

# Netis ADSL User Manual

This user manual is used for

DL4311/DL4311D/DL4322/DL4322D/DL4312/DL4312D/DL4323/DL4323D/DL4310

Screenshot and panel use on this document. We take DL4311 for example.




**1141 Budapest, Fogarasi út 77.**  
Tel.: \*220-7940, 220-7814, 220-7959,  
220-8881, 364-3428 Fax: 220-7940  
Mobil: 30 531-5454, 30 939-9989

**1095 Budapest, Mester u. 34.**  
Tel.: \*218-5542, 215-9771, 215-7550,  
216-7017, 216-7018 Fax: 218-5542  
Mobil: 30 940-1970, 20 949-2688

**[www.netis-systems.hu](http://www.netis-systems.hu)**

E-mail: [info@delton.hu](mailto:info@delton.hu) Web: [www.delton.hu](http://www.delton.hu)

## Copyright Statement

 is a registered trademark of Netis Corporation. Other trademark or trade name may be used in this document to refer to either the entities claiming the marks and names or their products.

Reproduction in any manner without the permission of Netis Corporation is strictly forbidden.

All the information in this document is subject to change without notice.

## Certification

### FCC CE

## FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This unit complies with Part 15 & 68 of FCC Rules. Operation is subject to following two conditions:

- 1) This device may not cause harmful interference
- 2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

**INFORMATION TO BE SUPPLIED TO USERS**

We confirm that the following information will be supplied to the users of this equipment. This information will be provided with the user's manual.

**FCC REQUIREMENTS**

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the exterior of the cabinet of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. A product identifier in the format US: **T58DL4311R**. If requested, this number must be provided to the telephone company.

FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. See Installation Instructions for details. The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. Typically, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line (as determined by the total RENs) contact the local telephone company. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. The telephone company may make changes to its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice so you can make the necessary modifications to maintain uninterrupted service. For technical support, contact **Netis Systems USA Corp.** at **18541 Gale Avenue, City of Industry, CA 91748** or call **TEL: 626-486- 9208**. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

# Contents

<b>1. Introduction.....</b>	<b>2</b>
1.1 Product Overview.....	2
1.2 Main Features .....	2
<b>2. Hardware Installation.....</b>	<b>3</b>
2.1 Front Panel.....	3
2.2 Rear Panel .....	4
2.3 Physical Connection .....	4
<b>3. Quick Installation .....</b>	<b>6</b>
3.1 Configure Your PC .....	6
3.2 Login .....	9
<b>4. Software Configuration .....</b>	<b>10</b>
4.1 Quick Start.....	10
4.2 Status .....	12
4.2.1 Device Information.....	12
4.2.2 Statistics .....	14
4.3 Setup .....	15
4.3.1 WAN .....	16
4.3.2 LAN .....	25
4.3.3 WLAN .....	31
4.3.4 Wireless.....	39
4.3 Advanced Setup .....	41
4.3.1 Route .....	42
4.3.2 NAT .....	45
4.3.3 QoS .....	52
4.3.4 CWMP .....	58
4.3.5 Port Mapping .....	59
4.4 Firewall.....	60
4.5 Maintenance .....	71
<b>Appendix A: Troubleshooting .....</b>	<b>84</b>



# 1. Introduction

## 1.1 Product Overview

Thank you for choosing netis DL4311 150Mbps wireless N ADSL2+ Modem Router.

The Wireless N ADSL2+ Modem Router is a device with routing capability, wireless access point, multiple ADSL lines transmission mode (ADSL2+, ADSL2, T1.413, G.Dmt and G.lite) and provides 10/100Base-T Ethernet interface. The ADSL Router supports wireless 802.11n/b/g and the following security protocols: WEP, WPA, WPA2 and 802.1x. Through the ADSL access, the router can provides user with access to Internet.

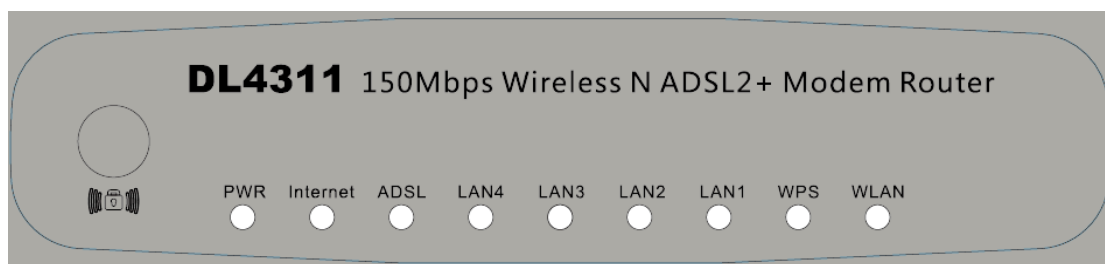
## 1.2 Main Features

- Wireless AP, Router, 4 Port Switch and Firewall
- Support ITU-T G.992.1 (G.dmt), ANSI T1.413, G.992.2 (G.Lite), ADSL2 and ADSL2+
- Support 802.11n, compatible with 802.11b and 802.11g
- Up to 54 Mbps wireless operation rate
- 64/128 bits WEP for security
- WPA and WPA2 support
- 4 10/100MBase-T Ethernet interface (LAN)
- RFC-1483/2684 LLC/VC-Mux bridge/route mode
- RFC-1577 Classical IP over ATM
- RFC-2516 PPPoE
- RFC-2364 PPPoA
- ITU-T 1.610 F4/F5 OAM send and receive loop-back
- 802.1d Spanning-Tree Protocol
- DHCP Client/Server/Relay
- NAT
- RIP v1/v2
- DNS Relay Agent
- Support DMZ, virtual server, ALG
- IGMP Proxy/Snooping
- Protection against Denial of Service attack
- IP Packet filtering
- MAC filtering
- URL filtering

- IP QoS
- Dynamic DNS
- UPnP support
- System log support, can record the state of the router
- Remote management
- SNMP v1/v2/Trap
- Firmware upgrade through FTP, TFTP and HTTP
- Configuration backup/restore
- Diagnostic tools

## 2. Hardware Installation

### 2.1 Front Panel



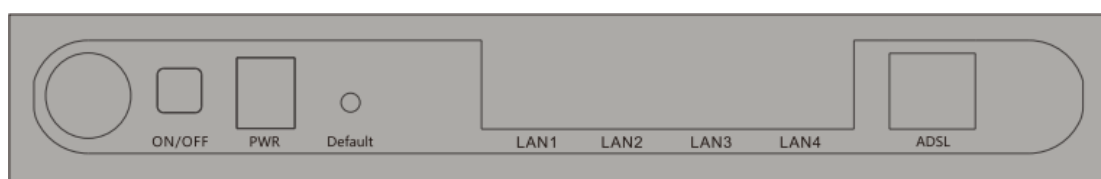
The front panel of the wireless ADSL2+ Modem Router includes one power indicator and eight function indicators, as explained in table below:

LED	Status	Indication
Power	On	Power is on
	Off	Power is off
Internet	Green	A successful PPP connection has been built
	Off	The ADSL port is linked down or the Modem Router works in Bridge mode
	Red	The PPP connection failed to be established
DSL	On	The ADSL port is linked up
	Blink	The ADSL port is linked down
LAN (1-4)	On	There is a successful connection on the corresponding LAN port



	Off	There is no connection on the corresponding LAN port
	Blink	Data is being transferred over the corresponding LAN port
WPS	On	A wireless device is successfully connected to the network by WPS function
	Off	A wireless device failed to be added to the network by WPS function
	Blink	A wireless device is connecting to the network by WPS function
WLAN	On	The wireless function is enabled
	Off	The wireless function is disabled
	Blink	Sending or receiving data over wireless network

## 2.2 Rear Panel



The rear panel of the wireless ADSL2+ Modem Router includes 1 power ON/OFF switch, 1 PWR connector, 1 WPS button, 1 Default button, 4 LAN interfaces and 1 ADSL interface, as explained in table below:

Interface/Button	Indication
ON/OFF	Turn on/off the power of Modem Router
PWR	Connect with a power adapter
Default	Used to restore your Modem to factory default settings
LAN (1-4)	Connect to your network devices
ADSL	Connect to the Modem port of splitter or directly to the wall jack

## 2.3 Physical Connection

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. You need to connect the device to the

phone jack, the power outlet, and your computer or network. Before cable connection, turn off the power supply and keep your hands dry. You can follow the steps below to install it.

**Step 1:** Connect the ADSL cable.

**Method one:** Plug one end of the twisted-pair ADSL cable into the ADSL port on the rear panel of DL4311, and insert the other end into the wall socket.

**Method two:** You can use a separate splitter. External splitter can divide digital data and voice, and then you can access internet and make calls at the same time. The external splitter has three ports:

- LINE: Connect to the wall jack.
- PHONE: Connect to the phone sets.
- MODEM: Connect to the ADSL port of DL4311. Plug one end of the twisted-pair ADSL line into the ADSL port on the rear panel of DL4311. Connect the other end to the MODEM port of the external splitter.

**Step 2:** Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the DL4311.

**Step 3:** Attach the power adapter. Connect the AC power adapter to the PWR connector on the rear of the device and plug in the adapter to a wall outlet or power extension.

**Step 4:** Turn on your computers and power on the Modem Router.



**Note:**

- 1) If you currently use a modem, disconnect it now. The Modem Router will replace your old modem.

- 2) After the physical connection, please check whether the LED indicators of the Modem Router display normally as above describes in 2.1 section.

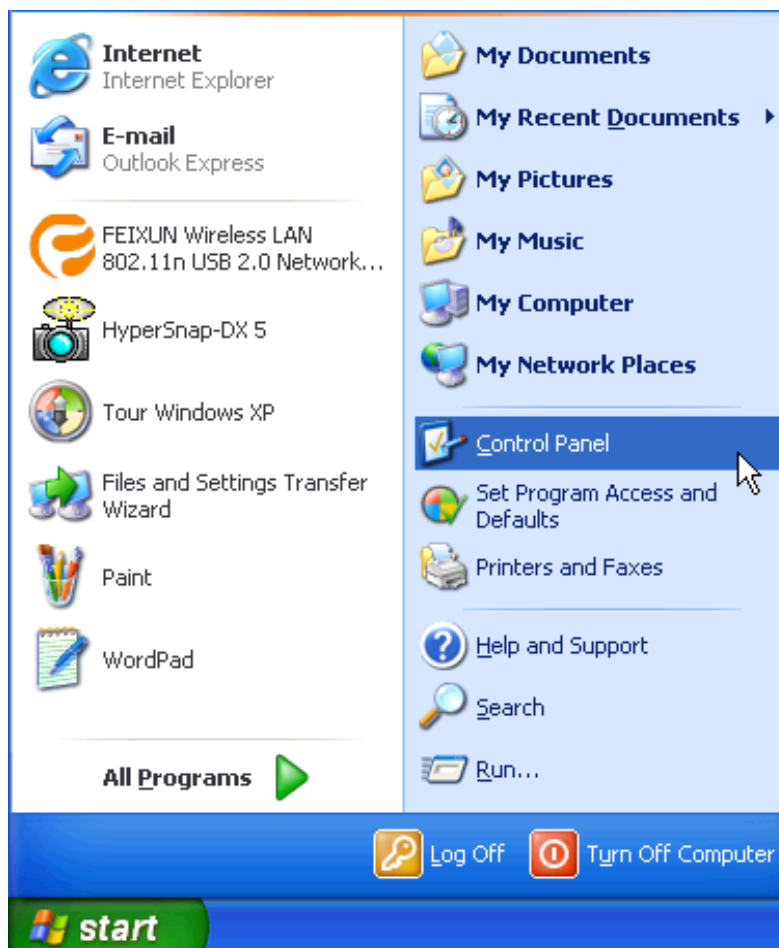
## 3. Quick Installation

### 3.1 Configure Your PC

After you directly connect your PC to DL4311 or a Hub/Switch which has connected to the Modem Router, we suggest you set your computer to obtain IP address automatically.

➤ **For Windows XP/2000**

**Step 1:** Click Start, open the Control Panel.

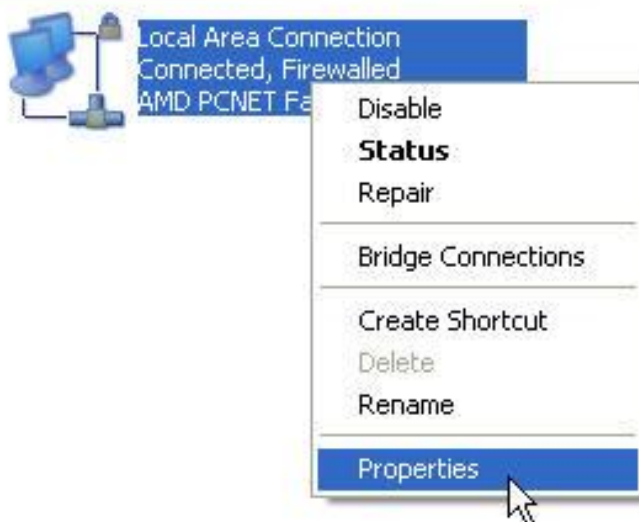


**Step 2:** Double click Network Connection.

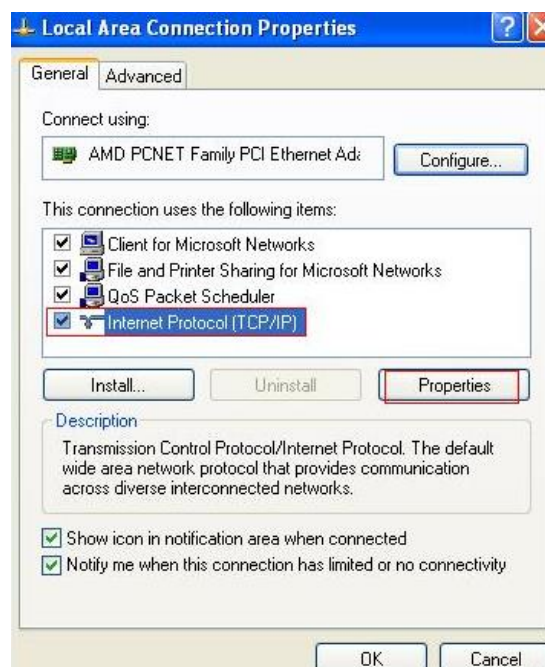


**Step 3:** Right click "Local Area Connection" and then select "Properties".

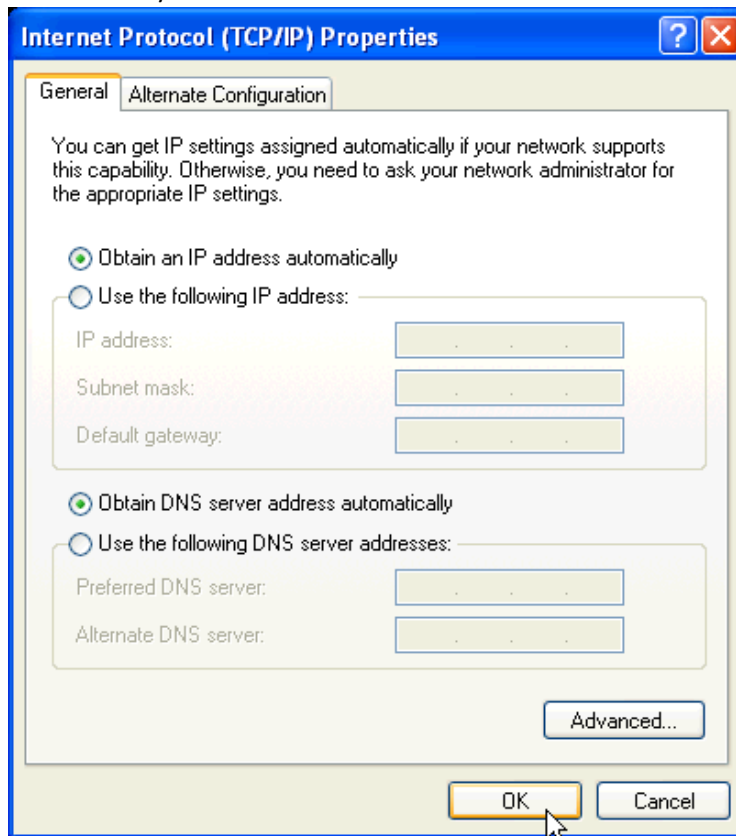
### LAN or High-Speed Internet



**Step 4:** Select Internet Protocol (TCP/IP) and click Properties.



**Step 5:** Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” on the screen below. And then click “OK”.



**Step 6:** Run the Ping command in the command prompt to verify the network connection.

Please click the Start menu on your desktop, select Run tab, type “cmd” in the field, and then type ping 192.168.1.1 on the next screen, and then press Enter.

If the screen looks like the following, you have succeeded

```
C:\Documents and Settings\ying.zhou>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

➤ **For Windows Vista/7/8 :**

- 1) Click “Start”, open the “Control Panel”.

- 2) Click “Network and Sharing Center” and then click “Manage network connection” (“Change adapter settings” for Windows 7).
  - 3) Right click “Local Area Connection” and then click “Properties”.
  - 4) Select “Internet Protocol Version 4 (TCP/IPv4)” and click “Properties”.
  - 5) Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”.
- Click OK.

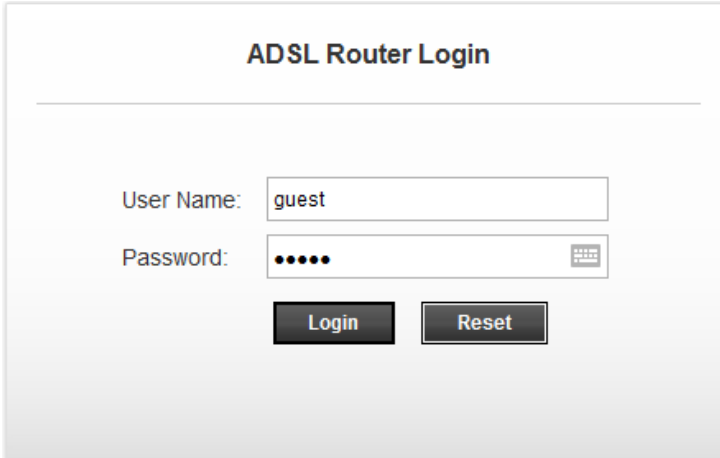
**Note:** After your computer is configured successfully, go to the next section to configure the Modem Router via web. Otherwise, refer to the section of Troubleshooting T1 to reset the modem.

## 3.2 Login

After the initial configuration is done, you can login to the Web based UI. Here are the steps to log in the UI.

**Step 1:** Start your web browser and enter <http://192.168.1.1> in the browser address bar.

**Step 2:** When ADSL connection is OK, the following login box will pop up. Enter default user name (admin) and password (admin) as shown below. The user name and password are case-sensitive, they are both in lower case. Click “Login” to enter the Web-based UI of the Modem Router.



ADSL Router Login

User Name:

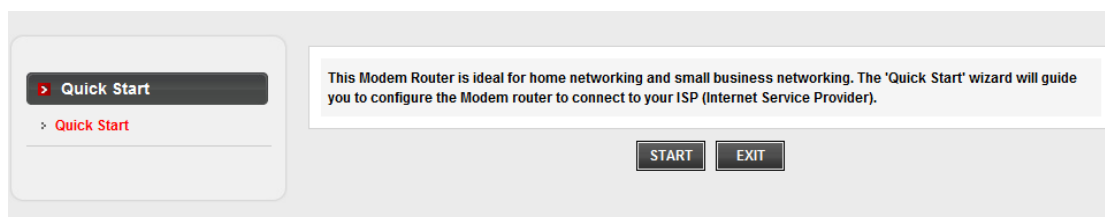
Password:

**Note:** If this Window would not pop up, you can refer to the Troubleshooting T4 to get the solution.

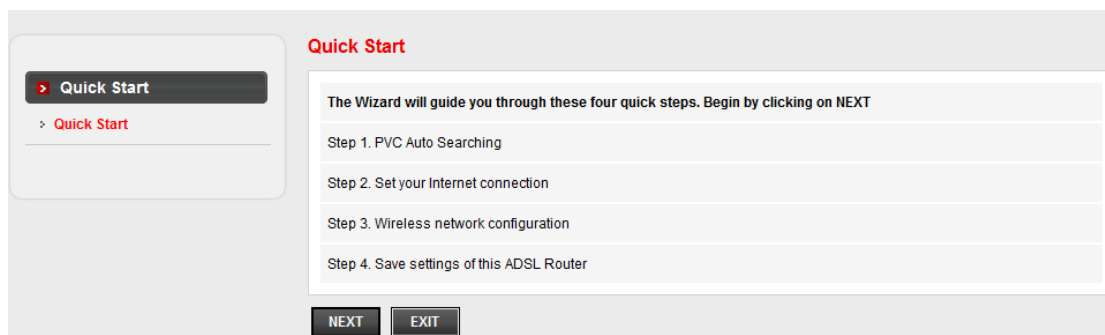
## 4. Software Configuration

This User Manual recommends using the Quick Installation Guide for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, you will get help from this chapter to configure the advanced settings through the Web-based UI. After your successful login, you can configure and manage the device. There are main menus on the top of the Web-based UI, submenus will be available after you click one of the main menus. On the center of the Web-based UI, there are the detailed configurations or status information. To apply any settings you have altered on the page, please click the APPLY/SAVE button.

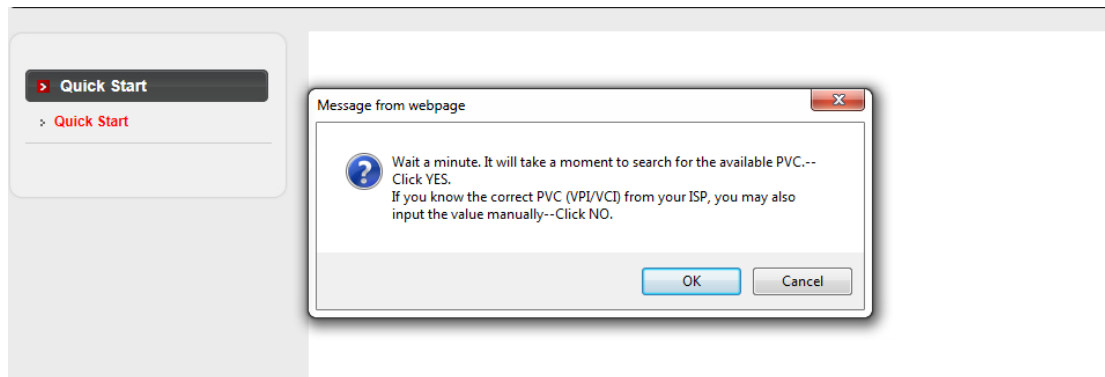
### 4.1 Quick Start



Click START to start Quick Start guide



The Wizard will guide you through these four quick steps. Begin by clicking on NEXT



Click NO if you know the correct PVC(VPI/VCI) from your ISP, you can input the value manually. And if you don't know the correct value, please click OK , it will take a moment to search for the available PVC.

After the PVC value be input or searched, please click NEXT.

Choose the correct way to access the internet which you have got from your ISP.

Enter the PPPoE/PPPoA information provided to you by your ISP, Click NEXT to continue.



You may enable/disable Wireless, change the wireless SSID and authentication type in this page, then click NEXT to continue.

Click NEXT to save the current settings

Save Change !

## 4.2 Status

Choose **Status**, you can see the next submenus: Device info and Statistics.

Click any of them, and you will be able to see the information and statistics of the Modem Router.

### 4.2.1 Device Information

**Device\_info>Device\_info** shows the basic information of the Modem Router, including System, DSL, LAN Configuration, DNS Status, WAN Configuration and WAN IPV6 Configuration.

**ADSL Router Status**

This page shows the current status and some basic settings of the device.

### System

Alias Name	ADSL Modem
Uptime	0 0:11:50
Date/Time	Thu Jan 1 0:11:50 1970
Firmware Version	V2.11
Built Date	Sep 12 2012 11:55:33
Serial Number	081078111135

### DSL

Operational Status	--
Upstream Speed	--
Downstream Speed	--

### LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	08:10:78:11:11:35

### DNS Status

DNS Mode	Auto
DNS Servers	
IPv6 DNS Mode	Auto
IPv6 DNS Servers	

### WAN Configuration

Interface	VPI/VC1	Encap	Droute	Protocol	IP Address	Gateway	Status
pppoe1	0/35	LLC	On	PPPoE	0.0.0.0	0.0.0.0	down 0 0:0:0 /0 0:0:0 <a href="#">connect</a>

### WAN IPV6 Configuration

Interface	VPI/VC1	Encap	Protocol	IPv6 Address	Gateway	Droute	Status
pppoe1	0/35	LLC	PPPoE				down

[Refresh](#)

**Device\_info>ADSL** shows the setting of the Modem Router.

### ADSL Configuration

This page shows the setting of the ADSL Router.

Adsl Line Status	ACTIVATING.
Adsl Mode	--
Up Stream	--
Down Stream	--
Attenuation Down Stream	--
Attenuation Up Stream	--
SNR Margin Down Stream	--
SNR Margin Up Stream	--
Vendor ID	
Firmware Version	4923c106
CRC Errors	--
Up Stream BER	--
Down Stream BER	--
Up Output Power	--
Down Output Power	--
Down Stream ES	--
Up Stream ES	--
Down Stream SES	--
Up Stream SES	--
Down Stream UAS	--
Up Stream UAS	--

Adsl Retrain:
Retrain
Refresh

## 4.2.2 Statistics

**Status>Statistics** shows the packet statistics for transmission and reception regarding to network interface.

**Statistics**

This page shows the packet statistics for transmission and reception regarding to network interface.

**Statistics:**

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
e1	666	0	0	631	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	56045	0	0	1526	0	63014
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
w6	0	0	0	0	0	0
w7	0	0	0	0	0	0
w8	0	0	0	0	0	0
w9	0	0	0	0	0	0
w10	0	0	0	0	0	0
w11	0	0	0	0	0	0
w12	0	0	0	0	0	0
w13	0	0	0	0	0	0

## 4.3 Setup

Choose **Setup**, you can see the next submenus: WAN, LAN and WLAN.

Click any of them, and you will be able to configure the corresponding functions.

## 4.3.1 WAN

### 4.3.1.1 WAN-(Channel Configuration)

To enjoy the surfing, we should have the most basic configuration of the router at first. In this chapter, you can set the basic network parameters required to access the Internet.

The router supports the following three common means to access:

Dynamic IP access: ISP (such as China Telecom) assigns IP address to users via DHCP.

Static IP access: ISP provides a static IP address to users.

PPPoE/PPPoA dial-up access(ADSL): use PPPoE/PPPoA virtual dial-up connection to the Internet.

Choose **Setup> WAN>WAN** menu, you will be able to configure the parameters for the channel operation modes of your ADSL Modem/Router

**Channel Configuration**  
This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

Default Route Selection: ☐ Auto ☒ Specified

VPI:  VCI:

Encapsulation: ☒ LLC ☐ VC-Mux

Channel Mode:  (Dropdown menu shows: 1483 Bridged, 1483 MER, PPPoE, PPPoA, 1483 Routed, IPoA)

Enable IGMP: ☐ Enable NAPT: ☐

PPP Settings:

User Name:  Password:

Type:  Idle Time (min):

WAN IP Settings:

Type: ☒ Fixed IP ☐ DHCP

Local IP Address:  Remote IP Address:

Netmask:

Default Route: ☐ Disable ☒ Enable ☐ Auto

Unnumbered: ☐

Connect Disconnect Add Modify Delete Undo Refresh

Current ATM VC Table:

There are many parameters on the channel configuration:

**VPI:** ATM VPI for the PVC channel. The valid range is from 0 to 255. Please input the value provided by your ISP.

**VCI:** ATM VCI for the PVC channel. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.

**Encapsulation:** AAL5 encapsulation mode for the PVC channel: LLC/SNAP or VC-mux.

**Channel mode:** operation of the PVC channel, it can be 1483 Bridged, 1483 MER, PPPoE, PPPoA, 1483 Routed and IPoA.

**Enable NAPT:** Enable or disable the NATP function of the PVC channel.

**Enable IGMP:** Enable or disable the IGMP function of the PVC channel.

**User name:** username of the PPP connection.

**Password:** Password of the PPP connection.

**Type:** The type of PPP dial-up: continuous, manual or connect-on-demand.

**Idle time:** The idle time of the PPP connection when the type is connect-on-demand.

#### **WAN IP settings :**

**Type:** the type of the wan IP settings: fixed or DHCP.

**Local IP address:** the IP address of the router on the PVC channel.

**Remote IP address:** the gateway's IP address of the router on the PVC channel.

**Netmask:** the subnet mask of the router on the PVC channel.

**Default route:** the mode of the default route of the router.

#### **1. Dynamic IP Address·**

Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

## Channel Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

Default Route Selection:		<input type="radio"/> Auto <input checked="" type="radio"/> Specified	
VPI: <input type="text" value="0"/>	VCI: <input type="text" value="35"/>		
Encapsulation:	<input checked="" type="radio"/> LLC <input type="radio"/> VC-Mux		
Channel Mode: <input type="text" value="1483 MER"/>	Enable NAPT: <input checked="" type="checkbox"/>		
Enable IGMP: <input type="checkbox"/>			
IP Protocol:		<input type="text" value="Ipv4/Ipv6"/>	
PPP Settings:			
User Name: <input type="text"/>	Password: <input type="text"/>		
Type: <input type="text" value="Continuous"/>	Idle Time (min): <input type="text"/>		
WAN IP Settings:			
Type:	<input type="radio"/> Fixed IP <input checked="" type="radio"/> DHCP		
Local IP Address:	<input type="text"/>	Remote IP Address:	<input type="text"/>
Netmask:	<input type="text"/>		
Default Route:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="radio"/> Auto		
Unnumbered:	<input type="checkbox"/>		
IPv6 WAN Setting:			
Address Mode:	<input type="text" value="Slac"/>		
Enable DHCPv6 Client: <input type="checkbox"/>			
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>			

**VPI/VCI:** enter the VPI/VCI provided by your ISP.

**Channel Mode:** Select "1483 MER".

**WAN IP Settings:** set "Type" as DHCP

**Default Route:** Enable

Then click the “Add” button to setup a new connection, when the connection is setup, you can see the router will obtain an IP address.

## 2. Static IP Address

If your means of access to the Internet is “Static IP” mode, enter the fixed IP address, mask, gateway address the ISP offers to you.

### Channel Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

Default Route Selection:		<input type="radio"/> Auto <input checked="" type="radio"/> Specified	
VPI: <input type="text" value="0"/>	VCI: <input type="text" value="35"/>		
Encapsulation:	<input checked="" type="radio"/> LLC <input type="radio"/> VC-Mux		
Channel Mode: <input type="text" value="1483 MER"/>	Enable NAPT: <input checked="" type="checkbox"/>		
Enable IGMP: <input type="checkbox"/>			
IP Protocol:		<input type="text" value="Ipv4/Ipv6"/>	
PPP Settings:			
User Name: <input type="text"/>	Password: <input type="text"/>		
Type: <input type="text" value="Continuous"/>	Idle Time (min): <input type="text"/>		
WAN IP Settings:			
Type:	<input checked="" type="radio"/> Fixed IP	<input type="radio"/> DHCP	
Local IP Address:	<input type="text" value="192.168.1.111"/>	Remote IP Address:	<input type="text" value="192.168.2.240"/>
Netmask:	<input type="text" value="255.255.255.0"/>		
Default Route:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	<input type="radio"/> Auto



Unnumbered:	<input type="checkbox"/>
IPv6 WAN Setting:	
Address Mode:	Slaac ▼
Enable DHCPv6 Client: <input type="checkbox"/>	
<div>Connect Disconnect Add Modify Delete Undo Refresh</div>	

**VPI/VCI:** enter the VPI/VCI provided by your ISP.

**Channel Mode:** Select “1483 MER”.

**WAN IP Settings:** set “Type” as Fixed IP

**Default Route:** Enable

Then click the “Add” button to setup a new connection, when the connection is setup, you can see the router will obtain an IP address.

**Note:** Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x), such as 192.168.1.100. The Router will not accept the IP address if it is not in this format.

### 3. PPPoE/PPPoA

If your means of access to the Internet is “ADSL virtual dial-up” mode, enter the username and password the ISP provide to your account, and choose the type of PPP connection.

## Channel Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

Default Route Selection:		<input type="radio"/> Auto <input checked="" type="radio"/> Specified	
VPI: <input type="text" value="0"/>	VCI: <input type="text" value="35"/>		
Encapsulation:	<input checked="" type="radio"/> LLC <input type="radio"/> VC-Mux		
Channel Mode: <input type="text" value="PPPoE"/>	Enable NAPT: <input checked="" type="checkbox"/>		
Enable IGMP: <input type="checkbox"/>			
IP Protocol:		<input type="text" value="Ipv4/Ipv6"/>	
PPP Settings:			
User Name: <input type="text" value="test"/>	Password: <input type="text" value="*****"/>		
Type: <input type="text" value="Continuous"/>	Idle Time (min): <input type="text"/>		
<div> Continuous  Continuous  Connect on Demand  Manual </div>			
WAN IP Settings:			
Type:	<input checked="" type="radio"/> Fixed IP	<input type="radio"/> DHCP	
Local IP Address:	<input type="text"/>	Remote IP Address:	<input type="text"/>
Netmask:	<input type="text"/>		
WAN IP Settings:			
Type:	<input checked="" type="radio"/> Fixed IP	<input type="radio"/> DHCP	
Local IP Address:	<input type="text"/>	Remote IP Address:	<input type="text"/>
Netmask:	<input type="text"/>		
Default Route:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	<input type="radio"/> Auto
Unnumbered:	<input type="checkbox"/>		
IPv6 WAN Setting:			
Address Mode:	<input type="text" value="Slac"/>		
Enable DHCPv6 Client: <input type="checkbox"/>			
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>			

**VPI/VCI:** enter the VPI/VCI provided by your ISP.

**Channel Mode:** Select “PPPoE” or “PPPoA”.

**PPP Settings:** Select “Continuous” or “Connect on demand” or “Manual”. (If the type is “connect on demand”, you should also set the Idle Time.)

**Encapsulation:** For both PPPoA/PPPoE connection, you need to specify the type of Multiplexing, either LLC or VC -Mux.

**Default Route:** Enable

Then click the “Add” button to setup a new connection, when the connection is setup, you can show the router will obtain an IP address after the dial-up.

#### 4. Bridge Mode

If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

The screenshot shows a configuration window for Bridge Mode. Under the 'Encapsulation' heading, there are four radio button options: 'Dynamic IP Address', 'Static IP Address', 'PPPoA/PPPoE', and 'Bridge Mode'. The 'Bridge Mode' option is selected. Below this, under the 'Bridge Mode' heading, there is a label 'Encapsulation' followed by a dropdown menu currently showing '1483 Bridged Only LLC'. At the bottom of the window are two buttons: 'APPLY/SAVE' and 'DELETE'.

**Note:** After you finish the internet configuration, please click **APPLY/SAVE** to make the settings take effect.

#### 4.3.1.2 Auto PVC configuration

Click Auto PVC in the left pane, page shown in the following figure appears. In this page, you can get PVC automatically through detecting function, and add or delete the PVC that you do not want.



**ATM Settings**

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS, PCR, CDVT, SCR and MBS.

VPI: <input type="text"/>	VCI: <input type="text"/>	Qos: <input type="text" value="UBR"/>	
PCR: <input type="text"/>	CDVT: <input type="text"/>	SCR: <input type="text"/>	MBS: <input type="text"/>

Adsl Retrain:

**Current ATM VC Table:**

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	0	35	UBR	6144	0	---	---

Click “Apply Changes” to save your configurations, and “Undo” to discard your settings.

**4.3.1.4 ADSL**

Choose **Setup> WAN> ADSL** menu, you can choose which ADSL modulation settings your modem router will support.

**ADSL Settings**

This page allows you to choose which ADSL modulation settings your modem router will support.

<b>ADSL modulation:</b>	<input type="checkbox"/> G.Lite
	<input checked="" type="checkbox"/> G.Dmt
	<input checked="" type="checkbox"/> T1.413
	<input checked="" type="checkbox"/> ADSL2
	<input checked="" type="checkbox"/> ADSL2+
<b>AnnexL Option:</b>	<input checked="" type="checkbox"/> Enabled
<b>AnnexM Option:</b>	<input type="checkbox"/> Enabled
<b>ADSL Capability:</b>	<input checked="" type="checkbox"/> Bitswap Enable
	<input checked="" type="checkbox"/> SRA Enable

Click “Apply Changes” after you configure the ADSL parameters.

### 4.3.2 LAN

Choose **Setup> LAN** menu, and you will see the sub-manuals including LAN, DHCP, DHCP Statistics and LAN IPv6. Please configure the parameters for LAN ports according to the descriptions below.

#### 4.3.2.1 LAN

Go to **Setup>LAN>LAN page**, you can configure the LAN interface of your ADSL Router. You may change the setting for IP address, subnet mask, etc..

#### LAN IP Setting:

**LAN Interface Setup**

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresss, subnet mask, etc..

Interface Name:	Ethernet1	
IP Address:	<input type="text" value="192.168.1.1"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>	
<input type="checkbox"/> Secondary IP		
IGMP Snooping:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable

**Apply Changes**

**IP address:** The IP address of the ADSL router's LAN interface, the default value is 192.168.1.1.

**Subnet mask:** The subnet mask of the ADSL router's LAN interface, the default value is 255.255.255.0.

**Secondary IP:** If you enable the "Secondary IP", you should configure another IP address and subnet mask for the LAN interface.

**IGMP Snooping:** You can enable/disable the IGMP Snooping function by the select radio.

#### Note:

If you change the IP address of the LAN interface, you should use the new IP address to reconnect to the web server.

The first IP and secondary IP must belong to different subnet.

## Ethernet Link Speed/Duplex Mode:

On LAN interface setup, you can also configure each Ethernet port's link speed/duplex mode.

LAN Port:	LAN4 ▼
Link Speed/Duplex Mode:	▼

**Modify**

**ETHERNET Status Table:**

Select	Port	Link Mode
<input type="radio"/>	LAN1	AUTO Negotiation
<input type="radio"/>	LAN2	AUTO Negotiation
<input type="radio"/>	LAN3	AUTO Negotiation
<input type="radio"/>	LAN4	AUTO Negotiation

**LAN Port:** specify the LAN port number of the switch, it can be LAN1, LAN2, LAN2 and LAN4

**Link Speed/Duplex Mode:** the mode of the selected LAN port, the default value is "Auto Negotiation"

Link Speed/Duplex Mode:	▼
-------------------------	---

**Modify**

**ETHERNET Status Table:**

Select	Port	Link Mode
<input type="radio"/>	LAN1	AUTO Negotiation
<input type="radio"/>	LAN2	AUTO Negotiation
<input type="radio"/>	LAN3	AUTO Negotiation
<input type="radio"/>	LAN4	AUTO Negotiation

You can select a LAN port to modify its link speed/duplex mode.

### Note:

If you configure the LAN port to a new mode, such as "100Mbps/Full Duplex", you must make the same configuration on the PC's NIC which the LAN port is connected to, that is means you should configure the mode on the PC's NIC to be "100Mbps/Full Duplex".

## MAC Address Control:

The router supports the MAC address control on Ethernet port.

<b>MAC Address Control:</b>	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4 <input type="checkbox"/> WLAN				
<input type="button" value="Apply Changes"/>					
<b>New MAC Address:</b>	<input type="text"/>		<input type="button" value="Add"/>		

Current Allowed MAC Address Table:	
MAC Addr	Action

**MAC Address Control:** select the LAN interface on which you want to run MAC Address Control

**New MAC Address:** a MAC address to be added

**Current Allowed MAC Address Table:** it shows the current allowed MAC address list

If you enable the MAC address control on a interface such as “LAN1”, then the traffic from the specified interface “LAN1” only whose MAC address matches the allowed list will be flowed, otherwise the traffic will be dropped by the router.

### 4.3.2.2 DHCP:

Go to the Setup->LAN->DHCP page, you can configure the DHCP mode of your ADSL Router as None, DHCP Relay or DHCP Server.

#### 4.3.2.2.1 None

If the DHCP mode is “None”, the router will do nothing when the hosts request an IP address by DHCP protocol.

#### 4.3.2.2.2 DHCP Server

The DHCP Server is used to configure correct TCP/IP protocol related parameters for the computer on you local network. If you enable the DHCP Server function of the ADSL router, you can make the DHCP Server automatically configure the TCP/IP protocol parameters (such as IP address, subnet mask, gate way and DNS servers) for the computer on you local network.



### DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.

(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.

(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

LAN IP Address:	192.168.1.1		
Subnet Mask:	255.255.255.0		
DHCP Mode	<div> <div>DHCP Server</div> <div>None</div> <div>DHCP Relay</div> <div>DHCP Server</div> </div>		
Interface:	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input checked="" type="checkbox"/> LAN4 <input checked="" type="checkbox"/> WLAN <input checked="" type="checkbox"/> VAP0 <input checked="" type="checkbox"/> VAP1 <input checked="" type="checkbox"/> VAP2 <input checked="" type="checkbox"/> VAP3		
IP Pool Range	192.168.1.64	-	192.168.1.253 <button>Show Client</button>
Subnet Mask:	0.0.0.0		
Default Gateway:	0.0.0.0		
Max Lease Time:	1440	minutes	

**DHCP Mode:** the DHCP mode can be DHCP Server, DHCP Relay and None.

**Interface:** you can specify which interface you want to enable DHCP Server.

**IP Pool Range:** the DHCP IP pool address. IP Address must be 192.168.1.2 or greater, but must smaller than 192.168.1.254.

**Default Gateway:** the default gateway address

**Max Lease Time:** the time that the DHCP client is allowed to maintain a network connection.

**Domain Name:** a user-friendly name that refers to the group of hosts ( subnet ) that will be assigned addresses from this pool

**DNS Server:** the IP address of DNS server used in option filed of DHCP message.

#### 4.3.2.2.3 DHCP Relay

If you are using the other DHCP Server to assign IP address to your hosts on the LAN, you can set the relay server's IP address.

### DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.

(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.

(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Mode	DHCP Relay ▼

Relay Server:	192.168.2.242
---------------	---------------

**DHCP Relay:** Select Relay, then you will see the next screen, the Modem Router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure that the routing table has the correct routing entry.

### 4.3.2.3 DHCP Static

DHCP Static IP table shows the IP address and MAC address the client obtained from the DHCP Server. You can manually input IP and MAC address to make a static assignment. Router searches the relevant entry in this table to assign IP address according to the client's MAC address. If the router can't find a corresponding static entry, it will choose an unallocated IP address from DHCP pool assign to the client.

Go to **Setup->LAN->DHCP Static** page, you can set the DHCP static rules.

**DHCP Static IP Configuration**

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address:	<input type="text" value="0.0.0.0"/>
Mac Address:	<input type="text" value="000000000000"/> (ex. 00E086710502)

**Current ATM VC Table:**

Select	IP Address	MAC Address
--------	------------	-------------

Then the client with MAC address "00:00:00:00:00:01" will be assigned an IP address of 192.168.1.64 through DHCP.

**4.3.2.4 IPv6**

Click LAN IPv6 in 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

WAN

LAN

LAN

DHCP

DHCP Static

LAN IPv6

WLAN

**LAN IPv6 Setting**

This page is used to configure ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

**Lan Global Address Setting**

Global Address:  /

**RA Setting**

Enable: ☒

M Flag: ☒

O Flag: ☒

Max Interval:  Secs

Min Interval:  Secs

Prefix Mode:	Auto
ULA Enable:	<input checked="" type="checkbox"/>
Prefix Address:	<input type="text"/>
Prefix Length:	<input type="text"/> [16 - 64]
Preferred Time:	<input type="text"/> [600 - 2147483647 S] or [-1 S]
Valid Time:	<input type="text"/> [600 - 2147483647 S] or [-1 S]
<b>Apply Changes</b>	
<b>DHCPv6 Setting</b>	
DHCPv6 Mode:	None
<b>Apply Changes</b>	

**Global Address:** Specify the lan global ipv6 address, may be assigned by ISP

**Enable:** Enable or disable the Router Advertisement feature

**M Flag:** Enable or disable the “Managed address configuration” flag in RA packet

**O Flag:** Enable or disable the “Other configuration” flag in RA packet

**Prefix Mode:** Specify the RA feature prefix mode: “Auto”: the RA prefix will use Wan dhcp-pd prefix.

**DHCPv6 Mode:** “Manual”: user will specify the prefix Address, Length, Preferred time and Valid time.

DHCPv6 Mode Specify the dhcpv6 server mode:

“None” : close dhcpv6 server.

“Manual” : dhcpv6 server is opened and user specify the dhcpv6 server address pool and other parameters.

“Auto” : dhcpv6 server is opened and it use Wan dhcp-pd prefix to generate address pool.

### 4.3.3 WLAN

To connect to the Wireless AP, we should have the most basic configuration of the router at first. In this section, you can set the wireless network parameters required to access the AP of your WLAN interface.

### 4.3.3.1 Basic Settings

Go to Setup->WLAN->Basic page, you can configure the wireless parameters.

**Wireless Basic Settings**  
This page is used to configure the parameters for your wireless network.

<input type="checkbox"/> Disable Wireless LAN Interface	
Band:	2.4 GHz (B+G+N) ▾
Mode:	AP ▾
SSID:	netis
Channel Width:	40MHZ ▾
Control Sideband:	Upper ▾
Channel Number:	Auto ▾ Current Channel: 1
Radio Power (Percent):	100% ▾
Associated Clients:	Show Active Clients

Apply Changes

Here you may enable or disable the wireless function. You can also change the wireless parameters, such as Band, SSID, Channel Width, Control Sideband, Channel Number and Radio Power.

**Band:** In the drop-down list you can select the band type. For example: 2.4G b+g+n allows 2.4G 802.11b, 802.11g and 802.11n wireless clients to connect to this wireless Modem Router.

**Mode:** In the drop-down list, you can select AP or AP+WDS, which allows wireless station to associate with AP or AP+WDS.

**Channel Number:** Select the channel you want to use from the drop-down List of channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

**Channel Width:** Select the Channel Width you want to use from the drop-down List. If bigger bandwidth is selected, device could transmit and receive data with higher speed.

### 4.3.3.2 Security

Go to Setup->WLAN-> Security page, you can configure the wireless security parameters.

**Wireless Security Setup**

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

<b>SSID TYPE:</b>	<input checked="" type="radio"/> Root <input type="radio"/> VAP0 <input type="radio"/> VAP1 <input type="radio"/> VAP2 <input type="radio"/> VAP3		
<b>Encryption:</b>	None WEP WPA (TKIP) WPA (AES) WPA2(AES) WPA2(TKIP) WPA2 Mixed	<input type="button" value="Set WEP Key"/>	
<input type="checkbox"/> Use 802.11n	<input type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits		
<b>WPA Authentication:</b>	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)		
<b>Pre-Shared Key Format:</b>	Passphrase		
<b>Pre-Shared Key:</b>	<input type="text"/>		
<b>Authentication RADIUS Server:</b>	Port <input type="text" value="1812"/>	IP address <input type="text" value="0.0.0.0"/>	Password <input type="text"/>

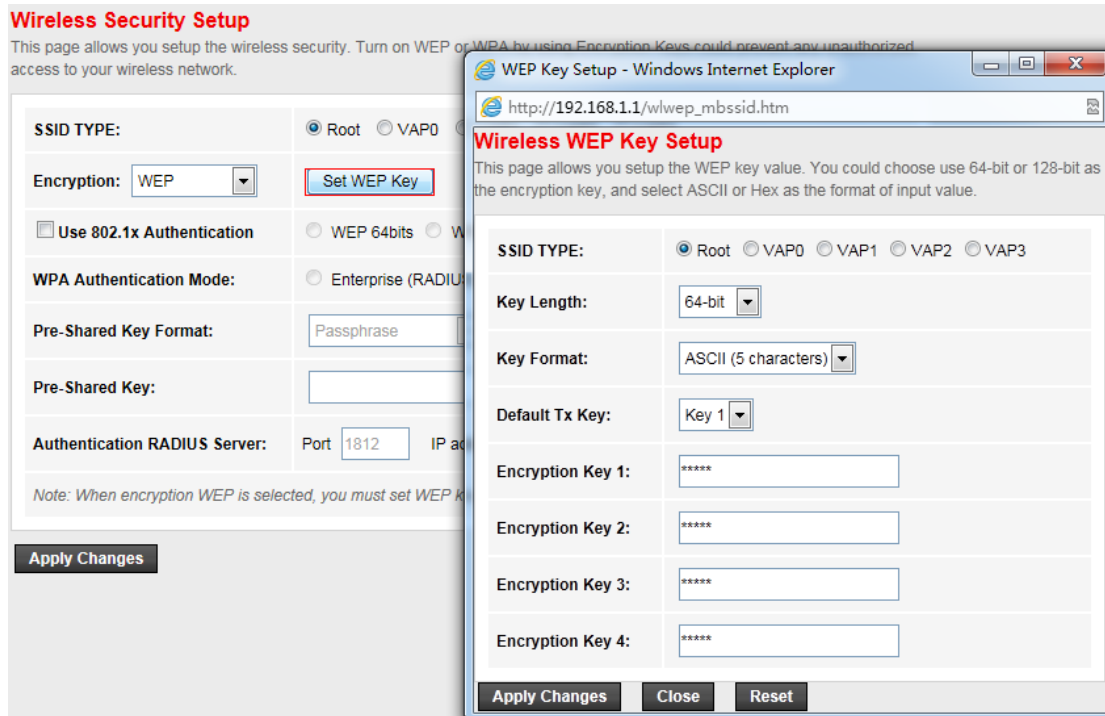
*Note: When encryption WEP is selected, you must set WEP key value.*

Here you can choose the encryption method to prevent any unauthorized access to your wireless network.

There are three most commonly used encryption method (a total of six encryption support), including the WEP encryption, WPA(TKIP), WPA2(AES), etc.

#### (1) WEP

If the encryption is WEP, you should click "Set WEP key" button to enter the WEP key setup page.



Here you can choose the SSID type (root SSID or virtual Access Point) and set the WEP key length, key format and Default Tx key.

- SSID TYPE: choose the SSID you want to configure, there are can be root SSID or virtual Access Point
- Key Length: the length of the WEP key, it can be 64 bits or 128 bits
- Key Format: the format of the WEP key, it can be ASCII or hex
- Encryption key: the WEP key
- Default Tx Key: you can select one key from the follow 4 Encryption key as the current key

If you want to use 802.1x authentication, you can enable this option on the checkbox. You should set the port, IP address and password for the authentication radius server.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

<b>SSID TYPE:</b>	<input checked="" type="radio"/> Root <input type="radio"/> VAP0 <input type="radio"/> VAP1 <input type="radio"/> VAP2 <input type="radio"/> VAP3		
<b>Encryption:</b>	WEP <span>▼</span>	Set WEP Key	
<input checked="" type="checkbox"/> Use 802.1x Authentication	<input type="radio"/> WEP 64bits <input checked="" type="radio"/> WEP 128bits		
<b>WPA Authentication Mode:</b>	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)		
<b>Pre-Shared Key Format:</b>	Passphrase <span>▼</span>		
<b>Pre-Shared Key:</b>	<input type="text"/>		
<b>Authentication RADIUS Server:</b>	Port <input type="text" value="1812"/>	IP address <input type="text" value="0.0.0.0"/>	Password <input type="password" value="....."/>
<i>Note: When encryption WEP is selected, you must set WEP key value.</i>			
Apply Changes			

### (2) WPA/WPA2

There are two WPA encryption rules: AES and TKIP, you can select anyone as the encryption. There are also two WPA Authentication mode, it can be either Enterprise (RADIUS) or Personal (Pre-Shared Key).

The most commonly used authentication mode is Pre-Shared Key. You should set the Pre-Shared Key Format and Pre-Shared Key value.

- Pre-Shared Key Format: it can be either Passphrase or Hex (64 characters)
- Pre-Shared Key: the value of the Pre-Shared Key

If the authentication mode is RADIUS, you should set the port, IP address and password for the authentication radius server.



### Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE:	<input checked="" type="radio"/> Root <input type="radio"/> VAP0 <input type="radio"/> VAP1 <input type="radio"/> VAP2 <input type="radio"/> VAP3		
Encryption:	WPA (TKIP) ▼	Set WEP Key	
<input type="checkbox"/> Use 802.1x Authentication	<input type="radio"/> WEP 64bits <input checked="" type="radio"/> WEP 128bits		
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)		
Pre-Shared Key Format:	Passphrase ▼		
Pre-Shared Key:	12345678		
Authentication RADIUS Server:	Port 1812	IP address 0.0.0.0	Password .....
<i>Note: When encryption WEP is selected, you must set WEP key value.</i>			
Apply Changes			

### 4.3.3.3 MBSSID

Go to Setup->WLAN-> MBSSID page, you can configure the parameters for the virtual access point.

### Wireless Multiple BSSID Setup

This page allows you to set virtual access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

<input checked="" type="checkbox"/> Enable VAP0	
SSID:	CTC-0000
broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
<input type="checkbox"/> Enable VAP1	
SSID:	CTC-1111
broadcast SSID:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

<input type="checkbox"/> Enable VAP2	
SSID:	CTC-2222
broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

<input checked="" type="checkbox"/> Enable VAP3	
SSID:	CTC-3333
broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

**Apply Changes**

#### 4.3.3.4 Access Control

Go to Setup>WLAN>Access Control Wireless access control function is used to allow or prohibit the client access to the wireless network by MAC address.

##### Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:	<div> <div>Allow Listed</div> <div>Disable</div> <div>Allow Listed</div> <div>Deny Listed</div> </div>	<b>Apply Changes</b>
MAC Address:	<input type="text" value="00e086710502"/>	<input type="button" value="Add"/> <input type="button" value="Reset"/>

Current Access Control List:	
MAC Address	Select
00e086710502	<input type="radio"/>

**Wireless Access Control Mode:** in the drop-down list, you can select "Disable", "Allow Listed" and "Deny Listed".

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

**MAC Address:** input the MAC address in the blank, and click “Add” to add it to “Current Access Control List”

#### 4.3.3.5 Advanced

Go to Setup>WLAN>Advanced page, you can configure the Wireless Advanced Settings.

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access

##### Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
DTIM Interval:	<input type="text" value="1"/> (1-255)
Data Rate:	<input type="text" value="Auto"/>
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Relay Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ethernet to Wireless Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wifi Multicast to Unicast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

**Apply Changes**

#### 4.3.3.6 Wi-Fi Protected Setup

Go to Setup>WLAN>WPS, you can change the setting for WPS (Wi-Fi Protected Setup).

Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

### Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

<input type="checkbox"/> Disable WPS		
WPS Status:	<input type="radio"/> Configured <input checked="" type="radio"/> UnConfigured	
Self-PIN Number:	<input type="text" value="46740144"/>	<input type="button" value="Regenerate PIN"/>
Push Button Configuration:	<input type="button" value="Start PBC"/>	
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>		
<input type="text"/>		<input type="button" value="Start PIN"/>

There are two modes of WPS settings:

#### 4.3.4 Wireless

**Broadcast SSID:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Modem Router. To broadcast the Router's SSID, keep the default setting. If you don't want to broadcast the Router's SSID, select No.

**Use WPS:** It allows you to add a new wireless device to an existing network quickly by pushing WPS button if your wireless adapter also supports Wi-Fi Protected Setup.

**WPS Settings:** These are the settings of WPS. It shows only when you enabled 'Use WPS'. In this condition, you can just leave the Authentication Type as OPEN.

**WPS state:** Show the configuration states of WPS function.

**WPS mode:** You can set the WPS either via pressing the WPS button or enter the PIN number manually.

##### I . PIN code

Please write down the PIN code of your wireless network adapter and enter it into the bar of enrollee PIN code. Then push the WPS button on your adapter. The WPS light will first get flashing then solid on if the operation succeeds.

##### II .PBC

First, push the button of WPS on this Modem Router, release it. Then turn to your wireless network adapter, push the WPS button and release it. Wait a moment, the WPS will become flashing then finally get solid on if the connection is successful.

**Note:**

**1) This feature is available only when OPEN, WPA-PSK, WPA2-PSK or WPA/WPA2-PSK mode is configured.**

**2) To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.**

**WPS progress:** Idle or In progress, shows the progress of WPS

**Authentication Type:** Select an authentication type from the drop-down list, which allows you to configure security features of the wireless LAN interface. Options available are: Disabled, WEP-64Bits, WEP-128Bits, WPA-PSK, and WPA2-PSK.

**I . WEP-64 Bits:**

To configure WEP-64Bits settings, select the WEP-64Bits option from the drop-down list. The menu will change to offer the appropriate settings. WPA-64Bits is a data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11g standard.

**II .WEP-128 Bits**

Select WEP-128 Bits, the menu will change to offer the appropriate settings. 128-bit is stronger than 64-bit.

**III. WPA-PSK**

To configure WPA-PSK settings, select the WPA-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

**IV. WPA2-PSK**

To configure WPA2-PSK settings, select the WPA2-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA2-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

**Encryption:** Select the encryption you want to use: Automatic, TKIP or AES (AES is an encryption method stronger than TKIP).

- **TKIP** (Temporal Key Integrity Protocol): A wireless encryption protocol that provides dynamic

encryption keys for each packet transmitted.

- **AES** (Advanced Encryption Standard): A security method that uses symmetric 128-bit blocks data encryption.

**Pre-Shared Key:** Enter the key shared by the Modem Router and your other network devices. It must be 8-63 ASCII characters or 64 Hexadecimal digits.

**Wireless MAC Address Filter:** Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. To filter wireless clients by MAC Address, either deny or allow access. If you do not wish to filter users by MAC Address, select Deactivated.

**Active:** Used to enable or disable this wireless Mac filter function.

**Action:** Choose Allow or Deny to allow or block wireless access from the devices listed on the screen.

**Mac Address:** Enter the MAC Address you wish to filter in the field.

## 4.3 Advanced Setup

Choose **Advanced Setup**, you can see the next submenus:

**Routing Configuration**  
This page is used to configure the routing information. Here you can add/delete IP routes.

Enable: ☒

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

Add Route Update Delete Selected Show Routes

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
--------	-------	-------------	-------------	---------	--------	-----

Click any of them, and you will be able to configure the corresponding function.

### 4.3.1 Route

Choose **Advanced** , you can see the next submenus:

**Routing Configuration**  
This page is used to configure the routing information. Here you can add/delete IP routes.

**Left Sidebar:**

- > **Route**
  - > **Static Route**
  - > IPv6 Static Route
  - > RIP
- > NAT
- > QoS
- > CWMP
- > Port Mapping
- > Others

**Main Form:**

Enable: ☒

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

**Buttons:** Add Route, Update, Delete Selected, Show Routes

**Static Route Table:**

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
--------	-------	-------------	-------------	---------	--------	-----

**Bottom Message:** Attention Config is modified to make it effective forever!

#### 4.3.1.1 Static Route:

Choose **Advanced** -> **Static Route** menu, and you will see the routing table list:

**Routing Configuration**  
This page is used to configure the routing information. Here you can add/delete IP routes.

**Left Sidebar:**

- > **Route**
  - > **Static Route**
  - > IPv6 Static Route
  - > RIP
- > NAT
- > QoS
- > CWMP
- > Port Mapping
- > Others

**Main Form:**

Enable: ☒

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

**Buttons:** Add Route, Update, Delete Selected, Show Routes

**Static Route Table:**

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
<input type="radio"/>	Enable	192.168.2.0	255.255.255.0	192.168.1.1	1	e1
<input type="radio"/>	Enable	192.168.1.0	255.255.255.0	192.168.1.1	1	e1
<input type="radio"/>	Enable	127.0.0.0	255.0.0.0	192.168.1.1	2	e1

**Bottom Message:** Attention Config is modified to make it effective forever!

Fill the blank space and click **Add Route** button to add a new route.

**Destination:** This parameter specifies the IP network address of the final destination.

**Subnet Mask:** Enter the subnet mask for this destination.

**Next hop:** Enter the IP address of the gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.

**Metric:** Metric represents the cost of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

**Interface:** the WAN interface to which a static route is to be applied.

The Static Route Table shows the current static route entries.

Static Route Table:						
Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
<input type="radio"/>	Enable	192.168.2.0	255.255.255.0	192.168.1.1	1	e1
<input type="radio"/>	Enable	192.168.1.0	255.255.255.0	192.168.1.1	1	e1
<input type="radio"/>	Enable	127.0.0.0	255.0.0.0	192.168.1.1	2	e1

#### 4.3.1.2 IPv6 Static Route:

Route

Static Route
IPv6 Static Route
RIP

NAT
QoS
CWMP
Port Mapping
Others

### IPv6 Routing Configuration

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

Destination:
Prefix Length:
Next Hop:
Interface:

Add Route
Delete Selected

### IPv6 Static Route Table:

Select	Destination	NextHop	Interface
--------	-------------	---------	-----------

**Destination:** Type the destination for the route. The destination can be a host address, network address, or the destination for the default route,

**Prefix length:** Type the prefix length of the destination. The prefix is the part of the address that specifies the network identifier. The prefix length identifies how many bits of the destination address in an IPv6 packet must match the Destination field in this route. A prefix length of 128 means that only an exact match of the destination address can use this route. A prefix length of 0 means that any destination address can use this route.



**Next hop:** Type the IPv6 address for next hop for this route. For LAN interfaces, the gateway address must be configured and must be a directly reachable IP address on the network segment of the selected interface. For demand-dial interfaces, the gateway address is not configured or used.

**Interface:** Lists the available LAN or demand-dial interfaces. Select the one to be used to forward the IP packet if this route is selected.

#### 4.3.1.3 RIP:

RIP is an internet protocol you can setup to share routing table information with other routing devices.

Choose **Advanced->Route->RIP** page, you can configure the RIP settings. Here you can enable or disable the RIP function.

**RIP Configuration**  
Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

RIP: ☐ Off ☒ On

interface:

Recv Version:

Send Version:

**Rip Config List:**

Select	interface	Recv Version	Send Version
--------	-----------	--------------	--------------

Attention Config is modified to make it effective forever!

**RIP:** enable or disable the RIP function of the router.

**Interface:** the interface on which you want to enable RIP

**Recv Version:** indicate the RIP version in which information must be passed to the device it can be accepted into its routing table

**Send Version:** indicate the RIP version this interface will use when it sends its route information to the other device

The RIP Config List shows the current RIP setting of the device.

Rip Config List:			
Select	interface	Recv Version	Send Version
<input type="radio"/>	br0	RIP1	RIP1
<input type="radio"/>	pppoe1	Both	RIP2

## 4.3.2 NAT

Choose **Advanced** -> **NAT** menu, you can setup the NAT (Network Address Translation) function.

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

**DMZ**

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

☐ Enable DMZ

DMZ Host IP Address:

Apply Changes Reset

Attention Config is modified to make it effective forever!

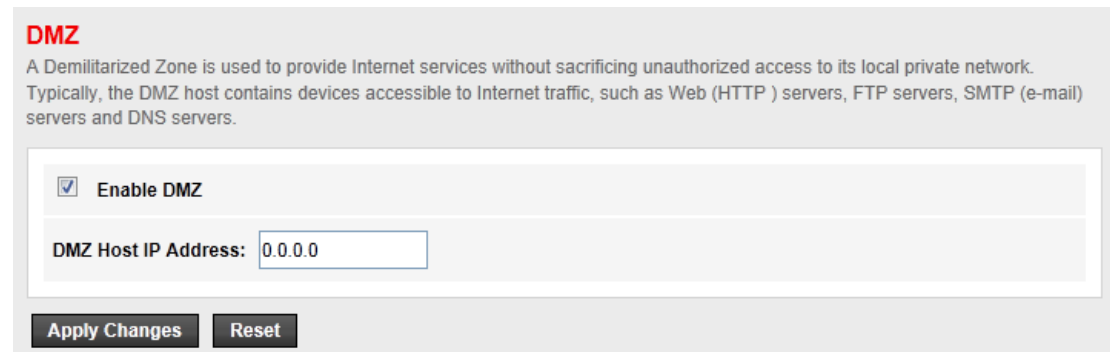
### 4.3.2.1 DMZ:

A Demilitarized Zone (DMZ) allows a single host on your LAN to expose ALL of its ports to the Internet.

Choose **Advanced**->**NAT**->**DMZ** page, you can configure the DMZ settings.

A DMZ (demilitarized zone) is a host between a private local network and the outside public network. Users of the public network outside the company can access to the DMZ host. It allows you to expose one network user to the internet for some special-purpose service such as internet gaming or video conferencing. DMZ hosting forwards all the ports at the same time to

one computer. You should assign a static IP address to the destination computer before you use this feature.



**DMZ**

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

☒ Enable DMZ

DMZ Host IP Address:

**Apply Changes** **Reset**

**DMZ Host IP Address:** Enter the specified IP Address for DMZ host on the LAN side.

**Note:** For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

#### 4.3.2.2 Virtual Server:

Choose **Advanced** -> **NAT**-> **Virtual Server**, you can configure the Virtual Server. The Virtual Server is the servers behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world. You should assign a static IP address to the destination computer before you use this feature.

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

### Virtual Server

This page allows you to config virtual server,so others can access the server through the Gateway.

Service Type:

☒ Usual Service Name: AUTH
 ☐ User-defined Service Name:

Protocol: TCP

WAN Setting: Interface

WAN Interface: pppoe1

WAN Port: 113 (ex. 5001:5010)

LAN Open Port: 113

LAN Ip Address:

Apply Changes

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
FTP	udp	192.168.1.103	22-52	192.168.1.101	22-52	Enable	Delete Disable
Netis	tcp	192.168.1.103	21-21	pppoe1	113-113	Disable	Delete Enable

Attention Config is modified to make it effective forever!

save

**Usual Service Name & User-defined Service Name:** the name of this virtual server

**Protocol:** the protocol of this virtual server used, it include TCP & UDP type.

**WAN Setting:** the WAN setting of this virtual server used; it can be interface and IP address.

**WAN Interface:** the interface on which the virtual server used on WAN side

**WAN IP Address:** the IP address which the virtual server used on WAN side. You can access this IP and WAN port from WAN side to obtain the service.

**WAN Port:** the open port on WAN side. It can be either a single port or a port range.

**LAN Open Port:** Enter the specific start and end port number you want to forward. If it is one port only, you can enter the end port number the same as start port number. For example, you want to set the FTP virtual server, you can set the start and end port number to 21.

**LAN IP Address:** the IP address of the host which provides the service on LAN side.

**Current Virtual Server Forwarding Table:** This displays the information about the virtual servers you establish.

Current Virtual Server Forwarding Table:							
ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
FTP	udp	192.168.1.103	22-52	192.168.1.101	22-52	Enable	Delete Disable
Netis	tcp	192.168.1.103	21-21	pppoe1	113-113	Disable	Delete Enable

Click **Delete/Disable**、**Enable** to make your operation get corresponding effect.

#### 4.3.2.3 ALG:

The router supports several NAT ALG and pass-Through function.

Choose **Advanced->NAT->ALG** page, you can configure the ALG settings. Here you can enable or disable the ALG or pass-through function for each application.

**NAT ALG and Pass-Through**  
Setup NAT ALG and Pass-Through configuration

IPSec Pass-Through:	<input checked="" type="checkbox"/> Enable
L2TP Pass-Through:	<input checked="" type="checkbox"/> Enable
PPTP Pass-Through:	<input checked="" type="checkbox"/> Enable
FTP:	<input checked="" type="checkbox"/> Enable
H.323:	<input checked="" type="checkbox"/> Enable
SIP:	<input checked="" type="checkbox"/> Enable
RTSP:	<input checked="" type="checkbox"/> Enable
ICQ:	<input checked="" type="checkbox"/> Enable
MSN:	<input checked="" type="checkbox"/> Enable

Apply Changes Reset

Attention Config is modified to make it effective forever!  
save

#### 4.3.2.4 NAT EXCLUDE IP:

Click NAT Exclude IP in the left pane, the page shown in the following figure appears. In the page, you can configure some source IP addresses which use the purge route mode when accessing internet through the specified interface.

▼ Route

▼ NAT

> DMZ

> Virtual Server

> ALG

> NAT Exclude IP

> Port Trigger

> FTP ALG Port

> Nat IP Mapping

▼ QoS

▼ CWMP

▼ Port Mapping

▼ Others

Attention Config is modified to make it effective forever!  

save

### NAT EXCLUDE IP

This page is used to config some source ip address which use the purge route mode when access internet through the specified interface.

interface:

pppoe1

IP Range:

 ---

Apply Changes

Reset

⚙️ Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action
pppoe1	192.168.1.10	192.168.1.102	<div>Delete</div>

#### 4.3.2.5 Port Trigger:

Port trigger is used to restrict certain types of data packets from your local network to internet. Use of such filters can be helpful in securing and restricting your local network.

Choose **Advanced->NAT->Port Trigger** page, you can configure the port trigger rules.

**Nat Port Trigger**

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Nat Port Trigger: ☐ Enable ☒ Disable

Apply Changes

Application Type:

☒ Usual Application Name:

☐ User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing

Apply Changes

Current Port Trigger Table:

**Nat Port trigger:** enable or disable the port trigger function on the device

**Application Type:** you can select the service from the “Usual Application Name” or define the name from “User-defined Application Name”

**Start Match Port / End Match port:** the start and end port to match

**Trigger Protocol:** the protocol to trigger the rule, it can be TCP, UDP or TCP/UDP

**Start Relate Port / End Relate Port:** the start and end relate port

**Open Protocol:** it can be TCP, UDP or TCP/UDP

**NAT Type:** it can be outgoing or incoming

#### 4.3.2.6 FTP ALG Port:

FTG ALG port is used to configure the FTP server ALG and FTP client ALG ports.

Choose **Advanced->NAT-> FTP ALG Port page**, you can configure the ftp ALG ports.

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

Attention Config is modified to make it effective forever!

save

FTP ALG Configuration

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

FTP ALG port:

Add Dest Ports Delete Selected DestPort

FTP ALG ports Table:

Select	Ports
<input type="radio"/>	21

If the FTP server listen the port on 2100, you can add a FTP ALG port 2100 on the device.

FTP ALG Configuration

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

FTP ALG port:

Add Dest Ports Delete Selected DestPort

FTP ALG ports Table:

Select	Ports
<input type="radio"/>	21
<input checked="" type="radio"/>	2100

#### 4.3.2.7 Nat IP Mapping:

NAT IP mapping allows you to configure one IP pool for specified source IP address from LAN, so a packet whose source IP is in range of the specified address will select one IP address from pool for NAT.

Choose **Advanced->NAT->NAT IP Mapping page**, you can configure the mapping rules.



**NAT IP MAPPING**

Entries in this table allow you to config one IP pool for specified source ip address from lan, so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

Type:

Local Start IP:

Local End IP:

Global Start IP:

Global End IP:

**Current NAT IP MAPPING Table:**

Local Start IP	Local End IP	Global Start IP	Global End IP	Action
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>				

Attention Config is modified to make it effective forever!

**Type:** the type of this mapping rule. It can be “One-to-One”,

“Many-to-One”, “Many-to-Many” and “One-to-Many”.

- One-to-One: one local IP will be mapped to one global IP
- Many-to-One: the IP between “Local Start IP” and “Local End IP” will be mapped to a global IP
- Many-to-Many: the IP between “Local Start IP” and “Local End IP” will be mapped to the IP between “Global Start IP” and “Global End IP”
- One-to-Many: one local IP will be mapped to any of the IP between “Global Start IP” and “Global End IP”

**Local Start IP:** a local IP address

**Local End IP:** a local IP address

**Global Start IP:** a global IP address used for NAT

**Global End IP:** a global IP address used for NAT

### 4.3.3 QoS

Router provides a control mechanism which serves traffic with different priority. The traffic is classified by criteria. A classification rule contains three configuration blocks: Qos policy, schedule mode and traffic rule. The Qos policy enables you to classify packet on the basis of

various fields in the packet; the schedule mode enables you to configure which priority queue you want to use; the traffic rule enables you to assign the precedence or add marker for different streams.

Choose **Advanced->QoS**, you can configure the precedence for each incoming packet based on specified policy.

**IP QoS**

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.  
Config Procedure:  
1: set traffic rule.  
2: assign the precedence or add marker for different stream.

IP QoS: ☐ disable ☒ enable

Apply

QoS Policy:

Schedule Mode:

**QoS Rule List:**

stream rule						behavior			
src IP	src Port	dest IP	dest Port	proto	phy port	prior	DSCP	802.1p	sel
<input type="button" value="Add rule"/> <input type="button" value="Delete"/> <input type="button" value="Delete all"/>									

**IP QoS:** Enable or disable the IP QoS function on the device

**QoS Policy:** policy of QoS. The traffic will be classified on the base of this policy. It can be based on stream, 802.1p or DSCP.

**Schedule Mode:** the schedule mode of the IP QoS function, it can be strict prior or WFQ (4:3:2:1).

- **Strict prior**  
traffic with different priority will be send by its priority, the higher priority the traffic is, the higher priority the traffic will be send out.
- **WFQ (4:3:2:1)**  
traffic with different priority will be send in proportion of its priority, the four priority traffic will be send out in proportion to 4:3:2:1.

### (1) Stream

If the QoS policy is “stream based”, you should configure the QoS rule. Press the “add rule” button to add a new rule.

**QoS Rule List:**

stream rule						behavior			
src IP	src Port	dest IP	dest Port	proto	phy port	prior	DSCP	802.1p	sel
<div> <div>Add rule</div> <div>Delete</div> <div>Delete all</div> </div>									

**Add QoS Rule**

Src IP:	<input type="text"/>
Src Mask:	<input type="text"/>
Dest IP:	<input type="text"/>
Dest Mask:	<input type="text"/>
Src Port:	<input type="text"/>
Dest Port:	<input type="text"/>
Protocol:	<input type="text"/> ▼
Phy Port:	<input type="text"/> ▼
set priority:	p3(Lowest) ▼
<input type="checkbox"/> insert or modify QoS mark	

add rule

**Src IP:** the source IP address of the rule

**Src Mask:** the source mask of the rule

**Dest IP:** the destination IP address of the rule

**Dest Mask:** the destination mask of the rule

**Src Port:** the source port number of the rule. If the protocol filed is not been selected or is selected as ICMP, the Src port filed can't be configured.

**Dest Port:** the destination port number of the rule. If the protocol filed is not been selected or is selected as ICMP, the Dest port filed can't be configured.

**Protocol:** the protocol of the rule. It can be TCP, UDP, ICMP and TCP/UDP.

**Phy port:** the incoming port of the rule. It indicates the physical port of the traffic is incoming.

The screenshot shows a web interface for configuring QoS rules. It includes a 'Phy Port' dropdown menu, a 'set priority:' field, a checkbox for 'insert or modify QoS mark', and an 'add rule' button. The dropdown menu is open, displaying a list of network interfaces: LAN1, LAN2, LAN3, LAN4, WLAN, WLAN-VAP0, WLAN-VAP1, WLAN-VAP2, and WLAN-VAP3.

**Set Priority:** the priority of the rule. It can be p0(highest), p1,p2,p3(lowest). The traffic matches the rule will be assigned the priority you have configured.

Insert or modify QoS mark: you can insert or modify the DSCP or 802.1p tag. The traffic matches the rule will be added or modified the mark.

**Note:**

**If you select 802.1p tag, please make sure 802.1q is enabled in specified WAN interface, otherwise 802.1p tag will not be tagged.**

The QoS Rule list shows the current rules on the device.

QoS Rule List:

stream rule						behavior			
src IP	src Port	dest IP	dest Port	proto	phy port	prior	DSCP	802.1p	sel
192.168.1.102/32				UDP	LAN2	p2			<input checked="" type="radio"/>
192.168.1.105/32			80	TCP	LAN1	p3			<input type="radio"/>

**Delete:** select a rule then press “delete” button, the selected rule will be deleted from Qos rule list.

**Delete all:** delete all the rules from QoS rule list.

## (2) 802.1p

If the QoS policy is “802.1p based”, you should configure the 802.1p setting. Press the “802.1p config” button to configure the 802.1p priority.

**IP QoS**

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.  
 Config Procedure:  
 1: set traffic rule.  
 2: assign the precedence or add marker for different stream.

IP QoS: ☐ disable ☒ enable

**Apply**

QoS Policy: 802.1p based ▼

Schedule Mode: strict prior ▼

---

**802.1p Set**

this page is used to config 802.1p priority.

⚙️ 802.1p rule list:

802.1p tag	send priority
0	p3(lowest) ▼
1	p3(lowest) ▼
2	p3(lowest) ▼
3	p3(lowest) ▼
4	p3(lowest) ▼
5	p3(lowest) ▼
6	p3(lowest) ▼
7	p3(lowest) ▼

**modify** **close**

**802.1p tag:** the number of 802.1p tag

**Send priority:** the priority to transmit. The traffic matches the 802.1p filed will be assigned this priority.

### (3) DSCP

If the QoS policy is “DSCP based”, you should configure the DSCP setting. Press the “DSCP config” button to configure the DSCP priority.

**IP QoS**

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.

Config Procedure:

1: set traffic rule.

2: assign the precedence or add marker for different stream.

IP QoS:

☐ disable ☒ enable

Apply

QoS Policy:

DSCP based

Schedule Mode:

strict prior

**DSCP Set**  
this page is used to config dscp priority.

DSCP tag: 24 (0-63)

Transmit Prior: p2

Delete Add close

⚙️ dscp rule list:

Select	DSCP tag	Transmit priority
<input checked="" type="radio"/>	24	p2
<input type="radio"/>	25	p3

**DSCP tag:** the value of the DSCP filed

**Transmit prior:** the priority to transmit. The traffic matches the DSCP filed will be assigned this priority.

**DSCP Set**  
this page is used to config dscp priority.

DSCP tag: (0-63)

Transmit Prior: p3(lowest)

Delete Add close

⚙️ dscp rule list:

Select	DSCP tag	Transmit priority
<input checked="" type="radio"/>	0	p2
<input type="radio"/>	8	p1
<input type="radio"/>	24	p2
<input type="radio"/>	25	p3

### 4.3.4 CWMP

CPE WAN Management Protocol (CWMP) is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

Choose **Advanced->CWMP**, you can configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

Route

NAT

QoS

CWMP

CWMP

Port Mapping

Others

Attention Config is modified to make it effective forever!

save

#### TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

ACS:

Enable:

☒

URL:

http://172.21.70.44/cpe/?pd128

User Name:

rtk

Password:

rtk

Periodic Inform Enable:

☐ Disable ☒ Enable

Periodic Inform Interval:

300

seconds

Connection Request:

User Name:

rtk

Password:

rtk

Path:

/tr069

Port:

7547

Debug:

ACS Certificates CPE:

☒ No ☐ Yes

Show Message:

☒ Disable ☐ Enable

CPE Sends GetRPC:

☒ Disable ☐ Enable

Skip MReboot:

☒ Disable ☐ Enable

Delay:

☐ Disable ☒ Enable

Auto-Execution:

☐ Disable ☒ Enable

Apply Changes

Reset

Certificate Management:

CPE Certificate Password:

client

Apply

Undo

CPE Certificate:

浏览...

Upload

Delete

CA Certificate:

浏览...

Upload

Delete

defined in “Periodic Inform Interval” field; when this field is disabled, the device will only send Inform RPC to the ACS server once at the system startup.

Periodic Inform Interval: the interval to send Inform RPC

**Connection Request parameters:**

**User Name:** username the remote ACS should use when connecting to the device

**Password:** password the remote ACS should use when connecting to the device

**Path:** the path of the device Connection Request URL.

**Port:** the port of the device Connection Request URL

### 4.3.5 Port Mapping

The device provides multiple interface groups, up to five interface groups are supported including one default group. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the device can isolate traffic from group to group for some application. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.

Choose Advanced->Port Mapping page, you can configure the mapping group.



Route

NAT

QoS

CWMP

Port Mapping

Port Mapping

Others

Attention Config is modified to make it effective forever!

save

### Port Mapping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

☐ Disable
☒ Enable

WAN

pppoe1

LAN

LAN2  
LAN3  
wlan  
wlan-vap2  
wlan-vap3

Add>

<Del

LAN1  
LAN4  
wlan-vap1  
wlan-vap0

Select	Interfaces	Status
Default	LAN1, LAN2, LAN3, LAN4, wlan, wlan-vap0, wlan-vap1, wlan-vap2, wlan-vap3, pppoe1	Enabled
<input checked="" type="radio"/> Group1		--
<input type="radio"/> Group2		--
<input type="radio"/> Group3		--
<input type="radio"/> Group4		--

Apply

You can enable or disable the port mapping function of the device by the select radio button.

If "Enable" radio is selected, you can configure the mapping group as follow steps:

**Step1:** Select a group from the table, then you can see the available interface (LAN and WAN) and grouped interface list

**Step2:** Select interfaces from the available and grouped interface list and add it to the "Interface group" using "Add>" button or delete it to the "Interface group" using ">Del" button to manipulate the required mapping of the ports.

**Step3:** Click "Apply" button to finish the configuration.

## 4.4 Firewall

### 4.4.1 MAC filter

In order to management your local network better, you can use the MAC address filter function to control the internet access.

Go to **Firewall->MAC Filter** page, you can set the MAC filtering rules.

**Outgoing/Incoming Default Policy:** the default action of outgoing/incoming connection. It can be “Deny” or “Allow”. If the connection doesn’t match any MAC filtering rules, the router will handle the connection with the default action you have set.

**Direction:** the direction of the filter entry, it can be “Outgoing” or “Incoming”.

**Action:** the action of the filter entry, it can be “Deny” or “Allow”. If the action is “Deny”, the connection matches the filter rule will be denied, if the action is “Allow”, the connection matches the filter rule will be allowed.

**Source MAC:** the source MAC address of the filter entry, if empty means matches any source MAC address.

**Destination MAC:** the destination MAC address of the filter entry, if empty means matches any source MAC address.

**Current MAC Filter Table:** it shows the current MAC filtering rules. You can delete the entry on the list.

Current MAC Filter Table:				
Select	Direction	Source MAC	Destination MAC	Action
<input type="checkbox"/>	outgoing	00:e0:86:71:05:02	00:e0:86:71:05:01	deny
<input type="checkbox"/>	incoming	00:e0:86:71:05:02	00:e0:86:71:05:03	deny
<input type="checkbox"/>	outgoing	00:e0:86:71:05:02	00:e0:86:71:05:04	allow

## 4.4.2 IP/Port Filter

### 4.4.2.1 IP/Port Filter

Go to **Firewall->IP/Port Filter** page, you can set the IP/Port filter rules to secure or restrict your local network.

MAC Filter

IP/Port Filter

IP/Port Filter

IPV6/Port Filter

URL Filter

ACL

DoS

Attention Config is modified to make it effective forever!

#### IP/Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy

☒ Permit ☐ Deny

Incoming Default Policy

☐ Permit ☒ Deny

Rule Action:

☒ Permit ☐ Deny

Protocol:

IP

Direction:

Upstream

Source IP Address:

Mask Address:

255.255.255.255

Dest IP Address:

Mask Address:

255.255.255.255

SPort:

-

DPort:

-

Enable:

☒

#### Current Filter Table:

Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action
------	----------	----------------	-------	--------------	-------	-------	-----------	--------

On the front of the page, you can see the default action of outgoing/incoming connection. If the IP connection doesn't match any filter rules, the router will handle the connection with the default action setting.

**Rule Action:** the filter mode of this entry, it can be “Permit” and “Deny”. If the mode is “Permit”, the IP connection matches the rule will be permitted, if the mode is “Deny”, the IP connection matches the rule will be denied.

**Protocol:** the protocol of this entry, it can be “IP”, “ICMP”, “TCP” and “UDP”.

**Direction:** the direction of this entry, it can be “upstream” and “Downstream”.

**Source IP Address/ Mask Address:** the source IP address and mask address of the entry.

**Dest IP Address/ Mask Address:** the destination IP address and mask address of the entry.

**Sport:** If the protocol is “TCP” or “UDP”, you should set the source port of the entry, it can be a single port or a port range.

**Dport:** If the protocol is “TCP” or “UDP”, you should set the destination port of the entry, it can be a single port or a port range.

**Enable:** enable or disable this filter entry.

**Current Filter table:** it shows the current filter rules. You can enable or disable or delete the filter entry.

Current Filter Table:								
Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action
permit	ip	192.168.1.100/255.255.255.255		192.168.1.102/255.255.255.255		enable	Upstream	<div>disable</div> <div>Delete</div>

#### 4.4.2.2 IPv6/Port Filter

Click IPv6/Port Filter in the left pane, the page shown in the following figure appears.

Entries in this table are used to restrict certain types of ipv6 datapackets from your local network to the Internet through the Gateway.

MAC Filter

IP/Port Filter

IP/Port Filter

IPv6/Port Filtering

URL Filter

ACL

DoS

### IPv6/Port Filtering

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy

☒ Permit ☐ Deny

Incoming Default Policy

☐ Permit ☒ Deny

Rule Action:

☒ Permit ☐ Deny

Protocol:

IPv6

Icmp6Type:

PING6

Direction:

Upstream

Source IPv6 Address:

Prefix Length:

Dest IPv6 Address:

Prefix Length:

SPort:

-

DPort:

-

Enable:

☒

Apply Changes

Reset

Help

Current Filter Table:

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6Type	State	Direction	Action
------	----------	--------------------	-------	------------------	-------	-----------	-------	-----------	--------

**Outgoing Default Action:** Display current lan to wan default action

**Incoming Default Action:** Display current wan to lan default action

**Rule Action:** Specify the rule action: Permit or Deny

**Protocol:** Specify the rule protocols: IPv6, ICMP6,TCP or UDP

**Icmp6Type:** When protocol is selected ICMP6, user specify icmp6type, now only support PING6

**Direction:** “Upstream” means lan to wan; “Downstream” meanswan to lan.

**Source IPv6 Address:** Specify the source ipv6 address

**Prefix Length:** Specify the source ipv6 address prefix length

**Dest IPv6 Address:** Specify the destination ipv6 address

**Prefix Length:** Specify the destination ipv6 address prefix length

**Sport:** Specify source port when select TCP or UDP

**DPort:** Specify destination port when select TCP or UDP

**Enable:** Enable or disable this filter rule

**Apply Changes:** Add the rule to system

**Reset:** Reset above items

### 4.4.3 URL filter

In order to manage the site control of your local LAN client, you can use URL filtering function to specify which site can't be accessed.

Go to **Firewall->URL Filter** page, you can add and delete the filtered keyword.

**URL Blocking Capability:** Enable or disable the URL filtering function. If it is enabled, the access to the site which matches the keyword will be blocked by the router, if it is disabled, nothing will be done.

**Keyword:** the keyword of the site you want to block.

**URL Blocking Table:** it shows the current URL filtering entry. You can delete the selected entry.

URL Blocking Table:	
Select	Filtered Keyword
<input type="radio"/>	google.com.hk
<input type="radio"/>	hao123.com

#### 4.4.4 ACL

ACL function is used to specify which services are accessible from LAN or WAN side.

##### 4.4.4.1 ACL

Go to Firewall->ACL page, you can set the ACL entry.

MAC Filter

IP/Port Filter

URL Filter

ACL

IPv6 ACL

DoS

Attention Config is modified to make it effective forever!

save

### ACL Configuration

You can specify which services are accessible from LAN or WAN side. Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway. Using of such access control can be helpful in securing or restricting the Gateway management.

Direction Select:
☒ LAN
☐ WAN

LAN ACL Switch:
☐ Enable
☒ Disable

Apply

IP Address:
 - 
(The IP 0.0.0.0 represent any IP )

Services Allowed:

☐ any

☐ web
☐ telnet
☐ ssh
☐ ftp
☐ tftp
☐ snmp
☐ ping

Add
Reset

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action
--------	-----------	----------------------	---------	------	--------

**Direction Select:** the direction of this ACL entry, it can be LAN or WAN.

**LAN ACL Switch:** you can enable or disable the ACL function on LAN side. If it is disabled, all hosts on LAN side can access the services which your router provide. If it is enabled, only the hosts on the ACL list can access the specify services.

**IP Address:** the IP address of the host, if the IP is 0.0.0.0, it means any IP.

**Service Allowed (LAN side):** the allowed services which the host can access. It can be “any”, or any specified service, such as “web”, “telnet”, “ftp”, “tftp”, “snmp” and “ping”. If select “any”, it means the host can access all the services the router provides.

If the direction is WAN, there are some different settings with LAN side.

MAC Filter

IP/Port Filter

URL Filter

ACL

IPv6 ACL

DoS

Attention Config is modified to make it effective forever!

save

### ACL Configuration

You can specify which services are accessible from LAN or WAN side.  
 Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.  
 Using of such access control can be helpful in securing or restricting the Gateway management.

Direction Select:
☐ LAN
☒ WAN

WAN Setting:

Interface

WAN Interface:

pppoe1

Services Allowed:

web

telnet

ssh

ftp

tftp

snmp

ping

Add

Reset

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action
--------	-----------	----------------------	---------	------	--------

**WAN Setting:** the setting of WAN side, it can be “Interface” or “IP Address”.

WAN Setting:

Interface

Interface

IP Address

WAN Interface:

pppoe1

Services Allowed:

If it is “Interface”, you should specify a WAN interface for this ACL entry.

Direction Select:

☐ LAN
☒ WAN

WAN Setting:

Interface

WAN Interface:

pppoe1

pppoe1

any

Services Allowed:

If the WAN setting is “IP Address”, you should specify the IP address of the host on WAN side.

67



Direction Select:	<input type="radio"/> LAN <input checked="" type="radio"/> WAN	
WAN Setting:	IP Address ▼	
IP Address:	192.168.1.100 - 192.168.1.109	(The IP 0.0.0.0 represent any IP )
Services Allowed:		

**Service Allowed:** you can specify the service and opened port for this service on WAN side.

The host access the specified port can obtain the specified service the router provides.

Direction Select:	<input type="radio"/> LAN <input checked="" type="radio"/> WAN	
WAN Setting:	Interface ▼	
WAN Interface:	any ▼	
Services Allowed:		

<input checked="" type="checkbox"/> web	Port: 80
<input checked="" type="checkbox"/> telnet	Port: 23
<input checked="" type="checkbox"/> ssh	Port: 22
<input checked="" type="checkbox"/> ftp	Port: 21
<input checked="" type="checkbox"/> tftp	Port: 69
<input checked="" type="checkbox"/> snmp	Port: 161
<input checked="" type="checkbox"/> ping	

**Current ACL Table:** it shows the current ACL setting.

Current ACL Table:					
Select	Direction	IP Address/Interface	Service	Port	Action
0	LAN	0.0.0.0	web	80	Delete
1	WAN	pppoe1	telnet	23	Delete

#### 4.4.4.2 ACL IPv6 Configuration

Click IPv6 ACL in the left pane, the page shown in the following figure appears. Entries in this ACL table permit certain types of data packets from your local network or the Internet to the Gateway

**ACL Configuration**

You can specify which services are accessible from LAN or WAN side.  
 Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.  
 Using of such access control can be helpful in securing or restricting the Gateway management.

**Direction Select:** ☒ LAN ☐ WAN

**LAN ACL Switch:** ☐ Enable ☒ Disable

**IP Address:**  /

**Services Allowed:**

☒ Any

**Current IPv6 ACL Table:**

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	<input type="button" value="Delete"/>

**Direction Select:** Select the router interface. You can select LAN or WAN. In this example, LAN is selected

**LAN ACL Switch:** Select it to enable or disable ACL function.

**IP Address:** Enter the IPv6 address of the specified interface. Only the IPv6 address that is in the same network segment with the IPv6 address of the specified interface can access the router.

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

**Add:** After setting the parameters, click it to add an entry to the Current IPv6 ACL Table

**Reset:** Click it to refresh this page.

Set direction of the data packets to WAN, the page shown in the following figure appears

**ACL Configuration**

You can specify which services are accessible from LAN or WAN side. Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway. Using of such access control can be helpful in securing or restricting the Gateway management.

**Direction Select:** ☐ LAN ☒ WAN

**WAN Setting:** Interface

**WAN Interface:** WAN1

**Services Allowed:**

- ☐ web
- ☐ telnet
- ☐ ssh
- ☐ ftp
- ☐ tftp
- ☐ snmp
- ☐ ping6

**Add** **Reset**

**Current IPv6 ACL Table:**

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	-	<a href="#">Delete</a>

**Direction Select:** Select the router interface. You can select LAN or WAN. In this example, WAN is selected.

**WAN Setting:** You can choose Interface or IPv6 Address.

**WAN Interface:** Choose the interface that permits data packets from WAN to access the router.

**IP Address:** Enter the IPv6 address on the WAN. Only the IPv6 address that is in the same network segment with the IPv6 address on the WAN can access the router.

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

**Add:** After setting the parameters, click it to add an entry to the Current IPv6 ACL Table.

**Reset:** Click it to refresh this page

## 4.4.5 DoS

### DoS

The router provides a protection of Denial of Service attack.

Go to Firewall->DoS page, you can configure the dos parameters. You can enable or disable the DoS prevention, and you can also specify the hack item.

MAC Filter

IP/Port Filter

URL Filter

ACL

DoS

DoS

### DoS Setting

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ Enable DoS Prevention

<input type="checkbox"/> Whole System Flood: SYN	100	Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	100	Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	100	Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	100	Packets/Second
<input type="checkbox"/> TCP/UDP PortScan	Low	Sensitivity
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		
<input type="checkbox"/> TCP Scan		
<input type="checkbox"/> TCP SynWithData		
<input type="checkbox"/> UDP Bomb		
<input type="checkbox"/> UDP EchoChargen		

Select ALL

Clear ALL

☐ Enable Source IP Blocking
 300 Block time (sec)

Apply Changes

## 4.5 Maintenance

### 4.5.1 Upgrade

#### 4.5.1.1 Firmware upgrade

The router supports the firmware upgrade from HTTP.

Go to Maintenance->Update->Firmware Update page, you can upgrade the firmware to the new version on the screen. Make sure the firmware or romfile you want to use is on the local hard drive of the computer. Click **Browse** to find the local hard drive and locate the firmware or romfile to be used for upgrade.

**Upgrade Firmware**

This page allows you upgrade the ADSL Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Note: System will reboot after file is uploaded.

Select File:  [Browse...](#)

[Upload](#) [Reset](#)

**To upgrade the router's firmware, follow these instructions below:**

Step 1: Download a more recent firmware upgrade file.

Step 2: Type the path and file name of the update file into the 'Select File' field. Or click the Browse button to locate the update file.

Step 3: Click the Upload button.

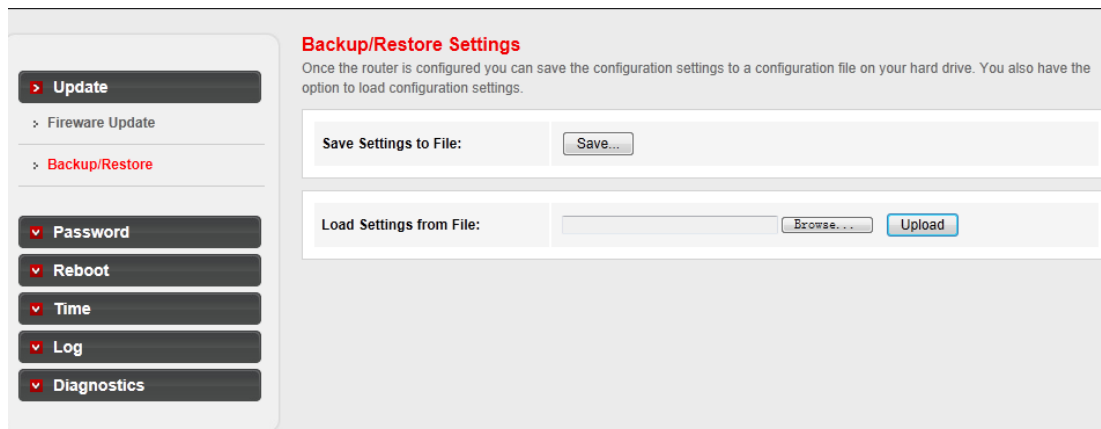
**Note:**

- 1) New firmware versions are posted at <http://www.netis-systems.com> and can be downloaded for free. If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use.
- 2) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.
- 3) Do not turn off the router or press the Reset button while the firmware is being upgraded.
- 4) The router will reboot after the upgrading has been finished.

You should select the correct firmware image first, and then apply the "Upload" button.

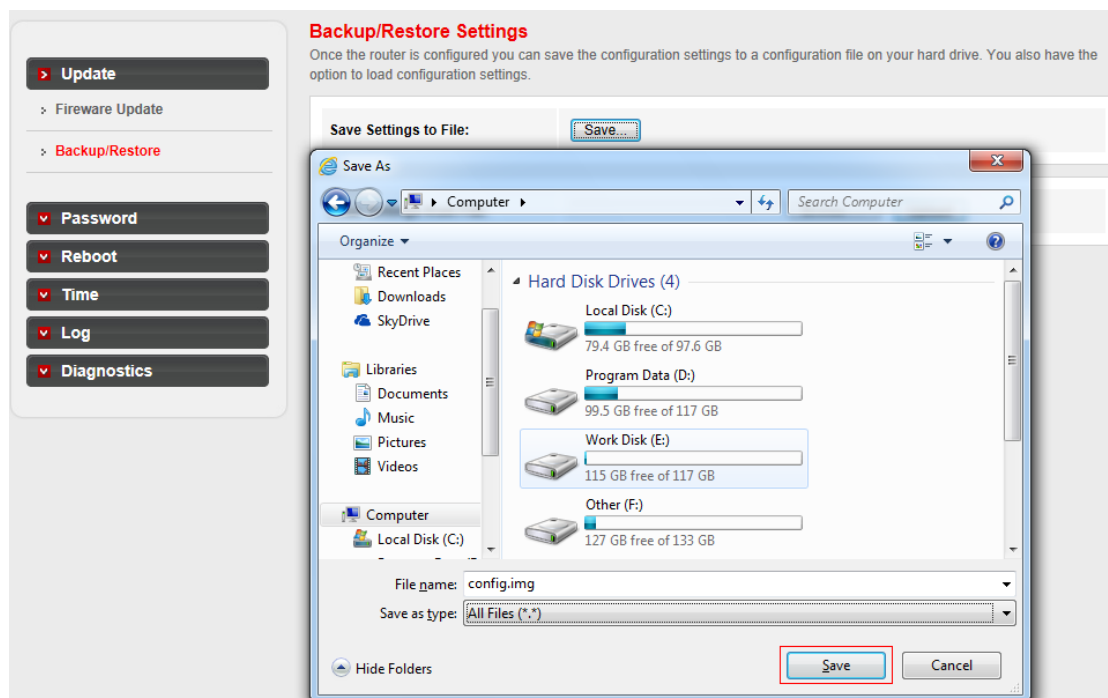
#### 4.5.1.2 Backup/Restore

Go to Maintenance->Update->Backup/Restore page, you can save the current configuration settings to a file, and you can also restore the settings from a configuration file.



### To back up the Modem Router's current settings:

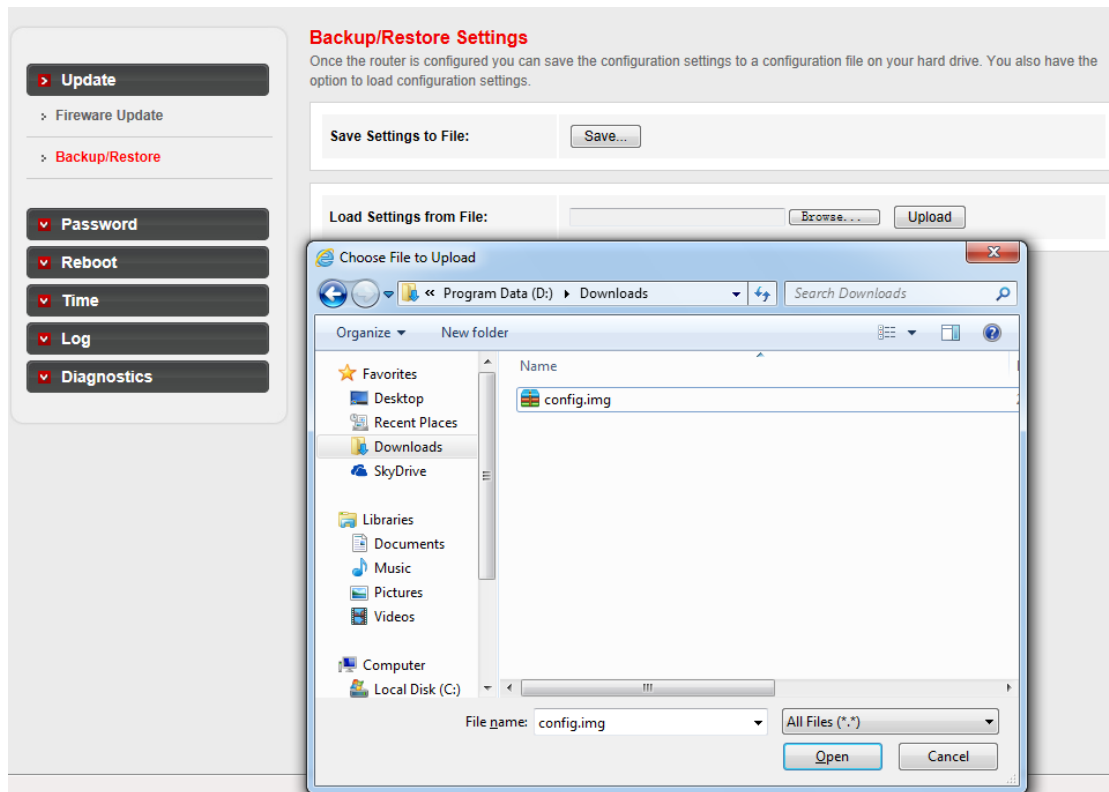
Step 1: Click the Save button, you can see:



Step 2: Click Save button to save the file as the appointed file.

### To restore the Modem Router's settings:

Step 1: Click the Browse button, you can see:



Step 2: Choose the file which you have saved and Click Open button to restore the settings

## 4.5.2 Password

Go to Maintenance->Password page, you can configure the user account of the router. Here you can add user account to access the web server, and modify the password of the specified user.

**User Account Configuration**

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	<input type="text"/>
Privilege:	<div> <div>User</div> <div>User</div> <div>Root</div> </div>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

**User Account Table:**

Select	User Name	Privilege
<input type="radio"/>	admin	root
<input type="radio"/>	user	user

**To create a account:**

Step 1: Type a user name and it's password which you have remembered

**User Account Configuration**

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	<input type="text" value="user2"/>
Privilege:	User <input type="button" value="v"/>
Old Password:	<input type="text"/>
New Password:	<input type="password" value="..."/>
Confirm Password:	<input type="password" value="..."/>

Step 2: Click Add button to create a user account

⚙ User Account Table:		
Select	User Name	Privilege
<input type="radio"/>	admin	root
<input type="radio"/>	user	user
<input type="radio"/>	user2	user

To change a password of a account:

Step 1: Choose a account which you want to change the password.

⚙ User Account Table:		
Select	User Name	Privilege
<input type="radio"/>	admin	root
<input checked="" type="radio"/>	user	user
<input type="radio"/>	user2	user

Step 2: Fill up the Old password, New password and Confirm password , then click Modify button to save it.



### User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	<input type="text" value="user"/>
Privilege:	<input type="text" value="User"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

#### Note:

- 1) If you login the router by root account you can change all accounts' password , There is only root account that can access Web-Management interface. The default User Name is admin, and the password is admin.
- 2) When you change the password, you should enter the new password twice, and then click Add to make the new password take effect.

## 4.5.3 Reboot

Go to **Maintenance->Reboot** page, you can commit changes to system memory and reboot your device with different configuration.

Update

Password

Reboot

Reboot

Time

Log

Diagnostics

Attention Config is modified to make it effective forever!

save

### Commit/Reboot

This page is used to commit changes to system memory and reboot your system with different configurations.

Reboot from:

**Commit/Reboot**  
This page is used to commit changes to system memory and reboot your system with different configurations.

Reboot from: Save Current Configuration Save Current Configuration Factory Default Configuration

Commit Changes Reset Reboot

Attention Config is modified to make it effective forever!  
save

## 4.5.4 Time

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP server.

Go to **Maintenance->Time** page, you can configure the system time.

**System Time Configuration**  
This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time: 1970 Year Jan Month 1 Day 5 Hour 48 min 54 sec

DayLight: LocalTIME

Apply Changes Reset

**NTP Configuration:**

State: ☒ Disable ☐ Enable

Server:

Server2:

Interval: Every 1 hours

Time Zone: (GMT) Gambia, Liberia, Morocco, England

GMT time: Thu Jan 1 5:48:54 1970

Apply Changes Reset

NTP Start: Get GMT Time

Attention Config is modified to make it effective forever!  
save

**Server/Server2:** the IP address or the host name of the NTP server.

**Interval:** the interval time of NTP function

**Time Zone:** the time zone in which the device resides.

When you set the NTP configuration correctly, press the button “Get GMT Time” to start the NTP function. Then you can see the GMT time obtained from NTP server.

**Note:** The ADSL Router built-in some NTP Servers, when the Modem Router connects to internet, it will get the system time automatically from the NTP Server. You can also configure the NTP Server address manually, then it will get the time from the specific server firstly.

## 4.5.5 Log

Go to Maintenance->Log page, you can configure the parameters of the system log, and view the system log information.

**Log Setting**  
This page is used to display the system event log table. By checking Error or Notice ( or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

Error: ☒ Notice: ☒

**Apply Changes** **Reset**

**Event log Table:**

**Save Log to File** **Clean Log Table**

Old |<< < > >>| New

Time	Index	Type	Log Information
Thu Jan 1 0:27:49 1970	0	other	admin web login successfully.
Thu Jan 1 0:46:43 1970	1	other	admin web login successfully.
Thu Jan 1 2:22:56 1970	2	other	admin web login successfully.
Thu Jan 1 2:33:31 1970	3	other	admin web login successfully.
Thu Jan 1 2:39:58 1970	4	other	user web login successfully.
Thu Jan 1 2:42:5 1970	5	other	admin web login successfully.
Thu Jan 1 2:54:44 1970	6	other	admin web login successfully.
Thu Jan 1 2:56:8 1970	7	other	username=admin password=admin fail
Thu Jan 1 2:56:15 1970	8	other	admin web login successfully.
Thu Jan 1 3:30:47 1970	9	other	username=admin password=admin fail
Thu Jan 1 3:30:56 1970	10	other	admin web login successfully.
Thu Jan 1 5:37:1 1970	11	other	username=admin password=admin fail
Thu Jan 1 5:37:9 1970	12	other	admin web login successfully.
Thu Jan 1 5:54:57 1970	13	other	admin web login successfully.

Page: 1/1

Attention Config is modified to make it effective forever!  
**save**

The router provides several useful diagnostic tools.

### 4.5.6.1 Ping

The router provides a ping command to send a message to the host you specify.

Go to **Maintenance->Diagnostics->Ping** page, you can ping a host you wanted.

The screenshot shows the 'Ping Diagnostic' page. On the left is a sidebar with a menu containing: Update, Password, Reboot, Time, Log, and Diagnostics (expanded). Under Diagnostics, there are links for Ping (highlighted in red), Ping6, Traceroute, OAM Loopback, ADSL Diagnostic, and Diag-Test. Below the menu is a red message: 'Attention Config is modified to make it effective forever!' with a 'save' button. The main content area is titled 'Ping Diagnostic' and contains a 'Host :' label followed by a text input field containing '192.168.1.100'. Below this is a 'PING' button.

**Host:** an IP address or host name you want to ping.

#### 4.5.6.2 Ping6 Diagnostic

The router provides a ping command to send a message to the host you specify

The screenshot shows the 'Ping6 Diagnostic' page. The sidebar menu is identical to the previous screenshot, but 'Ping6' is highlighted in red. The main content area is titled 'Ping6 Diagnostic' and contains two input fields: 'Target Address:' followed by a text input field, and 'Interface:' followed by a dropdown menu. Below these fields is a 'PING' button.

#### 4.5.6.3 Traceroute

Host: an IP address or host name you want to run trace route command

NumberOfTries: the number of try

Timeout: the time for the trace route command timeout

Datasize: data size of the trace route packet

DSCP

MaxHopCount: the maximum hop count

Interface: the interface to which the trace route is to be applied.

For example, you can set the host to [www.baidu.com](http://www.baidu.com), and then click the “traceroute” button to start the trace route process. Several times later, you can see the trace route result.



## Traceroute Diagnostic

Traceroute 220.181.6.19:

```

1 ****
2 172.29.38.252 10ms **
3 172.29.63.253 10ms **
4 ****
5 218.4.16.65 10ms **
6 222.92.175.54 10ms 10ms 10ms
7 202.97.34.53 30ms 30ms 30ms
8 220.181.16.58 40ms 30ms 30ms
9 220.181.16.134 40ms 30ms 30ms
10 220.181.17.150 30ms 30ms 30ms
11 ****
12 220.181.6.19 30ms **

```

**traceroute finished!**

[back](#)

### 4.5.6.4 OAM loopback

OAM Loopback allows you to verify the connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. ATM uses two cell flows: F4 used in VPs and F5 used in VCs.

Go to Maintenance->Diagnostics->OAM Loopback page, you can perform the loopback function to check the connectivity of the VCC.

The screenshot shows the 'OAM Fault Management - Connectivity Verification' page. On the left is a sidebar menu with options: Update, Password, Reboot, Time, Log, Diagnostics (expanded), Ping, Ping6, Traceroute, OAM Loopback (highlighted), ADSL Diagnostic, and Diag-Test. The main content area has a title 'OAM Fault Management - Connectivity Verification' and a description: 'Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.' Below this, there is a 'Flow Type' section with four radio button options: 'F5 Segment' (selected), 'F5 End-to-End', 'F4 Segment', and 'F4 End-to-End'. There are input fields for 'VPI:' and 'VCI:'. At the bottom is a 'Go !' button.

Flow type: the ATM OAM flow type. The selection can be F5 Segment, F5 End-to-End, F4 Segment or F4 End-to-End.

VPI: the VPI number you want to do the loopback diagnostics

VCI: the VCI number you want to do the loopback diagnostics

#### 4.5.6.5 ADSL diagnostics

ADSL diagnostics allows you to diagnostics the ADSL tone.

Go to Maintenance->Diagnostics->ADSL diagnostics page, you can start the ADSL tone diagnostic.

▼ Update

▼ Password

▼ Reboot

▼ Time

▼ Log

▶ Diagnostics

> Ping  
 > Ping6  
 > Traceroute  
 > OAM Loopback  
 > **ADSL Diagnostic**  
 > Diag-Test

### Diagnostic ADSL

Adsl Tone Diagnostic

Start

ADSL Diagnostics failed !!

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					

Click the “Start” button to start the diagnostic, and then wait several minutes later you will see the test result.

Adsl Tone Diagnostic

Start

ADSL Diagnostics successful !!

	Downstream	Upstream
Hlin Scale	36718	36143
Loop Attenuation(dB)	0.2	1.5
Signal Attenuation(dB)	0.2	0.4
SNR Margin(dB)	9.6	6.0
Attainable Rate(Kbps)	28188	1168
Output Power(dBm)	5.3	5.3

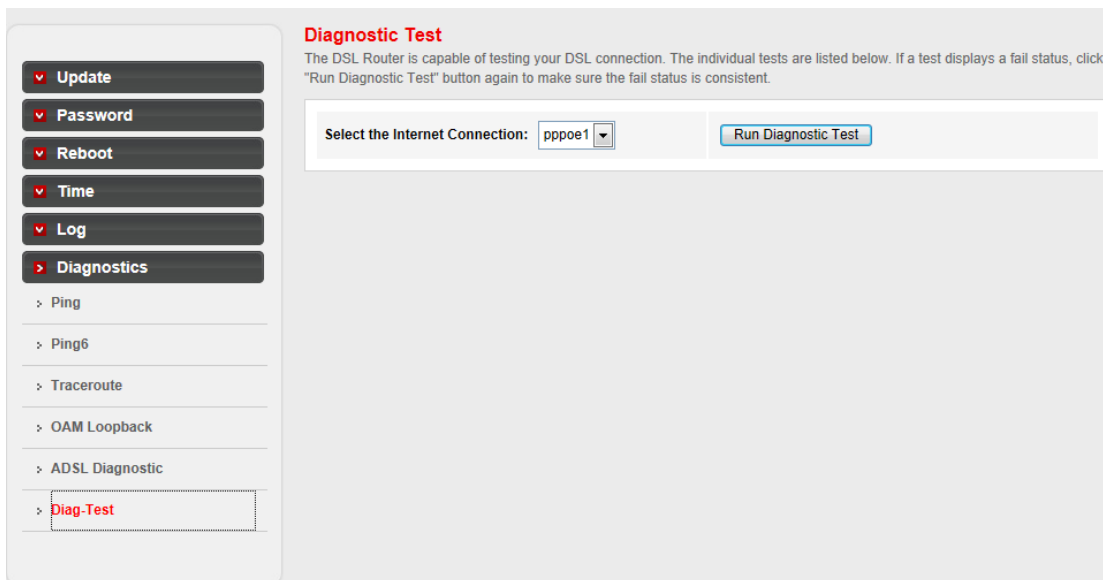
  

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0	0.000	0.000	0.0	-150.5	-96.3
1	0.000	0.000	0.0	-118.5	-96.3
2	0.000	0.000	0.0	-118.0	-96.3
3	0.000	0.000	0.0	-120.0	-96.3
4	0.000	0.000	0.0	-117.5	-96.3
5	0.000	0.000	0.0	-119.0	-96.3
6	0.000	0.000	0.0	-118.0	-96.3
7	0.472	0.124	33.0	-119.0	-6.2
8	0.499	0.658	38.5	-113.5	-1.7
9	0.052	-1.079	42.0	-113.0	0.7
10	0.499	1.084	43.5	-111.0	1.5
11	0.857	0.857	45.5	-112.5	1.7
12	1.030	0.615	47.5	-111.5	1.6
13	-1.093	0.406	48.0	-114.0	1.4
14	1.102	0.244	47.5	-114.0	1.0
15	-1.096	0.133	47.5	-112.5	0.8

#### 4.5.6.6 Diag-test

The Diagnostic Test allows you to test your DSL connection of the physical layer and protocol layer for both LAN and WAN sides.

Go to Maintenance->Diagnostics-> Diag-test page, you can select a interface to run diagnostic



Click the “Run Diagnostic Test” button to start the test, and then wait several times later you can see the diagnostic result.

LAN Connection Check	
Test Switch LAN PORT 1	DOWN
Test Switch LAN PORT 2	UP
Test Switch LAN PORT 3	DOWN
Test Switch LAN PORT 4	DOWN

WLAN Connection Check	
Test WLAN Root AP	UP/UNLINKED
Test WLAN Virtual AP0	DOWN
Test WLAN Virtual AP1	DOWN
Test WLAN Virtual AP2	DOWN
Test WLAN Virtual AP3	DOWN

ADSL Connection Check	
Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	PASS
Test ATM OAM F5 End-to-end Loopback	PASS
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

Internet Connection Check	
Test WAN IP Address: 192.168.2.72	PASS
Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS



## Appendix A: Troubleshooting

### **T1. How do I restore my Modem Router to its factory default settings?**

With the Modem Router powered on, press and hold the Reset button on the rear panel for 5 seconds before releasing it.

### **T2. What can I do if I forgot my password?**

1) Restore the Modem Router to factory default settings. If you don't know how to do it, please refer to section **T1**.

2) Use the default user name and password: **admin, admin**.

3) Configure the Modem Router again since you have ever reset it.

### **T3. What can I do if I cannot access the Internet?**

1) Check to see if all the connectors are connected well, including the telephone line, Ethernet cable and power adapter.

2) Check to see if you can login to the web management page of the Modem Router. If you can, try the following steps. If you cannot, please set your computer referring to **T4** then try to see if you can access the Internet.

3) Consult your ISP and make sure all the VPI/VCI、Connection Type and related information are correct. If there are any mistakes, please correct the settings and try again.

4) If you still cannot access the Internet, please restore your Modem Router and reconfigure it.

### **T4. Why the LAN's and the NIC's LEDs are both bright, but the configuration interface is inaccessible?**

1) Use the order of ping 192.168.1.1 to check the accuracy of connection.

2) If you are using Windows XP, please open the control panel, click network and internet connections, choose internet options, go to the connection tab, check 'Never dial up a connection'.

3) Check the setup of the IP address on your computer. If you disabled the DHCP function, the IP address can't be obtained automatically, so you have to specify the IP address for your computer manually.

- 4) Run the ***ipconfig*** command in the windows system to check whether the IP address, subnet mask, and default gateway have been assigned by DHCP.
- 5) Reset the ADSL Modem to factory default configuration if necessary.

**T5. What related parameters are required when you want to access the Internet by ADSL2+ Modem Router?**

- 1) Dial user: Connection type, User name, Password, Value of VPI/VCI, Encapsulation mode.
- 2) Static IP user: Connection protocol, WAN IP Address, Subnet Mask, Gateway, Value of VPI/VCI, Encapsulation mode and so on.

**T6. Have completed all configurations, but can't dial through computer**

- 1) Check the indicator of DSL and Internet. It should be acting normally.
- 2) Check the value of VPI/VCI, Encapsulation mode and so on, and whether you need to install the dial software, such as Winpoet, Enternet.
- 3) The PPP dial procedure is inside the product, so you will not need to use the dial software if your protocol is PPPoA or PPPoE. ADSL Modem will connect automatically.
- 4) You can check whether your ADSL Modem succeeds in connection or not with **PING** command.

**T7. Why the wireless stations cannot connect to the Modem Router?**

- 1) Make sure the 'Enable Wireless Router Radio' is checked.
- 2) Make sure that the wireless stations' SSID accord with the Router's SSID.
- 3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.
- 4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

**T8. How to assign a static IP for your computer?**

- 1) For Windows XP, open the control panel, double click network connections, choose local area connection, right click it and click properties, check 'use the following IP address' and 'use the following DNS server addresses', enter the network parameter.
- 2) For Windows 7, open the control panel, double click network and sharing center, click change adapter settings, choose local area connection, right click it and go to properties, check 'use the following IP address' and 'use the following DNS server addresses', enter the network parameter.