

Wireless-N ADSL2+ Modem Router

Instruction Manual

CWR150NS-AU

SONIQ

Contents

1	Introduction	- 3 -
1.1	Packing List	- 3 -
1.2	Safety Precautions	- 3 -
1.3	LEDs and Interfaces	- 4 -
1.4	System Requirements	- 6 -
1.5	Features	- 7 -
2	Hardware Installation	- 8 -
3	Web Configuration	- 11 -
3.1	Access the Router	- 11 -
3.2	Status	- 12 -
3.2.1	System	- 12 -
3.2.2	LAN	- 13 -
3.2.3	WLAN	- 13 -
3.2.4	WAN	- 14 -
3.2.5	Port Mapping	- 15 -
3.2.6	Statistics	- 15 -
3.2.7	ARP Table	- 17 -
3.3	Wizard	- 18 -
3.4	Network	- 27 -
3.4.1	LAN	- 27 -
3.4.2	WAN	- 35 -
3.4.3	WLAN	- 41 -
3.5	Service	- 51 -
3.5.1	DNS	- 51 -
3.5.2	Firewall	- 54 -
3.5.3	UPNP	- 63 -
3.5.4	IGMP Proxy	- 63 -
3.5.5	TR-069	- 64 -
3.5.6	ACL	- 66 -
3.6	Advance	- 69 -
3.6.1	Bridge Setting	- 69 -
3.6.2	Routing	- 70 -

3.6.3	Port Mapping	- 74 -
3.6.4	QoS.....	- 76 -
3.6.5	SNMP	- 79 -
3.6.6	Others	- 80 -
3.7	Admin	- 80 -
3.7.1	Commit/Reboot.....	- 80 -
3.7.2	Upgrade	- 81 -
3.7.3	System Log.....	- 82 -
3.7.4	Password.....	- 83 -
3.7.5	Time Zone.....	- 85 -
3.8	Diagnostic.....	- 86 -
3.8.1	Ping.....	- 86 -
3.8.2	ATM Loopback.....	- 87 -
3.8.3	ADSL	- 87 -
3.8.4	Diagnostic Test	- 88 -

1 Introduction

The GD-W910N is an ADSL access device that supports multiple line modes. It provides one 10/100Base-T Ethernet interface at the user end. The device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net cafes and office users. The device provides high performance access to the Internet, downlink up to 24 Mbps and uplink up to 1 Mbps.

The device supports WLAN access. It can connect to the Internet through a WLAN AP or WLAN device. It complies with IEEE 802.11, 802.11b/g/n specifications, WEP, WPA, and WPA2 security specifications.

1.1 Packing List

- 1 x GD-W910N
- 1 x external splitter
- 1 x power adapter
- 2 x telephone cables (RJ11)
- 1 x Ethernet cable (RJ45)
- 1 x CD

1.2 Safety Precautions

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

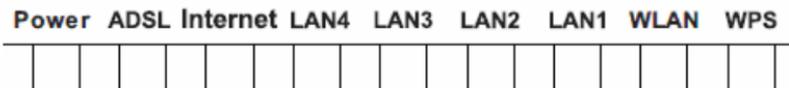
- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are

designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.

- Do not put this device close to a place where a heat source exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.3 LEDs and Interfaces

Front Panel

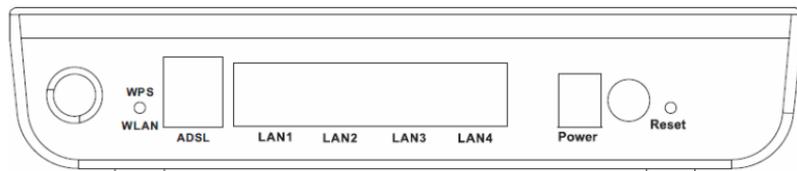


The following table describes the LEDs of the device:

LED	Color	Status	Description
Power	Green	On	The device is powered on and the initialization is normal.
		Off	The power is off.
	Red	On	The device is self-testing or self-testing is failed.
ADSL	Green	Slow Blinks	No signal is detected.
		Fast Blinks	The device is handshaking with the physical layer of the office.
		On	The device is connected to the physical layer of the office.
Internet	Green	On	The Internet connection is normal in the

LED	Color	Status	Description
			routing mode (for example: PPP dial-up is successful), and no Internet data is being transmitted.
		Blinks	Internet data is being transmitted in the routing mode.
		Off	The device is in the bridge mode.
	Red	On	The Internet connection fails after successful synchronization in the routing mode (for example: PPP dial-up is failed).
		On	The LAN connection is normal.
		Blinks	Data is being transmitted through the LAN interface, or the Internet data is being transmitted in the bridge mode.
LAN4-1	Green	Off	The LAN connection is not established.
		On	The WLAN connection has been activated.
		Blinks	Data is being transmitted through the WLAN interface.
WLAN	Green	Off	The WLAN connection is not activated.
		Blinks	WPS is activated and the device is waiting for negotiation with the clients.
		Off	WPS is not activated.
WPS	Green	Blinks	WPS is activated and the device is waiting for negotiation with the clients.
		Off	WPS is not activated.

Rear Panel



The following table describes the interfaces of the device:

Interface/Button	Description
WPS/WLAN	<ul style="list-style-type: none"> ● Press the button silently less than 1s to enable WLAN function. ● Press the button for more than 5s to enable WPS function. <p>If you press the button between 1s and 5s, no function takes effect.</p>
ADSL	RJ-11 interface, for connecting to the ADSL interface or a splitter through a telephone cable.
LAN4/3/2/1	RJ-45 interface, for connecting to the Ethernet interface of a PC or the Ethernet device through an Ethernet cable.
Power	Power interface for connecting to the power adapter of 12 V DC ,1A.
○	Power switch, power on or off the device.
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and insert a needle into the hole for over 8 seconds and release. The device is reset to the factory default configuration.

1.4 System Requirements

Recommended system requirements are as follows:

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

1.5 Features

The device supports the following features:

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

2 Hardware Installation

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

The splitter has three interfaces:

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

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



Note:

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

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

Connection 1

Figure 1 shows the application diagram for the connection of the router, PC, splitter and the telephone sets, when no telephone set is placed before the splitter.

Hardware Installation

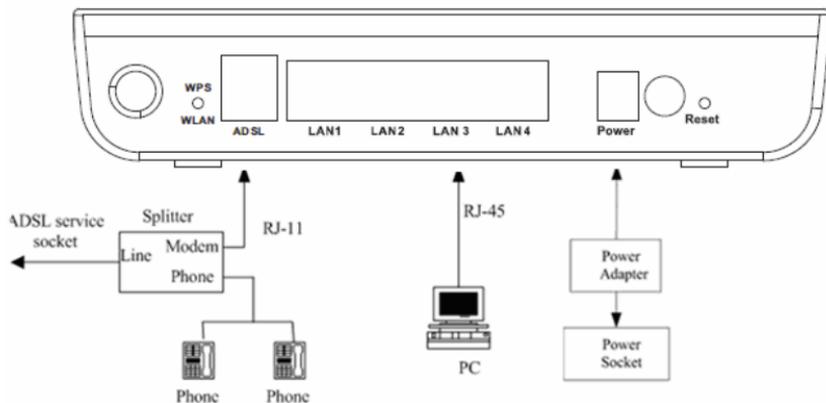


Figure 1 Connection diagram (Without connecting telephone sets before the splitter)

Connection 2

Figure 2 shows the connection when the splitter is installed close to the router.

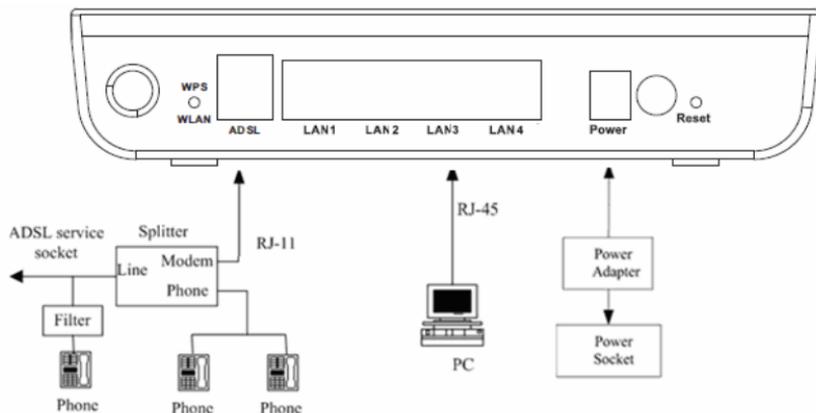


Figure 2 Connection diagram (Connecting a telephone set before the splitter)

**Note:**

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure2. Do not use the splitter to replace the filter.

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

3 Web Configuration

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

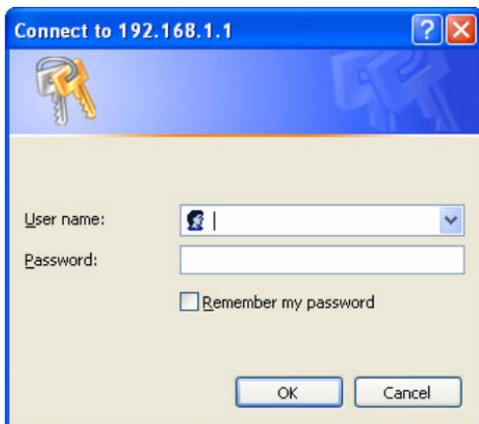
3.1 Access the Router

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

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

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

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



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



System Status

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

System	
Alias Name	CWR150NS
Uptime(hh:mm:ss)	0 0:1:58
Software Version	V2.1.1
DSP Version	2918b224
DSL	
Operational Status	--
Upstream Speed	--
Downstream Speed	--

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



Note:

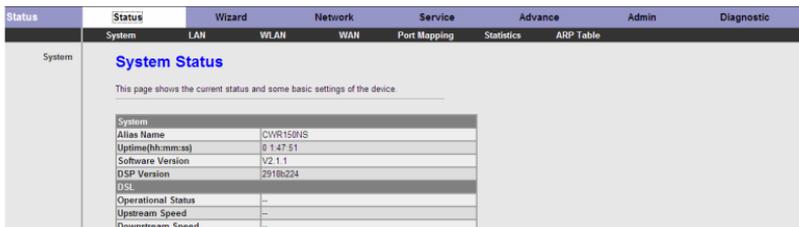
In the Web configuration page, you can click **Apply Changes** to save the settings temporarily. If you want to save the settings of this page permanently, click **save** of **Attention** that appears at the bottom of the Web page after the configuration.

3.2 Status

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

3.2.1 System

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



System Status

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

System	
Alias Name	CWR150NS
Uptime(hh:mm:ss)	0 1:47:51
Software Version	V2.1.1
DSP Version	2918b224
DSL	
Operational Status	--
Upstream Speed	--
Downstream Speed	--

3.2.2 LAN

Choose **Status > LAN**. The page that is displayed shows some basic LAN settings of the router. In this page, you can view the LAN IP address, DHCP server status, MAC address and DHCP client table. If you want to configure the LAN network, refer to chapter 3.4.1.1 LAN IP.

LAN Status

This page shows basic LAN settings of the device.

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:1F:A4:DD:F6:B9

DHCP Client Table				
Name	IP Address	MAC Address	Expiry(s)	Type

3.2.3 WLAN

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

WLAN Status

This page shows some basic settings of wireless LAN (WLAN).

Wireless Configuration					
Wireless	Enabled				
Band	2.4 GHz (B+G+N)				
Mode	AP				
Broadcast SSID	Enabled				
Root					
Status	Enabled				
SSID	GOLDWEB_ddf6b9				
Authentication Mode	Auto				
Encryption Mode	None				
VAP0					
Status	Disabled				
VAP1					
Status	Disabled				
VAP2					
Status	Disabled				
VAP3					
Status	Disabled				
Wireless Client List					
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---
Current Access Control List					
Mode	Disabled				

3.2.4 WAN

Choose **Status** > **WAN**. The page that is displayed shows some basic WAN settings of the router. In this page, you can view basic status of WAN and DNS server. If you want to configure the WAN network, refer to chapter 3.4.2.1 WAN.

WAN Status

This page shows some basic WAN settings.

Interface	VPI/VCI	Encapsulation	Default Route	Protocol	IP Address	Gateway	Status
pppoe1	0/36	LLC	On	PPPoE	0.0.0.0	0.0.0.0	down 0 0:0:0 /0 0:0:0 <input type="button" value="connect"/>
DNS Servers							

3.2.5 Port Mapping

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

Port Mapping

This page shows the mapping relation and the status of port mapping.

Status: Disabled

Mapping Relation

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3	Enabled
Group1		--
Group2		--
Group3		--
Group4		--

3.2.6 Statistics

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

3.2.6.1 Traffic Statistic

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

Traffic Statistics

ADSL Statistics

Traffic Statistics

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

Interface	Rx Packet	Rx Error	Rx Drop	Tx Packet	Tx Error	Tx Drop
e1	966	0	0	1013	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	410055	0	0	19164	0	41
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

3.2.6.2 ADSL Statistic

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

Traffic Statistics

ADSL Statistics

ADSL Statistics

This page shows the ADSL settings of the device.

ADSL Line Status	ACTIVATING.
ADSL Mode	--
Upstream	--
Downstream	--
Attenuation Downstream(db)	--
Attenuation Upstream(db)	--
SNR Margin Downstream(db)	--
SNR Margin Upstream(db)	--
Vendor ID	RETK
DSP Version	2918b224
CRC Errors	--
Upstream BER	--
Downstream BER	--
Up Output Power	--
Down Output Power	--
ES	--
SES	--
UAS	--

ADSL Retrain:

3.2.7 ARP Table

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

ARP Table

This page shows current ARP entries by interrogating the current protocol data.

IP Address	MAC Address
192.168.1.1	00:1F:A4:DD:F6:B9
192.168.1.15	00:22:B0:69:0D:64

3.3 Wizard

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either PPP, ADSL, or both. The technical information about the properties of your Internet connection is provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol that you use to communicate on the Internet. The **Wizard** page guides fast and accurate configuration of the Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **NEXT** to enable your Internet connection.

In the navigation bar, choose **Wizard**. The page shown in the following figure appears.

The following table describes the parameters in this page:

Field	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 0 .
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. (0 to 31 is reserved for local management of ATM traffic) Enter the correct VCI provided by your ISP. By default, VCI is set to 35 .

Web Configuration

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

There are five WAN connection types: **PPP over ATM (PPPoA)**, **PPP over Ethernet (PPPoE)**, **1483 MER**, **1483 Routed** and **1483 Bridged**. The following describes them respectively.

PPPoE/PPPoA

In the **Connection Type** page, set the WAN connection type to **PPP over Ethernet (PPPoE)**, the encapsulation mode to **LLC/SNAP**.

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use.

WAN Connection Type: PPP over ATM(PPPoA)
 PPP over Ethernet(PPPoE)
 1483 MER
 1483 Routed
 1483 Bridged

Encapsulation Mode:

< Back

Next >

The following table describes the parameters in this page:

Field	Description
WAN Connection Type	There are five WAN connection types: PPP over ATM (PPPoA) , PPP over Ethernet (PPPoE) , 1483 MER , 1483 Routed , and 1483 Bridged . In this example, the connection type is set to PPPoE .
Encapsulation Mode	You can select LLC/SNAP or VC-Mux . In this example, the encapsulation mode is set to LLC/SNAP .

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

WAN IP Settings

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

Obtain an IP address automatically
 Use the following IP address:

WAN IP Address:

Enable NAT

The following table describes the parameters in this page:

Field	Description
Obtain an IP address automatically	Select it, the DHCP assigns the IP address for PPPoE connection.
Use the following IP address	Select it, you need to enter the IP address for PPPoE connection, which is provided by your ISP.
Enable NAT	Select the checkbox to enable network address translation (NAT). If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is required to enable NAT.

Web Configuration

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

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password :

PPP Connection Type:

Continuous

Connect on Demand

Idle Time:

Manual

< Back

Next >

The following table describes the parameters in this page:

Field	Description
PPP Username	Enter the username for PPPoE dial-up, which is provided by your ISP.
PPP Password	Enter the password for PPPoE dial-up, which is provided by your ISP.
PPP Connection Type	<p>You can select Continuous, Connect on Demand, or Manual.</p> <ul style="list-style-type: none"> ● Continuous: After dial-up is successful, PPPoE connection is always on-line, no matter whether the data is being transmitted or not. It is recommended to select it. ● Connect on Demand: After dial-up is successful, within the preset idle time, no data is being transmitted, the router automatically disconnects the PPPoE connection. In this case, you need to enter the idle time. ● Manual: Select it, you need to dial up and disconnect the connection manually.

**Note:**

If the WAN connection type is set to **PPPoA**, the parameters of the WAN connection type are the same as that of **PPPoE**. For the parameters in these pages, refer to the parameter description of **PPPoE**.

1483 MER/1483 Routed

In the **Connection Type** page, set the WAN connection type to **1483 MER**, the encapsulation mode to **LLC/SNAP**.

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use.

- WAN Connection Type:** PPP over ATM(PPPoA)
 PPP over Ethernet(PPPoE)
 1483 MER
 1483 Routed
 1483 Bridged

Encapsulation Mode:

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

Web Configuration

WAN IP Settings

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

- Obtain an IP address automatically
- Use the following IP address:
- WAN IP Address:
- WAN Netmask:
- Default Gateway:
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
- Primary DNS server:
- Secondary DNS server:
- Enable NAT

< Back

Next >

The following table describes the parameters in this page:

Field	Description
Obtain an IP address automatically	Select it, DHCP automatically assigns the IP address for WAN connection.
Use the following IP address	Select it, you need to manually enter the IP address, subnet mask, and default gateway for WAN connection, which are provided by your ISP.
Obtain DNS server addresses automatically	Select it, DHCP automatically assigns DNS server address.
Use the following DNS server addresses	Select it, you need to manually enter the primary DNS server address and secondary DNS server address.
Enable NAT	Select it to enable network address translation (NAT). If you do not select it and you want to access the Internet normally,

Field	Description
	you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is required to enable NAT.

**Note:**

If the WAN connection type is set to **1483 Routed**, the parameters of the WAN connection type are the same as that of **1483 MER**. For the parameters in these pages, refer to the parameter description of **1483 MER**.

1483 Bridged

In the **Connection Type** page, set the WAN connection type to **1483 Bridged**, the encapsulation mode to **LLC/SNAP**.

WAN IP Settings

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

- Obtain an IP address automatically
 Use the following IP address:
 WAN IP Address:
 WAN Netmask:
 Default Gateway:
- Obtain DNS server addresses automatically
 Use the following DNS server addresses:
 Primary DNS server:
 Secondary DNS server:
- Enable NAT

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

Web Configuration

WAN IP Settings

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

- Obtain an IP address automatically
- Use the following IP address:
- WAN IP Address:
- WAN Netmask:
- Default Gateway:
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
- Primary DNS server:
- Secondary DNS server:
- Enable NAT

< Back

Next >

The following table describes the parameters in this page:

Field	Description
LAN Interface Setup	
LAN IP	Enter the IP address of LAN interface. Its valid value is in the range of 192.168.1.1 to 192.168.255.254. The default IP address is 192.168.1.1 .
LAN Netmask	Enter the subnet mask of LAN interface. Its valid value is in the range of 255.255.0.0 to 255.255.255.254.
Enable Secondary IP	Select the checkbox to enable the secondary LAN IP. The two LAN IP addresses must be in the different network.
DHCP Server	
Enable DHCP Server	Select the checkbox to enable DHCP server.

Field	Description
Start IP	Enter the start IP address that the DHCP sever assigns.
End IP	Enter the end IP address that the DHCP server assigns.
Max Lease Time	The lease time determines the period that the PCs retain the assigned IP addresses before the IP addresses change.

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

fast configure - Summary

Click "Finish" to save these settings. Click "Back" to make any modifications. Click "Reset" to drop these settings.

The parameters you set:

WAN Setup:

VPI:	0
VCI:	35
Encapsulation:	LLC/SNAP
Connection Type:	1483 bridge

LAN Setup:

LAN IP:	192.168.1.1 / 255.255.255.0
Secondary IP:	0.0.0.0 / 0.0.0.0
DHCP Server:	Enabled
DHCP IP Range:	192.168.1.2 ~ 192.168.1.254
DHCP Lease Time:	1 Day 0 Hour 0 Min

Click **BACK** to modify the settings.

Click **FINISH** to save the settings.

Click **RESET** to cancel the settings.

**Note:**

After you saving the settings in the **Wizard** page, the PVC in the **Wizard** page replaces that in the **Channel Configuration** page. The preset PVCs in the **Channel Configuration** page do not take effect any more.

3.4 Network

In the navigation bar, click **Network**. The **Network** page displayed contains **LAN**, **WAN** and **WLAN**.

3.4.1 LAN

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

3.4.1.1 LAN IP

Click **LAN IP** 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.

LAN	Status	Wizard	Network	Service	Advance	Admin	Diagnostic
		LAN	WAN	WLAN			
LAN IP DHCP DHCP Static IP	LAN Interface Setup						
This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP address, subnet mask, etc.							
Interface Name: e1							
IP Address: 192.168.1.1							
Subnet Mask: 255.255.255.0							
<input type="checkbox"/> Secondary IP							
IGMP Snooping: <input checked="" type="radio"/> Disable <input type="radio"/> Enable							
<input type="button" value="Apply Changes"/>							
LAN Port: <input type="button" value="v"/>							
Link Speed/Duplex Mode: <input type="button" value="v"/>							
<input type="button" value="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					
MAC Address Control: <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"/>							
New MAC Address: <input type="text"/> <input type="button" value="Add"/>							
Current Allowed MAC Address Table:							
	MAC Addr	Action					

The following table describes the parameters of this page:

Field	Description
IP Address	Enter the IP address of LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is 192.168.1.1- 192.168.255.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in the different network.
LAN Port	You can choose the LAN interface you want to configure.
Link Speed/Duplex Mode	You can select the following modes from the drop-downlist: 100Mbps/FullDuplex, 100Mbps/Half

Field	Description
	Duplex,10Mbps/FullDuplex,10Mbps/Half Duplex,Auto Negotiation.
MAC Address Control	It is the access control based on MAC address. Select it, and the host whose MAC address is listed in the Current Allowed MAC Address Table can access the modem.
Add	Enter MAC address, and then click it to add a new MAC address.

3.4.1.2 DHCP

Dynamic Host Configuration Protocol (DHCP) allows the individual PC to obtain the TCP/IP configuration from the centralized DHCP server. You can configure this router as a DHCP server or disable it. The DHCP server can assign IP address, IP default gateway, and DNS server to DHCP clients. This router can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from an actual real DHCP server to clients. You can enable or disable DHCP server. Click **DHCP** in the left pane, the page shown in the following figure appears.

LAN IP <input type="checkbox"/> DHCP DHCP Static IP	<h2 style="color: blue;">DHCP Mode</h2> <p>This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.</p> <p>(1) Set the DHCP mode to DHCP Server if you are using this device as a DHCP server. This page lists an IP address pool available to hosts on your LAN. The device assigns IP addresses in the pool to hosts on your network when they request Internet access.</p> <p>(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.</p> <p>(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.</p> <hr/> <p>LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0</p> <p>DHCP Mode: <input type="text" value="DHCP Server"/></p> <p>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</p> <p>IP Pool Range: 192.168.1.2 - 192.168.1.254 <input type="button" value="Show Client"/></p> <p>Default Gateway: <input type="text" value="192.168.1.1"/></p> <p>Max Lease Time: <input type="text" value="1440"/> minutes</p> <p>Domain Name: <input type="text" value="domain.name"/></p> <p>DNS Servers: <input type="text" value="192.168.1.1"/> <input type="text"/> <input type="text"/></p> <p style="text-align: center;"> <input type="button" value="Apply Changes"/> <input type="button" value="Reset"/> </p> <p style="text-align: center;"><input type="button" value="Set VendorClass IP Range"/></p>
---	---

The following table describes the parameters of this page:

Field	Description
DHCP Mode	If set to DHCP Server , the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows95, Windows NT and other operation systems that support the DHCP client.
IP Pool Range	It specifies the first and the last IP address in the IP address pool. The router assigns IP address that is in the IP pool range to the host.
Show Client	Click it, the Active DHCP Client Table appears. It shows IP addresses assigned to clients.
Default Gateway	Enter the default gateway of the IP address pool.
Max Lease Time	The lease time determines the period that the host

Web Configuration

Field	Description
	retains the assigned IP addresses before the IP addresses change.
Domain Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
DNS Servers	You can configure the DNS server ip addresses for DNS Relay.
Set VendorClass IP Range	Click it, the Device IP Range Table page appears. You can configure the IP address range based on the device type.

Click **Show Client** in the **DHCP Mode** page, the page shown in the following figure appears. You can view the IP address assigned to each DHCP client.

Active DHCP Client Table

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

Name	IP Address	MAC Address	Expiry(s)	Type
<input type="button" value="Refresh"/> <input type="button" value="Close"/>				

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

Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for

Field	Description
	example, 00-A0-C5-00-02-12.
Expiry (s)	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

Click **Set VendorClass IP Range** in the **DHCP Mode** page, the page as shown in the following figure appears. In this page, you can configure the IP address range based on the device type.

Device IP Range Table

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

Device Name:

Start Address:

End Address:

Router Address:

Option60:

IP Range Table:

Select	Device Name	Start Address	End Address	Default Gateway	Option60
--------	-------------	---------------	-------------	-----------------	----------

In the **DHCP Mode** field, choose **None**. The page shown in the following figure appears.

Web Configuration

DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.

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

(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.

(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode:

Apply Changes

Reset

Set VendorClass IP Range

In the **DHCP Mode** field, choose **DHCP Relay**. The page shown in the following figure appears.

DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.

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

(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.

(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode:

Relay Server:

Apply Changes

Reset

Set VendorClass IP Range

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

Field	Description
DHCP Mode	If set to DHCP Relay , the router acts a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings of this page.
Reset	Click it to refresh this page.

3.4.1.3 DHCP Static IP

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

DHCP Static IP Configuration

This page lists the static IP address and MAC address on your LAN. The device assigns the IP addresses to hosts on your network when they request Internet access.

IP Address:

MAC Address: (ex. 00E086710502)

DHCP Static IP Table:

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

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

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the DHCP Static IP

Field	Description
	Table.
Delete Selected	Select a row in the DHCP Static IP Table , then click it, this row is deleted.
Reset	Click it to refresh this page.
DHCP Static IP Table	It shows the assigned IP address based on the MAC address.

3.4.2 WAN

Choose **Network > WAN**. The **WAN** page that is displayed contains **WAN, ATM Setting** and **ADSL Setting**.

3.4.2.1 WAN

Click **WAN** in the left pane, the page shown in the following figure appears. In this page, you can configure WAN interface of your router.

The screenshot shows the 'Channel Configuration' page for the WAN interface. The page is divided into several sections:

- Default Route Selection:** Radio buttons for 'Auto' and 'Specified'.
- VPt:** Input field with '0'.
- VCI:** Input field.
- Encapsulation:** Radio buttons for 'LLC' (selected) and 'VC-Mux'.
- Channel Mode:** Dropdown menu showing '1483 Bridged'.
- Enable NAPT:** Check box.
- Enable IGMP:** Check box.
- PPP Settings:**
 - User Name:** Input field.
 - Password:** Input field.
 - Type:** Dropdown menu showing 'Continuous'.
 - Idle Time (min):** Input field.
- WAN IP Settings:**
 - Type:** Radio buttons for 'Fixed IP' (selected) and 'DHCP'.
 - Local IP Address:** Input field.
 - Gateway:** Input field.
 - Netmask:** Input field.
 - Default Route:** Radio buttons for 'Disable', 'Enable', and 'Auto'.
 - Unnumbered:** Check box.
- Buttons:** 'Add', 'Modify', 'Delete', 'Reset', 'Refresh'.
- Current ATM VC Table:** A table with columns: Select, Intf, Mode, VPI, VCI, Encap, NAPT, IGMP, Onroute, IP Addr, Gateway, NetMask, User Name, Unnumber, Status, Edit.

Select	Intf	Mode	VPI	VCI	Encap	NAPT	IGMP	Onroute	IP Addr	Gateway	NetMask	User Name	Unnumber	Status	Edit
<input type="radio"/>	pppoa1	PPPoA	0	36	LLC	On	On	On	0.0.0.0	0.0.0.0	255.255.255.255	1	--	down	

The following table describes the parameters of this page:

Field	Description
Default Route Selection	You can select Auto or Specified .
VPI	The virtual path between two points in an ATM network, ranging from 0 to 255.
VCI	The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols)
Encapsulation	You can choose LLC and VC-Mux .
Channel Mode	You can choose 1483 Bridged , 1483 MER , PPPoE , PPPoA , 1483 Routed or IPoA .
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enabel IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
PPP Settings	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose Continuous , Connect on Demand , or Manual .
Idle Time (min)	If set the type to Connect on Demand , you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings	
Type	You can choose Fixed IP or DHCP .

Web Configuration

Field	Description
	<ul style="list-style-type: none"> ● If select Fixed IP, you should enter the local IP address, remote IP address and subnet mask. ● If select DHCP, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Unnumbered	Select this checkbox to enable IP unnumbered function.
Add	After configuring the parameters of this page, click it to add a new PVC into the Current ATM VC Table .
Modify	Select a PVC in the Current ATM VC Table , then modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
Current ATM VC Table	This table shows the existed PVCs. It shows the interface name, channel mode, VPI/VCI, encapsulation mode, local IP address, remote IP address and other information. The maximum item of this table is eight.

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

PPP Interface - Modify

Protocol: PPPoE
 ATM VCC: 0/36
 Login Name:
 Password:
 Authentication Method:
 Connection Type:
 Idle Time(s):
 Bridge:
 Bridged Ethernet (Transparent Bridging)
 Bridged PPPoE (Implies Bridged Ethernet)
 Disable Bridge
 AC Name:
 Service Name:
 802.1q: Disable Enable
 VLAN ID(1-4095):
 MTU (1-1500):
 Static IP:
 Source Mac address: (ex.00:E0:86:71:05:02)

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

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose AUTO , CHAP , or PAP .
Connection Type	You can choose Continuous , Connect on Demand , or Manual .

Field	Description
Idle Time (s)	If choose Connect on Demand , you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
Bridge	You can select Bridged Ethernet , Bridged PPPoE , or Disable Bridge .
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select Disable or Enable . After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
Apply Changes	Click it to save the settings of this page temporarily.
Return	Click it to return to the Channel Configuration page.
Reset	Click it to refresh this page.
Source Mac address	The MAC address you want to clone.
MAC Clone	Click it to enable the MAC Clone function with the MAC address that is configured.

3.4.2.2 ATM Setting

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

WAN ATM Setting ADSL Setting	<h2 style="color: blue;">ATM Settings</h2> <p>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.</p> <p>VPI: <input type="text"/> VCI: <input type="text"/> QoS: <input type="text" value="UBR"/></p> <p>PCR: <input type="text"/> CDVT: <input type="text"/> SCR: <input type="text"/> MBS: <input type="text"/></p> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>Current ATM VC Table:</p> <table border="1"> <thead> <tr> <th>Select</th> <th>VPI</th> <th>VCI</th> <th>QoS</th> <th>PCR</th> <th>CDVT</th> <th>SCR</th> <th>MBS</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td>0</td> <td>36</td> <td>UBR</td> <td>6144</td> <td>0</td> <td>---</td> <td>---</td> </tr> </tbody> </table>	Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS	<input checked="" type="radio"/>	0	36	UBR	6144	0	---	---
Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS										
<input checked="" type="radio"/>	0	36	UBR	6144	0	---	---										

The following table describes the parameters of this page:

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

3.4.2.3 ADSL Setting

Click **ADSL Setting** in the left pane, the page shown in the following figure appears. In this page, you can select the DSL modulation. Mostly, you need to remain this factory default settings. The router supports these modulations: **G.Lite**, **G.Dmt**, **T1.413**, **ADSL2**, **ADSL2+**, **AnnexL** and **AnnexM**. The router negotiates the modulation modes with the DSLAM.

ADSL Settings

This page is used to configure ADSL settings of the device.

ADSL Modulation:

- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+

AnnexL Option:

- Enable

AnnexM Option:

- Enable

ADSL Capability:

- Bitswap Enable
- SRA Enable

Apply Changes

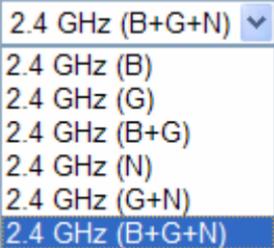
3.4.3 WLAN

3.4.3.1 Basic Settings

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

WLAN	Status	Wizard	Network	Service	Advance	Admin	Diagnostic
Basic Setting Security Access Control Advanced Setting WPS	<h3>Wireless Basic Settings</h3> <p>This page is used to configure the parameters for your wireless network.</p> <p><input type="checkbox"/> Disable Wireless LAN Interface</p> <p>Band: <input type="text" value="2.4 GHz (B+G+N)"/></p> <p>Mode: <input type="text" value="AP"/></p> <p>SSID: <input type="text" value="GOLDWEB_00000"/></p> <p>Channel Width: <input type="text" value="40MHz"/></p> <p>Control Sideband: <input type="text" value="Upper"/></p> <p>Channel Number: <input type="text" value="Auto"/> Current Channel: 6</p> <p>Radio Power (Percent): <input type="text" value="100%"/></p> <p>Associated Clients: <input type="text" value="Show Active Clients"/></p> <p><input type="button" value="Apply Changes"/></p>						

The following table describes the parameters of this page:

Field	Description
Band	<p>Choose the working mode of the modem. You can choose from drop-down list.</p> 
Mode	<p>Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is AP.</p>
SSID	<p>The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.</p>
Channel Number	<p>A channel is the radio frequency used by 802.11b/g/n wireless devices. There are 13 channels (from 1 to 13) available depending on the geographical area. You may have a choice of</p>

Field	Description
	channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap. Choose a channel from the drop-down list box.
Radio Power	You can choose the transmission power of the radio signal. The default one is 100% . It is recommended to choose the default value 100% .
Show Active Clients	Click it to view the information of the wireless clients that are connected to the modem.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click Save in the lower left corner.

3.4.3.2 Security

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

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.

Encryption:

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format:

Pre-Shared Key:

Authentication RADIUS Server:

Port IP address Password

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

The following table describes the parameters of this page:

Field	Description
Encryption	<p>Configure the wireless encryption mode. You can choose None, WEP, WPA (TKIP), WPA (AES), WPA2 (AES), WPA2 (TKIP), or WPA2 Mixed.</p> <ul style="list-style-type: none"> ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. <p>Key differences between WPA and WEP are user authentication and improved data encryption.</p>
Set WEP Key	It is available when you set the encryption mode

Web Configuration

Field	Description
	to WEP . Click it, the Wireless WEP Key Setup page appears.
WPA Authentication Mode	<ul style="list-style-type: none"> ● Select Personal (Pre-Shared Key), enter the pre-shared key in the Pre-Shared Key field. ● Select Enterprise (RADIUS), enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem. <p>If the encryption is set to WEP, the modem uses 802.1 X authentication, which is Radius authentication.</p>

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

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:	<input type="text" value="64-bit"/>
Key Format:	<input type="text" value="ASCII (5 characters)"/>
Default Tx Key:	<input type="text" value="Key 1"/>
Encryption Key 1:	<input type="text" value="*****"/>
Encryption Key 2:	<input type="text" value="*****"/>
Encryption Key 3:	<input type="text" value="*****"/>
Encryption Key 4:	<input type="text" value="*****"/>

The following describes the parameters of this page:

Field	Description
Key Length	Choose the WEP key length. You can Choose 64-bit or 128-bit .

Field	Description
Key Format	<ul style="list-style-type: none"> ● If you choose 64-bit, you can choose ASCII (5 characters) or Hex (10 characters). ● If you choose 128-bit, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Choose the index of WEP Key. You can choose Key 1 , Key 2 , Key 3 , or Key 4 .
Encryption Key 1 to 4	<p>The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission.</p> <ul style="list-style-type: none"> ● If you choose 64-bit and ASCII (5 characters), enter any 5 ASCII characters. ● If you choose 64-bit and Hex (10 characters), enter any 10 hexadecimal characters. ● If you choose 128-bit and ASCII (13 characters), enter any 13 ASCII characters. ● If you choose 128-bit and Hex (26 characters), enter any 26 hexadecimal characters.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click Save in the lower left corner.

3.4.3.3 Access Control

Choose **WLAN > Access Control** and the following page appears. In this page, you can configure the access control of the wireless clients.

Wireless Access Control

This page is used to configure the wireless access control.

If you set the wireless access control mode to **Allowed Listed**, only those clients whose wireless MAC addresses are in the access control list are allowed to connect to your access point (AP).

If you set the wireless access control mode to **Deny Listed**, those clients whose wireless MAC addresses are in the access control list are blocked from connecting to your AP.

Wireless Access Control Mode:

MAC Address: (ex. 00E086710502)

Current Access Control List:

MAC Address	Select

Choose **Allow Listed** as the access control mode to enable white list function. Only the devices whose MAC addresses are listed in the **Current Access Control List** can access the modem.

Choose **Deny Listed** as the access control mode to enable black list function. The devices whose MAC addresses are listed in the **Current Access Control List** are denied to access the modem.

3.4.3.4 Advanced Settings

Choose **Wireless > Advanced Settings** and the following page appears. In this page, you can configure the wireless advanced parameters. It is recommended to use the default parameters.

**Note:**

The parameters in the **Advanced Settings** are modified by the professional personnel, it is recommended to keep the default values.

Wireless Advance 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: Open System Shared Key Auto

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

DTIM Interval: (1-255)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enable Disable

Relay Blocking: Enable Disable

Ethernet to Wireless Blocking: Enable Disable

Wifi Multicast to Unicast: Enable Disable

Aggregation: Enable Disable

Short GI: Enable Disable

The following table describes the parameters of this page:

Field	Description
Authentication	Select the modem operating in the open system or

Web Configuration

Field	Description
	<p>encryption authentication. You can choose Open System, Shared Key, or Auto.</p> <ul style="list-style-type: none"> ● In the open system, the wireless client can directly connect to the device ● In the encryption authentication, the wireless client connects to the modem through the shared key.
Data Rate	<p>Choose the transmission rate of the wireless data. You can choose Auto, 1 M, 2 M, 5.5 M, 11 M, 6 M, 9 M, 12 M, 18 M, 24 M, 36 M, 48 M, 54M, MSC0-MSC15.</p>
PreambleType	<ul style="list-style-type: none"> ● Long Preamble: It means this card always use long preamble. ● Short Preamble: It means this card can support short preamble capability.
Broadcast SSID	<p>Select whether the modem broadcasts SSID or not. You can select Enable or Disable.</p> <ul style="list-style-type: none"> ● Select Enable, the wireless client searches the modem through broadcasting SSID. ● Select Disable to hide SSID, the wireless clients can not find the SSID.
Relay Blocking	<p>Wireless isolation. Select Enable, the wireless clients that are connected to the modem can not intercommunication.</p>
Ethernet to Wireless Blocking	<p>Whether the wireless network can communicate with the Ethernet network or not.</p>
Wifi Multicast to Unicast	<p>Enable it to using unicast to transmit multicast packet</p>
Aggregation	<p>It is applied when the destination end of all MPDU are for one STA.</p>
Short GI	<p>It is not recommended to enable GI in obvious environment of Multi-path effect.</p>

Field	Description
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click Save in the lower left corner.

3.4.3.5 WPS

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

Wi-Fi Protected Setup

This page is used to configure Wi-Fi protected setup (WPS). Using this feature could let your wireless client automatically synchronize its setting and connect to the access point (AP) in 2 minutes without any hassle.

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

15571519

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Client PIN Number:

Start PIN

There are two ways for the wireless client to establish the connection with the modem through WPS. The modem generates PIN, see the above figure. Click **Regenerate PIN** to generate a new PIN, and then click **Start PBC**. In the wireless client tool, enter the PIN which is generated by the modem, start connection. The client will automatically establish the connection with the modem through the encryption mode, and you need not to enter the key. The other way is the wireless client generates PIN. In the above figure, enter PIN of the wireless client in the **Client PIN Number** field, then click **Start PIN** to establish the connection.

**Note:**

The wireless client establishes the connection with the modem through WPS negotiation. The wireless client must support WPS

3.5 Service

In the navigation bar, click **Service**. In the **Service** page that is displayed contains **DNS, Firewall, UPnP, IGMP Proxy, TR-069** and **ACL**.

3.5.1 DNS

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

Choose **Service > DNS**. The **DNS** page that is displayed contains **DNS** and **DDNS**.

3.5.1.1 DNS

Click **DNS** in the left pane, the page shown in the following figure appears.

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

Field	Description
Obtain DNS	Select it, the router accepts the first received DNS

Field	Description
Automatically	assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it, enter the IP addresses of the primary and secondary DNS server.
Apply Changes	Click it to save the settings of this page.
Reset	Click it to start configuring the parameters in this page.

3.5.1.2 DDNS

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

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider:

Host Name:

Interface:

Enable:

DynDns Settings:

User Name:

Password:

TZO Settings:

Email:

Key:

Dynamic DDNS Table:

Select	State	Service	Host Name	User Name	Interface
--------	-------	---------	-----------	-----------	-----------

The following table describes the parameters of this page:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose DynDNS.org or TZO .
Host Name	The DDNS identifier.
Interface	The WAN interface of the router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.
Email	The email provided by DDNS provider.

Field	Description
Key	The key provided by DDNS provider.

3.5.2 Firewall

Choose **Service > Firewall**. The **Firewall** page that is displayed contains **IP/Port Filterer**, **MAC Filter**, **URL Blocking**, **Virtual Server**, **IP Address Mapping**, **DMZ Setting**, **NAT EXCLUDE IP**, **ALG Setting** and **Anti-DoS**.

3.5.2.1 IP/Port Filter

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

The screenshot shows the 'IP/Port Filter' configuration page. The left sidebar contains a list of configuration options: IP/Port Filter, MAC Filter, URL Blocking, Virtual Server, IP Address Mapping, DMZ Setting, NAT EXCLUDE IP, ALG Setting, and Anti-DoS. The main content area is titled 'IP/Port Filter' and includes the following configuration options:

- Outgoing Default Action: Permit Deny
- Incoming Default Action: Permit Deny
- Rule Action: Permit Deny
- Protocol: IP
- Direction: Upstream
- Source IP Address: [Text Box] Subnet Mask: 255.255.255.255
- Destination IP Address: [Text Box] Subnet Mask: 255.255.255.255
- Source Port: [Text Box] - [Text Box] Destination Port: [Text Box] - [Text Box]
- Enable:
- Buttons: Apply Changes, Reset, Help

At the bottom, there is a 'Current Filter Table' header with columns: Rule, Protocol, Source IP/Mask, SPort, Dest IP/Mask, DPort, State, Direction, and Action.

3.5.2.2 MAC Filter

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

MAC Filter

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 Deny Allow

Incoming Default Policy Deny Allow

Apply

Direction:

Action: Deny Allow

Source MAC Address: (ex. 00E086710502)

Destination MAC Address: (ex. 00E086710502)

Add

Current MAC Filter Table:

Select	Direction	Source MAC Address	Destination MAC Address	Action

Delete

Delete All

3.5.2.3 URL Blocking

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

URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: Disable Enable

Apply Changes

Keyword:

AddKeyword

Delete Selected Keyword

URL Blocking Table:

Select	Filtered Keyword
--------	------------------

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

Field	Description
URL Blocking Capability	You can choose Disable or Enable . <ul style="list-style-type: none"> ● Select Disable to disable URL blocking function and keyword filtering function. ● Select Enable to block access to the URLs and keywords specified in the URL Blocking Table.
Keyword	Enter the keyword to block.
AddKeyword	Click it to add a keyword to the URL Blocking Table .
Delete Selected Keyword	Select a row in the URL Blocking Table and click it to delete the row.
URL Blocking Table	A list of the URL (s) to which access is blocked.

3.5.2.4 Virtual Server

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

Web Configuration

Virtual Server

The page is used to configure virtual server.
So other users on the Internet can access the server on your LAN through the device.

Service Type:

Usual Service Name:

User-defined Service Name:

Protocol:

WAN Setting:

WAN Interface:

WAN Port: (ex. 5001:5010)

LAN Open Port:

LAN IP Address:

Apply Changes

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
------------	----------	------------------	------------	----------------	----------	-------	--------

The following table describes the parameters of this page:

Field	Description
Service Type	You can select the common service type, for example, AUTH , DNS , or FTP . You can also define a service name. <ul style="list-style-type: none"> ● If you select Usual Service Name, the corresponding parameter has the default settings. ● If you select User-defined Service Name, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose TCP or UDP .
WAN Setting	You can choose Interface or IP Address .
WAN Interface	Choose the WAN interface that will apply virtual server.
WAN Port	Choose the access port on the WAN.

Field	Description
LAN Open Port	Enter the port number of the specified service type.
LAN IP Address	Enter the IP address of the virtual server. It is in the same network segment with LAN IP address of the router.

3.5.2.5 IP Address Mapping

NAT is short for Network Address Translation. The Network Address Translation Settings window allows you to share one WAN IP address for multiple computers on your LAN.

Click **IP Address Mapping** in the left pane, the page shown in the following figure appears.

Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.

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"/>		

3.5.2.6 DMZ Setting

Demilitarized Zone (DMZ) 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.

Click **DMZ Setting** in the left pane, the page shown in the following figure appears. The following describes how to configure DMZ.

Step 3 Select **Enable DMZ** to enable this function.

Step 4 Enter an IP address of the DMZ host.

Step 5 Click **Apply Changes** to save the settings of this page temporarily.

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:

3.5.2.7 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.

NAT EXCLUDE IP

In the page ,you can config some source IP address which use the purge route mode when access internet through the specified interface.

interface:

IP Range: -

Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action
---------------	--------	---------	--------

3.5.2.8 ALG Setting

Click **ALG Setting** in the left pane, the page shown in the following figure appears.

NAT ALG and Pass-Through

This page is used to configure NAT ALG and pass-through.

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

3.5.2.9 Anti-DoS

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

Click **Anti-DoS** in the left pane, the page shown in the following figure appears. In this page, you can prevent DoS attacks.

Anti-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
- Whole System Flood: SYN Packets/Second
 - Whole System Flood: FIN Packets/Second
 - Whole System Flood: UDP Packets/Second
 - Whole System Flood: ICMP Packets/Second
 - Per-Source IP Flood: SYN Packets/Second
 - Per-Source IP Flood: FIN Packets/Second
 - Per-Source IP Flood: UDP Packets/Second
 - Per-Source IP Flood: ICMP Packets/Second
 - TCP/UDP PortScan Sensitivity
 - ICMP Smurf
 - IP Land
 - IP Spoof
 - IP TearDrop
 - PingOfDeath
 - TCP Scan
 - TCP SynWithData
 - UDP Bomb
 - UDP EchoChargen

- Enable Source IP Blocking Block time (sec)

3.5.3 UPnP

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

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPnP:

Disable Enable

WAN Interface:

Apply Changes

3.5.4 IGMP Proxy

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

IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

- . Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- . Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Multicast Allowed:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Robust Count:	<input type="text" value="2"/>	
Last Member Query Count:	<input type="text" value="2"/>	
Query Interval:	<input type="text" value="60"/>	(seconds)
Query Response Interval:	<input type="text" value="100"/>	(*100ms)
Group Leave Delay:	<input type="text" value="2000"/>	(ms)

3.5.5 TR-069

Choose **Service > TR-069**, the page shown in the following page appears. In this page, you can configure the TR-069 CPE.

TR-069 Configuration

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

ACS:

Enable:

URL:

User Name:

Password:

Periodic Inform Enable: Disable Enable

Periodic Inform Interval:

Connection Request:

User Name:

Password:

Path:

Port:

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

Certificate Management:

CPE Certificate:

Password:

CPE Certificate:

CA Certificate:

The following table describes the parameters of this page:

Field	Description
ACS	
URL	The URL of the auto-configuration server to connect to.
User Name	The user name for logging in to the ACS.
Password	The password for logging in to the ACS.
Periodic Inform Enable	Select Enable to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Debug	
Show Message	Select Enable to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select Enable , the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.

3.5.6 ACL

Choose **Service > ACL**, the page shown in the following figure appears. In this page, you can permit the data packets from LAN or WAN to access the router. You

Web Configuration

can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.



Note:

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

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 Changes

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

Services Allowed:

Any

Add

Reset

Current ACL Table:

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

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

Field	Description
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 IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can

Field	Description
	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 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:

WAN Interface:

Services Allowed:

- Web
 Telnet
 FTP
 TFTP
 SNMP
 PING

Current ACL Table:

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

Web Configuration

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

Field	Description
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 IP Address .
WAN Interface	Choose the interface that permits data packets from WAN to access the router.
IP Address	Enter the IP address on the WAN. Only the IP address that is in the same network segment with the IP 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 ACL Table .
Reset	Click it to refresh this page.

3.6 Advance

In the navigation bar, click **Advance**. In the **Advance** page that is displayed contains **Bridge Setting**, **Routing**, **Port Mapping**, **QoS**, **SNMP** and **Others**.

3.6.1 Bridge Setting

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

The screenshot shows the 'Bridge Setting' page within the 'Advance' section of the SONIQ web configuration interface. The navigation bar at the top includes 'Advance', 'Status', 'Wizard', 'Network', 'Service', 'Advance', 'Admin', and 'Diagnostic'. Under 'Advance', there are sub-tabs for 'Bridge Setting', 'Routing', 'Port Mapping', 'QoS', 'SNMP', and 'Others'. The 'Bridge Setting' sub-tab is active, displaying the title 'Bridge Setting' and a description: 'This page is used to configure the bridge parameters. In this page, you can modify the settings or view some information of the bridge and its attached ports.' Below the description, there are configuration fields: 'Aging Time' set to '300 (seconds)', and '802.1d Spanning Tree' with radio buttons for 'Disable' (selected) and 'Enable'. At the bottom, there are three buttons: 'Apply Changes', 'Reset', and 'Show MACs'.

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

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

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

Forwarding Table

MAC Address	Port	Type	Aging Time
01:80:c2:00:00:00	0	Static	300
01:00:5e:00:00:09	0	Static	300
00:22:b0:69:0d:64	1	Dynamic	300
00:1f:a4:dd:f6:b9	0	Static	300
ff:ff:ff:ff:ff:ff	0	Static	300

Refresh Close

3.6.2 Routing

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

3.6.2.1 Static Route

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

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:

Static Route Table:

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
--------	-------	-------------	-------------	----------	--------	-----------

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

Field	Description
Enable	Select it to use static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the Static Route Table .
Update	Select a row in the Static Route Table and modify the

Field	Description
	parameters. Then click it to save the settings temporarily.
Delete Selected	Select a row in the Static Route Table and click it to delete the row.
Show Routes	Click it, the IP Route Table appears. You can view a list of destination routes commonly accessed by your network.
Static Route Table	A list of the previously configured static IP routes.

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

IP Route Table

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

Destination	Subnet Mask	Next Hop	Interface
192.168.1.1	255.255.255.255	*	e1

Refresh Close

3.6.2.2 RIP

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

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: Disable Enable

Interface:

Receive Version:

Send Version:

RIP Configuration List:

Select	Interface	Receive Version	Send Version
--------	-----------	-----------------	--------------

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

Field	Description
RIP	Select Enable , the router communicates with other RIP-enabled devices.
Apply Changes	Click it to save the settings of this page.
Interface	Choose the router interface that uses RIP.
Receive Version	Choose the interface version that receives RIP messages. You can choose RIP1 , RIP2 , or Both . <ul style="list-style-type: none"> Choose RIP1 indicates the router receives RIP v1 messages. Choose RIP2 indicates the router receives RIP v2 messages. Choose Both indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose RIP1 or RIP2 . <ul style="list-style-type: none"> Choose RIP1 indicates the router broadcasts

Field	Description
	RIP1 messages only. <ul style="list-style-type: none">● Choose RIP2 indicates the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the Rip Configuration List .
Delete	Select a row in the Rip Configuration List and click it to delete the row.

3.6.3 Port Mapping

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

Port Mapping Configuration

The procedure for operating a mapping group is as follows:

1. Enable port mapping.
2. Select a group from the table.
3. Select interfaces from the available interface list and add it to the grouped interface list by using the arrow buttons to bind the ports.
4. Click "Apply Changes" to save the settings.

Note: The selected interfaces will be removed from their original groups and added to the new group.

Disable Enable

WAN

Interface Group

Add >

< Del

LAN

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3,pppoe1	Enabled
Group 1 <input type="radio"/>		--
Group 2 <input type="radio"/>		--
Group 3 <input type="radio"/>		--
Group 4 <input type="radio"/>		--

Apply Changes

The procedure for manipulating a mapping group is as follows:

- Step 6** Select **Enable** to enable this function.
- Step 7** Select a group from the table.
- Step 8** Select interfaces from the WAN and LAN interface list and add them to the grouped interface list using the arrow buttons to manipulate the required mapping of the ports.

Click **Apply Changes** to save the changes.

3.6.4 QoS

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

IP QoS

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

The procedure for configuring quality of service (QoS) is as follows:

1. Enable QoS.
2. Set traffic rule.
3. Assign the precedence or add marker for different stream.

IP QoS: Disable Enable

Apply

Step 1 Enable IP QoS and click **Apply** to enable IP QoS function.

Step 2 Click **add rule** to add a new IP QoS rule.

The page shown in the following figure appears.

IP QoS

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

The procedure for configuring quality of service (QoS) is as follows:

1. Enable QoS.
2. Set traffic rule.
3. 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	IP Preced	IP ToS	802.1p	WAN Itf	Sel

Add Rule

Delete

Delete All

Add QoS Rule

Source IP: Source Mask:

Destination IP: Destination Mask:

Source Port: Destination Port:

Protocol: Physical Port:

Set Priority:

Insert or Modify QoS Mark

Add Rule

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

Field	Description
IP QoS	Select to enable or disable IP QoS function. You need to enable IP QoS if you want to configure the parameters of this page.
QoS Policy	You can choose stream based , 802.1p based , or DSCP based .
Schedule Mode	You can choose strict prior or WFQ (4:3:2:1) .
Source IP	The IP address of the source data packet.
Source Mask	The subnet mask of the source IP address.
Destination IP	The IP address of the destination data packet.
Destination Mask	The subnet mask of the destination IP address.
Source Port	The port of the source data packet.
Destination Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rules. You can choose TCP , UDP , or ICMP .
Physical Port	The LAN interface responds to the IP QoS rules.
Set priority	The priority of the IP QoS rules. P0 is the highest priority and P3 is the lowest.
IP Precedence	You can choose from 0 to 7 define the priority in the ToS of the IP data packet.
IP ToS	The type of IP ToS for classifying the data package You can choose Normal Service , Minimize Cost , Maximize Reliability , Maximize Throughput , or Minimize Delay .
802.1p	You can choose from 0 to 7.
Delete	Select a row in the QoS rule list and click it to delete the row.
Delete all	Select all the rows in the QoS rule list and click it to delete the rows.

3.6.5 SNMP

Choose **Advance > SNMP**, the page shown in the following figure appears. You can configure the SNMP parameters.

SNMP Protocol Configuration

This page is used to configure the Simple Network Management Protocol (SNMP). In this page, you can modify the settings of system description, trap IP address, and community name and so on.

Enable SNMP

System Description: ADSL Router/Modem IGD

System Contact:

System Name: GD-W810N

System Location:

Trap IP Address:

Community Name (Read-only): public

Community Name (Read-Write): public

The following table describes the parameters of this page:

Field	Description
Enable SNMP	Select it to enable SNMP function. You need to enable SNMP, and then you can configure the parameters of this page.
Trap IP Address	Enter the trap IP address. The trap information is sent to the corresponding host.
Community Name (Read-only)	The network administrators must use this password to read the information of this router.
Community Name (Read-Write)	The network administrators must use this password to configure the information of the router.

3.6.6 Others

Choose **Advance** > **Others**, the page shown in the following figure appears.

Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to continuous.

Half Bridge: Disable Enable

Interface:

3.7 Admin

In the navigation bar, click **Admin**. The **Admin** page that is displayed contains **Commit/Reboot**, **Upgrade**, **System Log**, **Password**, **Time Zone** and **Logout**.

3.7.1 Commit/Reboot

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

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

Field	Description
Reboot from	You can choose Save the current configuration or Restore to the factory

Field	Description
	<p>default configuration.</p> <ul style="list-style-type: none"> ● Save the current configuration: Save the current settings, and then reboot the router. ● Restore to the factory default configuration: Reset to the factory default settings, and then reboot the the router.
Reboot	Click it to reboot the router.

3.7.2 Upgrade

Choose **Admin > Upgrade**. The **Upgrade** page that is displayed contains **Upgrade Firmware** and **Backup/Restore**.



Caution:

Do not turn off the router or press the Reset button while the procedure is in progress.

3.7.2.1 Upgrade Firmware

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

Upgrade Firmware
Backup/Restore

Upgrade Firmware

This page is used to upgrade the firmware to a new version.
System will reboot after the file is uploaded.

Caution: Do not power off the device during uploading. Otherwise, it may crash the system.

Select File:

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

Field	Description
-------	-------------

Select File	Click Browse to select the firmware file.
Upload	After selecting the firmware file, click Upload to starting upgrading the firmware file.
Reset	Click it to starting selecting the firmware file.

3.7.2.2 Backup/Restore

Click **Backup/Restore** in the left pane, the page shown in the following figure appears. You can backup the current settings to a file and restore the settings from the file that was saved previously.

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

Field	Description
Save Settings to File	Click it, and select the path. Then you can save the configuration file of the router.
Load Settings from File	Click Browse to select the configuration file.
Upload	After selecting the configuration file of the router, click Upload to start uploading the configuration file of the router.

3.7.3 System Log

Choose **Admin > System Log**, the page shown in the following figure appears. In this page, you can enable or disable system log function and view the system log.

Log Setting

This page is used to show the system event log.
You can set the log flag to Error or Notice (or both). Click ">>|", and the table shows the latest log information.

Error: Notice:

Event Log Table:

Old | << < > >> | New

Time	Index	Type	Log Information

Page: 1/1

3.7.4 Password

Choose **Admin > Password**, the page shown in the following figure appears. By default, the user name and password are **admin** and **admin** respectively. The common user name and password are **user** and **user** respectively.

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:

Privilege:

Old Password:

New Password:

Confirm Password:

User Account Table:

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

The following table describes the parameters of this page:

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

3.7.5 Time Zone

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

System Time Configuration

This page is used to configure the system time and Network Time Protocol (NTP) server. In this page, you can modify the settings or view some information of the system time and NTP parameters.

System Time:	<input type="text" value="1970"/> year	<input type="text" value="Jan"/> month	<input type="text" value="1"/> day	<input type="text" value="2"/> hour	<input type="text" value="52"/> min	<input type="text" value="12"/> sec
DayLight :	<input type="text" value="LocalTIME"/>					
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>						

NTP Configuration:

State:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Primary Server:	<input type="text"/>
Secondary Server:	<input type="text"/>
Interval:	Every <input type="text" value="1"/> hours
Time Zone:	<input type="text" value="(GMT) Gambia, Liberia, Morocco, England"/>
Local Time:	Thu Jan 1 2:52:12 1970
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

NTP Start:

The following table describes the parameters of this page:

Field	Description
System Time	Set the system time manually.
NTP Configuration	
State	Select enable or disable NTP function. You need to enable NTP if you want to configure the parameters of NTP.
Primary Server	Set the primary NTP server manually.
Secondary Server	Set the secondary NTP server manually.
Time Zone	Choose the time zone in which area you are from the drop down list.

3.8 Diagnostic

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

3.8.1 Ping

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



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

Field	Description
Host	Enter the valid IP address or domain name.
Run Ping	Click it to start to Ping.

3.8.2 ATM Loopback

Choose **Diagnostic > ATM Loopback**. The page shown in the following figure appears. In this page, you can use VCC loopback function to check the connectivity of the VCC. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

OAM Fault Management - Connectivity Verification

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.

Flow Type:

- F5 Segment
- F5 End-to-End
- F4 Segment
- F4 End-to-End

VPI:

VCI:

Click **Run Loopback** to start testing.

3.8.3 ADSL

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

Diagnostic ADSL

This page is used to diagnose the ADSL tone.

Start

	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					

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

3.8.4 Diagnostic Test

Choose **Diagnostic > Diagnostic Test**, the page shown in the following figure appears. In this page, you can test the DSL connection. You can also view the LAN status connection and ADSL connection.

Diagnostic Test

The device is capable of testing your ADSL connection. After selecting an interface, click "Run Diagnostic Test". The result of each test item is listed below. If a test shows a fail status, click "Run Diagnostic Test" again to ensure that the the fail status is consistent.

Select the Interface:

Run Diagnostic Test

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

SONIQ