

# **SW200**

## **User Manual**

V1.0

## Contents

1 Introduction.....	1
1.1 Safety Precautions.....	1
1.2 LEDs and Interfaces.....	2
1.3 System Requirements.....	3
1.4 Features.....	4
2 Hardware Installation.....	6
3 About the Web Configuration.....	9
3.1 Access the Router.....	9
3.2 Status.....	10
3.3 Wizard.....	12
3.4 Setup.....	18
3.4.1 WAN Configuration.....	18
3.4.1.1 WAN.....	18
3.4.1.2 ATM Setting.....	24
3.4.1.3 ADSL Setting.....	25
3.4.2 LAN.....	25
3.4.2.1 LAN.....	25
3.4.2.2 DHCP.....	27
3.4.2.3 DHCP Static.....	32
3.4.3 WLAN.....	33
3.4.3.1 Basic Settings.....	33
3.4.3.2 Security.....	35
3.4.3.3 Multi-BSSID.....	38
3.4.3.4 Access Control.....	40
3.4.3.5 Advanced.....	40
3.4.3.6 WPS.....	42
3.5 Advanced.....	44
3.5.1 Route.....	44
3.5.1.1 Static Route.....	44
3.5.1.2 RIP.....	45
3.5.2 NAT.....	47
3.5.2.1 DMZ.....	47

3.5.2.2 Virtual Server.....	48
3.5.2.3 ALG.....	50
3.5.2.4 NAT Exclude IP.....	50
3.5.2.5 Port Trigger.....	51
3.5.2.6 FTP ALG PORT.....	53
3.5.2.7 Nat IP Mapping.....	53
3.5.3 QoS.....	54
3.5.4 CWMP.....	57
3.5.5 Port Mapping.....	59
3.5.6 Others.....	64
3.5.6.1 Bridge Setting.....	64
3.5.6.2 Client Limit.....	65
3.5.6.3 Others.....	65
3.6 Service.....	66
3.6.1 IGMP.....	66
3.6.1.1 IGMP Proxy.....	66
3.6.2 UPnP.....	67
3.6.3 SNMP.....	68
3.6.4 DNS.....	69
3.6.4.1 DNS.....	69
3.6.5 DDNS.....	70
3.6.6 FTP Server.....	71
3.7 Firewall.....	71
3.7.1 MAC Filter.....	71
3.7.2 IP/Port Filter.....	72
3.7.2.1 IP/Port Filter.....	72
3.7.3 URL Filter.....	73
3.7.4 ACL.....	74
3.7.4.1 ACL.....	74
3.7.5 DoS.....	78
3.8 Maintenance.....	80
3.8.1 Update.....	80
3.8.1.1 Firmware Update.....	80
3.8.1.2 Backup/Restore.....	81

---

3.8.2 Password.....	81
3.8.3 Reboot.....	82
3.8.4 Time.....	83
3.8.5 Log.....	85
3.8.6 Diagnostics.....	85
4 Q&A.....	87

# 1 Introduction

The device supports multiple line modes. It provides four 10/100 base-T Ethernet interfaces at the user end. The device provides high-speed ADSL2/2+ broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high performance access to the Internet.

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

## 1.1 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.

## 1.2 LEDs and Interfaces

### Front Panel



The following table describes the LEDs of the device.

LEDs	Status	Description
Power 	On	The initialization of the device is successful.
	Off	The device is powered off.
DSL 	On	DSL link up / link synchronized.
	Off	Link disconnection.
	Blinking	Link training / DSL link not synchronized.
INT 	On	Successful PPP session.
	Blinking	Failure PPP session (1 minute after link up).
	Off	Before DSL link up.
WiFi 	On	The WLAN connection has been activated.
	Off	The WLAN connection is not activated.
LAN1~4 	On	The LAN connection is normal and activated.
	Off	The LAN interface is disconnected.
WPS 	Blinking	WPS is triggered, and is waiting for client to negotiate.
	Off	WPS is idle.

### Rear Panel

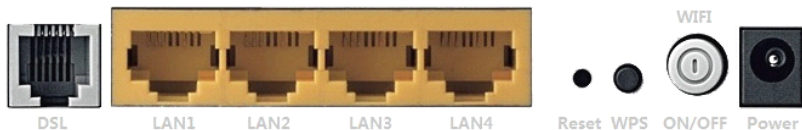


Figure 1

The following table describes the interfaces and buttons of the device:

Interface	Description
Reset	Reset to the factory default configuration. Keep the device powered on, and insert a needle into the hole for 3 seconds, then release it. The device is reset to the factory default configuration.
ON/OFF	Power switch, power on or power off the device.
Power	Power interface, for connecting to the power adapter of DC 12V, 0.5A.
LAN1~4	RJ45 interface, for connecting to the Ethernet interface of a PC or the Ethernet devices through an Ethernet cable.
DSL	RJ11 interface, for connecting to the ADSL interface or a splitter through a telephone cable.
WLAN/WPS	<ul style="list-style-type: none"><li>● Press the button between 1s and 5s to enable WLAN function.</li><li>● Press the button for more than 5s to enable WPS (Wi-Fi Protected Setup) function.</li></ul>

## 1.3 System Requirements

Recommended system requirements are as follows:

- Service subscriber
- 10 Base T/100 Base T Ethernet card
- Hub or switch (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows 98 SE, Windows 2000, Windows ME, Windows XP, Windows Vista, Window 7
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or FireFox 1.5 or higher

## 1.4 Features

The device supports the following features:

- Various line modes (line auto-negotiation)
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483B/1483R/MER access
- Multiple PVCs (eight at most)
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Auto PVC
- DHCP server
- IPv4/IPv6
- NAT/NAPT
- ALG
- TR-069
- SNMP
- Static route
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- DNS relay
- Virtual server
- Two-level passwords and usernames
- Web interface
- Telnet CLI
- System status display
- PPP session PAP/CHAP
- IP/Port filter
- Remote access control
- Line connection status test
- Remote management (Telnet; HTTP )
- Backup and restoration of configuration file
- IP quality of service (QoS)
- Universal plug and play (UPnP)



- WLAN with high-speed data transmission rate, compatible with IEEE 802.11b/g/n, 2.4 GHz compliant equipment

## 2 Hardware Installation

**Step 1** Connect the **DSL** interface of the router 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 modem with the network card of the PC through an Ethernet line (MDI/MDIX).



**Note:**

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

**Step 3** Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** interface of the modem.

### Connection 1

Figure1 displays the application diagram for the connection of the modem, PC, splitter, and telephone sets, when no telephone set is placed before a splitter. This type of connection is recommended.

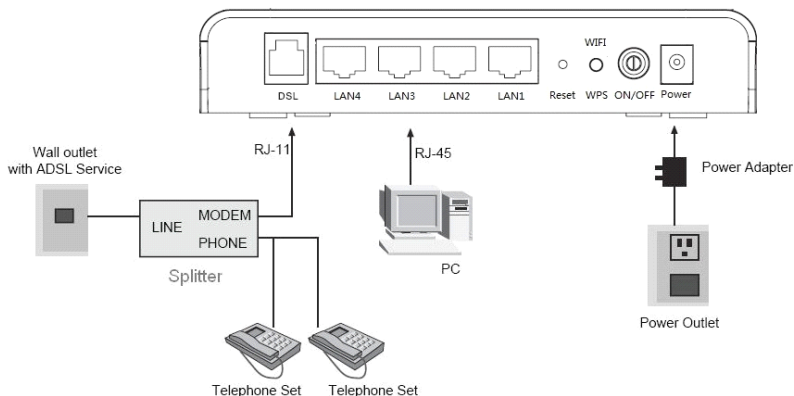


Figure 2 Connection diagram (no telephone set is placed before the splitter)

## Connection 2

Figure 2 displays the connection when the telephone set is placed before a splitter.

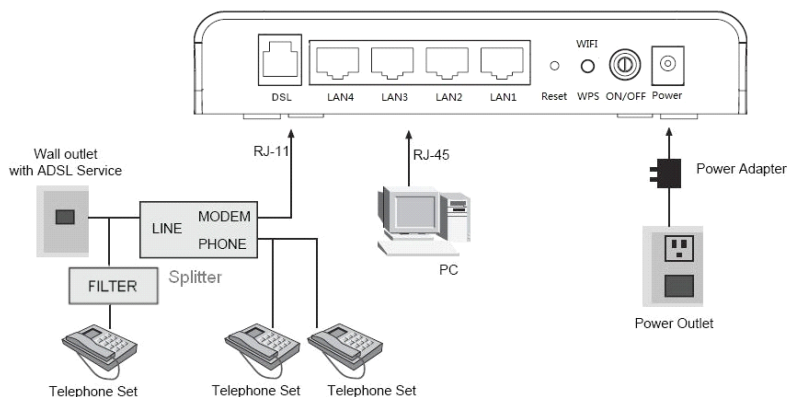


Figure 3 Connection diagram (a telephone set is placed before the splitter)



**Note:**

In actual application, it is recommended to following connection 1. 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 a failure of connection between the modem and the device of LAN side, or cannot access into the Internet, or slow the connection speed. If you really need to add a telephone set before the splitter, you have to add a micro filter before connecting to a telephone set. Do not connect several telephones before the splitter. Do not connect several telephones with the micro filter.

## 3 About the Web Configuration

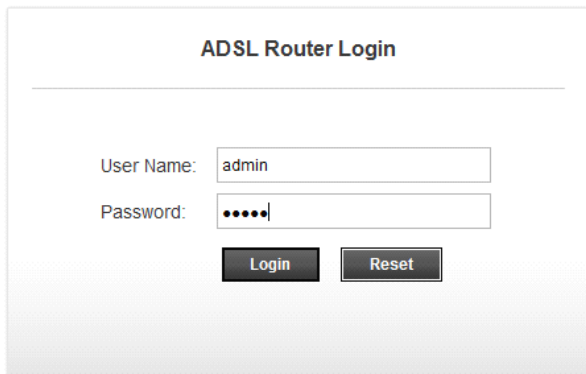
This chapter describes how to configure the router by using the Web-based configuration utility.

### 3.1 Access the Router

The following is the detailed description of accessing the router for the first time. Configure the IP address of the PC as 192.168.1.X (2~254), Subnet Mask as 255.255.0.

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



**ADSL Router Login**

---

User Name:

Password:

If you log in as a super user, you will see the **Device Info** page as shown below appears. You can check the basic settings of the modem, such as firmware version, upstream speed, downstream speed, LAN MAC address, LAN IP address, DHCP server status. You can also view the basic status of WAN and DNS server.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

> Device\_info

> Device\_info

> ADSL

> Statistics

### ADSL Router Status

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

System

Alias Name	ADSL Modem
Uptime	0 0:37:5
Date/Time	Sun Jan 1 0:37:5 2012
Firmware Version	V2.1.1
Built Date	Dec 14 2012 09:55:33
Serial Number	0019E0016690

DSL

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

CWMP Status

Inform Status	Inform is broken
Connecion Request Status	No connection request

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:19:E0:01:66:90

DNS Status

DNS Mode	Auto
DNS Servers	

WAN Configuration

Interface	VPI/VCI	Encap	Droute	Protocol	IP Address	Gateway	Status
pppoe1	8/35	LLC	On	PPPoE	0.0.0.0	0.0.0.0	down 0 0:0:0 /0 0:0:0 <a href="#">connect</a>

Refresh

## 3.2 Status

The tab **Status** contains **Device Info** and **Statistics**. Click **Status** > **Device Info** > **ADSL**, the following page appears. You can see the router settings such as the Adsl Line Status, Vendor ID and Firmware Version.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

> Device\_info

> Device\_info

> ADSL

> Statistics

### ADSL Configuration

This page shows the setting of the ADSL Router.

Adsl Line Status	ACTIVATING.
Adsl Mode	--
Up Stream	--
Down Stream	--
Attenuation Down Stream	--
Attenuation Up Stream	--
SNR Margin Down Stream	--
SNR Margin Up Stream	--
Vendor ID	
Firmware Version	4925ca26
CRC Errors	--
Up Stream BER	--
Down Stream BER	--
Up Output Power	--
Down Output Power	--
Down Stream ES	--
Up Stream ES	--
Down Stream SES	--
Up Stream SES	--
Down Stream UAS	--
Up Stream UAS	--

Adsl Retrain:
 

Retrain

Refresh

Click **Status** > **Statistics**, the following page appears. In this page, you can view the statistics of each network port.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Device\_info

Statistics

Statistics

### Statistics

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

Statistics:

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
e1	5877	0	0	4949	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	515	0	0	33	0	74
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

Refresh

## 3.3 Wizard

In the navigation bar, click **Wizard**. The tab **Wizard** only contains **Wizard**.



1) Change the VPI or VCI values which are used to define a unique path for your connection. If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP.

2) Please select the Connection Type given by your ISP.

<b>Connection Mode:</b>	<input type="radio"/> 1483 Bridged
	<input type="radio"/> 1483 MER
	<input checked="" type="radio"/> PPP over Ethernet(PPPoE)
	<input type="radio"/> PPP over ATM(PPPoA)
	<input type="radio"/> 1483 Routed

3) Here we use PPPoE as an example. Enter the Username, Password and Confirm Password given by your ISP, and then click Next.

<b>PPP Settings:</b>	Username: <input type="text"/>	Password: <input type="text"/>
----------------------	--------------------------------	--------------------------------

4) On the Wireless screen, we use the default SSID, select a Mode. Set a Password or select Disable Security(Disable Security is not recommended.), and then click **Next** to continue.

**Fast Config**

Step 2: Wireless Fast Settings:

Please config basic settings about wireless.

WLAN:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band:	2.4 GHz (B+G+N) ▼
SSID:	<input type="text" value="WLAN_Emvr"/>
Encryption:	WPA2(AES) ▼
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
	Pre-Shared Key Format: <input type="text" value="Passphrase"/> ▼
	Pre-Shared Key: <input type="text" value="1345678"/>

prev

next

5) On this page, please confirm all parameters. Click **Prev** to modify or click the **Apply Changes** button to save your configuration.

**Fast Config****Step 3: Save Settings**

If you need finish settings in the fast config, please click "Apply Changes". otherwise please click "Cancel" or "Prev".

**Settings as follow:**

VPI:	8
VCI:	35
Encapsulation:	LLC/SNAP
Channel Mode:	pppoe
ppp username:	12345678
ppp password:	12345678
DNS Setting:	DNS Automatically
WLAN :	Enable

Prev

Apply Changes

Cancel

6) You will see the Complete screen below.



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

DSL CWMP Status

LAN Configuration

 **DNS Status**

### WAN Configuration

Refresh

## 3.4 Setup

In the navigation bar, click **Setup**. The tab **Setup** contains **WAN**, **LAN** and **WLAN**.

### 3.4.1 WAN Configuration

#### 3.4.1.1 WAN

Choose **Setup > WAN > WAN** and the page shown in the following figure appears.

In this page, you can configure WAN interface of your router.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

> WAN

> WAN

> ATM

> ADSL

> LAN

> WLAN

### Channel Configuration

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

Default Route Selection:

☐ Auto
 ☒ Specified

VPI:

VCI:

Encapsulation:

☒ LLC
 ☐ VC-Mux

Channel Mode: 1483 Bridged

Enable NAPT: ☐

Enable IGMP: ☐

#### PPP Settings:

User Name:

Password:

Type: Continuous

Idle Time (min):

#### WAN IP Settings:

Type:

☐ Fixed IP
 ☒ DHCP

Local IP Address:

Remote IP Address:

Netmask:

Default Route:

☐ Disable
 ☒ Enable
 ☐ Auto

Unnumbered: ☐

Connect

Disconnect

Add

Modify

Delete

Undo

Refresh

#### Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	DRoute	IP Addr	Remote IP	NetMask	User Name	Status	Edit
<input type="radio"/>	pppoe1	PPPoE	8	35	LLC	On	Off	On	0.0.0.0	0.0.0.0	255.255.255.255	12345678	down	

The following table describes the parameters of this page.

Field	Description
Default Route Selection	You can select <b>Auto</b> or <b>Specified</b> .
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





Field	Description
	31 are reserved for known protocols)
Encapsulation	You can choose <b>LLC</b> and <b>VC-Mux</b> .
Channel Mode	You can choose <b>1483 Bridged</b> , <b>1483 MER</b> , <b>PPPoE</b> , <b>PPPoA</b> , <b>1483 Routed</b> or <b>IPoA</b> .
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.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
IP Protocol	Select this interface support ipv4/ipv6, ipv4 or ipv6.
<b>PPP Settings</b>	
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 <b>Continuous</b> , <b>Connect on Demand</b> or <b>Manual</b> .
Idle Time (min)	If set the type to <b>Connect on Demand</b> , 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.
<b>WAN IP Settings</b>	
Type	You can choose <b>Fixed IP</b> or <b>DHCP</b> . <ul style="list-style-type: none"> <li>● If select <b>Fixed IP</b>, you should enter the local IP address, remote IP address and subnet mask.</li> <li>● If select <b>DHCP</b>, the router is a DHCP</li> </ul>




Field	Description
	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.
IPv6 WAN Setting	Set ipv6 wan setting if this interface support ipv6
Address Mode	Select this interface support Slaac or Static to generate wan ipv6 addresses.
Enable DHCPv6 Client	Enable or disable dhcpv6 client on this interface, if enable, user can specify if the dhcpv6 client request Address or request Prefix.
Add	After configuring the parameters of this page, click it to add a new PVC into the <b>Current ATM VC Table</b> .
Modify	Select a PVC in the <b>Current ATM VC Table</b> , then modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
Delete	Select a PVC in the Current ATM VC Table, and then click <b>Delete</b> to delete it
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.

After proper settings, click Add and the following page appears.

### Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	DRoute	IP Addr	Remote IP	NetMask	User Name	Status	Edit
<input type="radio"/>	pppoe1	PPPoE	8	35	LLC	On	Off	Off	0.0.0.0	0.0.0.0	255.255.255.255	12345678	down	 
<input type="radio"/>	pppoe2	PPPoE	0	35	LLC	On	Off	On	0.0.0.0	0.0.0.0	255.255.255.255	123456	down	 

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:	8/35
Login Name:	<input type="text" value="12345678"/>
Password:	<input type="password" value="*****"/>
Authentication Method:	AUTO ▾
Connection Type:	Continuous ▾
Idle Time (s):	<input type="text" value="0"/>
Bridge:	<input type="radio"/> Bridged Ethernet (Transparent Bridging) <input type="radio"/> Bridged PPPoE (implies Bridged Ethernet) <input checked="" type="radio"/> Disable Bridge
AC-Name:	<input type="text"/>
Service-Name:	<input type="text"/>

802.1q:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VLAN ID(1-4095):	<input type="text" value="0"/>
MTU (1-1500):	<input type="text" value="1492"/>
Static:	<input type="text"/>
Source Mac address:	<input type="text" value="00:19:E0:01:66:90"/> (ex:00:E0:86:71:05:02) <input type="button" value="MACCLONE"/>

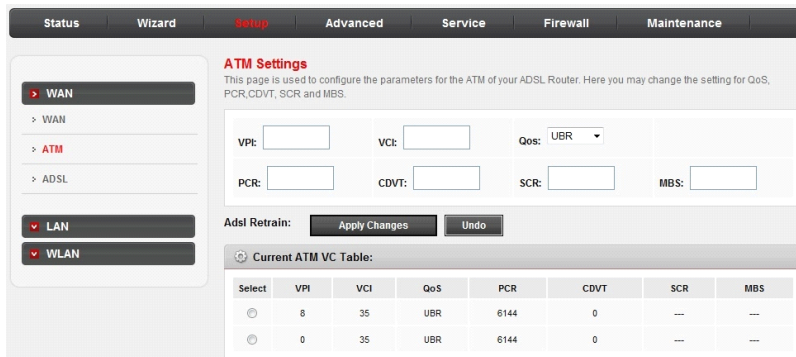



The following table describes the parameters and buttons of this page.

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 <b>AUTO</b> , <b>PAP</b> or <b>CHAP</b> .
Connection Type	You can choose <b>Continuous</b> , <b>Connect on Demand</b> or <b>Manual</b> .
Idle Time (s)	If choose <b>Connect on Demand</b> , 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 <b>Bridged Ethernet</b> , <b>Bridged PPPoE</b> or <b>Disable Bridge</b> .
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select <b>Disable</b> or <b>Enable</b> . 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 <b>Channel Configuration</b> 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.

### 3.4.1.2 ATM Setting

Click **ATM** 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.



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

VPI:  VCI:  QoS:

PCR:  CDVT:  SCR:  MBS:

Adsl Retrain:

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	8	35	UBR	6144	0	---	---
<input type="radio"/>	0	35	UBR	6144	0	---	---

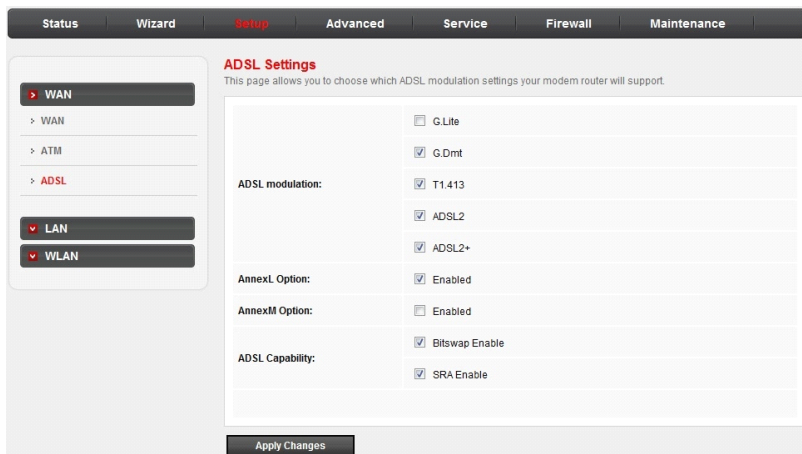
The following table describes the parameters of this page.

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 <b>UBR, CBR, rt-VBR</b> or <b>nrt-VBR</b> .
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	Sustain 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.

Field	Description
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.

### 3.4.1.3 ADSL Setting

Click **ADSL** in the left pane, the page shown in the following figure appears. In this page, you can select the DSL modulation. Generally you need to remain this factory default settings. The router negotiates the modulation modes with the DSLAM.



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

ADSL modulation:

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

AnnexL Option: ☒ Enabled

AnnexM Option: ☐ Enabled

ADSL Capability:

- ☒ Bitswap Enable
- ☒ SRA Enable

Apply Changes

## 3.4.2 LAN

### 3.4.2.1 LAN

Click **LAN** 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

▼ WAN

> LAN

> DHCP

> DHCP Static

▼ WLAN

### 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:

Ethernet1

IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

☐ Secondary IP

IGMP Snooping:

☒ Disable
 ☐ Enable

Apply Changes

LAN Port:

▼

Link Speed/Duplex Mode:

▼

Modify

ETHERNET Status Table:

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

MAC Address Control:

☐ LAN1
 ☐ LAN2
 ☐ LAN3
 ☐ LAN4
 ☐ WLAN

Apply Changes

New MAC Address:

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

Field	Description
	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: <b>100Mbps/FullDuplex, 100Mbps/Half Duplex, 10Mbps/FullDuplex, 10Mbps/Half Duplex</b> and <b>Auto Negotiation</b> .
Modify	Select the index from Ethernet status table, and then click <b>modify</b> .
Ethernet Status Table	It shows the current Ethernet status list.
MAC Address Control	Select the LAN interface on which you want to run MAC Address Control.
New MAC Address	A MAC address to be added.
Current Allowed MAC Address Table	It shows the current allowed MAC address list.

### 3.4.2.2 DHCP

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
--------	--------	-------	----------	---------	----------	-------------

WAN

LAN

LAN

DHCP

DHCP Static

WLAN

### DHCP Mode

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

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

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

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

LAN IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

DHCP Mode

DHCP Server

Interface:

☒ LAN1
 ☒ LAN2
 ☒ LAN3
 ☒ LAN4
 ☒ WLAN
 ☒ VAP0
 ☒ VAP1
 ☒ VAP2
 ☒ VAP3

IP Pool Range

192.168.1.2

-

192.168.1.254

Show Client

Subnet Mask:

255.255.255.0

Default Gateway:

192.168.1.1

Max Lease Time:

1440

minutes

Domain Name:

domain.name

192.168.1.1

DNS Servers:

Apply Changes

Undo

Set VendorClass IP Range

The following table describes the parameters of this page.


Field	Description
DHCP Mode	If set to <b>DHCP Server</b> , 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 IP address in the IP address pool. The router assigns IP address that base on the IP



Field	Description
	pool range to the host.
Pool Size	It allows the size machines that can be set up
Show Client	Click it, the <b>Active DHCP Client Table</b> 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 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 <b>Device IP Range Table</b> 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

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 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 Vendor Class 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:	<input type="text"/>
start address:	<input type="text"/>
end address:	<input type="text"/>
Router address:	<input type="text"/>
option60	<input type="text"/>

⊙ IP Range Table:

select:	device name:	start address:	end address:	default gateway:	option60:
---------	--------------	----------------	--------------	------------------	-----------

Choose **None** in the **DHCP Mode** field, and the page shown in the following figure appears.

### DHCP Mode

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

- (1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.  
 (2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.  
 (3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Mode	None ▼

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

### DHCP Mode

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

- (1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.  
 (2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.  
 (3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

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

Relay Server:

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

Field	Description
DHCP Mode	If set to <b>DHCP Relay</b> , the router acts a surrogate DHCP Server and relays the DHCP requests and reponses 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.
Undo	Click it to refresh this page.

### 3.4.2.3 DHCP Static

Click **DHCP Static** 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 fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address:

Mac Address:
 
 (ex. 00E086710502)

Add

Delete Selected

Undo

Current ATM VC Table:
 

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

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

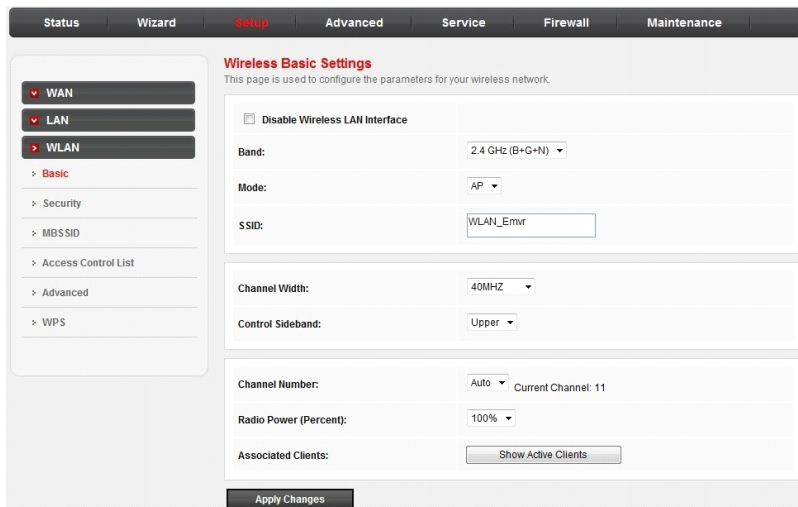
Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the <b>DHCP Static IP Table</b> .
Delete Selected	Select a row in the <b>DHCP Static IP Table</b> , then click it, this row is deleted.
Undo	Click it to refresh this page.
DHCP Static IP Table	It shows the assigned IP address based on the MAC address.

### 3.4.3 WLAN

Choose **Setup > WLAN**. The WLAN page that is displayed contains **Basic**, **Security**, **MBSSID**, **Access Control**, **Advanced** and **WPS**.

#### 3.4.3.1 Basic Settings

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



The screenshot shows the 'Wireless Basic Settings' page. At the top, there is a navigation bar with tabs: Status, Wizard, Setup (highlighted), Advanced, Service, Firewall, and Maintenance. On the left, a sidebar contains a tree view with 'WAN', 'LAN', and 'WLAN' (expanded). Under 'WLAN', there are sub-items: Basic (highlighted), Security, MBSSID, Access Control List, Advanced, and WPS. The main content area is titled 'Wireless Basic Settings' and includes a subtitle: 'This page is used to configure the parameters for your wireless network.' The settings are organized into several sections:
 

- Disable Wireless LAN Interface:** A checkbox that is currently unchecked.
- Band:** A dropdown menu set to '2.4 GHz (B+G+N)'.
- Mode:** A dropdown menu set to 'AP'.
- SSID:** A text input field containing 'WLAN\_Emr'.
- Channel Width:** A dropdown menu set to '40MHZ'.
- Control Sideband:** A dropdown menu set to 'Upper'.
- Channel Number:** A dropdown menu set to 'Auto', with 'Current Channel: 11' displayed next to it.
- Radio Power (Percent):** A dropdown menu set to '100%'.
- Associated Clients:** A button labeled 'Show Active Clients'.

 At the bottom of the settings area, there is an 'Apply Changes' button.

The following table describes the parameters of this page.

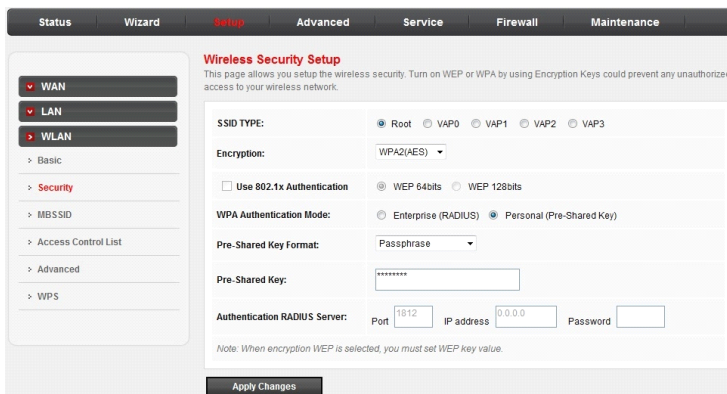
Field	Description
Band	Choose the working mode of the modem. You can choose from drop-down list.

Field	Description
	<div> <div>2.4 GHz (B+G+N) ▼</div> <div>           2.4 GHz (B)            2.4 GHz (G)            2.4 GHz (B+G)            2.4 GHz (N)            2.4 GHz (G+N)            2.4 GHz (B+G+N)         </div> </div>
Mode	Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is <b>AP</b> .
SSID	The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.
Broadcast SSID	Enable or disable this function.
Channel Width	You can choose <b>20MHZ</b> , <b>40MHZ</b> or <b>20/40MHZ</b> .
Control Sideband	You can choose Upper or Lower.
Country/Area	Select the country from the drop-down list.
Channel Number	A channel is the radio frequency used by 802.11b/g/n wireless devices. 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 <b>100%</b> . It is recommended to choose the default value <b>100%</b> .
Show Active Clients	Click it to view the information of the wireless

Field	Description
	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 <b>Save</b> in the lower left corner.

### 3.4.3.2 Security

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



The screenshot shows the 'Wireless Security Setup' page in a web interface. The top navigation bar includes Status, Wizard, Setup (highlighted), Advanced, Service, Firewall, and Maintenance. On the left, a sidebar shows WLAN, LAN, and WLAN (selected) with sub-options: Basic, Security (selected), MBSSID, Access Control List, Advanced, and WPS. The main content area is titled 'Wireless Security Setup' and includes a note: '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.' The settings include: SSID TYPE (Root selected), Encryption (WPA2(AES) selected), Use 802.1x Authentication (unchecked), WPA Authentication Mode (Enterprise (RADIUS) selected), Pre-Shared Key Format (Passphrase selected), Pre-Shared Key (masked), and Authentication RADIUS Server (Port 1812, IP address 0.0.0.0, Password). A note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.' An 'Apply Changes' button is at the bottom.

The following table describes the parameters of this page.

Field	Description
SSID Type	Service Set Identifier, is a name of a local area network
Encryption	<p>Configure the wireless encryption mode. You can choose <b>None</b>, <b>WEP</b>, <b>WPA (TKIP)</b>, <b>WPA (AES)</b>, <b>WPA2 (AES)</b>, <b>WPA2 (TKIP)</b> or <b>WPA2 Mixed</b>.</p> <ul style="list-style-type: none"> <li>Wired equivalent privacy0 (WEP) encrypts data frames before transmitting over the wireless network.</li> <li>Wi-Fi protected access (WPA) is a subset of</li> </ul>

Field	Description
	<p>the IEEE802.11i security specification draft.</p> <ul style="list-style-type: none"> <li>WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2.</li> </ul> <p>Key differences between WPA and WEP are user authentication and improved data encryption.</p>
Set WEP Key	<p>It is available when you set the encryption mode to <b>WEP</b>. Click it, the <b>Wireless WEP Key Setup</b> page appears.</p>
WPA Authentication Mode	<ul style="list-style-type: none"> <li>Select <b>Personal (Pre-Shared Key)</b>, enter the pre-shared key in the <b>Pre-Shared Key</b> field.</li> <li>Select <b>Enterprise (RADIUS)</b>, 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.</li> </ul> <p>If the encryption is set to <b>WEP</b>, the modem uses 802.1 X authentication, which is Radius authentication.</p>

Click **Set WEP Key**, 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.

SSID TYPE:	<input checked="" type="radio"/> Root <input type="radio"/> VAP0 <input type="radio"/> VAP1 <input type="radio"/> VAP2 <input type="radio"/> VAP3		
Encryption:	WEP		
Key Length:	64-bit		
Key Format:	Hex (10 characters)		
Default Tx Key:	Key 1		
Encryption Key 1:	<input type="password"/>		
Encryption Key 2:	<input type="password"/>		
Encryption Key 3:	<input type="password"/>		
Encryption Key 4:	<input type="password"/>		
<input type="checkbox"/> Use 802.1x Authentication <input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits			
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)		
Pre-Shared Key Format:	Passphrase		
Pre-Shared Key:	<input type="password"/>		
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text" value="0.0.0.0"/>	Password <input type="password"/>
<i>Note: When encryption WEP is selected, you must set WEP key value.</i>			
<input type="button" value="Apply Changes"/>			

The following describes the parameters of this page.

Field	Description
Key Length	Choose the WEP key length. You can Choose <b>64-bit</b> or <b>128-bit</b> .
Key Format	<ul style="list-style-type: none"> <li>If you choose <b>64-bit</b>, you can choose ASCII (5 characters) or Hex (10 characters).</li> <li>If you choose <b>128-bit</b>, you can choose ASCII (13 characters) or Hex (26 characters).</li> </ul>
Default Tx Key	Choose the index of WEP Key. You can choose <b>Key</b>

Field	Description
	<b>1, Key 2, Key 3 or Key 4.</b>
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"> <li>● If you choose <b>64-bit</b> and <b>ASCII (5 characters)</b>, enter any 5 ASCII characters.</li> <li>● If you choose <b>64-bit</b> and <b>Hex (10 characters)</b>, enter any 10 hexadecimal characters.</li> <li>● If you choose <b>128-bit</b> and <b>ASCII (13 characters)</b>, enter any 13 ASCII characters.</li> <li>● If you choose <b>128-bit</b> and <b>Hex (26 characters)</b>, enter any 26 hexadecimal characters.</li> </ul>
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click <b>Save</b> in the lower left corner.

### 3.4.3.3 Multi-BSSID

Choose **WLAN > MBSSID**, and the following page appears. In this page, you can configure the multi-BSSID of the wireless clients.

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
--------	--------	-------	----------	---------	----------	-------------

WLAN

LAN

WLAN

Basic

Security

**MBSSID**

Access Control List

Advanced

WPS

### Wireless Multiple BSSID Setup

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

☐ Enable VAP0
 

SSID:

broadcast SSID: ☒ Enable ☐ Disable

Relay Blocking: ☐ Enable ☒ Disable

Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

☐ Enable VAP1
 

SSID:

broadcast SSID: ☒ Enable ☐ Disable

Relay Blocking: ☐ Enable ☒ Disable

Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

☐ Enable VAP2
 

SSID:

broadcast SSID: ☒ Enable ☐ Disable

Relay Blocking: ☐ Enable ☒ Disable

Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

☐ Enable VAP3
 

SSID:

broadcast SSID: ☒ Enable ☐ Disable

Relay Blocking: ☐ Enable ☒ Disable

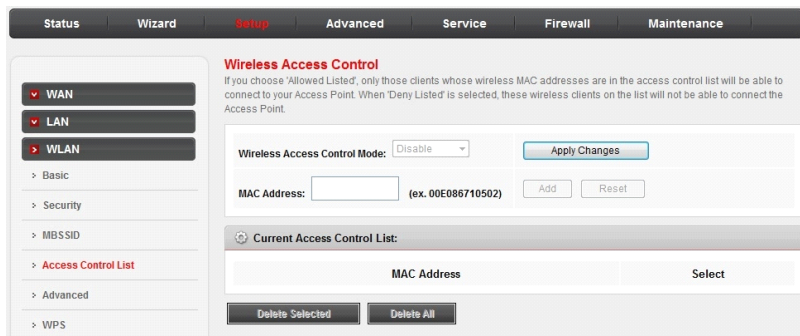
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

Apply Changes

It supports 4 virtual access points (VAPs). It is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same name. Enter a descriptive name that is used when the wireless client connecting to the modem.

### 3.4.3.4 Access Control

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



The screenshot shows the 'Wireless Access Control' configuration page. On the left is a sidebar menu with options: WAN, LAN, WLAN (selected), Basic, Security, MBSSID, Access Control List (highlighted), Advanced, and WPS. The main content area has a title 'Wireless Access Control' and a descriptive paragraph. Below this, there is a 'Wireless Access Control Mode' dropdown set to 'Disable' and an 'Apply Changes' button. A 'MAC Address' input field is shown with an example '(ex. 00E086710502)' and 'Add' and 'Reset' buttons. A section titled 'Current Access Control List' contains a table with two columns: 'MAC Address' and 'Select'. Below the table are 'Delete Selected' and 'Delete All' buttons.

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.

### 3.4.3.5 Advanced

Choose **Wireless > Advanced**, 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** are modified by the professional personnel, it is recommended to keep the default values.

### Wireless Advanced Settings

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

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

**Apply Changes**

The following table describes the parameters of this page.

Field	Description
Authentication	<p>Select the modem operating in the open system or encryption authentication. You can choose <b>Open System</b>, <b>Shared Key</b> or <b>Auto</b>.</p> <ul style="list-style-type: none"> <li>In the open system, the wireless client can directly connect to the device</li> <li>In the encryption authentication, the wireless client connects to the modem through the shared key.</li> </ul>

Field	Description
Data Rate	Choose the transmission rate of the wireless data. You can choose <b>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 ~ MSC7.</b>
Preamble Type	<ul style="list-style-type: none"> <li>● <b>Long Preamble:</b> It means this card always use long preamble.</li> <li>● <b>Short Preamble:</b> It means this card can support short preamble capability.</li> </ul>
Broadcast SSID	Select whether the modem broadcasts SSID or not. You can select <b>Enable</b> or <b>Disable</b> . <ul style="list-style-type: none"> <li>● Select <b>Enable</b>, the wireless client searches the modem through broadcasting SSID.</li> <li>● Select <b>Disable</b> to hide SSID, the wireless clients can not find the SSID.</li> </ul>
Relay Blocking	Wireless isolation. Select <b>Enable</b> , the wireless clients that are connected to the modem can not intercommunication.
Ethernet to Wireless Blocking	Whether the wireless network can communicate with the Ethernet network or not.
Wifi Multicast to Unicast	Enable it to using unicast to transmit multicast packet
Aggregation	It is applied when the destination end of all MPDU are for one STA.
Short GI	It is not recommended to enable GI in obvious environment of Multi-path effect.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click <b>Save</b> in the lower left corner.

### 3.4.3.6 WPS


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

### Wi-Fi Protected Setup

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

<input type="checkbox"/> Disable WPS		
WPS Status:	<input checked="" type="radio"/> Configured	<input type="radio"/> UnConfigured
Self-PIN Number:	<input type="text" value="09811041"/>	<input type="button" value="Regenerate PIN"/>
Push Button Configuration:	<input type="button" value="Start PBC"/>	

 **Current Key Info:**

Authentication	Encryption	Key
WPA2 PSK	AES	85512217

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 Advanced

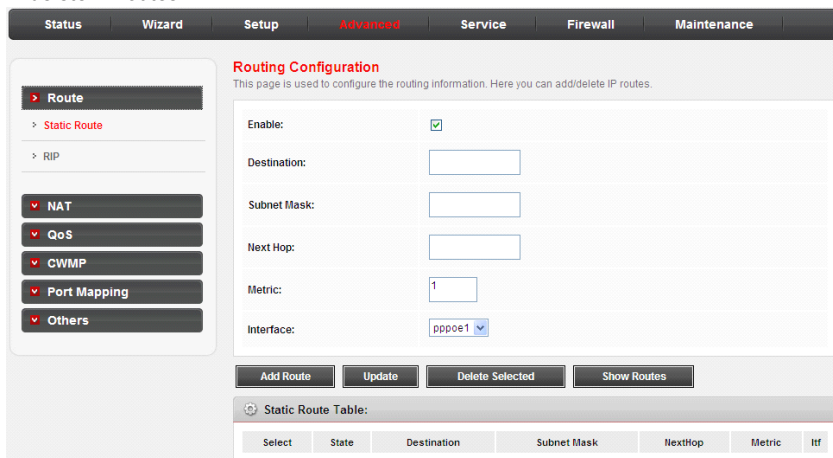
In the navigation bar, click **Advanced**. The tab **Advanced** contains **Route**, **NAT**, **QoS**, **CWMP**, **Port Mapping** and **Others**.

### 3.5.1 Route

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

#### 3.5.1.1 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.



The screenshot shows the 'Routing Configuration' page. At the top is a navigation bar with tabs: Status, Wizard, Setup, Advanced (selected), Service, Firewall, and Maintenance. On the left is a sidebar with a tree view containing 'Route' (expanded), 'Static Route' (selected), and 'RIP'. Below these are buttons for NAT, QoS, CWMP, Port Mapping, and Others. The main area is titled 'Routing Configuration' and contains a description: 'This page is used to configure the routing information. Here you can add/delete IP routes.' Below this is a form with the following fields: 'Enable' (checked), 'Destination' (text box), 'Subnet Mask' (text box), 'Next Hop' (text box), 'Metric' (text box with value 1), and 'Interface' (dropdown menu showing 'pppoe1'). At the bottom of the form are four buttons: 'Add Route', 'Update', 'Delete Selected', and 'Show Routes'. Below the buttons is a table titled 'Static Route Table:' with columns: Select, State, Destination, Subnet Mask, NextHop, Metric, and If.

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

Field	Description
Enable	Select it to use static IP routes.



Field	Description
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 <b>Static Route Table</b> .
Update	Select a row in the <b>Static Route Table</b> and modify the parameters. Then click it to save the settings temporarily.
Delete Selected	Select a row in the <b>Static Route Table</b> and click it to delete the row.
Show Routes	Click it, the <b>IP Route Table</b> 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

### 3.5.1.2 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Route

Static Route

RIP

NAT

QoS

CWMP

Port Mapping

Others

### RIP Configuration

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

RIP: ☒ Off ☐ On Apply

Interface: LAN

Recv Version: RIP1

Send Version: RIP1

Add Delete

**Rip Config List:**

Select	Interface	Recv Version	Send Version
--------	-----------	--------------	--------------

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

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

Field	Description
	RIP2 messages only.
Add	Click it to add the RIP interface to the <b>Rip Configuration List</b> .
Delete	Select a row in the <b>Rip Configuration List</b> and click it to delete the row.

## 3.5.2 NAT

### 3.5.2.1 DMZ

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 **NAT>DMZ** in the left pane, the page shown in the following figure appears. The following describes how to configure manual DMZ.

**Step 1** Select **WAN Interface**.

**Step 4** Enter an IP address of the DMZ host.

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

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

DMZ

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

WAN Interface:

pppoe1

DMZ Host IP Address:

Apply Changes

Reset

Current DMZ Table:

Select	WAN Interface	DMZ Ip
<input checked="" type="checkbox"/>	pppoe1	192.168.1.20

Delete Selected

### 3.5.2.2 Virtual Server

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

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

### Virtual Server

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

Service Type:

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

Protocol: TCP

WAN Setting: Interface

WAN Interface: pppoe1

WAN Port: 113 (ex. 5001:5010)

LAN Open Port: 113

LAN Ip Address:

Apply Changes

Current Virtual Server Forwarding Table:

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

The following table describes the parameters of this page.

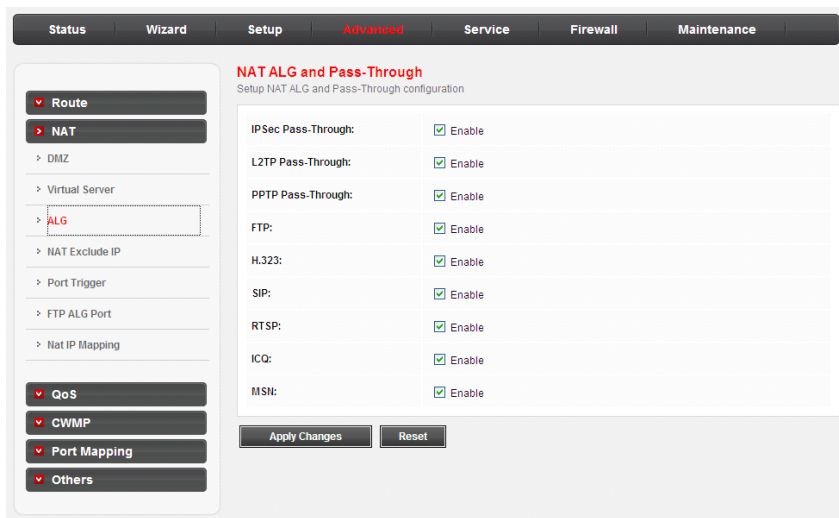
Field	Description
Service Type	<p>You can select the common service type, for example, <b>AUTH</b>, <b>DNS</b>, <b>FTP</b> or <b>POP3</b>. You can also define a service name.</p> <ul style="list-style-type: none"> <li>If you select <b>Usual Service Name</b>, the corresponding parameter has the default settings.</li> <li>If you select <b>User-defined Service Name</b>, you need to enter the corresponding parameters.</li> </ul>
Protocol	Choose the transport layer protocol that the service type uses. You can choose <b>TCP</b> or <b>UDP</b> .
WAN Setting	You can choose <b>Interface</b> or <b>IP Address</b> .
WAN Interface	Choose the WAN interface that will apply virtual server.

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

### 3.5.2.3 ALG

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

Choose the NAT ALG and Pass-Through options, and then click **Apply Changes**.



The screenshot shows the 'Advanced' configuration page for 'NAT ALG and Pass-Through'. The left sidebar contains a tree view with 'Route' expanded, and 'NAT' selected. Under 'NAT', 'ALG' is highlighted. The main area shows the configuration for 'Setup NAT ALG and Pass-Through configuration'. It includes a list of services with checkboxes to enable or disable them. All services are currently enabled.

Service	Status
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

At the bottom of the configuration area, there are two buttons: 'Apply Changes' and 'Reset'.

### 3.5.2.4 NAT Exclude IP

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

In the page, you can configure some source IP addresses which use the purge route mode when accessing internet through the specified interface.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

▼ Route

▼ NAT

> DMZ

> Virtual Server

> ALG

> NAT Exclude IP

> Port Trigger

> FTP ALG Port

> Nat IP Mapping

▼ QoS

▼ CWMP

▼ Port Mapping

▼ Others

NAT EXCLUDE IP

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

Interface:

ppoe1

IP Range:

---

Apply Changes

Reset

Current NAT Exclude IP Table:

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

### 3.5.2.5 Port Trigger

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

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

### Nat Port Trigger

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

Nat Port Trigger: ☐ Enable ☒ Disable

Apply Changes

Application Type:

☒ Usual Application Name:

☐ User-defined Application Name:

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

Apply Changes

Click the **Usual Application Name** drop-down menu to choose the application you want to setup for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

If the application you want to setup isn't listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port**, **Open Protocol** and **Nat type** settings for the port trigger you want to configure.

When you have finished click the **Apply changes** button.



### 3.5.2.6 FTP ALG PORT

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

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

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

#### FTP ALG Configuration

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

FTP ALG port:

Add Dest Ports

Delete Selected DestPort

FTP ALG ports Table:

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

### 3.5.2.7 Nat IP Mapping

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

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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Port Mapping

Others

### 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: One-to-One

Local Start IP:

Local End IP:

Global Start IP:

Global End IP:

Apply Changes

Reset

Current NAT IP MAPPING Table:

Local Start IP	Local End IP	Global Start IP	Global End IP	Action
<div> <div>Delete Selected</div> <div>Delete All</div> </div>				

### 3.5.3 QoS

Choose **Advanced > 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

▼ Route

▼ NAT

▶ QoS

> QoS

▼ CWMP

▼ Port Mapping

▼ Others

### IP QoS

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

IP QoS:

☐ disable
 ☒ enable

Apply

QoS Policy:

stream based ▼

Schedule Mode:

strict prior ▼

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

**Step 6** Click **add rule** to add a new IP QoS rule.

The page shown in the following figure appears.

IP QoS:

☐ disable ☒ enable

Apply

QoS Policy:

stream based ▼

Schedule Mode:

strict prior ▼

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 int	sel	

Add rule

Delete

Delete all

Add QoS Rule

Src IP:

Src Mask:

Dest IP:

Dest Mask:

Src Port:

Dest Port:

Protocol:

 ▼

Phy Port:

 ▼

set priority:

p3(Lowest) ▼

☐ 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 <b>stream based</b> , <b>802.1p based</b> or <b>DSCP based</b> .
Schedule Mode	You can choose <b>strict prior</b> or <b>WFQ (4:3:2:1)</b> .
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 <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> or <b>TCP/UDP</b> .
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.
802.1p	You can choose from 0 to 7.
delete	Select a row in the <b>QoS Rule list</b> and click it to delete the row.
delete all	Select all the rows in the <b>QoS Rule list</b> and click it to delete the rows.

### 3.5.4 CWMP

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

**ACS:**

Enable:



URL:

User Name:

Password:

Periodic Inform Enable:



Disable



Enable

Periodic Inform Interval:

seconds

**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

Apply Changes

Reset

**Certificate Management:**

CPE Certificate Password:

Apply

Undo

CPE Certificate:





CA Certificate:

The following table describes the parameters of this page:

Field	Description
<b>ACS</b>	
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 <b>Enable</b> to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
<b>Connection Request</b>	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
<b>Debug</b>	
Show Message	Select <b>Enable</b> to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select <b>Enable</b> , 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.

### 3.5.5 Port Mapping

Choose **Advanced > Port Mapping**, the page shown in the following page appears.

## Port Mapping Configuration

To manipulate a mapping group:

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

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

☐ Disable ☒ Enable

WAN

ppoe1

Add>

<Del

LAN

LAN3  
LAN4  
wlan  
wlan-vap0  
wlan-vap1  
wlan-vap2  
wlan-vap3

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3,ppoe1	Enabled
<input checked="" type="radio"/> Group1		--
<input type="radio"/> Group2		--
<input type="radio"/> Group3		--
<input type="radio"/> Group4		--

Apply

Create four rules through Group1 to Group4. The procedure is as follows:

**Step 1** Select **Enable** to enable port mapping.



**Step 7** Select Group1. Then the interfaces are added in the WAN and LAN table.

The following page appears.

**Step 8** Select the interfaces that are respectively added to WAN and LAN.

Press **Ctrl** while selecting multiple interfaces.

**Step 9** Click **Add** to add the interface to the rule.

The following page appears.

## Port Mapping Configuration

To manipulate a mapping group:

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

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

☐ Disable
☒ Enable

**WAN**

pppoe1

**LAN**

LAN3  
LAN4  
wlan  
wlan-vap0  
wlan-vap1  
wlan-vap2  
wlan-vap3

↑

↓

Add>

<Del

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

Apply

**Step 10** Click **Apply** to apply the settings, and the following page appears.

## Port Mapping Configuration

To manipulate a mapping group:

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

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

☐ Disable ☒ Enable

WAN

LAN

LAN2  
 LAN3  
 LAN4  
 wlan  
 wlan-vap0  
 wlan-vap1  
 wlan-vap2

Add>

<Del

LAN1  
pppoe1

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

Apply

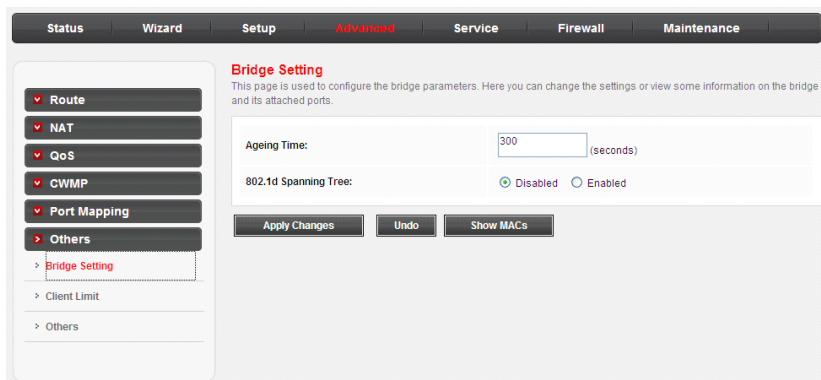
In this example, only interfaces of pppoe1 and LAN1 can communicate with each other. That is, only LAN1 can access the Internet through pppoe1 interface.

## 3.5.6 Others

Choose **Advanced > Others**. The page that is displayed contains **Bridge Setting, Client Limit, Tunnel** and **Others**.

### 3.5.6.1 Bridge Setting

Choose **Bridge Setting** in the left pane, 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. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, **Advanced**, Service, Firewall, and Maintenance. On the left, a sidebar contains a list of menu items: Route, NAT, QoS, CWMP, Port Mapping, **Others**, Bridge Setting (highlighted), Client Limit, and Others. The main content area is titled 'Bridge Setting' and includes a sub-header: 'This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.' Below this, there are two configuration fields: 'Ageing Time' with a text input set to '300' and '(seconds)' next to it, and '802.1d Spanning Tree' with radio buttons for 'Disabled' (selected) and 'Enabled'. At the bottom of the configuration area, there are three buttons: 'Apply Changes', 'Undo', and 'Show MACs'.

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

Field	Description
Ageing Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
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
00:05:1c:03:04:05	0	Static	300
01:00:5e:00:00:09	0	Static	300
54:04:a6:97:37:69	1(3)	Dynamic	300
靜態表項	0	Static	300

refresh close

### 3.5.6.2 Client Limit

Choose **Client Limit** in the left pane, the page shown in the following figure appears. This page is used to configure the capability of forcing how many devices can access to the Internet.

Status Wizard Setup **Advanced** Service Firewall Maintenance

✓ Route  
 ✓ NAT  
 ✓ QoS  
 ✓ CWMP  
 ✓ Port Mapping  
 > Others  
 > Bridge Setting  
 > **Client Limit**  
 > Others

#### Client Limit Configuration

This page is used to configure the capability of force how many device can access to Internet!

Client Limit Capability: ☒ Disable ☐ Enable

Apply Changes

### 3.5.6.3 Others

Choose **Others** in the left pane, the page shown in the following figure appears.

Status
 Wizard
 Setup
 **Advanced**
 Service
 Firewall
 Maintenance

▼ Route
 ▼ NAT
 ▼ QoS
 ▼ CWMP
 ▼ Port Mapping
 ▼ **Others**
 > Bridge Setting
 > Client Limit
 > **Others**

### 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:

Apply Changes
 Undo

## 3.6 Service

In the navigation bar, click **Service**. The tab **Service** contains **IGMP**, **UPnP**, **SNMP**, **DNS** and **DDNS**.

### 3.6.1 IGMP

Choose **Service** > **IGMP**, and the following page appears. The page that is displayed contains **IGMP Proxy**.

#### 3.6.1.1 IGMP Proxy

Click **IGMP Proxy** in the left pane, the page shown in the following figure appears. In this page, you can enable or disable IGMP proxy. If you disable IGMP proxy, the modem will discard all the received multicast data packets.

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
--------	--------	-------	----------	---------	----------	-------------

IGMP

IGMP Proxy

UPnP

SNMP

DNS

DDNS

FTP Server

### 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)

Apply Changes

Undo

### 3.6.2 UPnP

Click **UPnP** in the left pane, the page shown in the following figure appears. The system acts as a daemon after you enable UPnP.

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
--------	--------	-------	----------	---------	----------	-------------

IGMP

UPnP

SNMP

DNS

DDNS

FTP Server

### UPnP Configuration

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

UPnP:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
WAN Interface:	<input type="text" value="pppoe1"/>

Apply Changes

### 3.6.3 SNMP

Click **SNMP** in the left pane, the page shown in the following figure appears. You can configure the SNMP parameters.

Status
 Wizard
 Setup
 Advanced
 **Service**
 Firewall
 Maintenance

▼ IGMP
 ▼ UPnP
 > **SNMP**
 > SNMP
 ▼ DNS
 ▼ DDNS
 ▼ FTP Server

#### SNMP Protocol Configuration

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

☒ Enable SNMP

System Description

ADSL SoHo Router

System Contact

System Name

ADSL

System Location

Trap IP Address

0.0.0.0

Community name (read-only)

public

Community name (read-write)

public

Apply Changes

Reset

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.



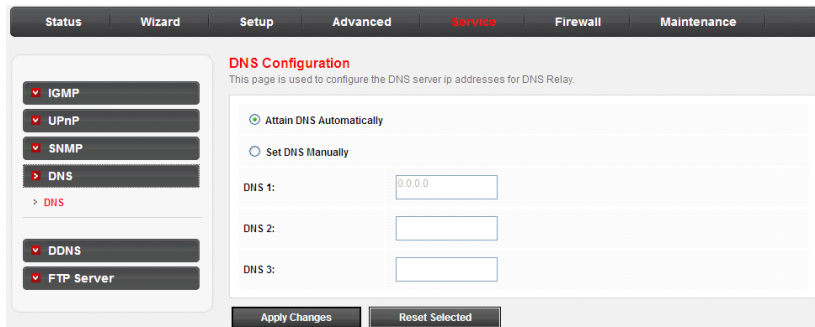
### 3.6.4 DNS

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**.

#### 3.6.4.1 DNS

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



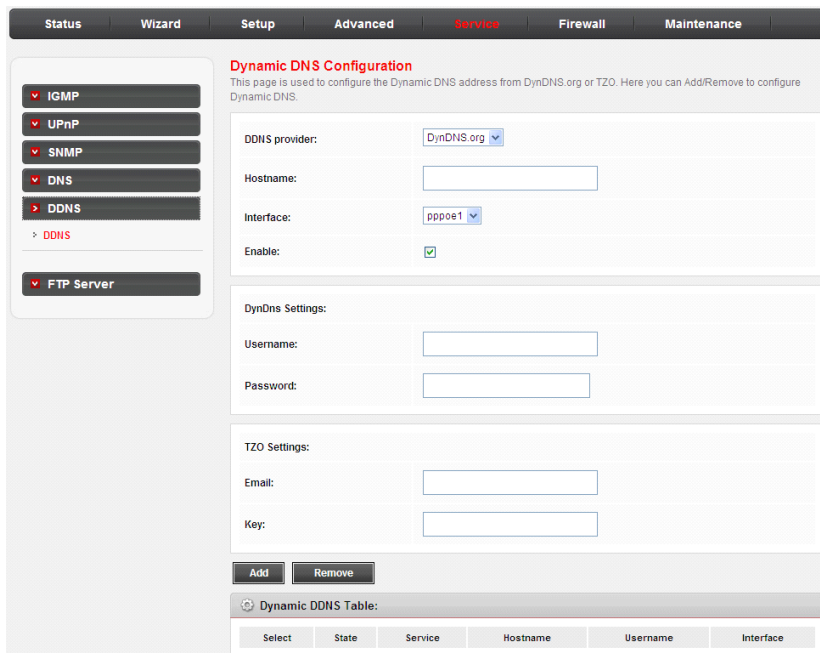
The following table describes the parameters and buttons of this page.

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

Field	Description
Reset Selected	Click it to start configuring the parameters in this page.

### 3.6.5 DDNS

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



The screenshot shows the 'Dynamic DNS Configuration' page. On the left is a sidebar with navigation options: IGMP, UPnP, SNMP, DNS, DDNS (selected), and FTP Server. The main content area has a top navigation bar with tabs: Status, Wizard, Setup, Advanced, Service (active), Firewall, and Maintenance. Below the tabs, the page title is 'Dynamic DNS Configuration' with a subtitle: 'This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.' The configuration section includes:
 

- DDNS provider:** A dropdown menu set to 'DynDNS.org'.
- Hostname:** An empty text input field.
- Interface:** A dropdown menu set to 'pppoe1'.
- Enable:** A checked checkbox.
- DynDns Settings:**
  - Username:** An empty text input field.
  - Password:** An empty text input field.
- TZO Settings:**
  - Email:** An empty text input field.
  - Key:** An empty text input field.

 At the bottom of the configuration section are 'Add' and 'Remove' buttons. Below these is a section titled 'Dynamic DDNS Table:' containing a table with columns: Select, State, Service, Hostname, Username, and Interface.

The following table describes the parameters of this page.

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose <b>DynDNS.org</b> or <b>TZO</b> .

Field	Description
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.
Key	The key provided by DDNS provider.

### 3.6.6 FTP Server

Choose **Service > FTP Server**, the page shown in the following figure appears. This page is used to start the FTP Server.



## 3.7 Firewall

### 3.7.1 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

MAC Filter

MAC Filter

IP/Port Filter

URL Filter

ACL

DoS

### MAC Filtering

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

Outgoing Default Policy

☐ Deny
 ☒ Allow

Incoming Default Policy

☐ Deny
 ☒ Allow

Apply

Direction:

Outgoing

Action:

☒ Deny
 ☐ Allow

Source MAC:

(ex. 00E086710502)

Destination MAC:

(ex. 00E086710502)

Add

Current MAC Filter Table:

Select	Direction	Source MAC	Destination MAC	Action
--------	-----------	------------	-----------------	--------

Delete

Delete All

## 3.7.2 IP/Port Filter

Choose **Firewall > IP/Port Filter**, the page shown in the following figure appears. The page that is displayed contains **IP/Port Filter**.

### 3.7.2.1 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

MAC Filter

IP/Port Filter

IP/Port Filter

URL Filter

ACL

DoS

### IP/Port Filtering

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

Outgoing Default Policy

☒ Permit
 ☐ Deny

Incoming Default Policy

☐ Permit
 ☒ Deny

Rule Action:

☒ Permit
 ☐ Deny

WAN Interface:

pppoe1

Protocol:

IP

Direction:

Upstream

Source IP Address:

Mask Address:

255.255.255.255

Dest IP Address:

Mask Address:

255.255.255.255

SPort:

-

DPort:

-

Enable:

☒

Apply Changes

Reset

Help

Current Filter Table:

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

### 3.7.3 URL Filter

Choose **Firewall > URL Filter**, the page shown in the following figure appears. This page is used to configure the filtered keyword. Here you can add/delete filtered keyword

Status
 Wizard
 Setup
 Advanced
 Service
 Firewall
 Maintenance

▼ MAC Filter
 ▼ IP/Port Filter
 ▼ URL Filter
 > URL Filter
 ▼ ACL
 ▼ DoS

### 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
<input type="radio"/>	123456

## 3.7.4 ACL

Choose **Firewall** > **ACL**, the page shown in the following figure appears. The page that is displayed contains **ACL**.

### 3.7.4.1 ACL

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



#### Note:

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

## 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.

LAN ACL Mode:	<input checked="" type="radio"/> White List	<input type="radio"/> Black List
WAN ACL Mode:	<input checked="" type="radio"/> White List	<input type="radio"/> Black List
<input type="button" value="Apply"/>		

Direction Select:	<input checked="" type="radio"/> LAN <input type="radio"/> WAN
-------------------	--

LAN ACL Switch:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

IP Address:	<input type="text"/> - <input type="text"/> (The IP 0.0.0.0 represent any IP )
Services Allowed:	
<input type="checkbox"/> any	
<input type="checkbox"/> web	
<input type="checkbox"/> telnet	
<input type="checkbox"/> ssh	
<input type="checkbox"/> ftp	
<input type="checkbox"/> tftp	
<input type="checkbox"/> snmp	
<input type="checkbox"/> ping	

<input type="button" value="Add"/>	<input type="button" value="Reset"/>
------------------------------------	--------------------------------------

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

Field	Description
Direction Select	Select the router interface. You can select <b>LAN</b> or <b>WAN</b> . In this example, <b>LAN</b> 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 access the router.
Services Allowed	You can choose the following services from LAN: <b>Web, Telnet, FTP, TFTP, SNMP</b> or <b>PING</b> . You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the <b>Current ACL Table</b> .
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.

LAN ACL Mode:	<input checked="" type="radio"/> White List	<input type="radio"/> Black List
WAN ACL Mode:	<input checked="" type="radio"/> White List	<input type="radio"/> Black List
<input type="button" value="Apply"/>		

Direction Select: ☐ LAN ☒ WAN

WAN Setting:

WAN Interface:

Services Allowed:

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

### 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 <b>LAN</b> or <b>WAN</b> . In this example, <b>WAN</b> is selected.
WAN Setting	You can choose <b>Interface</b> or <b>IP Address</b> .
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: <b>Web, Telnet, FTP, TFTP, SNMP</b> , or <b>PING</b> . You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the <b>Current ACL Table</b> .
Reset	Click it to refresh this page.

### 3.7.5 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. Choose **Firewall > DoS**, the page shown in the following figure appears. In this page, you can prevent DoS attacks.

## 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

☐ V/whole System Flood: SYN  Packets/Second

☐ V/whole System Flood: FIN  Packets/Second

☐ V/whole System Flood: UDP  Packets/Second

☐ V/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 SynVWithData

☐ UDP Bomb

☐ UDP EchoChargen

Select ALL

Clear ALL

☐ Enable Source IP Blocking  Block time (sec)

Apply Changes

## 3.8 Maintenance

In the navigation bar, click **Maintenance**. The **Maintenance** page that is displayed contains **Update**, **Password**, **Reboot**, **Time**, **Log** and **Diagnostics**.

### 3.8.1 Update

Choose **Maintenance > Update**. The **Update** page that is displayed contains **Firmware Update** and **Backup/Restore**.

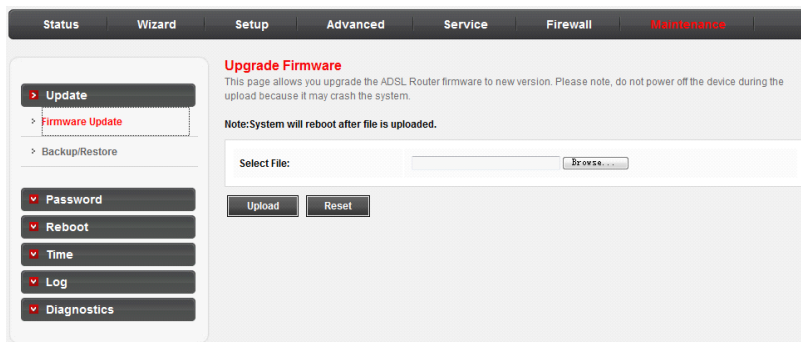


**Caution:**

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

#### 3.8.1.1 Firmware Update

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.

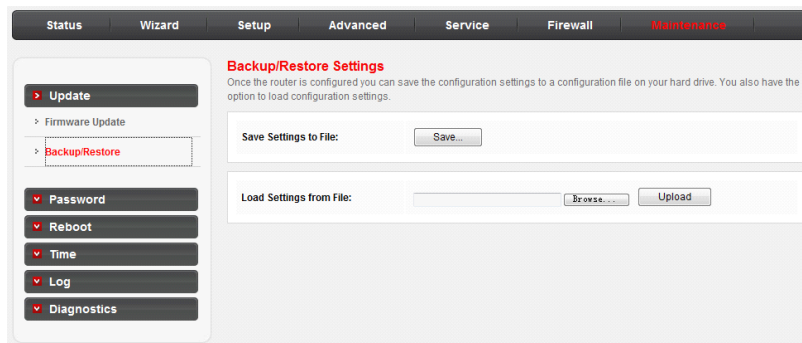


The following table describes the parameters and button of this page.

Field	Description
Select File	Click <b>Browse</b> to select the firmware file.
Upload	After selecting the firmware file, click <b>Upload</b> to starting upgrading the firmware file.
Reset	Click it to starting selecting the firmware file.

### 3.8.1.2 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 screenshot shows the 'Maintenance' tab selected in the top navigation bar. On the left sidebar, 'Update' is expanded, and 'Backup/Restore' is selected. The main content area is titled 'Backup/Restore Settings' and contains the following text: 'Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.'

Below the text, there are two sections:

- Save Settings to File:** Includes a 'Save...' button.
- Load Settings from File:** Includes a text input field, a 'Browse...' button, and an 'Upload' button.

The left sidebar also shows other options: Password, Reboot, Time, Log, and Diagnostics.

### 3.8.2 Password

Choose **Maintenance > 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.

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Update

Password

Password

Reboot

Time

Log

Diagnostics

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:

User

Old Password:

New Password:

Confirm Password:

Add

Modify

Delete

Reset

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 <b>admin</b> or <b>user</b> .
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.

### 3.8.3 Reboot

Choose **Maintenance > 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.

Status
 Wizard
 Setup
 Advanced
 Service
 Firewall
 Maintenance

Update
 Password
 Reboot
 > Reboot
 Time
 Log
 Diagnostics

### Commit/Reboot

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

Reboot from:
 

Save Current Configuration

Commit Changes
 Reset
 Reboot

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

Field	Description
Reboot from	<p>You can choose <b>Save Current Configuration</b> or <b>Factory Default Configuration</b>. Click <b>Reboot</b> to reboot the router.</p> <ul style="list-style-type: none"> <li>● <b>Save Current Configuration:</b> Save the current settings, and then reboot the router.</li> <li>● <b>Factory Default Configuration:</b> Reset to the factory default settings, and then reboot the the router.</li> </ul>

### 3.8.4 Time

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

Status

Wizard

Setup

Advanced

Service

Firewall

Maintenance

Update

Password

Reboot

Time

Log

Diagnostics

### System Time Configuration

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

System Time:

2012

Year

Jan

Month

1

Day

1

Hour

30

min

45

sec

DayLight:

LocalTIME

Apply Changes

Reset

#### NTP Configuration:

State:

☒ Disable
 ☐ Enable

Server:

Server2:

Interval:

Every

1

hours

Time Zone:

(GMT) Gambia, Liberia, Morocco, England

GMT time:

Sun Jan 1 1:30:45 2012

Apply Changes

Reset

NTP Start:

Get GMT Time

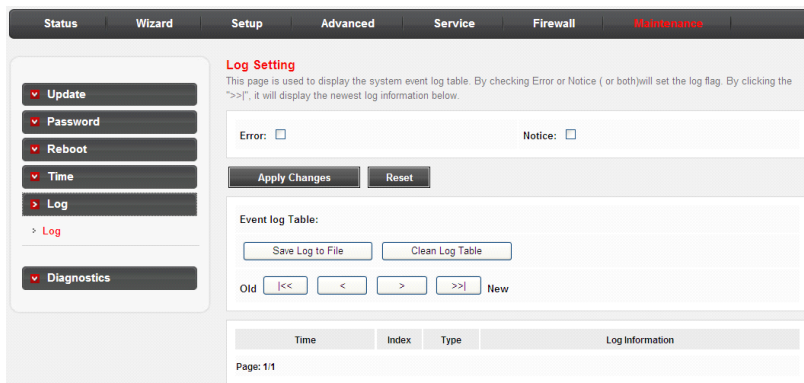
The following table describes the parameters of this page.

Field	Description
System Time	Set the system time manually.
<b>NTP Configuration</b>	
State	Select enable or disable NTP function. You need to enable NTP if you want to configure the parameters of NTP.
Server	Set the primary NTP server manually.
Server2	Set the secondary NTP server manually.
Time Zone	Choose the time zone in which area you are from the drop down list.



### 3.8.5 Log

Choose **Maintenance > 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.



The screenshot shows the 'Log Setting' page. At the top is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). On the left is a sidebar with a tree view containing: Update, Password, Reboot, Time, Log (highlighted in red), and Diagnostics. The main content area is titled 'Log Setting' and includes a description: 'This page is used to display the system event log table. By checking Error or Notice ( or both) will set the log flag. By clicking the ">>|", it will display the newest log information below.' Below this are checkboxes for 'Error:' and 'Notice:'. There are 'Apply Changes' and 'Reset' buttons. An 'Event log Table:' section contains 'Save Log to File' and 'Clean Log Table' buttons. Navigation buttons for the log table include '<<|', '<', '>', '>>|', and 'New'. At the bottom, there is a table header with columns: Time, Index, Type, and Log Information. The page number 'Page: 1/1' is displayed at the bottom left.

### 3.8.6 Diagnostics

Choose **Maintenance > Diagnostics**, the page shown in the following page appears. The page that is displayed contains **Ping, Tracert, OAM Loopback, ADSL Diagnostic** and **Diag-test**. Select the option that you want to run diagnostics.

[Status](#) | [Wizard](#) | [Setup](#) | [Advanced](#) | [Service](#) | [Firewall](#) | [Maintenance](#)

▼ Update

▼ Password

▼ Reboot

▼ Time

▼ Log

▼ Diagnostics

> Ping

> Traceroute

> OAM Loopback

> ADSL Diagnostic

> Diag-Test

### Ping Diagnostic

Host :

PING

## 4 Q&A

Question	Answer
Why are all the indicators off?	<ul style="list-style-type: none"> <li>● Check the connection between the power adapter and the power socket.</li> <li>● Check whether the power switch is turned on.</li> </ul>
Why is the <b>LAN</b> indicator not on?	Check the following: <ul style="list-style-type: none"> <li>● The connection between the device and the PC, the hub, or the switch.</li> <li>● The running status of the computer, hub, or switch.</li> </ul>
Why is the <b>DSL</b> indicator not on?	Check the connection between the <b>DSL</b> interface of the device and the socket.
Why does the Internet access fail when the <b>DSL</b> indicator is on?	Ensure that the following information is entered correctly: <ul style="list-style-type: none"> <li>● VPI and VCI</li> <li>● User name and password</li> </ul>
Why does the web configuration page of the device fail to be accessed?	Choose <b>Start &gt; Run</b> from the desktop. Enter <b>Ping 192.168.1.1</b> (the default IP address of the device) in the DOS window.  If the web configuration page still cannot be accessed, check the following configuration: <ul style="list-style-type: none"> <li>● The type of the network cable</li> <li>● The connection between the device and the computer</li> <li>● The TCP/IP properties of the network card of the computer</li> </ul>
How to restore the default configuration after incorrect configuration?	Keep the device powered on and press the <b>Reset</b> button for 3 seconds. Then, the device automatically reboots and is restored to the factory default configuration.  The default configurations of the device are as follows: <ul style="list-style-type: none"> <li>● IP address: 192.168.1.1</li> </ul>

Question	Answer
	<ul style="list-style-type: none"><li>● Subnet mask: 255.255.255.0.</li><li>● The user name and password of super user are <b>admin</b> and <b>admin</b> respectively.</li><li>● The user name and password of common user are <b>user</b> and <b>user</b> respectively.</li></ul>