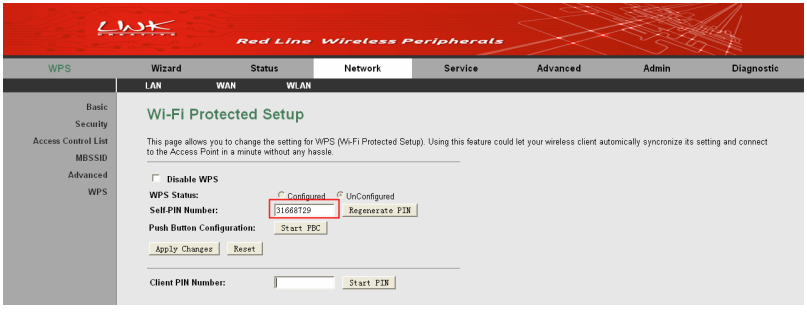


Figure 51 Registrar mode setup (ADSL router)

Step2 Select **Registrar** mode on the wireless client and enter the PIN code of the ADSL router within 2 minutes. After you click the **PIN** button, the wireless client will automatically connect to the ADSL router. See the following figure:

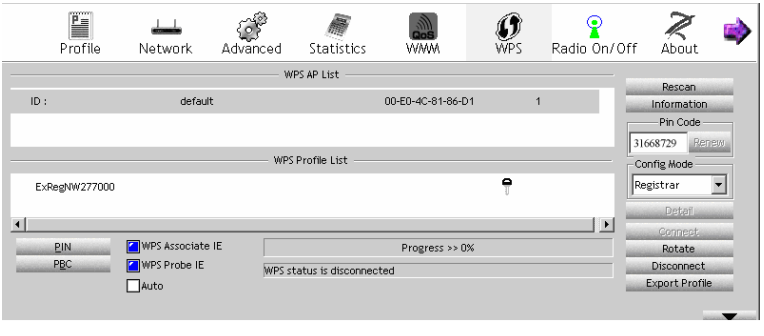


Figure 52 Registrar mode setup (client)

- **PBC Mode**

Step1 In the **Wi-Fi Protected Setup** page, click the **Start PBC** button or press the **WPS** button for more then 3 seconds on the rear panel of the ADSL router.

Step2 Press the WPS button on the wireless client within 2 minutes, and then the ADSL router will automatically establish the connection with the wireless client.

Note:

WPS can only be used with the wireless client devices that have a compatible WPS component.

3.5 Service

In the navigation bar, click **Service**. The submenus of **Service** contain **DNS**, **Firewall**, **UPnP**, **IGMP Proxy**, **TR-069**, and **ACL**.

3.5.1 DNS

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, DNS translates the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4. The DNS 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. Choose **Service** > **DNS**. The submenus of **DNS** include **DNS**, and **DDNS**.

3.5.1.1 DNS

Click **DNS** on the left pane and the following page appears.

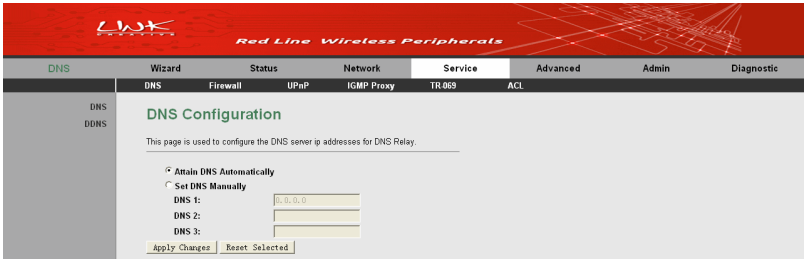


Figure 53 DNS configuration

The following table describes the parameters and buttons of this page:

Field	Description
Attain DNS Automatically	If you select it, the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	If you select it, enter the IP addresses of DNS server.
DNS1-3	Enter the IP addresses of the DNS servers.

After setting, click the **Apply Changes** button to save the settings.

3.5.1.2 DDNS

Click **DDNS** on the left pane, and 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.

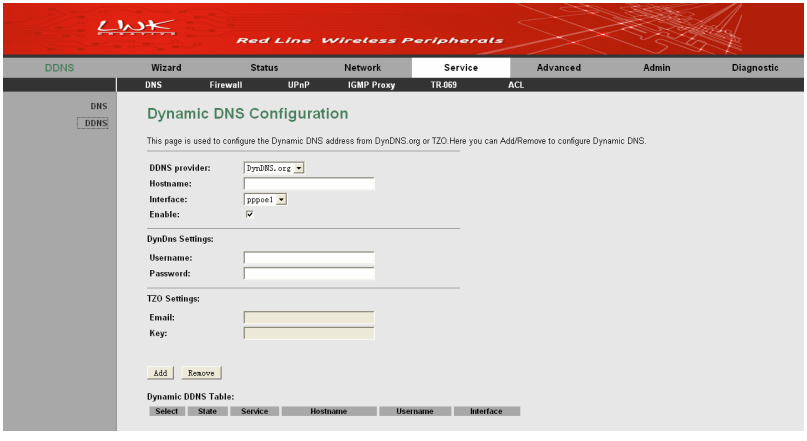


Figure 54 DDNS configuration

This page is used to configure the DDNS settings.
The router supports two providers “DynDNS.org” and “TZO”.
The following table describes the parameters in this page.

Field	Description
DDNS provider	Select the DDNS provider from the drop-down list. You can select **DynDNS.org** or **TZO**.
Hostname	Enter the hostname of DDNS.
Interface	Select the WAN interface of the router.
Enable	Enable or disable DDNS.
DynDns Settings	
Username	Enter the user name provided by DDNS provider.
Password	Enter the password provided by DDNS provider.
TZO Settings	
Email	Enter the email provided by DDNS provider.
Key	Enter the key provided by DDNS provider.

After setting, click the **Add** button to add a DDNS entry to the Dynamic DDNS Table.

3.5.2 Firewall

Choose **Service** > **Firewall**. The submenus of **Firewall** include **IP/Port Filter**, **MAC Filter**, **URL Filter, Anti-DoS**, and **Software Forbidden**.

3.5.2.1 IP/Port Filter

Click **IP/Port Filter** on the left pane, and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.

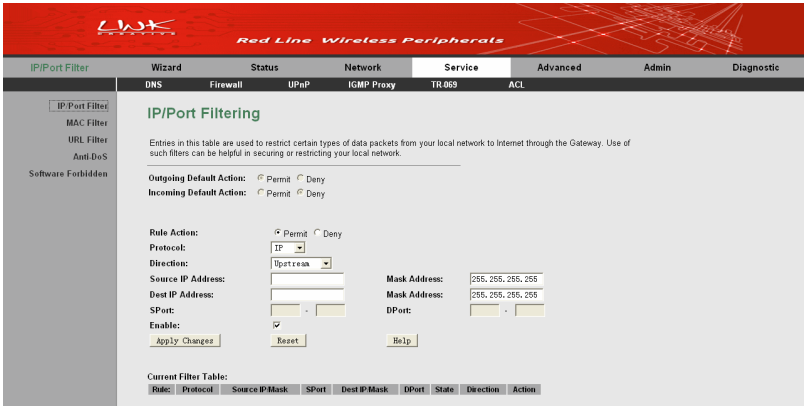


Figure 55 IP/Port filter

The following table describes the parameters in this page.

Field	Description
Outgoing Default Action	You may select **Permit** or **Deny**.
Incoming Default Action	You may select **Permit** or **Deny**.
Rule Action	You may select **Permit** or **Deny**.
Protocol	You may select **IP**, **ICMP**, **TCP**, or **UDP**.
Direction	You may select **Upstream** or **Downstream**.
Source IP	Enter the source IP address and subnet mask.

Field	Description
Address/ Mask Address	
Dest. IP Address/ Mask Address	Enter the destination IP address and subnet mask.
SPort/ DPort	Enter the source port and destination port.
Enable	Enable or disable the rule.

After finishing setting, click **Apply Changes** to add a new rule of the IP/Port filter.

3.5.2.2 MAC Filter

Click **MAC Filter** on the left pane, and the page shown in the following figure appears. Entries in the 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.

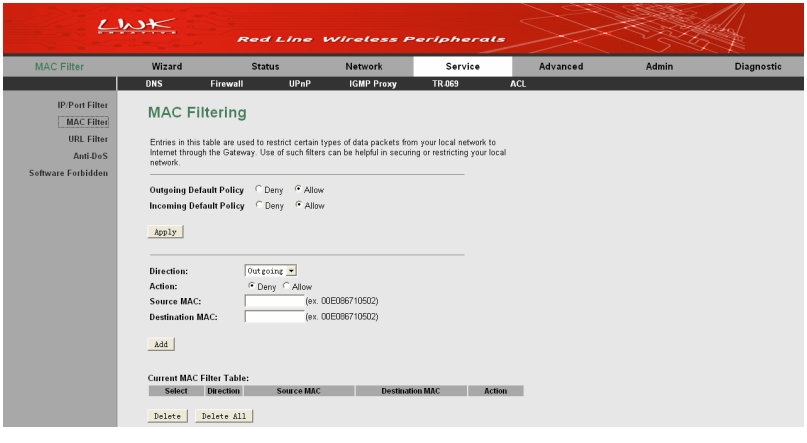


Figure 56 MAC filtering

The following table describes the parameters in this page.

Field	Description
Outgoing Default Policy	You may select **Deny** or **Allow**.
Incoming Default Policy	You may select **Deny** or **Allow**.
Direction	You may select **incoming** or **outcoming**.
Action	You may select **Deny** or **Allow**.
Source MAC	Set the source MAC address of the host that needs to be filtered.
Destination MAC	Set the destination MAC address of the host that needs to be filtered.

After finishing setting, click **Add** to add a new rule of the MAC filter.

3.5.2.3 URL Blocking

Click **URL Filter** on the left pane, and the page shown in the following figure appears. This page is used to block a fully qualified domain name, such as tw.yahoo.comand and filtered keyword. You can add or delete FQDN and filtered keyword.

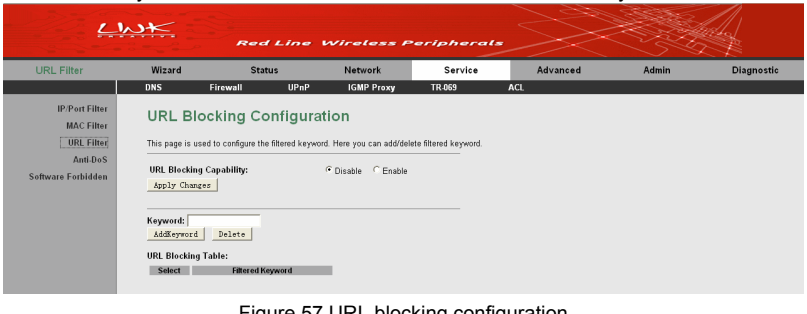


Figure 57 URL blocking configuration

The following table describes the parameters and buttons of this page:

Field	Description
URL Blocking Capability	You can choose **Disable** or **Enable**. ● Select **Disable** to disable URL blocking function

Field	Description
	and keyword filtering function. ● Select **Enable** to block access to the URLs and keywords specified in the **URL Blocking Table**.
Keyword	Enter the keyword to block.
AddKeyword	Click it to add a keyword to the **URL Blocking Table**.
Delete	Select an entry in the **URL Blocking Table** and click it to delete the entry.

After finishing setting, click the **Apply Changes** button save the settings.

3.5.2.4 Anti-DoS

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.

Click **Anti-DoS** on the left pane, and the page shown in the following figure appears.

Figure 58 DoS setting

In this page, you are allowed to configure the Anti-DoS. You should enable the DoS prevention first, and then you are allowed to set the parameters in this page.
After finishing the settings, click **Apply Changes** to apply the settings in this page.

3.5.2.5 Software Forbidden Settings

Click **Software Forbidden** on the left pane, and the page shown in the following figure appears.

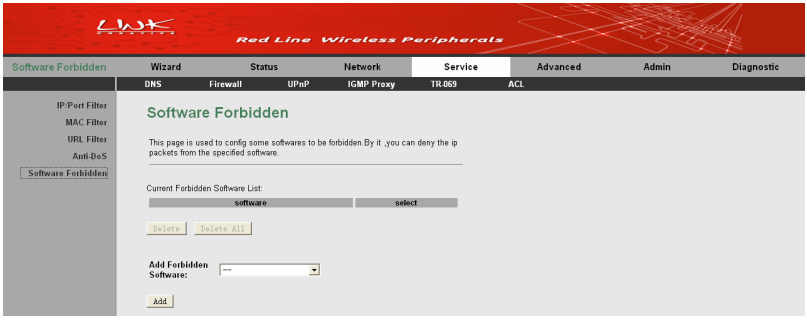


Figure 59 Software forbidden configuration

In this page, you can deny the IP packets from the specified software.

Select the proper software from the drop-down list and then click **Add** to add it to the **Current Forbidden Software List**.

3.5.3 UPnP

Choose **Service** > **UPnP** and 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.

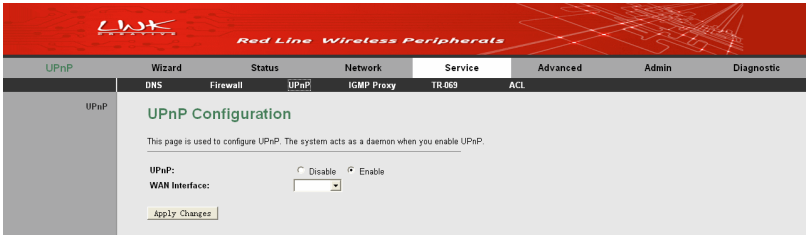


Figure 60 UPnP configuration

In this page, you can enable or disable the UPnP, and select a proper WAN interface for enabling the UPnP function.

After setting, click **Apply Changes** to save the settings.

3.5.4 IGMP Proxy

Choose **Service** > **IGMP Proxy** and 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 discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.

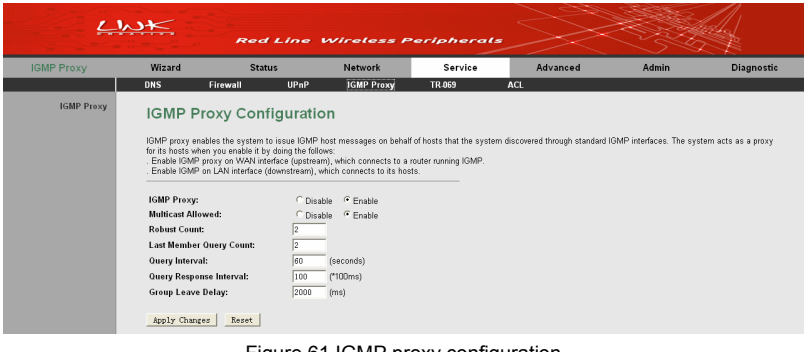


Figure 61 IGMP proxy configuration

The following table describes the parameters in this page.

Field	Description
IGMP Proxy	Enable or disable the IGMP proxy function.
Multicast Allowed	Enable or disable the **Multicast Allowed**.
Robust Count	The robustness variable is a way of indicating how susceptible the subnet is to the lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Last Member Query Count	The last member query count is the number of Group-Specific Query messages sent before the router assumes that there are no members of the host group being queried on this interface. The default last member query count is 2.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 60 seconds.
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 100 ms and must be less than the query interval.
Group Leave Delay	Set the group leave interval.

After setting, click **Apply Changes** to save the settings.

3.5.5 TR-069

Choose **Service** > **TR-069** and the page shown in the following page appears.

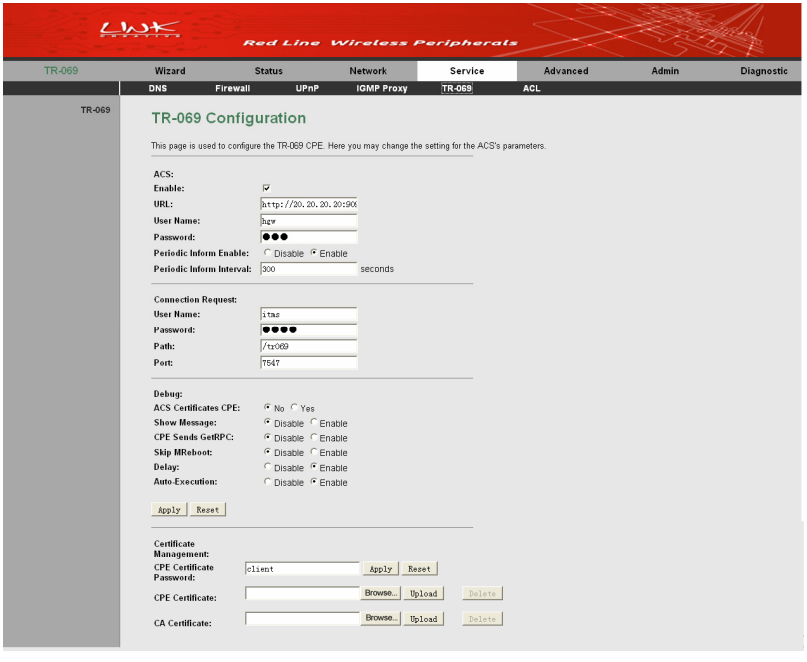


Figure 62 TR-069 configuration

This page is used to configure the TR-069 customer premises equipment (CPE). In this page, you can configure the parameters of auto-configuration server (ACS). The following table describes the parameters in this page.

Field	Description
ACS	
Enable	Enable or disable the auto-configuration server.
URL	The URL of the auto-configuration server.
User Name	The user name for logging in to the ACS.
Password	The password for logging in to the ACS.

Field	Description
Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Set the informing interval.
Connection Request	
User Name	The connection user name provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Path	The path for the ACS connecting the router.
Port	The port for the ACS connecting the router.
Debug	
ACS Certificates CPE	Specify whether to check the ACS certification of the router.
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable**, the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.
Certificate Management	
CPE Certificate Password	The certificate password of the router
CPE Certificate	For uploading the CPE certificate.
CA Certificate	For uploading the CA certificate.

After setting, click **Apply** to save the settings.

3.5.6 ACL

Choose **Service** > **ACL** and the page shown in the following figure appears. In this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

Note:

If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.

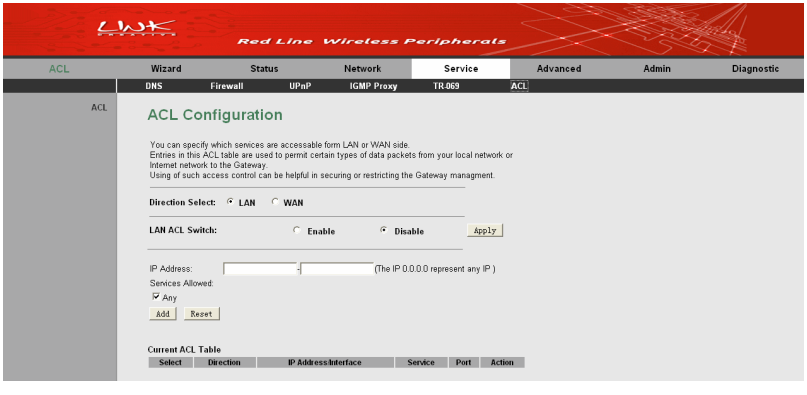


Figure 63 ACL configuration

The following table describes the parameters in this page:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.

Field	Description
Services Allowed	You can choose the following services from LAN: **Web**, **Telnet**, **FTP**, **TFTP**, **SNMP**, or **PING**. You can also choose all the services.

After setting the parameters, click the **Add** button to add the new rule to the **Current ACL Table**.

3.6 Advance

In the navigation bar, click **Advanced**. The submenus of **Advanced** settings contain **Routing**, **NAT**, **Port Mapping**, **IP QoS**, **SNMP** and **Others**.

3.6.1 Routing

The submenus of **Routing** contain **Static Route** and **RIP.**

3.6.1.1 Static Route

Click **Static Route** on the left pane, and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.

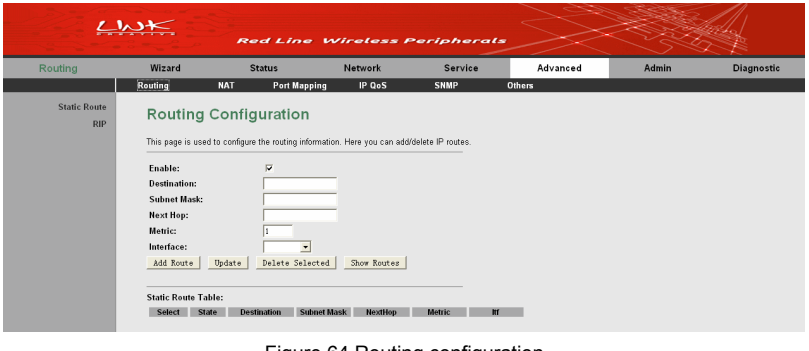


Figure 64 Routing configuration

The following table describes the parameters and buttons in this page:

Field	Description
Enable	Select it to use the static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric value of routing.
Interface	The interface for the specified route.
Add Route	Click this button to add the new static route to the table.
Update	Select an entry in the table to populate the configuration fields with that entry's values. Make any necessary changes to those values and click this button to save those changes.
Delete Selected	Select an entry in the table and click this button to delete the selected entry.
Show Routes	Click this button to display the **IP Route Table**. You can view a list of destination routes commonly accessed by your network.
Static Route Table	Display the configured route entries of static IP.

Click **Show Routes** to display the **IP Route Table** page.

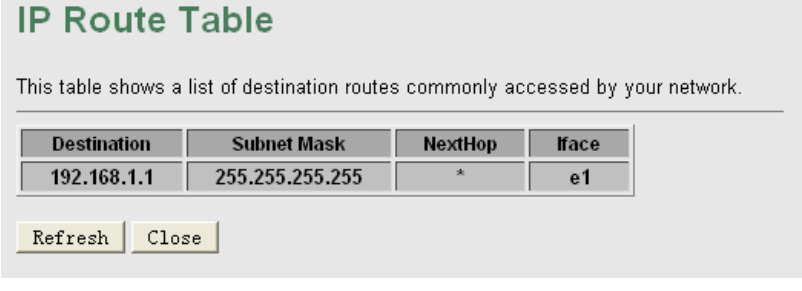


Figure 65 IP route table

This table shows a list of destination routes commonly accessed by your network.

3.6.1.2 RIP

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

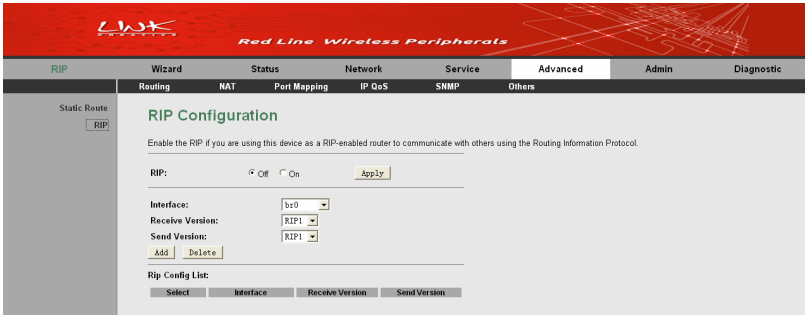


Figure 66 RIP configuration

The following table describes the parameters and buttons of this page:

Field	Description
RIP	Select **Enable**, and then the router communicates with other RIP-enabled devices.
Interface	Choose the router interface that uses RIP.
Receive Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**. ● Selecting **RIP1** indicates the router receives RIP v1 messages. ● Selecting **RIP2** indicates the router receives RIP v2 messages. ● Selecting **Both** indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Selecting **RIP1** indicates the router broadcasts RIP1 messages only.

Field	Description
	● Selecting **RIP2** indicates the router multicasts RIP2 messages only.
Add	Click this button to add the RIP interface to the **Rip Config List**.
Delete	Select an entry in the **Rip Config List** and click this button to delete the entry.

3.6.2 NAT

The submenus of **NAT** contain **Setup DMZ**, **Virtual Server**, **NAT Forwarding**, **ALG**, **NAT Exclude IP**, **Port Trigger**, **FTP ALG Port,** and **NAT IP Mapping.**

3.6.2.1 Setup DMZ

Demilitarized zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains the services accessible to the Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Click **Setup DMZ** on the left pane, and the page shown in the following figure appears.

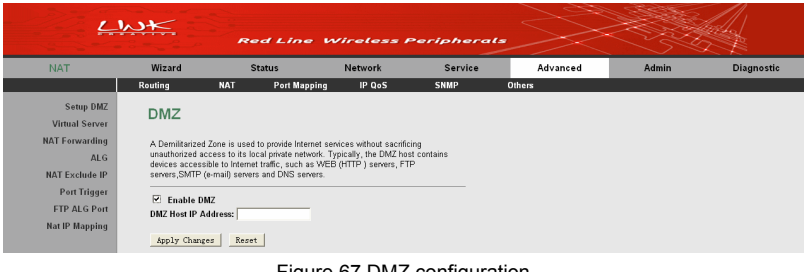


Figure 67 DMZ configuration

In this page, set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by the firewall and the host can realize bidirectional limitless communication with the Internet users and servers.

The configuration steps are as follows:

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.

3.6.2.2 Virtual Server

Firewall can prevent the unexpected stream on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Click **Virtual Server** on the left pane, and the page shown in the following figure appears.

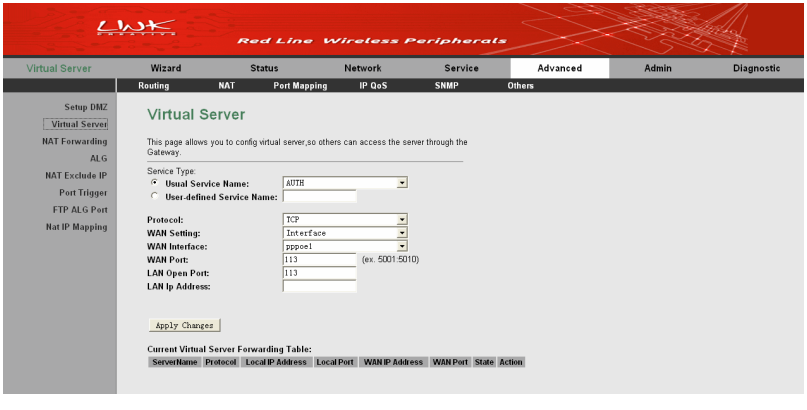


Figure 68 Virtual server configuration

In this page, you can configure the virtual server. Other users on the Internet access the server through the router.

The following table describes the parameters in this page.

Field	Description
Service Type	You can choose **Usual Service Name** or **User-defined Service Name**.
Protocol	Select the transport layer protocol that the service type uses. You can choose **TCP** or **UDP**.
WAN Setting	You can select **Interface** or **IP Address**.
WAN Interface	Select the router port that uses the virtual server.
WAN Port	Enter the access port on the WAN.
LAN Open Port	Enter the port number of the specified service type.
LAN IP Address	Enter the IP address of the virtual server.

After setting, click the **Apply Changes** button to save the settings.

3.6.2.3 NAT Forwarding

Click **NAT Forwarding** on the left pane, and the page shown in the following figure appears. This page is used to configure the NAT forwarding rules.

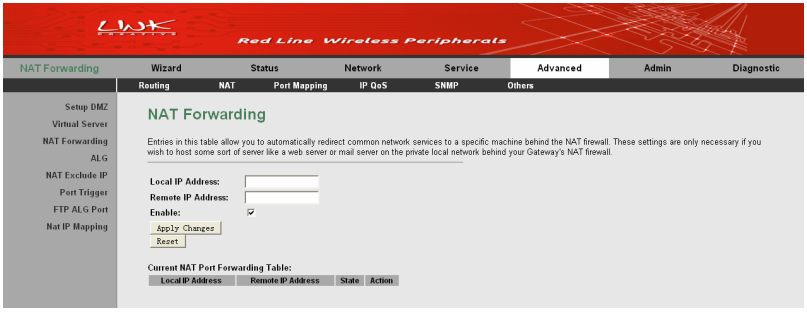


Figure 69 NAT forwarding configuration

Entries in the **Current NAT Port Forwarding Table** allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web

server or mail server on the private local network behind your Gateway's NAT firewall.

The following table describes the parameters in this page.

Field	Description
Local IP Address	Enter the local IP address.
Remote IP Address	Enter the remote IP address.
Enable	Enable or disable current rule.

After setting, click the **Apply Changes** button to save the settings.

3.6.2.4 NAT Exclude IP

Click **NAT Exclude IP** on the left pane, and the page shown in the following figure appears.

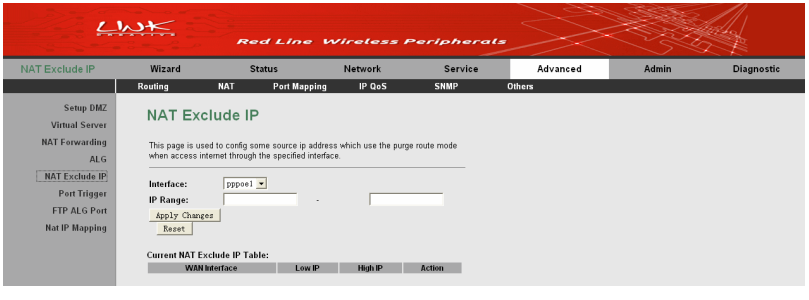


Figure 70 NAT excluding IP configuration

In the page, you can configure some source IP addresses which need not to use NAT when accessing internet through the specified interface.

The following table describes the parameters in this page.

Field	Description
Interface	Select a WAN interface for setting the function of NAT excluding IP.
IP Range	Set the valid IP range for setting the function of NAT excluding IP.

After setting, click the **Apply Changes** button to save the settings.

3.6.2.5 Port Triggering

Certain applications, such as WAN network games, video conferences, and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on a NAT router. When an application sends a connection request to a trigger port, the corresponding ports are open, for later connection and service provision.

Click **Port Trigger** on the left pane and the page shown in the following figure appears.

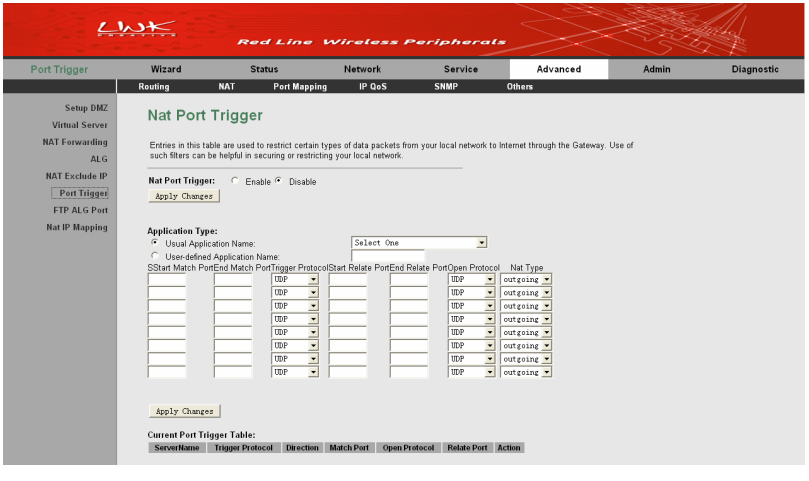


Figure 71 NAT port triggering configuration

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

The following table describes the parameters in this page.

Field	Description
Nat Port Trigger	Enable or disable the port triggering rule.
Usual Application Name	Select a proper application in the drop-down list.
User-defined Application Name	Manually define an application.
SStart Match	The start port number that the LAN user uses to trigger the open port.
Port End Match	The end port number that the LAN user uses to trigger the open port.
Port Trigger Protocol	Select the application protocol. You may select **UDP**, **TCP**, or. **TCP/UDP**.
Port Start Relate	The start port number that is opened to WAN.
Port End Relate	The end port number that is opened to WAN.
Port Open Protocol	Select the proper protocol that is opened to WAN. You may select **UDP**, **TCP**, or. **TCP/UDP**.
NAT Type	You may **outgoing** or **incoming**.

After setting, click the **Apply Changes** button to save the settings.

3.6.2.6 FTP ALG Port

Click **FTP ALG Port** on the left pane and the page shown in the following figure appears.

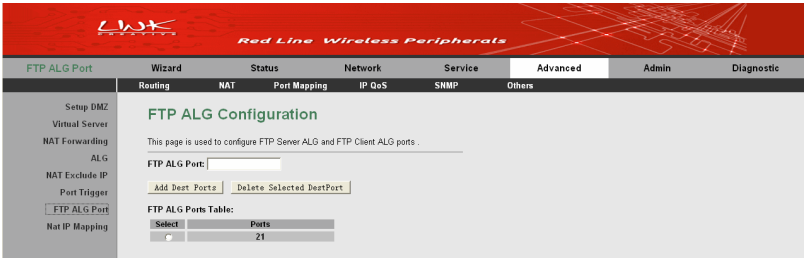


Figure 72 FTP ALG configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports.

In this page, enter the port number for configuring as a FTP ALG port, and then click the **Add Dest Ports** button to add a new entry to the **FTP ALG Ports Table**.

3.6.2.7 NAT IP Mapping

Click **Nat IP Mapping** on the left pane, and the page shown in the following figure appears.

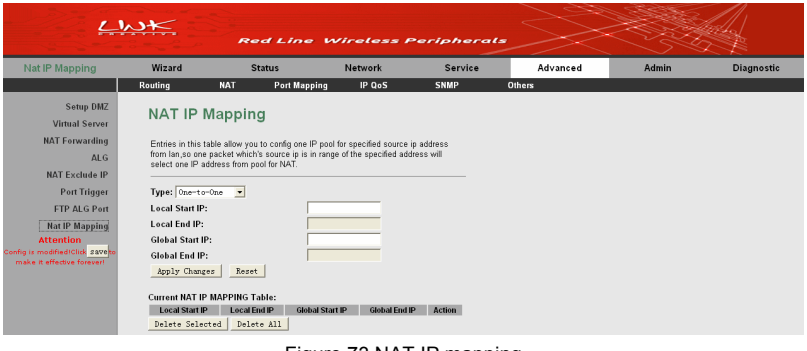


Figure 73 NAT IP mapping

In this page, you can set the entries of NAT IP mapping.

The following table describes the parameters in this page.

Field	Description
Type	You may select **one-to-one**, **many-to-one**, **many-to-many**, or **one-to-many**.
Local Start IP	Enter the local start IP.
Local End IP	Enter the local end IP.
Global Start IP	Enter the global start IP.
Global End IP	Enter the global end IP.

After setting, click the **Apply Changes** button to add an entry of NAT IP mapping.

3.6.3 Port Mapping

Choose **Advanced** > **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.

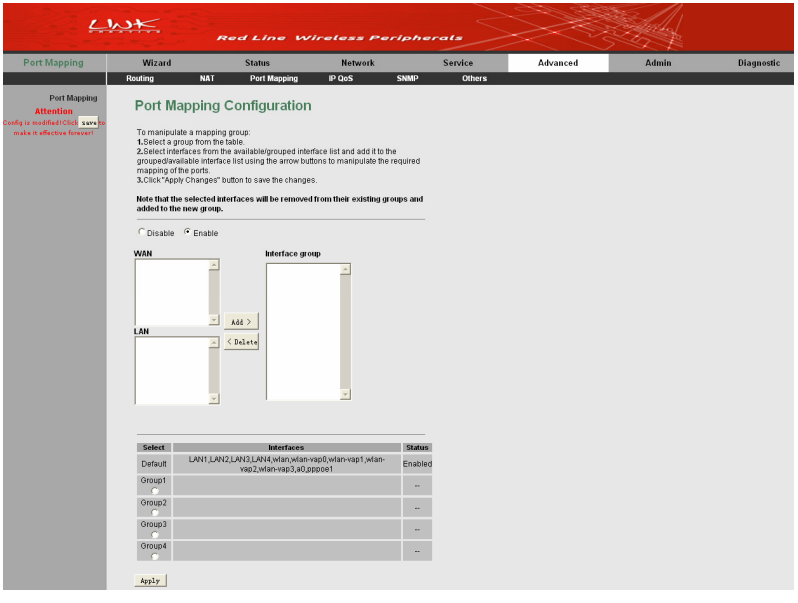


Figure 74 Port mapping configuration

In this page, you can bind the WAN interface and LAN interface to the same group. The procedure for operating a mapping group is as follows:

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

Step 2 Select a group from the table at the bottom of the page.

Step 3 Select the interfaces from the WAN and LAN interface lists and add them to the interface group list by using the **Add** button to manipulate the required mapping of the ports.

Step 4 Click **Apply** to save the settings.

3.6.4 IP QoS

Choose **Advanced** > **IP QoS** and the page shown in the following figure appears. Entries in the **QoS Rule List** are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, source IP address, destination IP address and other information.

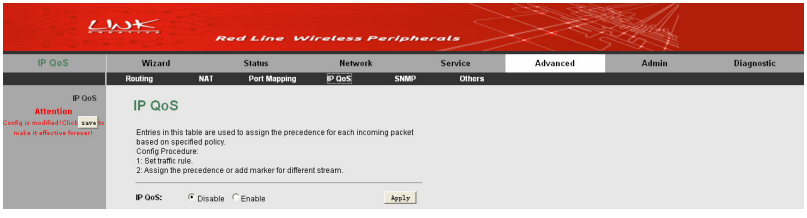


Figure 75 IP QoS configuration

By default, IP QoS is disabled.

Enable IP QoS, and then the following page appears.

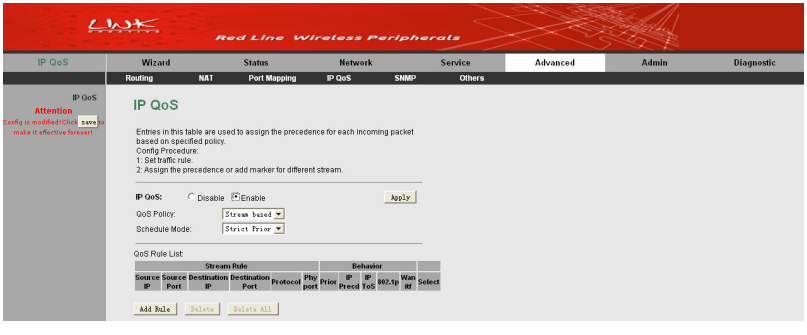


Figure 76 Enabling IP QoS

In this page, you can configure the QoS policy and schedule mode. Entries in the QoS rule list 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.

The following table describes the parameters in this page.

Field	Description
IP QoS	Enable or disable IP QoS.
QoS Policy	You can choose **stream based**, **802.1p based**, or **DSCP based**.
Schedule Mode	You can choose **strict prior** or **WFQ (4:3:2:1)**.

Click the **Add Rule** button to display the following figure.

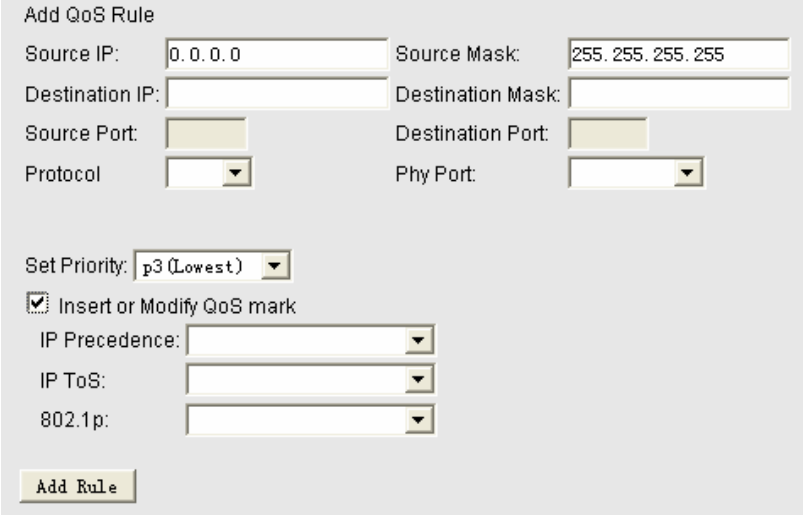


Figure 77 Adding a QoS rule

The following table describes the parameters for adding a QoS rule.

Field	Description
Source IP	The IP address of the source data packet.
Source Mask	The subnet mask of the source IP address.
Destination IP	The IP address of the destination data packet.
Destination Mask	The subnet mask of the destination IP address.
Source Port	The port of the source data packet.

Field	Description
Destination Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rule. You can choose **TCP**, **UDP**, or **ICMP**.
Phy Port	The LAN interface responds to the IP QoS rule.
Set priority	The priority of the IP QoS rule. P0 is the highest priority and P3 is the lowest.
Insert or Modify QoS Mark	Enable or disable this function.
IP Precedence	You can choose from 0 to 7 to define the priority level in the ToS of the IP data packet.
IP ToS	The type of IP ToS for classifying the data package You can choose **Normal Service**, **Minimize Cost**, **Maximize Reliability**, **Maximize Throughput**, or **Minimize Delay**.
802.1p	You can choose from 0 to 7.

After setting, click the **Add Rule** button to add the QoS rule to the QoS Rule List.

3.6.5 SNMP

Choose **Advanced** > **SNMP** and the page shown in the following figure appears.

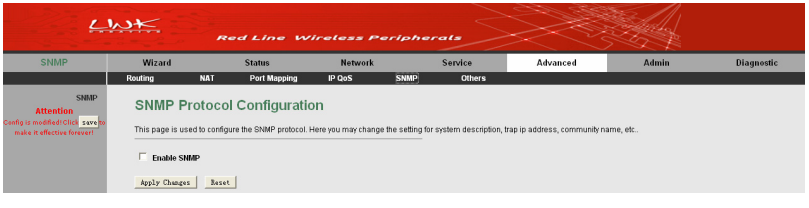


Figure 78 SNMP configuration

In this page, you can configure the parameters of Simple Network Management Protocol (SNMP).By default, SNMP is disabled.

Select **Enable SNMP**, and then the following page appears.

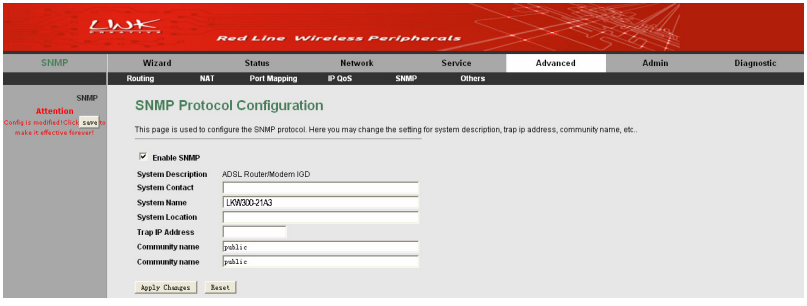


Figure 79 Enabling SNMP

The following table describes the parameters in this page:

Field	Description
Enable SNMP	After enabling SNMP, you are allowed to set the following parameters.
System Description	Display the system description.
System Contact	Enter the system contact.
System Name	You can modify the system name if necessary.
System Location	Enter the system location.
Trap IP Address	Enter the IP address of trap host. The trap information is sent to the host.
Community name (Read-only)	The common character string that is used for reading the device information is like a password. The network administrator uses this password to read the information of this router.
Community name (Read-write)	The common character string that is used for configuring the device is like a password. The network administrator uses this password to configure the information of the router.

After setting, click **Apply Changes** to save the settings.

3.6.6 Others

Choose **Advanced** > **Others** and the page shown in the following figure appears.

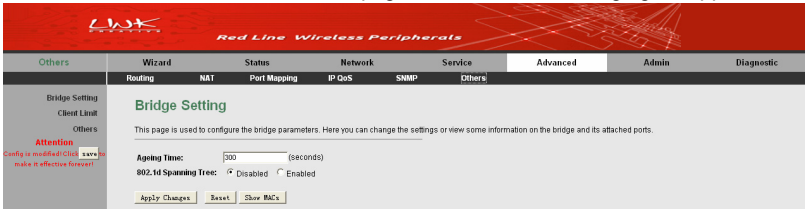


Figure 80 Bridge setting

This page is used to configure the bridge parameters. In this page, you can change the settings or view some information in the bridge mode and its attached ports.
The following table describes the parameters and button in this page:

Field	Description
Ageing Time	If the host is idle for 300 seconds (the default value), its entry is deleted from the bridge table.
802.1d Spanning Tree	Disable or Enable 802.1d Spanning Tree Protocol (STP). Select **Enable** to provide path redundancy while preventing undesirable loops in your network.
Show MACs	Click this button to show a list of the learned MAC addresses for the bridge.

Click **Show MACs** to display the following page.

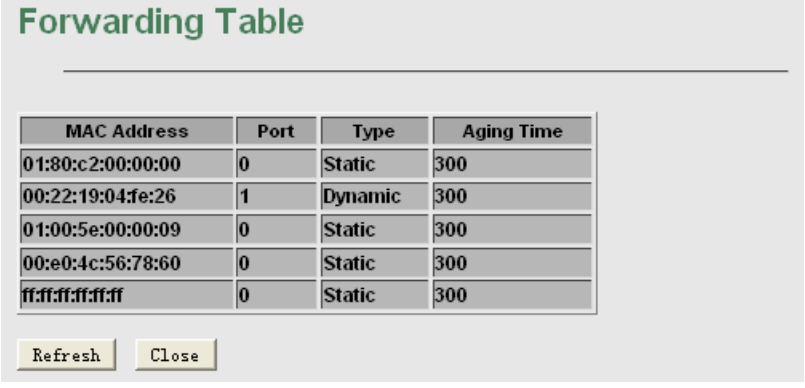


Figure 81 Forwarding table

This table shows a list of learned MAC addresses for this bridge.

3.7 Admin

In the navigation bar, click **Admin**. The submenus of **Admin** page contain **Commit/Reboot**, **Update**, **Log**, **Password**, **Time** and. **Logout.**

3.7.1 Commit/Reboot

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

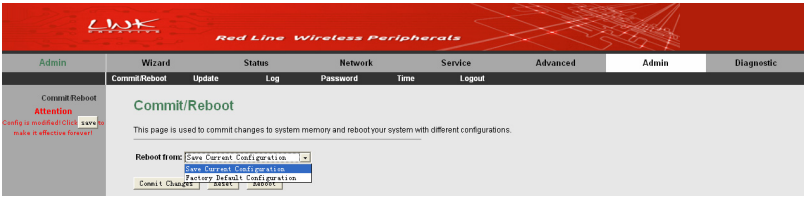


Figure 82 Saving or restoring the router settings

The following table describes the parameters and button of this page:

Field	Description
Reboot from	You can choose **Save Current Configuration** or **Factory Default Configuration**. ● **Save Current Configuration**: Save the current settings, and then reboot the router. ● **Factory Default Configuration**: Reset to the factory default settings, and then reboot the router.
Reboot	Click it to reboot the router.

3.7.2 Update

Choose **Admin** > **Update**. The submenus of **Update** contain **Upgrade Firmware** and **Backup/Restore**.

3.7.2.1 Upgrade Firmware

Click **Upgrade Firmware** on the left pane, and the page shown in the following figure appears. In this page, you can upgrade the firmware of the router.

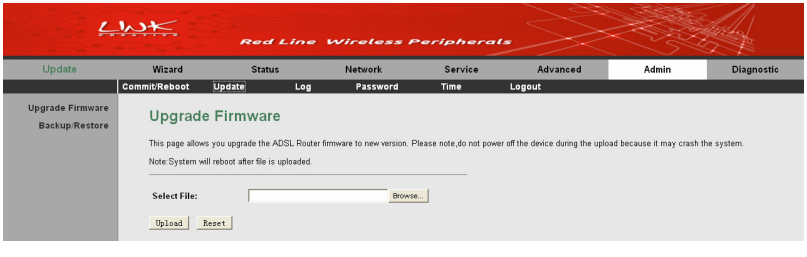


Figure 83 Upgrading firmware

In this page, you can upgrade the firmware of the router.

To upgrade the firmware, click **Browse…** to select the firmware file and then click **Upload** to begin upgrading the firmware.

⚠ **Caution:**

Do not turn off the router or press the Reset button while the procedure is in progress. Otherwise, system may crash.

3.7.2.2 Backup/Restore

Click **Backup/Restore** on the left pane, and the page shown in the following figure appears.

⚠ **Caution:**

Do not turn off the router or press the Reset button while the procedure is in progress. Otherwise, system may crash.

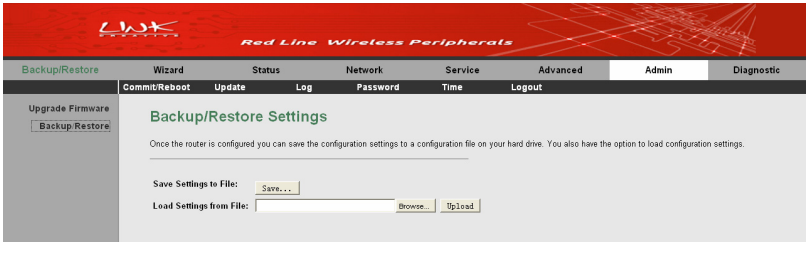


Figure 84 Backuping or uploading settings

In this page, you can backup the current settings to a file and restore the previous settings.

To save the settings, click the **Save…** button and select the path, then you can save the configuration file of the router.

To upload the settings, click **Browse…** to select the configuration file, and then click **Upload** to upload the router configuration.

⚠ **Caution:**

Do not turn off the router or press the Reset button while the procedure is in progress. Otherwise, system may crash.

3.7.3 System Log

Choose **Admin** > **Log** and the page shown in the following figure appears.

Figure 85 Log setting

In this page, you can view the log information.
You can set the log flag to **Error** or **Notice** (or both).
Click **Save Log to File** to save the log information to your PC.
Click **Clear Log Table** to clear the log information in the table.

3.7.4 Password

Choose **Admin** > **Password** and the page shown in the following figure appears.

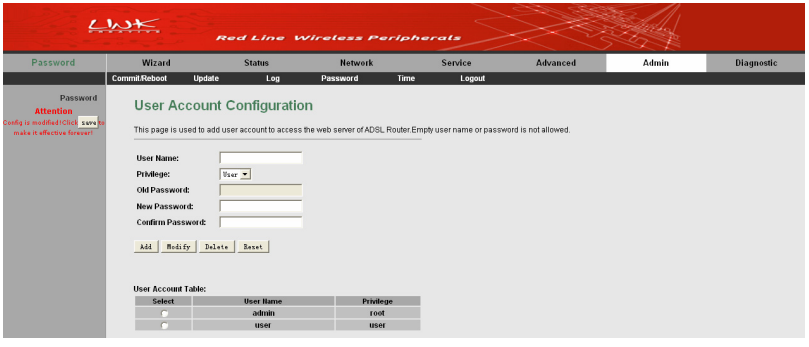


Figure 86 User account configuration

The following table describes the parameters in this page:

Field	Description
User Name	Set the user name for accessing the router.
Privilege	Choose the privilege for the account.
Old Password	Enter the old password
New Password	Enter the password to which you want to change the old password.
Confirm Password	Enter the new password again.

After setting, click **Add** to add a new entry to the **User Account Table**.

Note:

By default, the user name and password are **admin** and **admin** respectively.

The common user name and password are **user** and **user** respectively.

3.7.5 Time

Choose **Admin** > **Time** and the page shown in the following figure appears. You can configure the system time manually or get the system time from the time server.

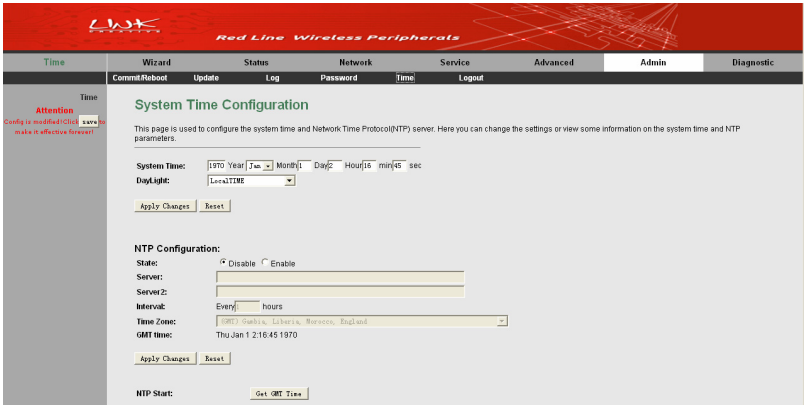


Figure 87 System time configuration

If you want the router to automatically acquire the system time from the time server, you need to configure the following parameters in this page.

Field	Description
State	Enable or disable SNTP.
Server	Enter the IP address or the domain name of the primary server.
Server 2	Enter the IP address or the domain name of the secondly server.
Interval	Set the synchronization interval between the router and time server.
Time Zone	Select the corresponding time zone where your router locates.
GMT time	Display the GMT time.

After setting, click **Get GMT Time** to make the router synchronize with the time server.

3.7.6 Logout

Choose **Admin** > **Logout** and the page shown in the following figure appears.

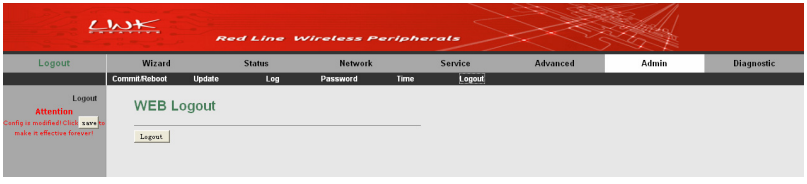


Figure 88 Web logout

In this page, click **Logout** to log out of the Web page of the ADSL router.

3.8 Diagnostic

In the navigation bar, click **Diagnostic**. The submenus of **Diagnostic** contain **Ping**, **Traceroute**, **OAM Loopback**, **ADSL Statistics**, and **Diag-Test**.

3.8.1 Ping Diagnosis

The ping diagnosis allows in simple ways to test a connection between 2 hosts in the same network or on different networks. If the command ping is successful, it means that there is a correct physical as well as a logical connection between 2 hosts in any network. (Unless if there is a firewall interfering somewhere in between.)

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

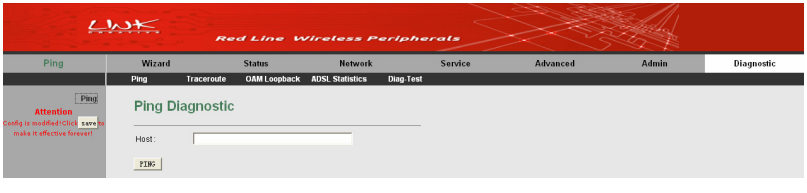


Figure 89 Ping diagnosis

In this page, enter the IP address of the host, and then click **PING** to begin to Ping the host address.

3.8.2 Traceroute Diagnosis

Traceroute diagnosis is used to find out which path a packet takes to reach its destination. It is a nice way to see which routers it passes and which networks it crosses to reach its destination.

Choose **Diagnostic** > **Traceroute** on the left pane and the page shown in the following figure appears.

Figure 90 Traceroute diagnosis

In this page, you can set the parameters of Traceroute diagnosis.

The following table describes parameters in this page.

Field	Description
Host	Enter the IP address that performs the operation of tracing routing.
NumberOfTries	Set the number of times to repeat.
Timeout	Set the timeout interval.
Datasize	Se the data size.
DSCP	Set the DSCP value.
MaxHopCount	Set the maximum routing number.
Interface	Select the proper interface.

After finishing the settings, click the **Traceroute** button to start the traceroute diagnosis. Click the **Show Result** button to view the information of traceroute diagnosis.

3.8.3 OAM Loopback

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

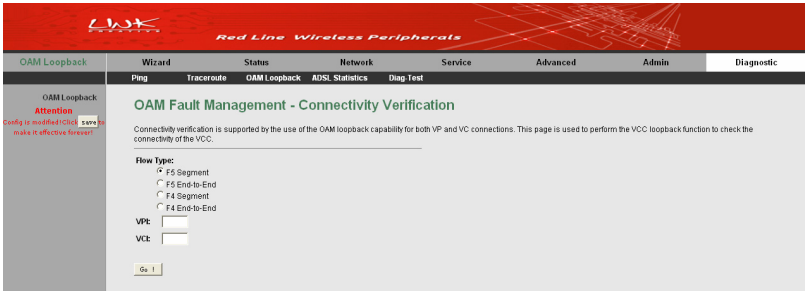


Figure 91 OAM fault management

In this page, select the flow type first, then enter the VPI value and VCI value, finally click **Go!** to perform OAM loopback diagnosis.

3.8.4 ADSL Statistics

Choose **Diagnostic** > **ADSL Statistics** and the page shown in the following figure appears.

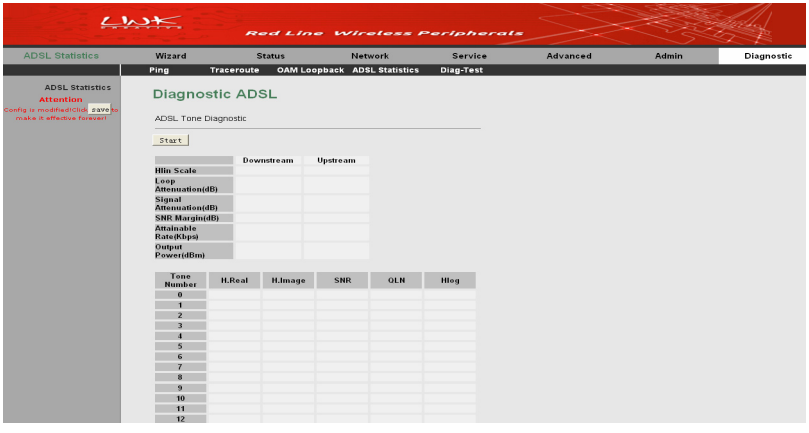


Figure 92 ADSL diagnosis

This page is used to diagnose the ADSL tone.
Click **Start** to begin ADSL tone diagnosis.

3.8.5 Diag-Test

Choose **Diagnostic** > **Diag-Test** and the page shown in the following figure appears. The ADSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "**Run Diagnostic Test**" button again to make sure the fail status is consistent.

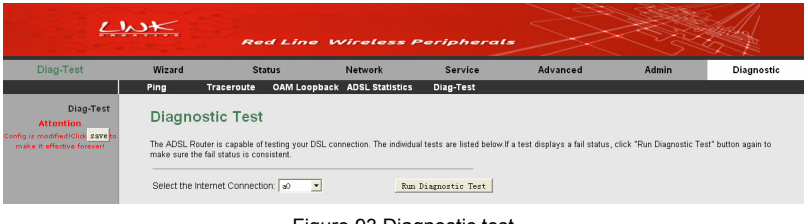


Figure 93 Diagnostic test

Select an Internet connection, and then click **Run Diagnostic Test** to begin the test.