

SW300

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.....	3
2 Hardware Installation.....	5
3 Web Configuration.....	8
3.1 Accessing the Router.....	8
3.2 Status.....	10
3.2.1 Device Info.....	10
3.2.2 Statistics.....	13
3.3 Wizard.....	13
3.4 Setup.....	15
3.4.1 WAN Configuration.....	16
3.4.2 LAN Configuration.....	22
3.5 Advanced.....	32
3.5.1 Route.....	32
3.5.2 NAT.....	37
3.5.3 QoS.....	45
3.5.4 CWMP.....	48
3.5.5 Others.....	51
3.6 Service.....	56
3.6.1 IGMP.....	57
3.6.2 UPnP.....	59
3.6.3 SNMP.....	60
3.6.4 DNS.....	61
3.6.5 DDNS.....	63
3.6.6 FTP Server.....	64
3.7 Firewall.....	64
3.7.1 MAC Filter.....	65
3.7.2 IP/Port Filter.....	65
3.7.3 URL Filter.....	67

3.7.4 ACL.....	68
3.7.5 DoS.....	73
3.8 Maintenance.....	74
3.8.1 Update.....	75
3.8.2 Password.....	77
3.8.3 Reboot.....	78
3.8.4 Time.....	79
3.8.5 Log.....	80
3.8.6 Diagnostics.....	80
4 Trouble Shooting.....	88

1 Introduction

The SW300 is an ADSL access device that supports multiple line modes. It provides one 10/100Base-T Ethernet interface at the user end. The device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. The device provides high performance access to the Internet, downlink up to 24 Mbps and uplink up to 1 Mbps.

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 exits 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

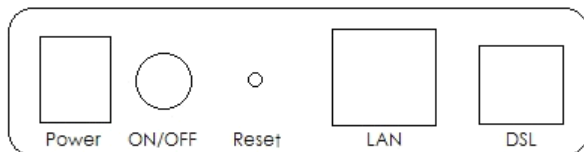
Front Panel



The following table describes the LEDs of the device:

LEDs	Status	Description
Power 	On	The device is powered on
	Off	The device is powered off
LAN 	On	There is a successful connection on the corresponding LAN port
	Off	There is no connection on the corresponding LAN port
	Blinking	Data is being transferred over the corresponding LAN port
DSL 	On	DSL link up/link synchronized
	Blinking	DSL link training/DSL link not synchronized
Internet 	On	Successful PPP session
	Off	Before DSL link up
	Blinking	There is data being transmitted or received

Rear Panel



The following table describes the interfaces of the device:

Items	Description
ON/OFF	Power switch for powering on/ off the device.
Power	Power interface for connecting to the power adapter.
LAN	RJ-45 interface for connecting to the Ethernet interface of PC or other Ethernet devices through the Ethernet cable.
DSL	RJ-11 interface for connecting to the ADSL interface or a splitter through the telephone cable.
Reset	Reset to the factory defaults. To reset to the factory defaults, you should keep the device powered on, push a needle into the hole and then press and hold more than 3 seconds.

1.3 System Requirements

Recommended system requirements are as follows.

- A 10/100 base-T Ethernet card installed in your PC
- A hub or Switch (connected to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows 98 SE, Windows 2000, Windows ME, Windows XP, Windows 7 or higher
- 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
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483Bridged/1483Routed/MER/IPoA access
- Multiple PVCs (up to eight) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- 802.1Q and 802.1P protocol
- DHCP server
- NAT
- Static route
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- DNS
- Virtual server
- DMZ
- Two-level passwords and usernames
- Web interface
- Telnet CLI
- System status display
- PPP session PAP/CHAP
- IP filter
- IP quality of service (QoS)
- Remote access control
- Line connection status test
- Remote managing through Telnet or HTTP
- Backup and restoration of configuration file
- Ethernet interface supporting crossover detection, auto-correction, and polarity correction
- Universal plug and play (UPnP)

2 Hardware Installation

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

The splitter has three interfaces:

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

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



Note:

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

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

Connection 1

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

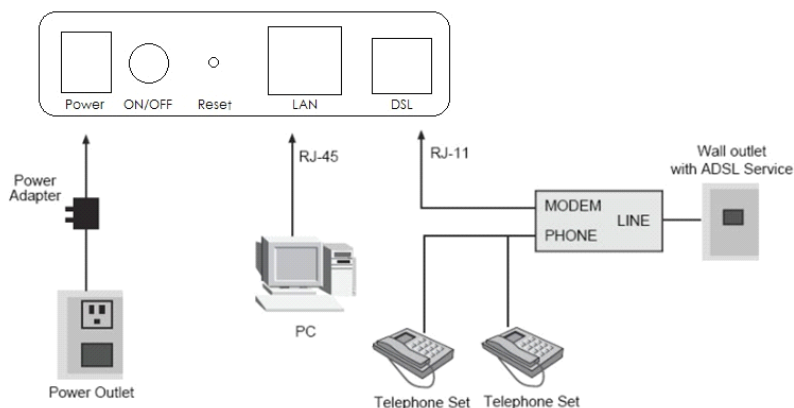


Figure 1 Connection diagram (Without connecting telephone sets before the splitter)

Connection 2

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

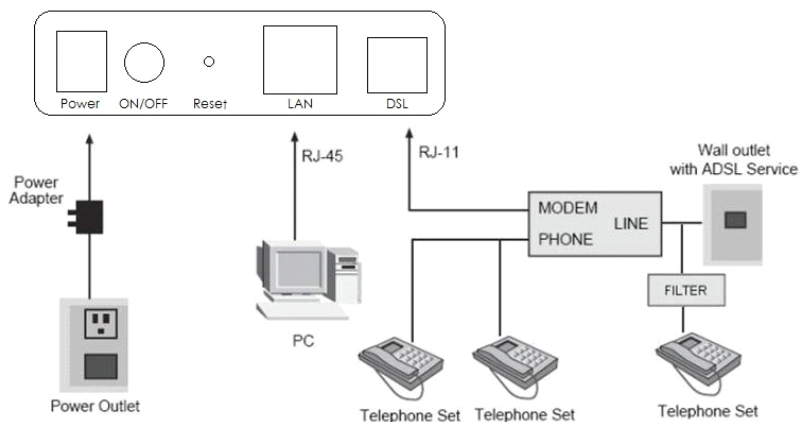


Figure 2 Connection diagram (Connecting a telephone set before the splitter)

**Note:**

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

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

3 Web Configuration

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

3.1 Accessing the Router

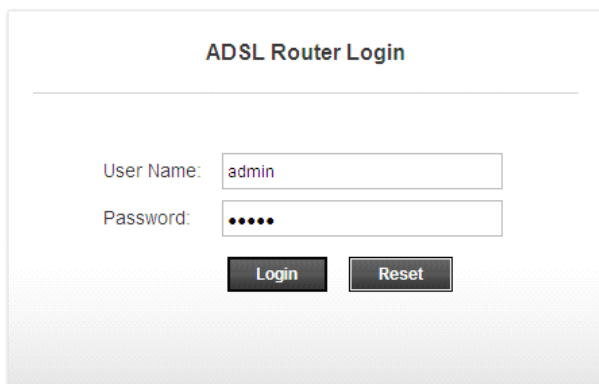
The following is the detailed description of accessing the router for the first time.

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

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

- 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, the page is shown as the following figure appears. You can view the status of your router.

Status

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	RTL897x ADSL Modem
Uptime	0 2:23:49
Date/Time	Sun Jan 1 2:23:49 2012
Firmware Version	E9_CT166A-1-TW-R9B010.EN
Built Date	Oct 24 2012 13:57:02
Serial Number	00051D030405

DSL

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

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IPv6 Address	fe80::205:1dff:fe03:405
DHCP Server	Enable
MAC Address	00:05:1D:03:04:05

DNS Status

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

WAN Configuration

Interface	VPI/VCI	Encap	Droute	Protocol	IP Address	Gateway	Status
a0	8/35	LLC	Off	br1483	0.0.0.0	0.0.0.0	down

WAN IPv6 Configuration

Interface	VPI/VCI	Encap	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status
a0	8/35	LLC	br1483					down

Refresh



Note:

In the Web configuration page, you can click **Apply Changes** to save the settings temporarily. If you want to save the settings of this page permanently,

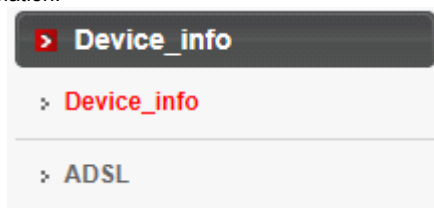
click **Save** of **Attention** that appears at the bottom of the left pane after the configuration. Click **Undo** to reverse an action.

3.2 Status

In the navigation bar, click **Status**. The **Status** page contains **Device-info** and **Statistics**.

3.2.1 Device Info

Choose **Status > Device_info**, the sub-menu of the **Device_info** appears on the left pane as follow. It contains **Device_info** and **ADSL**. Click each item to view the related information.



3.2.1.1 Device_info

Choose **Status > Device_info**, the page is shown as the following figure appears. In this page you can view the current information and some basic settings of the **System, DSL, LAN Configuration, DNS Status, WAN Configuration and WAN IPV6 Configuration**.

Status

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	RTL897x ADSL Modem
Uptime	0 2:23:49
Date/Time	Sun Jan 1 2:23:49 2012
Firmware Version	E9_CT166A-1-TW-R9B010.EN
Built Date	Oct 24 2012 13:57:02
Serial Number	00051D030405

DSL

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

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IPv6 Address	fe80::205:1dff:fe03:405
DHCP Server	Enable
MAC Address	00:05:1D:03:04:05

DNS Status

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

WAN Configuration

Interface	VPI/VCI	Encap	Droute	Protocol	IP Address	Gateway	Status
a0	8/35	LLC	Off	br1483	0.0.0.0	0.0.0.0	down

WAN IPv6 Configuration

Interface	VPI/VCI	Encap	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status
a0	8/35	LLC	br1483					down

Refresh

Click Refresh to refresh this page.

3.2.1.2 ADSL

Choose **Status > ADSL**, the page is shown as the following figure appears. In this page, you can view the ADSL line status, downstream rate, upstream rate and other information

Status

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	RETK
Firmware Version	4924c830
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:

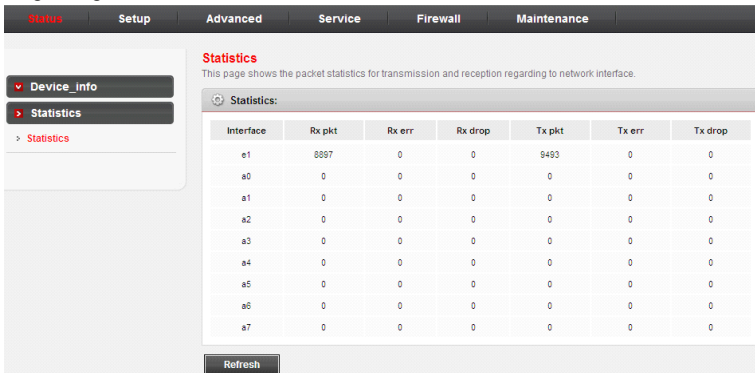
Retrain

Refresh

Click **Retrain**, the device interacts with the office end to reacquire the values and parameters of the router settings. If you want to refresh the page, click **Refresh**.

3.2.2 Statistics

Choose **Status > Statistics**, the page is shown as the following figure appears. In this page you can view the packet statistics for transmission and reception regarding to network interface.



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

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
e1	8897	0	0	9493	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

Refresh

Click Refresh to refresh this page.

3.3 Wizard

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

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

> Wizard
 > Wizard

Fast Config

The wizard will help you do some basic configurations step by step.
 Step 1: WAN Connection Setting
 Step 2: Save Setting

Step 1: WAN Connection Setting: Please select the wan connection mode

VPI/VCI: VPI: (0-255) VCI: (32-65535)

Encapsulation: ☒ LLC/SNAP ☐ VC-Mux
☐ 1483 Bridged
☐ 1483 MER

Connection Mode: ☒ PPP over Ethernet(PPPoE)
☐ PPP over ATM(PPPoA)
☐ 1483 Routed

PPP Settings: Username: Password:

Default Route: ☒ Enable ☐ Disable

DNS Settings: ☒ Attain DNS Automatically
☐ Set DNS Manually :

DNS Server 1:

DNS Server 2:

[next](#)

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.

VPI/VCI:	VPI: 8 (0-255)	VCI: 35 (32-65535)
----------	---	---

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

Connection Mode:	☐ 1483 Bridged
	☐ 1483 MER
	☒ PPP over Ethernet(PPPoE)
	☐ PPP over ATM(PPPoA)
	☐ 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.

PPP Settings:

Username:

Password:

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

Fast Config

Step 2: 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

Prev

Apply Changes

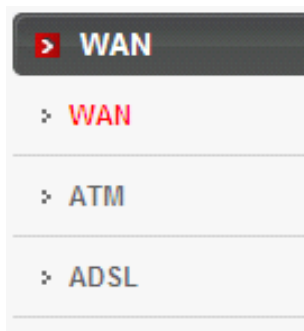
Cancel

3.4 Setup

In the navigation bar, click **Setup**. The **Setup** page contains **WAN** and **LAN** configuration.

3.4.1 WAN Configuration

In the **Setup** page, click **WAN** on the left pane, the sub-menu of the **WAN** appears as below.



3.4.1.1 WAN

Choose **Setup > WAN**, the page is show as the following figure appears. In this page you can set the channel configuration including channel operation modes, PPP settings and WAN IP settings.

Status

Setup

Advanced

Service

Firewall

Maintenance

WAN

WAN

ATM

ADSL

LAN

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:

0

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 Router:

☐ 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
☐	a0	br1483	8	35	LLC	Off	Off	Off	0.0.0.0	0.0.0.0	0.0.0.0	--	down	

The following table describes the parameters in this page:

Field	Description
Default Route Selection	You can select Auto or Specified .
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 8 .

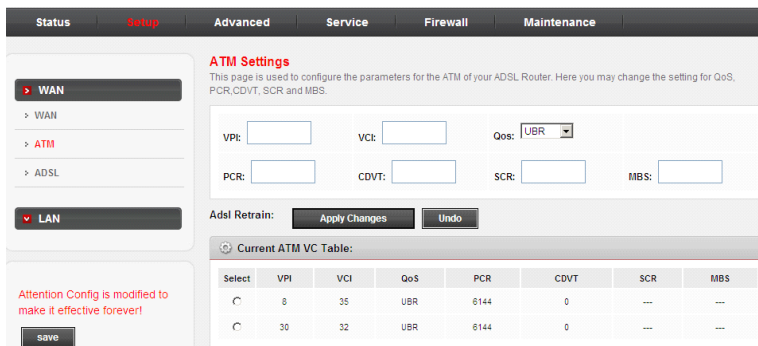
Field	Description
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. (0 to 31 is reserved for local management of ATM traffic) Enter the correct VCI provided by your ISP. By default, VCI is set to 35 .
Encapsulation	You can select LLC or VC-Mux . In this example, the encapsulation mode is set to LLC .
Channel Mode	You can choose 1483 Bridged, 1483 MER, PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), 1483 Routed, or IPoA .
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. NAPT is only effective in the channel mode of 1483 MER, PPPoE, PPPoA, 1483 Routed and IPoA . 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()	You can choose IPv4/IPv6, IPv4 and IPv6 . IP Protocol is only effective in the channel mode of 1483 MER, PPPoE, PPPoA, 1483 Routed and IPoA .
PPP Settings (Note: the parameters of PPP Settings are only available in the mode of PPPoE and PPPoA .)	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose Continuous, Connect on Demand or Manual .
Idle Time (min)	If set the type to Connect on Demand , you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the

Field	Description
	PPPoE connection.
WAN IP Settings (Note: WAN IP Settings is only available in the mode of 1483MER , 1483 ROUTED and IPOA .)	
Type	You can choose Fixed IP or DHCP . ● If select Fixed IP, you should enter the local IP address, remote IP address and subnet mask. ● If select DHCP, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the gateway IP address provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Unnumbered	Select this checkbox to enable IP unnumbered function. (Only effective in the mode of 1483 Routed .
Address Mode	You can choose Slaac or Static . Slaac :IPv6 Stateless address autoconfiguration Static :IPv6 static address configuration
Enable DHCPv6 Client	Here you can enable or disable IPv6 DHCP Client function.
Request Options	You can choose Request Address or Request Prefix .
Add	After configuring the parameters of this page, click it to add a new PVC into the Current ATM VC Table .
Modify	Select a PVC in the Current ATM VC Table , then modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
Current ATM VC Table	This table shows the existed PVCs. It shows the interface name, channel mode, VPI/VCI, encapsulation mode, local IP address, remote IP address and other information. The maximum item of this table is eight.

Field	Description
	Click it to modify the PVCs' parameters.

3.4.1.2 ATM

Choose **Setup > WAN > ATM**, the page is shown as the following figure appears. In this page you can set the parameters for 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
☐	8	35	UBR	6144	0	---	---
☐	30	32	UBR	6144	0	---	---

Attention Config is modified to make it effective forever!

The following table describes the parameters of this page:

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose UBR , CBR , nrt-VBR or rt-VBR .
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to

Field	Description
	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.
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

Choose **Setup** > **WAN** > **ADSL**, the page is shown as the following figure appears. In this page, you can select the **ADSL modulation**. Mostly, you need to remain this factory default settings. The router supports these modulations: **G.Lite**, **G.Dmt**, **T1.413**, **ADSL2**, **ADSL2+**, **AnnexL**, and **AnnexM**. The router negotiates the modulation modes with the DSLAM.

Status

Setup

Advanced

Service

Firewall

Maintenance

> WAN

> WAN

> ATM

> ADSL

< LAN

Attention Config is modified to make it effective forever!

save

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

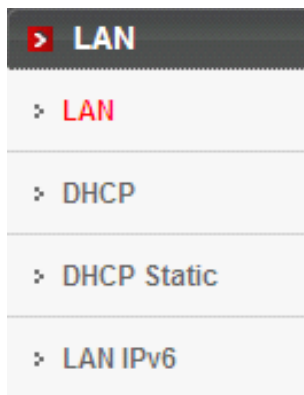
ADSL Capability:

☒ Bitswap Enable
☒ SRA Enable

Apply Changes

3.4.2 LAN Configuration

In the **Setup** page, click **LAN** on the left pane, the sub-menu of the LAN appears as below.



3.4.2.1 LAN

Choose **Setup > LAN > LAN**, the page is shown as the following figure appears. In this page, you can change IP address and subnet mask of the router. The default IP address is **192.168.1.1**, which is the private IP address of the router.

Status

Setup

Advanced

Service

Firewall

Maintenance

WAN

LAN

DHCP

DHCP Static

LAN IPv6

Attention Config is modified to make it effective forever!

save

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

Apply Changes

LAN Port:

Link Speed/Duplex Mode:

Modify

ETHERNET Status Table:

Select	Port	Link Mode
☐	LAN	AUTO Negotiation

MAC Address Control:

☐ LAN1

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 the LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is 192.168.1.1- 192.168.255.254 .
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254 .
Secondary IP	Select it to enable a secondary LAN IP address. The two LAN IP addresses must be in the different network.

Field	Description
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-down list: 100Mbps/FullDuplex, 100Mbps/Half Duplex, 10Mbps/FullDuplex, 10Mbps/Half Duplex, Auto Negotiation.
MAC Address Control	It is the access control based on MAC address. Select it and the host whose MAC address is listed in the Current Allowed MAC Address Table can access the modem.
Add	Enter MAC address, and then click it to add a new MAC address.

3.4.2.2 DHCP

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

Choose **Setup > LAN > DHCP**. In this page selects **None** in the **DHCP Mode** field and the page is shown as the following figure appears. In this mode the modem will do nothing when hosts request an IP address.

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

WLAN

LAN

LAN

DHCP

DHCP Static

LAN IPv6

Attention Config is modified to make it effective forever!

save

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

Apply Changes

Undo

Set Vendor/Class IP Range

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

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

WLAN

LAN

LAN

DHCP

DHCP Static

LAN IPv6

Attention Config is modified to make it effective forever!

save

DHCP Mode

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

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

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

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

LAN IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

DHCP Mode

DHCP Relay

Relay Server:

192.168.2.242

Apply Changes

Undo

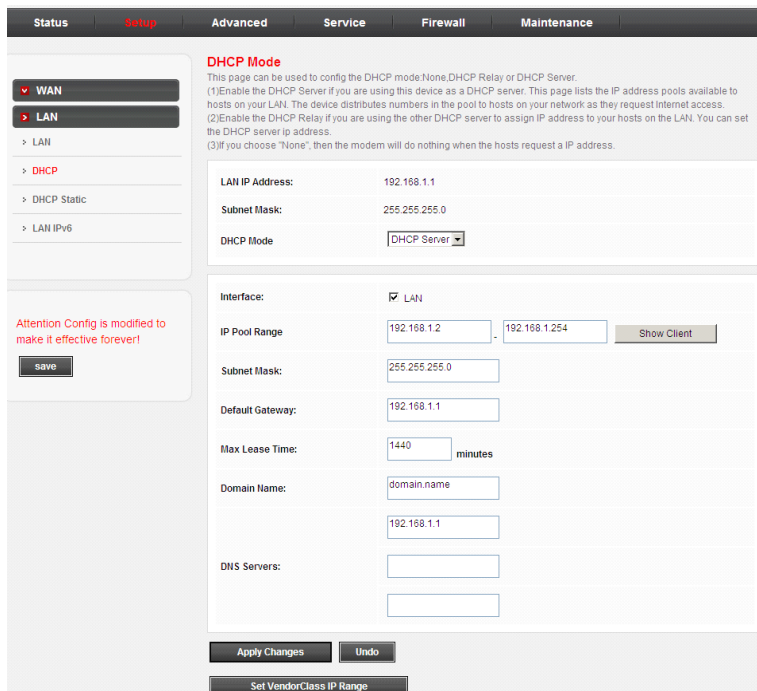
Set Vendor/Class IP Range

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

Field	Description
DHCP Mode	If set to DHCP Relay , the router acts a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.

Field	Description
Relay Server	Enter the DHCP server address provided by your ISP.

Choose **Setup > LAN > DHCP**. In this page selects **DHCP SERVER** in the **DHCP Mode** field. The page shown in the following figure appears.



The screenshot shows the DHCP configuration page. At the top, there are tabs: Status, Setup (selected), Advanced, Service, Firewall, and Maintenance. On the left, there is a sidebar with a tree view showing WAN, LAN (selected), DHCP, DHCP Static, and LAN IPv6. The main content area is titled 'DHCP Mode' and contains the following information:

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.

The configuration fields are as follows:

- LAN IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- DHCP Mode: DHCP Server (selected from a dropdown menu)

Below these fields, there is a section for the DHCP pool configuration:

- Interface: ☒ LAN
- IP Pool Range: 192.168.1.2 - 192.168.1.254 (with a 'Show Client' button)
- 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 (static IP address field)
- DNS Servers: (two empty input fields)

At the bottom, there are buttons for 'Apply Changes', 'Undo', and 'Set Vendor/Class IP Range'.

Figure 3

The following table describes the parameters of this page:

Field	Description
DHCP Mode	You can choose None, DHCP Relay and DHCP

Field	Description
	Server. If set to DHCP Server , the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows95, Windows NT and other operation systems that support the DHCP client.
IP Pool Range	It specifies the first and the last IP address in the IP address pool. The assigned IP address should be in the range of IP Pool.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway of the IP address pool.
Show Client	Click it, the Active DHCP Client Table appears. It shows the assigned IP address, MAC address and time expired for each DHCP leased client.
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 Device IP Range Table page appears. You can configure the IP address range based on the device type.

Click **Set VendorClass IP Range** in the **DHCP Mode** page, the page is shown a 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
Refresh Close				

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

Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, 00-A0-C5-00-02-12.
Expiry(s)	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

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

Device IP Range Table

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

device name:	
start address:	
end address:	
Router address:	
option60	

add	delete	modify	Close
------------------------------------	---------------------------------------	---------------------------------------	--------------------------------------

IP Range Table:

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

3.4.2.3 DHCP Static

Choose **Setup > LAN > DHCP Static**, and the page is shown as the following figure appears. In this page, you can assign the IP addresses to the specific individual PCs based on their MAC address.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

WAN
 LAN
 LAN
 DHCP
 DHCP Static
 LAN IPv6

Attention Config is modified to make it effective forever!

 Save

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 added row will be presented in the Current ATM VC Table .
Delete Selected	Select a row in the Current ATM VC Table , then click it, this row will be deleted.
Undo	Click it to reverse an action.
Current ATM VC Table	It shows the assigned IP address based on the MAC address.

3.4.2.4 LAN IPv6

Choose **Setup > LAN > LAN IPv6**, and the page is shown as the following figure appears. In this page, you can modify the IPv6 LAN parameters including the settings of LAN RA server work mode and LAN DHCPv6 server work mode

Status

Setup

Advanced

Service

Firewall

Maintenance

WAN

LAN

LAN

DHCP

DHCP Static

LAN IPv6

Attention Config is modified to make it effective forever!

Save

LAN IPv6 Setting

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

Global Address:

/

Apply Changes

RA Setting

Enable:

☒

M Flag:

☒

O Flag:

☒

Max Interval:

600

Secs

Min Interval:

200

Secs

Prefix Mode:

Auto

Apply Changes

DHCPv6 Setting

DHCPv6 Mode:

Auto Mode

Apply Changes

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

Field	Description
Global Address	Specify the LAN global ipv6 address, may be assigned by ISP.
RA Setting	
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the "Managed address configuration" flag in RA packet.
O Flag	Enable or disable the "Other configuration" flag in RA packet.
Max Interval	Maxium sending time interval.
Min Interval	Minimum sending time interval.

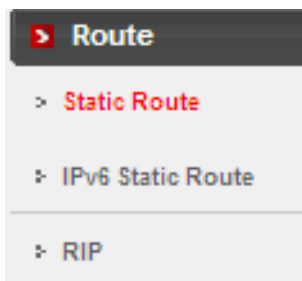
Field	Description
Prefix Mode	Specify the RA feature prefix mode: Auto: the RA prefix will use Wan dhcp-pd prefix; Manual: user will specify the prefix Address, Length, Preferred time and Valid time.
DHCPv6 Mode	Specify the dhcpv6 server mode: None: close dhcpv6 server. Manual: dhcpv6 server is opened and user specifies the dhcpv6 server address pool and other parameters. Auto: dhcpv6 server is opened and it use Wan dhcp-pd prefix to generate address pool.

3.5 Advanced

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

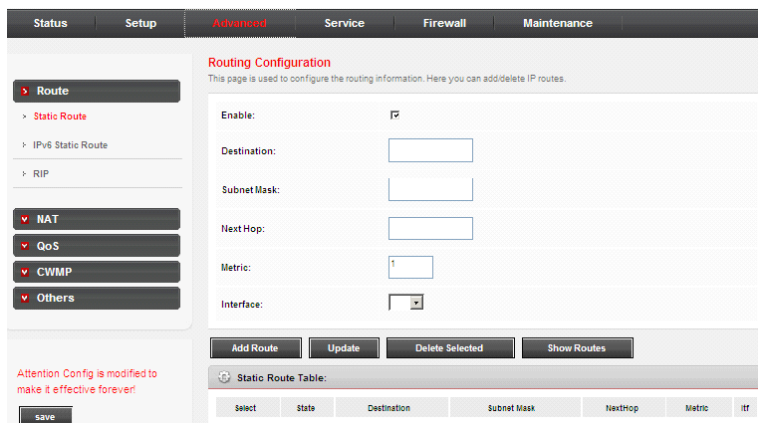
3.5.1 Route

In the **Advanced** page, click **Route** on the left pane, the sub-menu of **Route** appears as below.



3.5.1.1 Static Route

Choose **Advanced > Route > Static Route**, and the page is shown as the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



The screenshot shows the 'Static Route' configuration page. At the top, there are tabs: Status, Setup, **Advanced**, Service, Firewall, and Maintenance. On the left sidebar, under 'Route', there are options for 'Static Route' (selected), 'IPv6 Static Route', and 'RIP'. Below these are 'NAT', 'QoS', 'CWMP', and 'Others'. The main content area is titled 'Routing Configuration' and includes a sub-header: 'This page is used to configure the routing information. Here you can add/delete IP routes.' The configuration fields are: 'Enable' (checked), 'Destination' (text box), 'Subnet Mask' (text box), 'Next Hop' (text box), 'Metric' (text box with '1' entered), and 'Interface' (dropdown menu). Below these fields are four buttons: 'Add Route', 'Update', 'Delete Selected', and 'Show Routes'. At the bottom, there is a 'Static Route Table' with columns: Select, State, Destination, Subnet Mask, NextHop, Metric, and ID. A 'save' button is located at the bottom left of the sidebar area.

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

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

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

Click **Show Routes**, and the page is shown as 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	NextHop	Interface
192.168.1.1	255.255.255.255	*	e1

Refresh

Close

3.5.1.2 IPv6 Static Route

Choose **Advanced > Route > IPv6 Static Route**, and the page is shown as the following figure appears. This page is used to configure the IPv6 routing information.

Status

Setup

Advanced

Service

Firewall

Maintenance

Route

Static Route

IPv6 Static Route

RIP

NAT

QoS

CWMP

Others

IPv6 Routing Configuration

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

Destination:

Prefix Length:

Next Hop:

Interface:

Add Route

Delete Selected

IPv6 Static Route Table:

Select	Destination	NextHop	Interface

Attention Config is modified to make it effective forever!

save

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

Field	Description
Destination	Enter the IPv6 address of the destination device.
Prefix Length	Enter the prefix length of the IPv6 address.
Next Hop	Enter the IP address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the IPv6 Static Route Table .
Delete Selected	Select a row in the IPv6 Static Route Table and click it to delete the row.

3.5.1.3 RIP

Choose **Advanced > Route > RIP**, and the page is shown as 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

Setup

Advanced

Service

Firewall

Maintenance

> Route

> Static Route

> IPv6 Static Route

> RIP

NAT

QoS

CWMP

Others

Attention Config is modified to make it effective forever!

save

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
--------	-----------	--------------	--------------

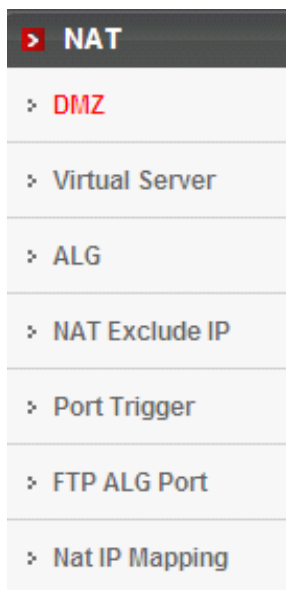
The following table describes the parameters and buttons of this page:

Field	Description
RIP	Select On , 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 RIP1 , RIP2 or Both . - Choose RIP1 indicates the router receives RIP v1 messages. - Choose RIP2 indicates the router receives RIP v2 messages. - Choose Both indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose RIP1 or RIP2 .

Field	Description
	- Choose RIP1 indicates the router broadcasts RIP1 messages only. - Choose RIP2 indicates the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the Rip Config List .
Delete	Select a row in the Rip Config List and click it to delete the row.

3.5.2 NAT

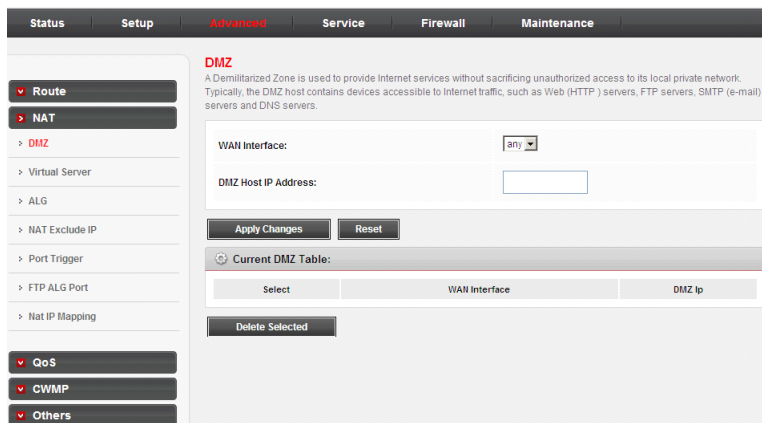
In the **Advanced** page, click **NAT** on the left pane, the sub-menu of **NAT** appears as below.



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.

Choose **Advanced > NAT > DMZ**, the page is shown as the following figure appears.

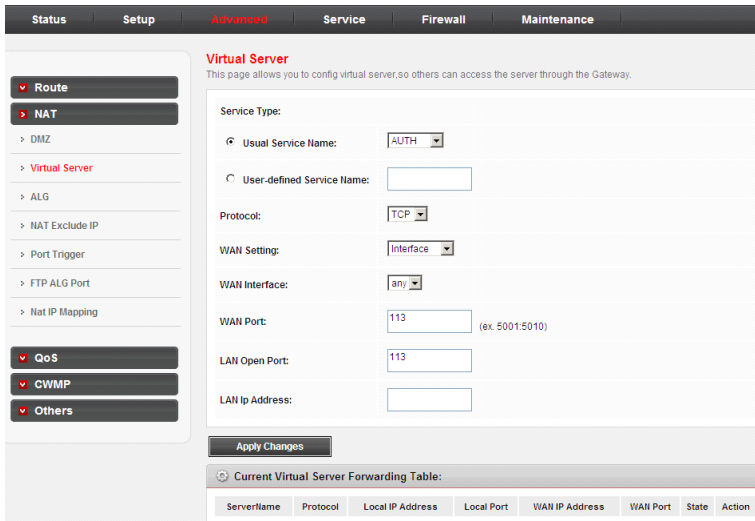


The following table describes the parameters of this page:

Field	Description
WAN Interface	Choose a WAN Interface.
DMZ Host IP Address	Enter an IP address of the DMZ host
Current DMZ Table	A list of the previously configured DMZ information

3.5.2.2 Virtual Server

Choose **Advanced > NAT > Virtual Server**, and the page is shown as the following figure appears. In this page you can configure virtual server, so others can access the server through the Gateway.



The screenshot shows the 'Virtual Server' configuration page. The top navigation bar includes Status, Setup, Advanced (selected), Service, Firewall, and Maintenance. On the left, a sidebar lists various configuration options: Route, NAT (selected), DMZ, Virtual Server, ALG, NAT Exclude IP, Port Trigger, FTP ALG Port, and Nat IP Mapping. Below these are QoS, CWMP, and Others. The main content area is titled 'Virtual Server' and includes a sub-header 'Service Type:'. Below this, there are two radio buttons: 'Usual Service Name:' (selected) and 'User-defined Service Name:'. The 'Usual Service Name:' option has a dropdown menu showing 'AUTH'. Below the radio buttons, there are several input fields: 'Protocol:' (dropdown showing 'TCP'), 'WAN Setting:' (dropdown showing 'Interface'), 'WAN Interface:' (dropdown showing 'any'), 'WAN Port:' (text box with '113' and a note '(ex. 5001:5010)'), 'LAN Open Port:' (text box with '113'), and 'LAN Ip Address:' (text box). At the bottom of the configuration area is an 'Apply Changes' button. Below the configuration area is a table titled 'Current Virtual Server Forwarding Table:'.

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

The following table describes the parameters of this page:

Field	Description
Service Type	You can select the common service type, for example, AUTH, DNS, FTP and so on. You can also define a service name. ● If Usual Service Name is selected, the corresponding parameters have the default settings. ● If User-defined Service Name is selected, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose TCP or UDP.

Field	Description
WAN Setting	You can choose Interface or IP Address .
WAN Interface	Choose the WAN interface that applies to virtual server. (Available when Interface is selected in WAN Setting field only).
WAN IP Address	Enter the corresponding WAN IP Address.(Available when IP Address is selected in WAN Setting field only.)
WAN Port	Choose the access port of 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

The NAT ALG (Application Layer Gateways) function enables the router to support various special application protocols with payloads containing IP addresses and port numbers, and tries to establish connection between these imbedded IP addresses and port numbers. Failure of the transformation of such information may results in problems. The NAT ALG function realizes payload detection and transformation to ensure normal operation of payloads under NAT environment, requiring no special configuration of users.

Choose **Advanced > NAT > ALG**, the page is shown as the following figure appears. In this page you can set NAT ALG and pass-through configuration.

Status

Setup

Advanced

Service

Firewall

Maintenance

▼ Route

▼ NAT

> DMZ

> Virtual Server

> ALG

> NAT Exclude IP

> Port Trigger

> FTP ALG Port

> Nat IP Mapping

▼ QoS

▼ CWMP

▼ Others

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

IPSec Pass-Through:	☒ Enable
L2TP Pass-Through:	☒ Enable
PPTP Pass-Through:	☒ Enable
FTP:	☒ Enable
H.323:	☒ Enable
SIP:	☒ Enable
RTSP:	☒ Enable
ICQ:	☒ Enable
MSN:	☒ Enable

Apply Changes

Reset

3.5.2.4 NAT Exclude IP

Choose **Advanced > NAT > NAT Exclude IP**, and the page is shown as 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

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

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:

IP Range: ---

Apply Changes

Reset

Current NAT Exclude IP Table:

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

3.5.2.5 Port Trigger

Choose **Advanced** > **NAT** > **Port Trigger**, and the page is shown as the following figure appears.

Status

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

DMZ

Virtual Server

ALG

NAT Exclude IP

Port Trigger

FTP ALG Port

Nat IP Mapping

QoS

CWMP

Others

Attention Config is modified to make it effective forever!

save

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:

Select One

☐ User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing

Apply Changes

Current Port Trigger Table:

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
------------	------------------	-----------	------------	---------------	-------------	--------

Click the **Usual Application Name** drop-down menu to choose the application you want to set up for port triggering. When you have chosen an application, the default trigger settings will be generated in the table below.

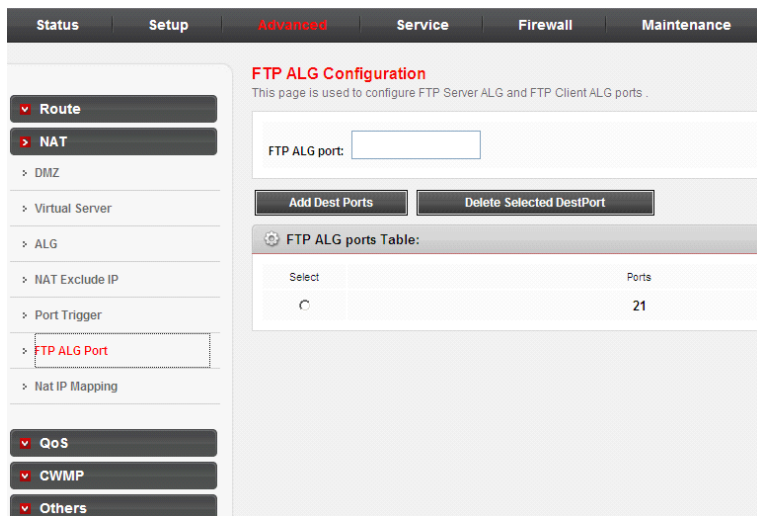
If the application you want to set up is not listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port**, **Open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

Click the Apply changes button to finish the setting.

43

3.5.2.6 FTP ALG Port

Choose **Advanced > NAT > FTP ALG Port**, and the page is shown as the following figure appears. The common port for FTP connection is port 21, and a common ALG monitors the TCP port 21 to ensure NAT pass-through of FTP. By enabling this function, when the FTPserver connection port is not a port 21, the FTP ALG module will be informed to monitor other TCP ports to ensure NAT pass-through of FTP.



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

Field	Description
FTP ALG port	Set a FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected DestPort	Delete a selected port configuration from the list.

3.5.2.7 NAT IP Mapping

NAT is the abbreviation for Network Address Translation. The Network Address Translation Settings allow you to share one WAN IP address for multiple computers on your LAN.

Choose **Advanced > NAT > NAT IP Mapping**, and the page is shown as the following figure appears. This page allows you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

Route
 NAT
 DMZ
 Virtual Server
 ALG
 NAT Exclude IP
 Port Trigger
 FTP ALG Port
 Nat IP Mapping

QoS
 CWMP
 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:

Current NAT IP MAPPING Table:

Local Start IP	Local End IP	Global Start IP	Global End IP	Action
Delete Selected Delete All				

Attention Config is modified to make it effective forever!

3.5.3 QoS

Choose **Advanced > IP QoS**, in this page you can enable the **IP QoS**, and the page is shown as the following figure appears.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

▼ Route
 ▼ NAT
 ▼ **QoS**
 > QoS
 ▼ CWMP
 ▼ Others

Attention Config is modified to make it effective forever!
 save

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

IP QoS: ☐ disable ☒ enable

Apply

QoS Policy:

Schedule Mode:

QoS Rule List:

stream rule							behavior				
src IP	src Port	dest IP	dest Port	proto	phy port	prior	IP Preced	IP ToS	802.1p	wan if	sel
Add rule Delete Delete all											

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

Field	Description
IP QoS	Select to enable or disable IP QoS function. You need to enable IP QoS if you want to configure the parameters of this page.
QoS Policy	You can choose stream based , 802.1p based or DSCP based .
Schedule Mode	You can choose strict prior or WFQ (4:3:2:1) .

Click **Add rule** at the bottom of the page and 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.

 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	

DSCP:	(0-63)
802.1p:	▼

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

Field	Description
Src IP	The IP address of the source data packet.

Field	Description
Src Mask	The subnet mask of the source IP address.
Dest IP	The IP address of the destination data packet.
Dest Mask	The subnet mask of the destination IP address.
Src Port	The port of the source data packet.
Dest Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rules. You can choose TCP , UDP , or ICMP .
Phy 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.
Insert or modify QoS mark	Add or modify the mark(IP Precedence, IP ToS,802.1P) of QoS
DSCP	Differentiated Services Code Point. One of QoS mode, you can config dscp priority from P0(highest) to P3(lowest)
802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization. You can choose from 0 to 7 levels.

3.5.4 CWMP

Choose **Advanced > CWMP**, the page is shown as the following figure appears. In this page you can configure the TR-069 CPE and change the setting for the ACS's parameters.

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

Route

NAT

QoS

CWMP

CWMP

Others

Attention Config is modified to make it effective forever!

save

TR-069 Configuration

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

ACS:

Enable: ☒

URL:

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 IRReboot: ☒ Disable ☐ Enable

Delay: ☐ Disable ☒ Enable

Auto-Execution: ☐ Disable ☒ Enable

Apply Changes

Reset

Certificate Management:

CPE Certificate Password:

Apply

Undo

CPE Certificate:

Browse...

Upload

Delete

CA Certificate:

Browse...

Upload

Delete

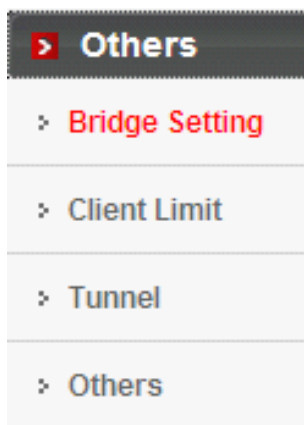
The following table describes the parameters of this page:

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

Field	Description
CPE Certificate Password	The Password of CPE Certificates.
CPE Certificate	The Certificate of CPE.
CA Certificate	The Certificate of certificate authority.

3.5.5 Others

In the **Advanced** page, click **Others** on the left pane, the sub-menu of **Others** appears as below.



3.5.5.1 Bridge Setting

Choose **Advanced > Others > Bridge setting**, and the page is shown as 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.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

▼ Route
 ▼ NAT
 ▼ QoS
 ▼ CWMP
 ▼ Others
 > Bridge Setting
 > Client Limit
 > Tunnel
 > Others

Attention Config is modified to make it effective forever!
 save

Bridge Setting

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.

Ageing Time:
 (seconds)

802.1d Spanning Tree:
 ☒ Disabled
 ☐ Enabled

Apply Changes
 Undo
 Show MACs

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

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

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

Forwarding Table

MAC Address	Port	Type	Aging Time
01:80:c2:00:00:00	0	Static	300
00:05:1d:03:04:05	0	Static	300
01:00:5e:00:00:09	0	Static	300
38:83:45:f2:35:86	1	Dynamic	300
ff:ff:ff:ff:ff:ff	0	Static	300

3.5.5.2 Client Limit

Choose **Advanced > Others > Client Limit**, and the page is shown as the following figure appears. This page is used to set the limitation on the quantity of the PCs which are allowed to connect to the router.

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

▼ Route

▼ NAT

▼ QoS

▼ CWMP

➤ Others

➤ Bridge Setting

➤ Client Limit

➤ Tunnel

➤ Others

Attention Config is modified to make it effective forever!

save

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

Maximum Devices:

4

Apply Changes

3.5.5.3 Tunnel

Choose **Advanced > Others > Tunnel**, and the page is shown as the following figure appears. This page is used to config tunnels to connect ipv4 and ipv6 networks.

Status

Setup

Advanced

Service

Firewall

Maintenance

Route

NAT

QoS

CWMP

Others

Bridge Setting

Client Limit

Tunnel

Others

Attention Config is modified to make it effective forever!

save

Tunnel Configuration

This page is used to config tunnels to connect ipv4 and ipv6 networks.

General v6inv4 Tunnel:

Interface Name:

Tunnel Endpoints (local ipv4-remote ipv4): -

Local IPv6 Address: /

Apply Changes

Current General Tunnel Table:

Interface Name	Tunnel Local	Tunnel Remote	Address	Action
Special v6inv4 Tunnel: Enable: ☐ Interface: gif0 Mode: Sto4 Tunnel Relay Router: Apply Changes				

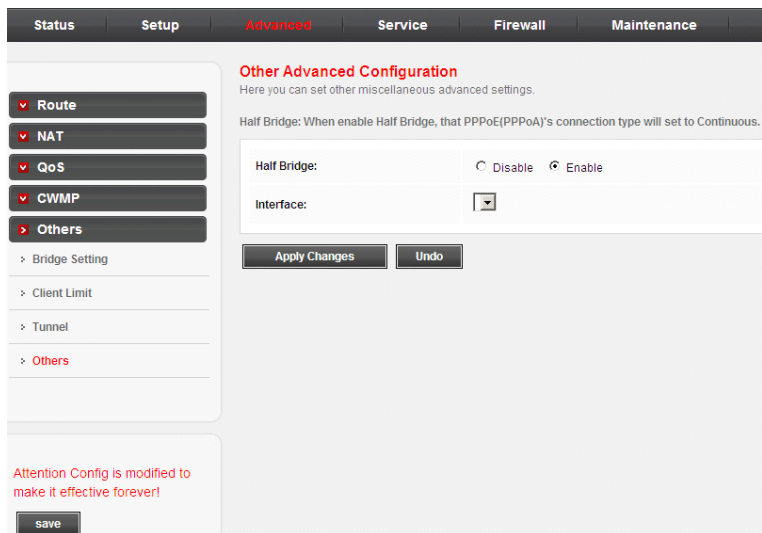
The following table describes the parameters and button of this page:

Field	Description
General v6inv4 Tunnel	
Interface Name	Select the tunnel interface name, user can set 2 v6inv4 tunnel
Tunnel Endpoints (local ipv4-remote ipv4)	Specify the ipv4 address for tunnel endpoints.
Local IPv6 Address	Specify the ipv6 address for tunnel local.
Current General Tunnel Table	Display current general v6inv4 tunnel setting.
Special v6inv4 Tunnel	

Field	Description
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select current wan interface used as tunnel interface.
Mode	Enable or disable special tunnel.

3.5.5.4 Others

Choose **Advanced > Others > Others**, and the page is shown as the following figure appears. In this page, you can enable half bridge so that the PPPoE or PPPoA connection will be set to Continuous



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:

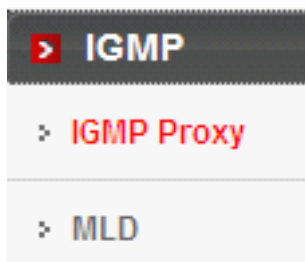
Attention Config is modified to make it effective forever!

3.6 Service

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

3.6.1 IGMP

In the **Service** page, click **IGMP** on the left pane, the sub-menu of **IGMP** appears as follow:



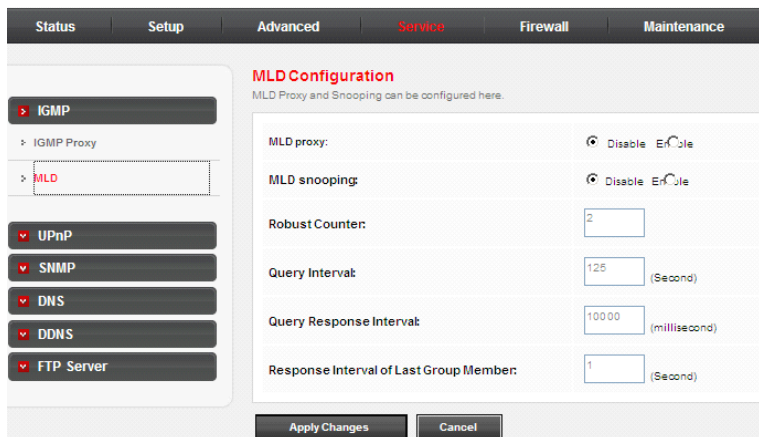
3.6.1.1 IGMP Proxy

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

Status	Setup	Advanced	Service	Firewall	Maintenance														
> IGMP > IGMP Proxy > MLD > 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. <table> <tr> <td>IGMP Proxy:</td> <td>☐ Disable ☒ Enable</td> </tr> <tr> <td>Multicast Allowed:</td> <td>☐ Disable ☒ Enable</td> </tr> <tr> <td>Robust Count</td> <td> 2 </td> </tr> <tr> <td>Last Member Query Count</td> <td> 2 </td> </tr> <tr> <td>Query Interval</td> <td> 60 (seconds)</td> </tr> <tr> <td>Query Response Interval</td> <td> 100 (~100ms)</td> </tr> <tr> <td>Group Leave Delay:</td> <td> 2000 (ms)</td> </tr> </table>						IGMP Proxy:	☐ Disable ☒ Enable	Multicast Allowed:	☐ Disable ☒ Enable	Robust Count	2	Last Member Query Count	2	Query Interval	60 (seconds)	Query Response Interval	100 (~100ms)	Group Leave Delay:	2000 (ms)
IGMP Proxy:	☐ Disable ☒ Enable																		
Multicast Allowed:	☐ Disable ☒ Enable																		
Robust Count	2																		
Last Member Query Count	2																		
Query Interval	60 (seconds)																		
Query Response Interval	100 (~100ms)																		
Group Leave Delay:	2000 (ms)																		
Apply Changes Undo																			

3.6.1.2 MLD

Choose **Service > IGMP > MLD**, the page is shown as the following figure appears.



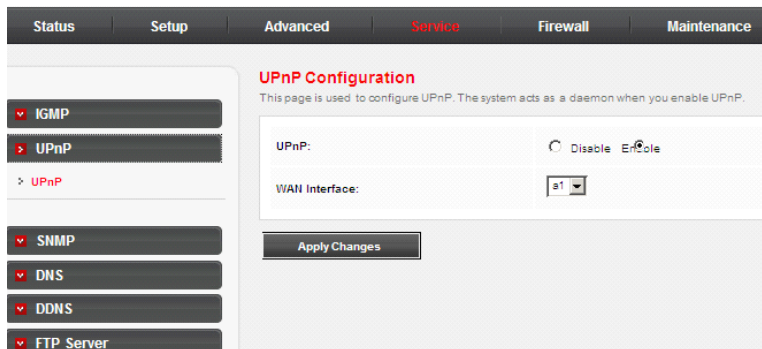
The following table describes the parameters and button of this page:

Field	Description
Enable MLD Proxy	MLD Proxy can be used to support IPv6 multicast data.
Enable MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.
Robust Counter	Robust factor of the MLD Counter.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier

Field	Description
	on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Response Interval of Last Group Member	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

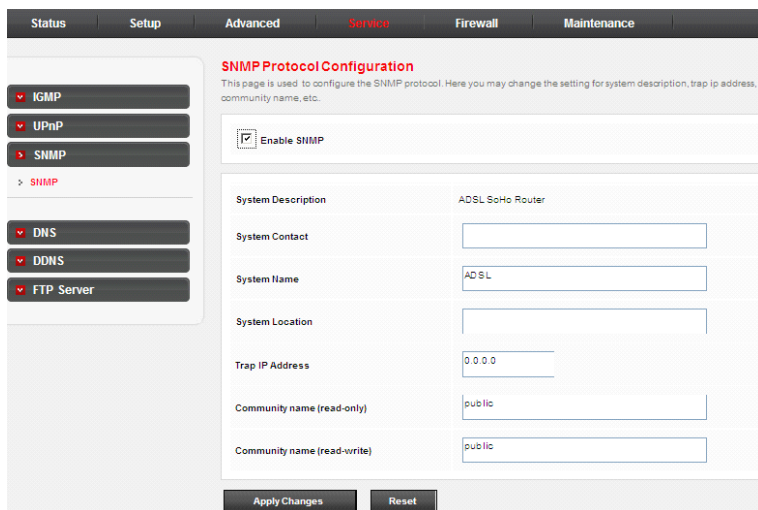
3.6.2 UPnP

In the **Service** page, click **UPnP** on the left pane, and the page is shown as the following figure appears. This page is used to configure UPnP. The system acts as a daemon after you enable it.



3.6.3 SNMP

In the **Service** page, click **SNMP** on the left pane. Check **Enable SNMP**, and then the page is shown as the following figure appears. This page is used to configure the SNMP protocol. You may change the setting for **system description, trap ip address, community name**, etc.



The screenshot shows the 'Service' tab selected in the top navigation bar. On the left sidebar, 'SNMP' is highlighted under the 'Service' section. The main content area is titled 'SNMP Protocol Configuration'. It includes a sub-header explaining the page's purpose: 'This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc.' Below this, there is a checkbox labeled 'Enable SNMP' which is checked. The configuration fields are as follows:

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

At the bottom of the form are two buttons: 'Apply Changes' and 'Reset'.

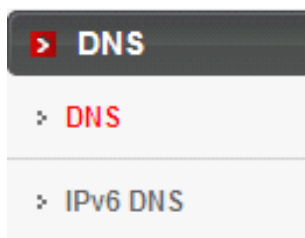
The following table describes the parameters of this page:

Field	Description
Enable SNMP	Select it to enable SNMP function. You need to enable SNMP, and then you can configure the parameters of this page.
System Contact	The contract of system
System Name	The name of system
System Location	The location of system
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.

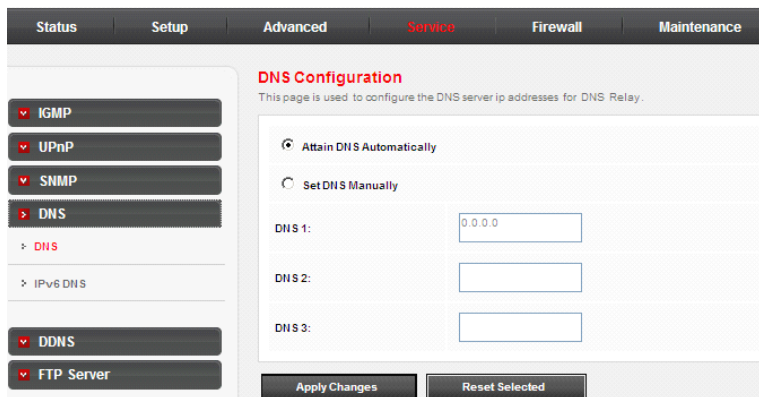
3.6.4 DNS

In the **Service** page, click **DNS** on the left pane, the sub-menu of **DNS** appears as follow:



3.6.4.1 DNS

Choose **Service** > **DNS** > **DNS**, and the page is shown as the following figure appears. This page is used to configure the DNS server ip addresses for DNS Relay

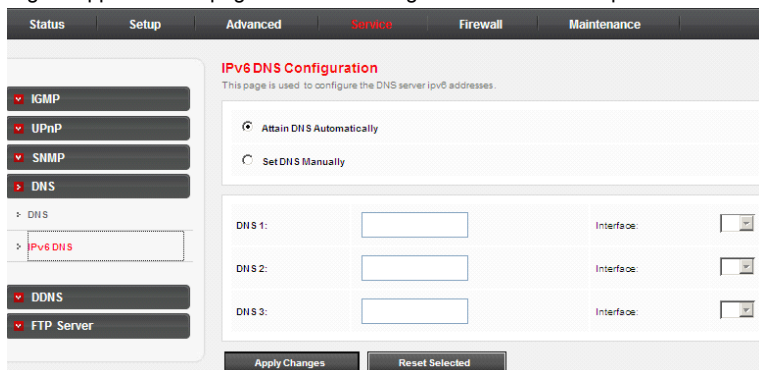


The following table describes the parameters and buttons of this page:

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

3.6.4.2 IPv6 DNS

Choose **Service > DNS > IPv6 DNS**, and the page is shown as the following figure appears. This page is used to configure the DNS server ipv6 addresses.



IPv6 DNS Configuration
 This page is used to configure the DNS server ipv6 addresses.

☒ Attain DNS Automatically
☐ Set DNS Manually

DNS 1:		Interface:	
DNS 2:		Interface:	
DNS 3:		Interface:	

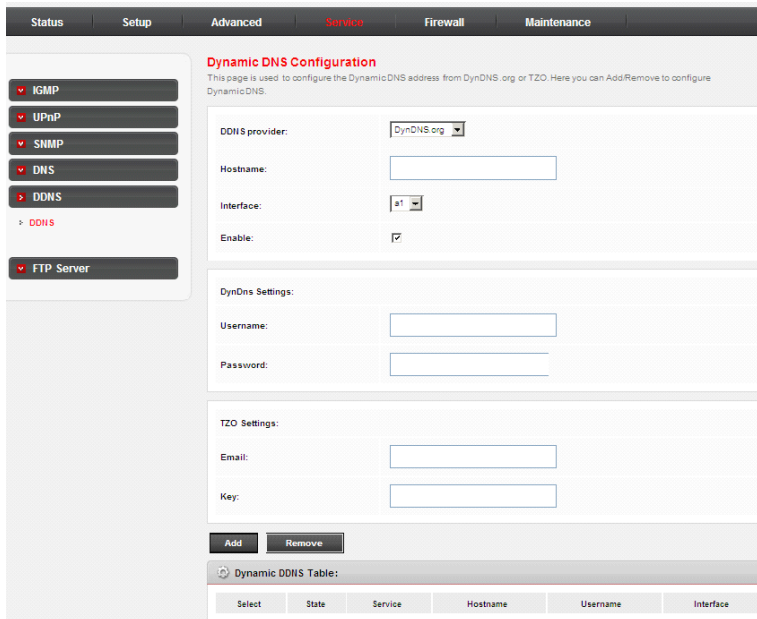
The following table describes the parameters and buttons of this page.

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 and choose the WAN interface of the primary, the secondary and the tertiary

Field	Description
	DNS server.
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

3.6.5 DDNS

In the **Service** page, click **DDNS** on the left pane. The page is shown as 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. At the top, there are tabs: Status, Setup, Advanced, **Service**, Firewall, and Maintenance. On the left sidebar, there are buttons for IGMP, UPnP, SNMP, DNS, **DDNS**, and FTP Server. The main content area is titled 'Dynamic DNS Configuration' and includes a subtitle: 'This page is used to configure the DynamicDNS address from DynDNS.org or TZO. Here you can Add/Remove to configure DynamicDNS.'

The configuration fields are as follows:

- DDNS provider:** A dropdown menu currently set to 'DynDNS.org'.
- Hostname:** A text input field.
- Interface:** A dropdown menu currently set to 'a1'.
- Enable:** A checkbox that is checked.

Below these are two sections for settings:

- DynDns Settings:** Includes fields for 'Username' and 'Password'.
- TZO Settings:** Includes fields for 'Email' and 'Key'.

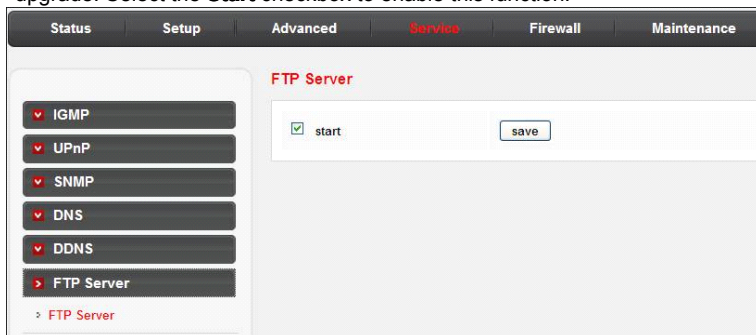
At the bottom, there are 'Add' and 'Remove' buttons. Below these is a table titled 'Dynamic DNS Table:' with columns: Select, State, Service, Hostname, Username, and Interface.

The following table describes the parameters of this page:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose DynDNS.org , TZO or PHDNS .
Hostname	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

In the **Service** page, click **FTP Service** on the left pane. The page is shown as the following figure appears. This page is used to enable the remote FTP upgrade. Select the **Start** checkbox to enable this function.



3.7 Firewall

In the navigation bar, click **Firewall**. The **Firewall** page contains **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL** and **DoS**.

3.7.1 MAC Filter

Click **MAC Filter** in the left pane, and the page is shown as 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
 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

In the **Firewall** page, click **IP/Port Filter** on the left pane, the sub-menu of **IGMP** appears as follow. The **IP/Port Filter** page contains **IP/Port Filter** and **IPv6/Port Filter**. This part is used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



3.7.2.1 IP/Port Filter

Choose **Firewall > IP/Port Filter > IP/Port Filter**, and the page is shown as the following figure appears.

Status	Setup	Advanced	Service	Firewall	Maintenance									
MAC Filter IP/Port Filter IPv6/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 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: <table border="1"> <thead> <tr> <th>Rule</th> <th>Protocol</th> <th>Source IP/Mask</th> <th>SPort</th> <th>Dest IP/Mask</th> <th>DPort</th> <th>State</th> <th>Direction</th> <th>Action</th> </tr> </thead> <tbody> </tbody> </table>						Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action
Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action						

3.7.2.2 IPv6/Port Filter

Choose **Firewall > IP/Port Filter > IPv6/Port Filter**, and the page is shown as the following figure appears.

Status

Setup

Advanced

Service

Firewall

Maintenance

MAC Filter

IP/Port Filter

IPV6/Port Filter

URL Filter

ACL

DoS

IPv6/Port Filtering

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

Outgoing Default Policy

☒ Permit
 ☐ Deny

Incoming Default Policy

☐ Permit
 ☒ Deny

Rule Action:

☒ Permit
 ☐ Deny

Protocol:

IPv6

ICMP6Type:

PING6

Direction:

Upstream

Source IPv6 Address:

Prefix Length:

Dest IPv6 Address:

Prefix Length:

SPort:

-

DPort:

-

Enable:

☒

Apply Changes

Reset

Help

Current Filter Table:

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

3.7.3 URL Filter

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

Status
 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:

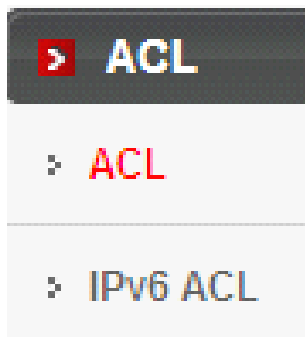
Select	Filtered Keyword
--------	------------------

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

Field	Description
URL Blocking Capability	You can choose Disable or Enable . - Select Disable to disable URL blocking function and keyword filtering function. - Select Enable to block access to the URLs and keywords specified in the URL Blocking Table.
Keyword	Enter the keyword to block.
AddKeyword	Click it to add a keyword to the URL Blocking Table .
Delete Selected Keyword	Select a row in the URL Blocking Table and click it to delete the row.
URL Blocking Table	A list of the URL (s) to which access is blocked.

3.7.4 ACL

In the **Firewall** page, click **ACL** on the left pane, the sub-menu of **ACL** appears as follow. The **ACL** page contains **ACL** and **IPv6 ACL**.



3.7.4.1 ACL

Choose **Firewall > ACL > ACL**, and the page is shown as 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.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

▼ MAC Filter
 ▼ IP/Port Filter
 ▼ URL Filter
 > **ACL**
 > ACL
 > IPv6 ACL
 ▼ DoS

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 such access control can be helpful in securing or restricting the Gateway management.

Direction Select:
 ☒ LAN
 ☐ WAN

LAN ACL Switch:
 ☐ Enable
 ☒ Disable

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

Services Allowed:

☒ any

Current ACL Table:

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

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

Field	Description
Direction Select	Select the router interface. You can select LAN or WAN . In this example, LAN is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: web, telnet, ssh, ftp, tftp, snmp or ping . You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the Current ACL Table .
Reset	Click it to refresh this page.

Set the direction of the data packets to **WAN**, then the page is shown as the following figure appears.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

▼ MAC Filter
 ▼ IP/Port Filter
 ▼ URL Filter
 ▼ ACL
 > ACL
 > IPv6 ACL
 ▼ DoS

ACL Configuration

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

Direction Select:

☐ LAN
 ☒ WAN

WAN Setting:

WAN Interface:

Services Allowed:

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

AddReset

⚙ Current ACL Table:

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

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

Field	Description
Direction Select	Select the router interface. You can select LAN or WAN . In this example, WAN is selected.
WAN Setting	You can choose Interface or IP Address .
WAN Interface	Choose the interface that permits data packets from WAN to access the router.
IP Address	Enter the IP address on the WAN. Only the IP address that is in the same network segment with the IP address on the WAN can access the router.
Services Allowed	You can choose the following services from WAN:

Field	Description
	web, telnet, ssh, ftp, tftp, snmp or ping . You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the Current ACL Table .
Reset	Click it to refresh this page.

3.7.4.2 IPv6 ACL

Choose **Firewall > ACL > IPv6 ACL** and the page is shown as the following figure appears. **IPv6 ACL** has the similar function as **ACL** does, just based on different network protocol. For the parameters description of **IPv6 ACL**, you can refer to the **ACL**.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

✓ MAC Filter
 ✓ IP/Port Filter
 ✓ URL Filter
 > ACL
 > **IPv6 ACL**
 ✓ DoS

ACL Configuration

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

Direction Select:
 ☒ LAN
 ☐ WAN

LAN ACL Switch:
 ☐ Enable
 ☒ Disable

IP Address:
 /

Services Allowed:

☒ Any

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	Delete

If **WAN** is selected in the field of **Direction Select**, the page is shown as the following figure appears.

Status

Setup

Advanced

Service

Firewall

Maintenance

MAC Filter

IP/Port Filter

URL Filter

ACL

ACL

IPv6 ACL

DoS

ACL Configuration

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

Direction Select:
☐ LAN
☒ WAN

WAN Setting:

Interface

WAN Interface:

any

Services Allowed:

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

Add

Reset

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	Delete

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.

Click **DoS** in the left pane and the page is shown as the following figure appears.

In this page, you can prevent DoS attacks.

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

MAC Filter

IP/Port Filter

URL Filter

ACL

DoS

DoS

DoS Setting

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

☐ Enable DoS Prevention

☐ Whole System Flood: SYN	100	Packets/Second
☐ Whole System Flood: FIN	100	Packets/Second
☐ Whole System Flood: UDP	100	Packets/Second
☐ Whole System Flood: ICMP	100	Packets/Second
☐ Per-Source IP Flood: SYN	100	Packets/Second
☐ Per-Source IP Flood: FIN	100	Packets/Second
☐ Per-Source IP Flood: UDP	100	Packets/Second
☐ Per-Source IP Flood: ICMP	100	Packets/Second
☐ TCP/UDP PortScan	Low	Sensitivity
☐ ICMP Smurf		
☐ IP Land		
☐ IP Spoof		
☐ IP TearDrop		
☐ PingOfDeath		
☐ TCP Scan		
☐ TCP SynWithData		
☐ UDP Bomb		
☐ UDP EchoChargen		

Select ALL

Clear ALL

☐ Enable Source IP Blocking
 Block time (sec)

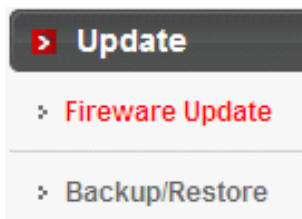
Apply Changes

3.8 Maintenance

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

3.8.1 Update

In the **Maintenance** page, click **Update** on the left pane, the sub-menu of **Update** appears as follow. The **Update** page contains **Fireware Update** and **Backup/Restore**.

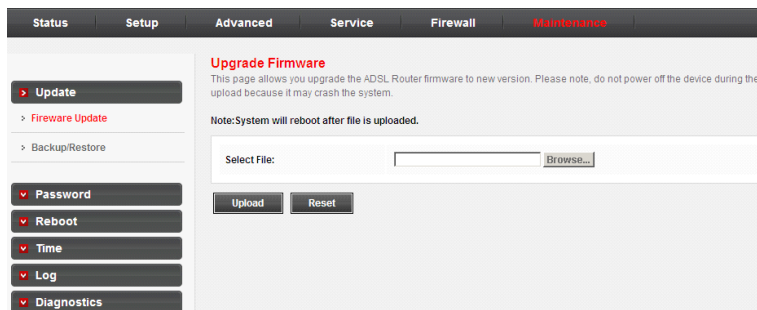


Caution:

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

3.8.1.1 Upgrade Firmware

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

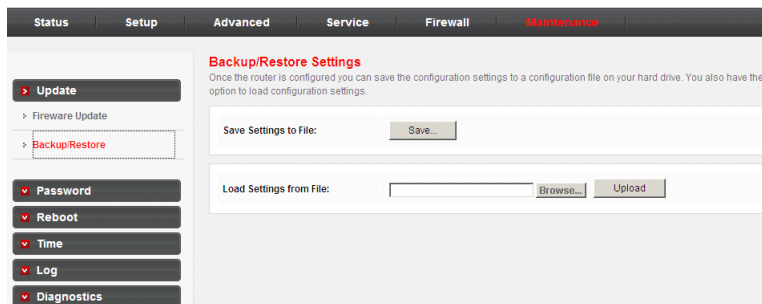


The following table describes the parameters and button of this page:

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

3.8.1.2 Backup/Restore

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

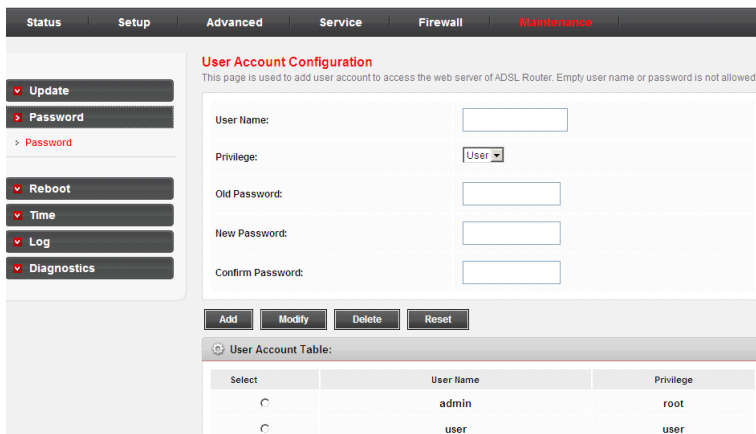


The following table describes the parameters and button of this page:

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

3.8.2 Password

Click **Password** on the left pane, and the page is shown as 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.



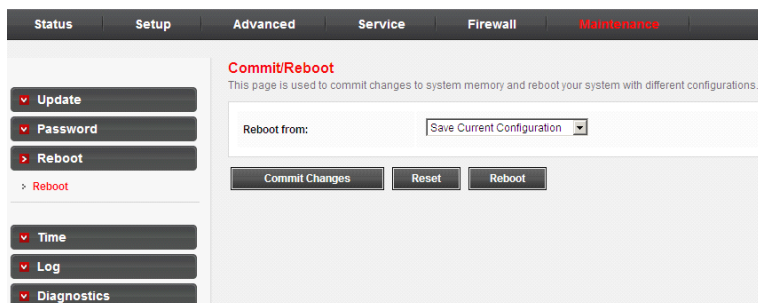
Select	User Name	Privilege
☐	admin	root
☐	user	user

The following table describes the parameters of this page:

Field	Description
User Name	Choose the user name for accessing the router. You can choose admin or user .
Privilege	Choose the privilege for the account. You can choose User or Root .
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

Click **Password** on the left pane and the page is shown as the following figure appears. You can set the router reset to the default settings or set the router to commit the current settings.



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

Field	Description
Reboot from	You can choose Save the current configuration or Restore to the factory default configuration. ● Save the current configuration: Save the current settings, and then reboot the router. ● Restore to the factory default configuration: Reset to the factory default settings, and then reboot the router.
Reboot	Click it to reboot the router.

3.8.4 Time

Click **Time** on the left pane and the page is shown as the following figure appears. You can configure the system time manually or get the system time from the time server.

Status
 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:
 Year 1970
 Month Jan
 Day 1
 Hour 5
 min 20
 sec 10

DayLight: LocalTIME

Apply Changes
 Reset

NTP Configuration:

State:
 ☒ Disable
 ☐ Enable

Server:

Server2:

Interval: Every 1 hours

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

GMT time: Thu Jan 1 5:20:10 1970

Apply Changes
 Reset

NTP Start: Get GMT Time

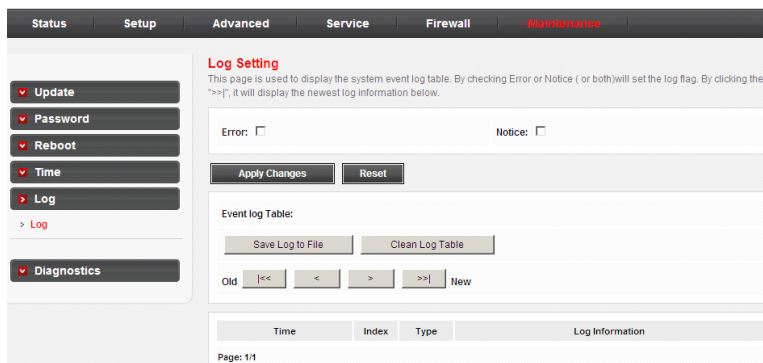
The following table describes the parameters of this page:

Field	Description
System Time	Set the system time manually.
DayLight	Daylight Saving Time.
NTP Configuration	
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.

Field	Description
Server2	Set the secondary NTP server manually.
Interval	NTP updating time interval.
Time Zone	Choose the time zone in which area you are from the drop down list.

3.8.5 Log

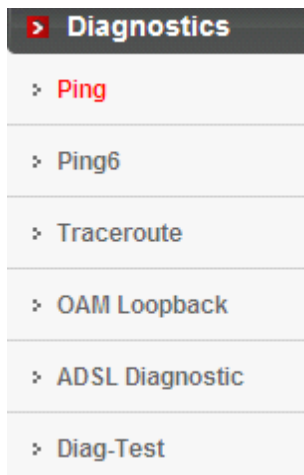
Click **Log** on the left pane and the page is shown as the following figure appears. You can enable or disable system log function and view the system log.



The screenshot shows the 'Log Setting' page. On the left is a navigation pane with options: Update, Password, Reboot, Time, Log (selected), and Diagnostics. The main content area has a title 'Log Setting' and 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', both currently unchecked. There are 'Apply Changes' and 'Reset' buttons. An 'Event log Table:' section contains 'Save Log to File' and 'Clean Log Table' buttons. Below the table are navigation controls: 'Old', '<<', '<', '>', '>>', 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 shown at the very bottom.

3.8.6 Diagnostics

In the **Maintenance** page, click **Diagnostics** on the left pane, the sub-menu of **Diagnostics** appears as follow. The **Diagnostics** page contains **Ping**, **Ping6**, **Traceroute**, **OAM Loopback**, **ADSL Diagnostic** and **Diag-Test**.



3.8.6.1 Ping

Choose **Maintenance > Diagnostic > Ping**. The page is shown as the following figure appears.

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

▼ Update

▼ Password

▼ Reboot

▼ Time

▼ Log

> Diagnostics

> Ping

> Ping6

> Traceroute

> OAM Loopback

> ADSL Diagnostic

> Diag-Test

Ping Diagnostic

Host :

PING

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

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

3.8.6.2 Ping6

Choose **Maintenance > Diagnostic > Ping6**. The page is shown as the following figure appears.

Status

Setup

Advanced

Service

Firewall

Maintenance

▼ Update

▼ Password

▼ Reboot

▼ Time

▼ Log

▼ Diagnostics

> Ping

> Ping6

> Traceroute

> OAM Loopback

> ADSL Diagnostic

> Diag-Test

Ping6 Diagnostic

Target Address:

Interface:

PING

Figure 4 The following table describes the parameter and button of this page:

Field	Description
Target Address	Enter the valid IP address or domain name.
Interface	Choose a WAN interface.
PING	Click it to start to Ping.

Figure 5

3.8.6.3 Traceroute

Choose **Maintenance > Diagnostic > Traceroute** and the page is shown as the following figure appears. Through this route diagnosis you know the route your PC data takes to another PC on the Internet.

Status

Setup

Advanced

Service

Firewall

Maintenance

Update

Password

Reboot

Time

Log

Diagnostics

> Ping

> Ping6

> Traceroute

> OAM Loopback

> ADSL Diagnostic

> Diag-Test

Traceroute Diagnostic

Host :

NumberOfTries :

3

Timeout :

5000

ms

Datasize :

38

Bytes

DSCP :

0

MaxHopCount :

30

Interface :

any

traceroute

Show Result

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

Field	Description
Host	The address of a destination host to be diagnosed.
NumberOfTries	Repeat times.
Timeout	Timeout duration.
Datasize	Data packet size.
DSCP	A differentiated services code point in the TOS identification byte for service categories in the IP header of every data packet. A DSCP prioritizes by coding values using the used 6-bit bytes and unused 2-bit bytes.
MaxHopCount	Maximum number of routes.
Interface	Select an interface.
Traceroute	Click to start tracing the route.
Show Result	Click to display the result.

3.8.6.4 OAM Loopback

Choose **Maintenance > Diagnostic > OAM Loopback** and the page is shown as the following figure appears. Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

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

Update

Password

Reboot

Time

Log

Diagnostics

Ping

Ping6

Traceroute

OAM Loopback

ADSL Diagnostic

Diag-Test

OAM Fault Management - Connectivity Verification

Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Flow Type:

☒ F5 Segment
☐ F5 End-to-End
☐ F4 Segment
☐ F4 End-to-End

VP:

VC:

Go !

Click **Run Loopback** to start testing.

3.8.6.5 ADSL Statistics

Choose **Maintenance > Diagnostic > ADSL Statistics** and the page is shown as the following figure appears. It is used for ADSL tone diagnostics.

Status
 Setup
 Advanced
 Service
 Firewall
 Maintenance

Update
 Password
 Reboot
 Time
 Log
 Diagnostics
 > Ping
 > Ping6
 > Traceroute
 > OAM Loopback
 > ADSL Diagnostic
 > Diag-Test

Diagnostic ADSL

Adsl Tone Diagnostic

Start

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

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					

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

3.8.6.6 Diag-Test

Choose **Maintenance > Diagnostic > Diag-Test** and the page is shown as the following figure appears. You can test the DSL connection. You can also view the LAN status connection and ADSL connection.

StatusSetupAdvancedServiceFirewallMaintenance

▼ Update

▼ Password

▼ Reboot

▼ Time

▼ Log

> Diagnostics

> Ping

> Ping6

> Traceroute

> OAM Loopback

> ADSL Diagnostic

> Diag-Test

D diagnostic Test

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select the Internet Connection:

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

4 Trouble Shooting

Question	Answer
Why are all the indicators off?	- Check the connection between the power adapter and the power socket. - Check whether the power switch is turned on.
Why is the LAN indicator off?	Check the following: - The connection between the device and your PC, hub or switch. - The running status of the computer, hub, or switch.
Why is the ADSL indicator off?	Check the connection between the Line port of the device and the wall jack.
Why Internet access fails while the ADSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why I fail to access the web configuration page of the DSL router?	Choose Start > Run from the desktop, and ping 192.168.1.1 (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.
How to load the default settings after incorrect configuration?	To restore the factory default settings, turn on the device, and press the reset button for about 3 seconds, and then release it. The default IP address and the subnet mask of the DSL router are 192.168.1.1 and 255.255.255.0 , respectively. - User/password of super user: admin/admin - User/password of common user: user/user