iball Baton®

802.11b/g/n wireless ADSL Router

Model No. DWA-N150Series

N 150M

Ver.: 1.0.0

FCC STATEMENT

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

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

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

Note: This device must be more than 20cm away from human body when using.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Contents

1 Introduction 3
Safety Precautions 4
2 Features 7
3 Hardware Connection 8
3.1 ADSL Connection 8
3.2 Broadband Connection 9
4 Router Configuration 10
4.1 Installation Guide 10
5 Method – II 12
Web Based GUI Configuring 12
5.1 Status 12
5.1.1 Device Information 12
5.1.2 ADSL Info. 15
5.1.3 Statistics 16
5.2 Quick Start 16
5.3 Network Setup 20
5.3.1 WAN 20
5.3.2 LAN 27
5.3.3 Wireless 35
5.4 Advanced Setting 47
5.4.1 Routing 47
5.4.2 NAT 50
5.4.3 QoS 55
5.4.4 TR-069 56
5.4.5 Virtual Port Group 57
5.4.6 Management 59
5.5 Access Management 59
5.5.1 IGMP 59
5.5.2 UPnP 60
5.5.3 SNMP 60
5.5.4 DNS 61
5.5.5 DynDNS 63

5.6 Security Settings 64
5.6.1 MAC Filter 64
5.6.2 IP/Port Filter 64
5.6.3 URL Filter 66
5.6.4 ACL 67
5.6.5 DoS 70

5.7 Maintenance 71
5.7.1 Update 71
5.7.2 Password 72
5.7.3 Restart 73
5.7.4 Time 73
5.7.5 System Log 74
5.7.6 Diagnostics Tools 75

Appendix A: Specifications 80

APPENDIX B: CONTACT DETAILS 79

1 Introduction

150M Wireless-N ADSL2+ & Broadband Router (iB-WRA150N2) is a router for high performance.

Enhanced Wireless transmission speed up to 150Mbps

Complies with IEEE 802.11 b/g/n wireless standards

Dual WAN Router

- ADSL Internet (xDSL): 1 - 10/100M (RJ11) WAN port
- Broaband Internet (Cable / DSL): 1 – 10/100M (RJ45) WAN Port

Wireless On/Off

- Allows users to turn off the wireless function not in use.

WPS (Wi-Fi Protected Setup)

- Automatically establishing WPA2 secure wireless connection LEDs and Interfaces

IPv6 Ready

5dBi Omni Directional Antennas

Package List

The following contents should be found in the product packaging:

- 150M Wireless-N ADSL2+ & Broadband Router
- 5dBi Antenna (Fixed),
- Power Adapter
- Cd & Quick Installation Guide
- RJ45 Patch Cord x 1
- ADSL Splitter x 1 & RJ11 Patch cord x 2

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your nearest dealer

Safety Precautions

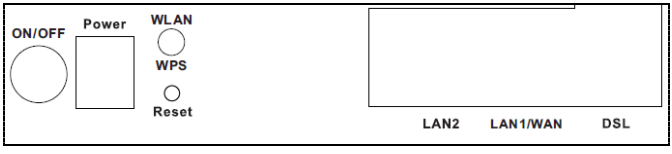
Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use the power adapter in the package.
- 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 should be left to avoid damage caused by overheating to the device. Do not cover the holes on the device which are designed for heat dissipation.
- Do not put this device close to heat sources or high temperature place.
- Do not expose the device to direct sunshine.
- Do not put this device close to an over damp place.

LED

LEDs	Color	Status	Description
Power	Red	On	The device is initializing.
DSL	Green	On	The DSL line is established.
		Blinking	The DSL Line is training.
		Off	No DSL signal.
Internet	Green	On	The Internet connection is normal in the routing mode (for example: PPP dial-up is successful), and no Internet data is being transmitted.
		Blinking	Internet data is being transmitted in the routing mode.
		Off	The device is in the bridge mode.
	Red	On	The device is initializing.
LAN1/2, LAN1/WAN	Green	On	The connection is normal and activated.
		Blinking	Data is being transmitted in the Broadband WAN.
		Off	The interface is not connected.
Wireless	Blue	On	Wireless connection has been activated.
		Blinking	Wireless data is being transmitted.
		Off	The Wireless connection is not activated.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blinking	WPS is enabled and the device is waiting for client to negotiate.
		Off	WPS is disabled.

Rear Panel



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

Interface	Description
ON/OFF	Power switch, power on or power off the device.
Power	Power interface, for connecting to the power adapter.
Wireless / WPS	● Press the button and hold it for 1 second to 5 seconds, to enable Wireless. ● Press the button and hold it for more than 5 seconds, to enable WPS function.
Reset	Reset to the factory default configuration. Keep the device powered on, and insert a needle into the hole for 3 seconds, then release it. The device is reset to the factory default configuration.
LAN1/2	RJ-45 interface, for connecting to the Ethernet interface of a PC or the Ethernet device through Ethernet cable.
LAN1/WAN	This Ethernet RJ-45 interface has two functions. ● Worked as a WAN interface that connects to the WAN for Broadband connection. ● Worked as a LAN interface that connects to the LAN port of the computer.
ADSL	RJ-11 interface, for connecting to the DSL interface or a splitter through a telephone cable for connection.

2 Features

- Complies with IEE802.3 & IEEE802.3u standards
- Complies with IEEE 802.11b/g/n standards
- **3-in-1**: 2-10/100M Auto-Negotiation (RJ45) Ethernet ports & 1-RJ11 (Internet) LINE port supporting Auto MDI/MDIX and Wireless-N Access Point
- Latest standards with downstream data rates up to 24Mbps, upstream data rates up to 3.5Mbps (With Annex M enabled).
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security
- Multi-SSID Security
- AP Isolation and wireless schedule
- IPv6 Ready
- Wi-Fi Button - Allows users to turn off the
- Wireless MAC filtering & DHCP Server
- Built-in firewall, supporting IP/MAC filter, Application filter and URL filter.
- Virtual Server, DMZ host and IP Address Mapping.
- Dynamic DNS, UPnP and Static Routing.
- With SNMP & DHCP server.
- 5-dBi Omni-Directional Antenna type.

3 Hardware Connection

3.1 ADSL Connection

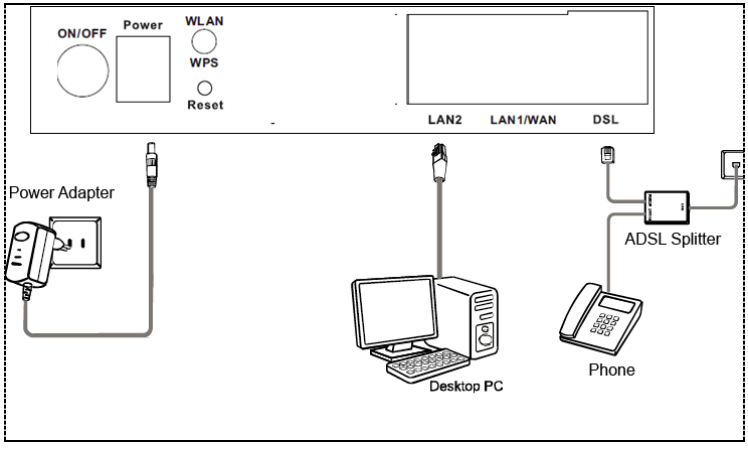
Method-I : Plug one end of the twisted-pair ADSL cable into the LINE port on the rear panel of iB-WRA150N2, and insert the other end into the wall socket.

Method-II: You can use a ADSL splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

1) Connect the Ethernet cable. Attach one end of a network cable to your computer's LAN port or a regular hub/switch port, and the other end to the LAN port on the iB-WRA150N2. (If you have the wireless NIC and want to use wireless connector, you can skip the connection of LAN port.)

2) Power on the computers and LAN devices.

3) Configure the ADSL connection in the router as per your ISP settings available from your ISP.

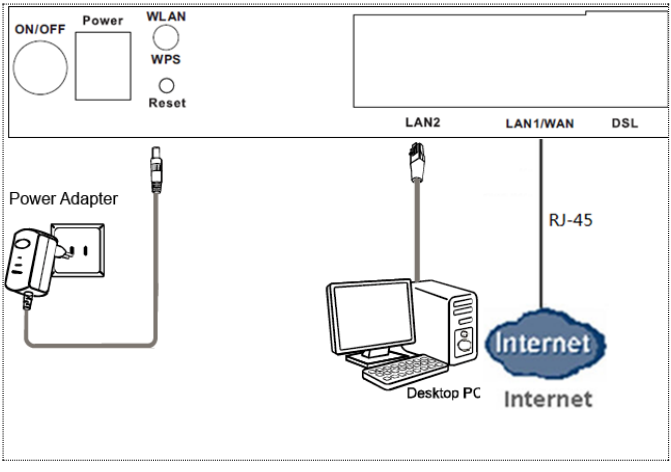


3.2 Broadband Connection

1) Connect the LAN Port of the Router to your PC with RJ45 Ethernet cable.

2) Connect the ISP RJ45 LAN Cable (Internet Link) to **LAN1/WAN** Port of the Router

3) Connect the power adapter to **Power** interface of the device.



4 Router Configuration

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

TCP / IP Network Setting

Step 1 **Choose Start > Control Panel > Network and Internet > Network and Sharing Center**

Step 2 Choose **Change Adapter Settings** > **Local Area Connection**. Right-click **Local Area Connection**, and choose **Properties**.

Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then click **OK**.
If you select **Use the following IP address**, set IP address of the PC as 192.168.1.X (2~254)
subnet mask as 255. 255.255.0, and enter DNS server provided by your ISP.

4.1 Installation Guide

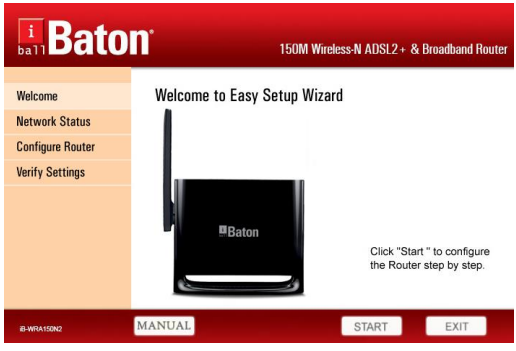
You can configure the router either with Web GUI menu or Easy Setup Wizard Utility

Method – I

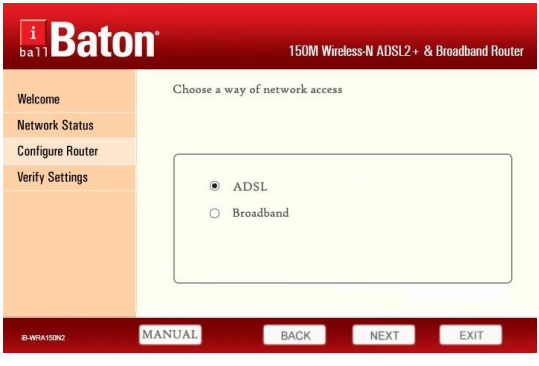
Configuring the Router via Easy Setup Wizard (Resource CD)

The **Easy Setup Wizard** will automatically pop up on the computer's screen.

Click on **Start** to start the Easy Setup Wizard.



Select Intenet connection type **ADSL or Broadband** as your ISP connection and click **Next**



Select the proper Connection type & provide the details of user name and password as provided from our ISP.

cL

5 Method – II

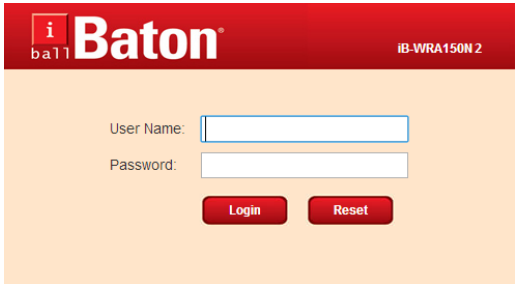
Web Based GUI Configuring

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

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

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

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



5.1 Status

5.1.1 Device Information

If you log in as a super user, the **ADSL Router Status** page shown in the following figure appears. In this page, you can view the following information: system, ADSL Status, TR-069 status, LAN configuration, DNS status, ADSL WAN Interfaces, ADSL WAN IPv6 configuration, Broadband WAN Interfaces, and Broadband WAN IPV6 Status.

In this page, click **connect button** to connect to Internet. If there is no preset WAN interface, refer **4.5.1 WAN** to do corresponding configuration.

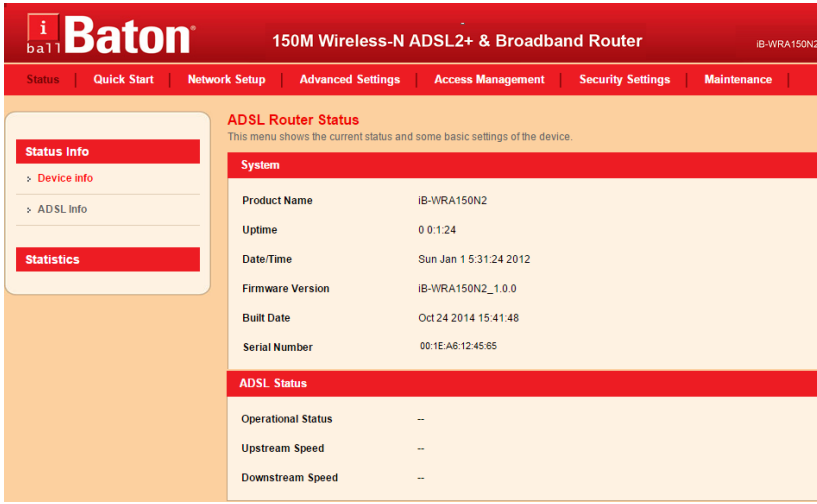


Figure 1 Status – 1

Figure 2 Status - 2

ADSL WAN Interfaces

Interface	VPI/VCI	Encap	AppMode	Droute	Protocol	IP Address	Gateway	Status
pppoe1	0/35	LLC	INTERNET	On	PPPoE	0.0.0.0	0.0.0.0	Down 0 0:0:0 /0 0:0:0 Connect
WAN1	8/77	LLC	TR069	Off	IPoE	0.0.0.0	0.0.0.0	Down

ADSL WAN IPV6 Configuration

Interface	VPI/VCI	Encap	AppMode	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status
pppoe1	0/35	LLC	INTERNET	PPPoE					Down
WAN1	8/77	LLC	TR069	IPoE					Down

Broadband WAN Interfaces

Interface	AppMode	Droute	Protocol	IP Address	Gateway	Status

Broadband WAN IPv6 Status

Interface	AppMode	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status

Refresh

Figure 3 Status – 3

5.1.2 ADSL Info.

Choose **Status** > **Status info** > **ADSL Info** and the following page appears. In this page, you can view information of ADSL configuration.

ADSL Configuration

This menu 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	iBall Baton
Firmware Version	4926dc02
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

5.1.3 Statistics

Choose **Status** > **Statistics** > **Statistics** and the following page appears. In this page, you can view statistics information.

Statistics

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

Statistics:

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
lan1	0	0	0	0	0	0
lan2	0	0	0	0	0	0
lan3	6967	0	0	3001	0	0
lan4	0	0	0	0	0	0
pppoe1	0	0	0	0	0	0
WAN1	0	0	0	0	0	0
w1	151132	0	0	1872	0	23868
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0
w6	0	0	0	0	0	0
w7	0	0	0	0	0	0
w8	0	0	0	0	0	0
w9	0	0	0	0	0	0
w10	0	0	0	0	0	0
w11	0	0	0	0	0	0
w12	0	0	0	0	0	0
w13	0	0	0	0	0	0

Refresh

5.2 Quick Start

The **Quick start** page guides fast and accurate configuration of the Internet connection and other important parameters. In the navigation bar, click **Quick Start**. The page as shown in the following figure appears.

Step 1 WAN connection setting

In following page, enter VPI and VCI provided by your Internet service provider (ISP). In this example, select **PPPoE** as connection mode. And then enter PPP username and password provided by your Internet service provider (ISP).

Quick Wizard

The Quick Start will guide you to configure the router step by step.
Step 1: WAN Settings
Step 2: Wireless Settings
Step 3: Save Setting

Step 1: WAN Settings: Please select the wan connection mode

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

Encapsulation: ◉ LLC/SNAP ○ VC-Mux

Connection Mode:
○ Bridge
◉ PPPoE
○ IPoE
○ PPPoA
○ 1483 Routed

IP Protocol: IPv4/IPv6

VLAN (802.1q) ○ Enable ◉ Disable

VLAN ID(1-4095):

PPP Settings: Username: Password:

Default Route: ◉ Enable ○ Disable

DNS Settings:
◉ Set DNS Automatically
○ Set DNS Manually :

Next

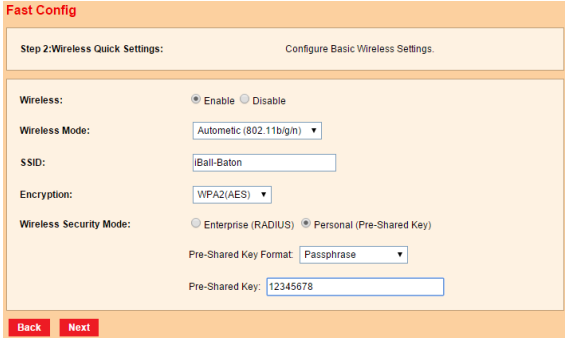
The following table describes the parameters in this page:

Field	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP.
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.
Encapsulation	You can select **LLC/SNAP** or **VC-Mux**. In this example, the encapsulation mode is set to **LLC/SNAP**.
Connection Mode	There are five WAN connection types: **PPPoA**, **PPPoE**, **IPoE**, **1483 Routed**, and **Bridge**. ● PPPoE/PPPoA: Need to enter PPP username and password provided by your ISP. ● IPoE/1483 Routed: You can select **Attain IP Automatically** or **IP Manually**. ● Bridge: You need to dial-up on PC to connect to the Internet.
IP Protocol	You can select it from drop-down list: Ipv4 Ipv4/Ipv6 Ipv4 Ipv6
Default Route	Enable or disable it.
DNS Settings	You can select **Set DNS Automatically** or **Set DNS Manually**. If you select **Set DNS Manually**, enter DNS server provided by your ISP.

For other entries which are not mentioned above, you can keep them as defaults.

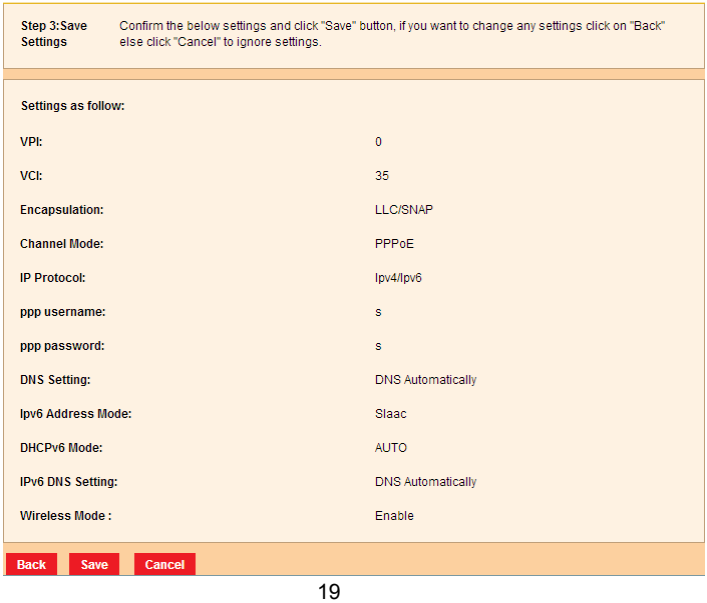
Step 2 Wireless Quick settings

In following page, you can select wireless band, set SSID and encryption. For wireless security, it is recommended to set the encryption mode to WPA2, and then enter a password.



Step 3 Save settings

If you want to finish setting, click **Save**. Otherwise click **Cancel**.



5.3 Network Setup

5.3.1 WAN

Choose **Network Setup** > **WAN**. The **WAN** page that is displayed contains **WAN**, **3G**, **Auto PVC**, **ATM**, and **ADSL**.

WAN

Choose **Network Setup** > **WAN** > **WAN**, the page shown in the following figure appears. In this page, you can add or configure WAN interface of your router.

The following table describes the parameters of this page:

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

Field	Description
	● When **Fixed IP** is selected, you should enter the local IP address, remote IP address and subnet mask. ● When **DHCP** is selected, the router is a DHCP client and the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Unnumbered	Select this checkbox to enable IP unnumbered function.
Add	After configuring the parameters of this page, click it to add a new PVC into the **Current ATM VC Table**.
Modify	Select a PVC from the **Current ATM VC Table**, then modify the parameters of this PVC. After setting, click it to apply the settings of this PVC.
	Click it, the **PPP Interface-Modify** appears. You can modify the PVCs' parameters.

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

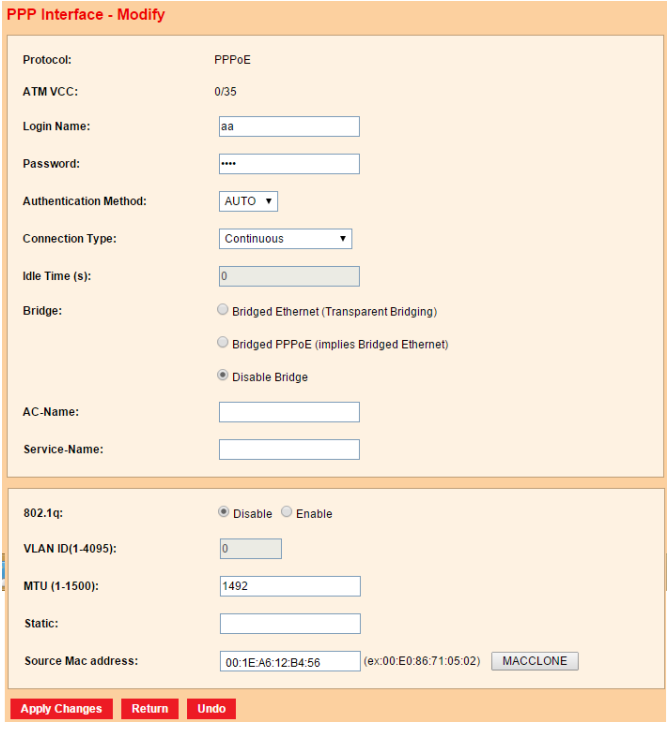


Figure 4

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

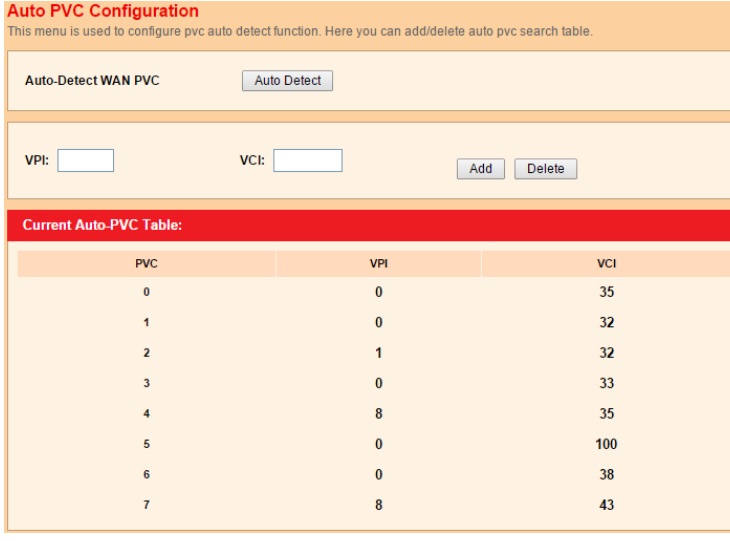
Field	Description
Protocol	It displays the protocol type used for this WAN connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication	You can choose **AUTO**,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

Field	Description
Method	
Connection Type	You can choose **Continuous**, **Connect on Demand**, or **Manual**.
Idle Time (s)	If choose **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
Bridge	You can select **Bridged Ethernet**, **Bridged PPPoE**, or **Disable Bridge**.
AC-Name	The accessed equipment type.
Service-Name	The service name.
VLAN	You can select **Disable** or **Enable**. After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
MTU	Maximum Transmission Unit. Sometimes you must modify this function to access network successfully.
Static	If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Source Mac address	The MAC address you want to clone.
MACCLONE	Click it to enable the MAC Clone function with the MAC address that is configured.

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

Auto PVC

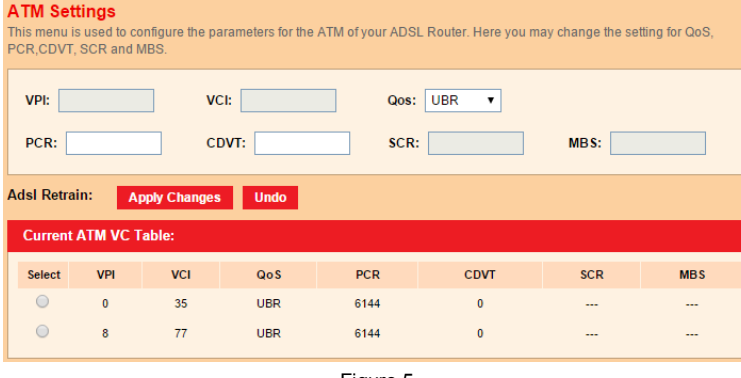
Choose **Network Setup** > **WAN** > **Auto PVC**, the page shown in the following figure appears. This page is used to configure PVC auto detect function, you can add or delete auto-pvc.



PVC	VPI	VCI
0	0	35
1	0	32
2	1	32
3	0	33
4	8	35
5	0	100
6	0	38
7	8	43

ATM Settings

Choose **Network Setup** > **WAN** > **ATM**, the page shown in the following figure appears. In this page, you can configure the parameters of the ATM, including QoS, PCR, CDVT, SCR, and MBS.



Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	0	35	UBR	6144	0	---	---
○	8	77	UBR	6144	0	---	---

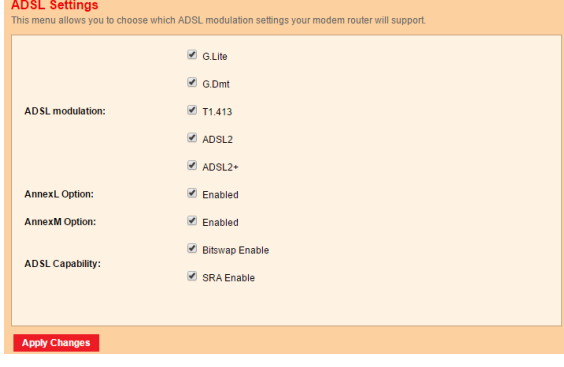
Figure 5

The following table describes the parameters of this page:

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose **UBR**, **CBR**, **rt-VBR**, or **nrt-VBR**.
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to 4294967295.
SCR	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.

ADSL Settings

Choose **Network Setup** > **WAN** > **ADSL**, the page shown in the following figure appears. In this page, you can select the DSL modulation. Mostly, you need to remain this factory default settings. The router negotiates the modulation modes with the DSLAM.

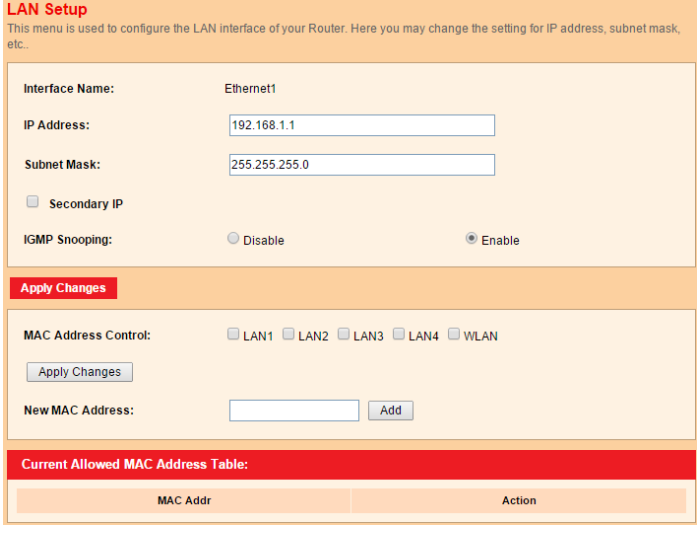


5.3.2 LAN

Choose **Network Setup** > **LAN**. The **LAN** page that is displayed contains **LAN**, **DHCP**, **DHCP Static**, and **LAN IPv6**.

IP Address

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



The following table describes the parameters of this page:

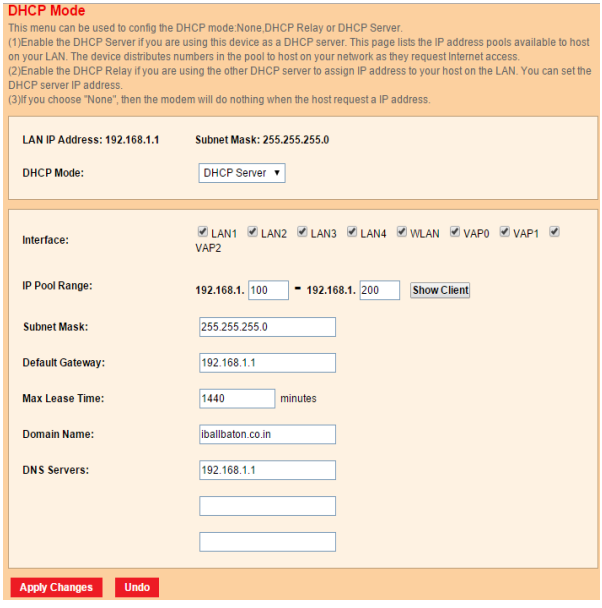
Field	Description
IP Address	Enter the IP address of LAN interface. It is recommended to enter an address ranged from 192.168.1.1 - 192.168.255.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in the different network segment.

Field	Description
IGMP Snooping	IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Only identified Multicast traffic will be forwarded to ports.
MAC Address Control	It is the access control based on MAC address. The designated LAN port, only for the **Current Allowed MAC Address** to access.
New MAC Address	Enter MAC address, and then click **Add** to add a new MAC address.

DHCP

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

Choose **Network Setup** > **LAN** > **DHCP**, the page shown in the following figure appears.

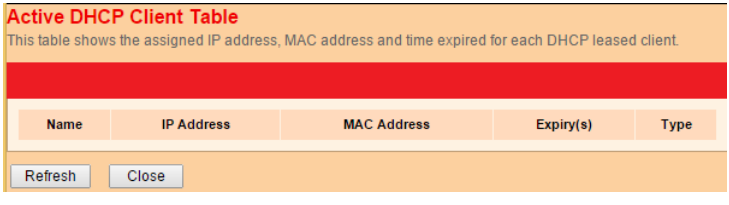


The following table describes the parameters of this page:

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

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

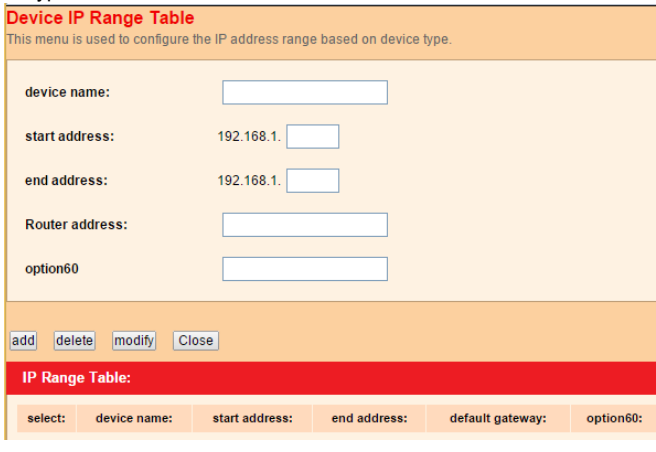


The following table describes the parameters and buttons in this page:

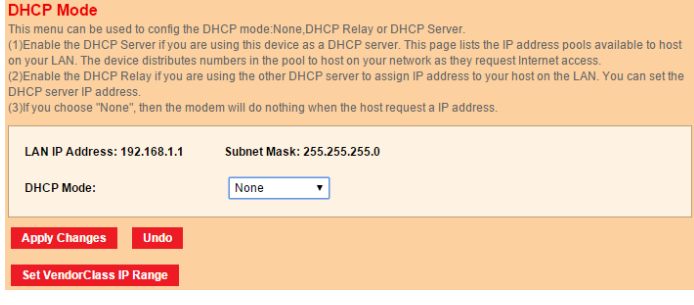
Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, 00-A0-C5-00-02-12.

Field	Description
Expired (s)	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

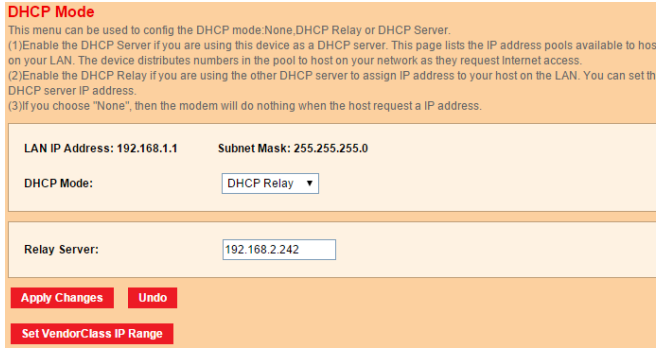
Click **Set VendorClass IP Range** in the **DHCP Mode** page, the page as shown in the following figure appears. In this page, you can configure the IP address range based on the device type.



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



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

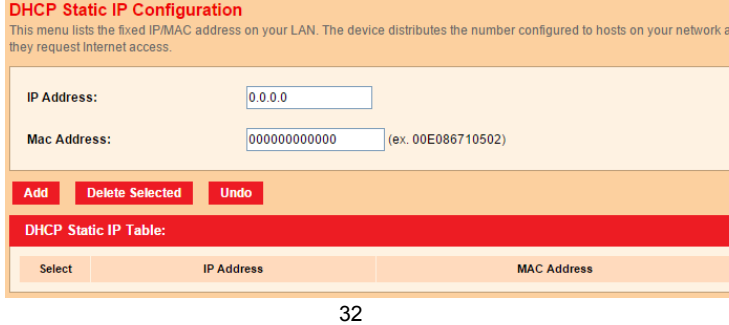


The following table describes the parameters and buttons of this page:

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

DHCP Static

Choose **Network Setup** > **LAN** > **DHCP Static IP**, the page shown in the following figure appears. You can assign the IP addresses on the LAN to the specific individual PCs based on their MAC address.



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

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

LAN IPv6

Choose **Network Setup** > **LAN** > **LAN IPv6**, the page shown in the following figure appears.

LAN IPv6 Setting

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

Lan Global Address Setting

Global Address: /

Apply Changes

RA Setting

Enable: ☑

M Flag: ☐

O Flag: ☑

Max Interval: 600 Secs

Min Interval: 200 Secs

Prefix Mode: Auto

ULA Enable: ☐

RA DNS Enable: ☐

Apply Changes

DHCPv6 Setting

DHCPv6 Mode: Auto Mode

IPv6 Address Suffix Pool: ::1 - ::ffff (ex. ::1:1:1:1 or ::1)

IPv6 DNS Mode: Auto

Apply Changes

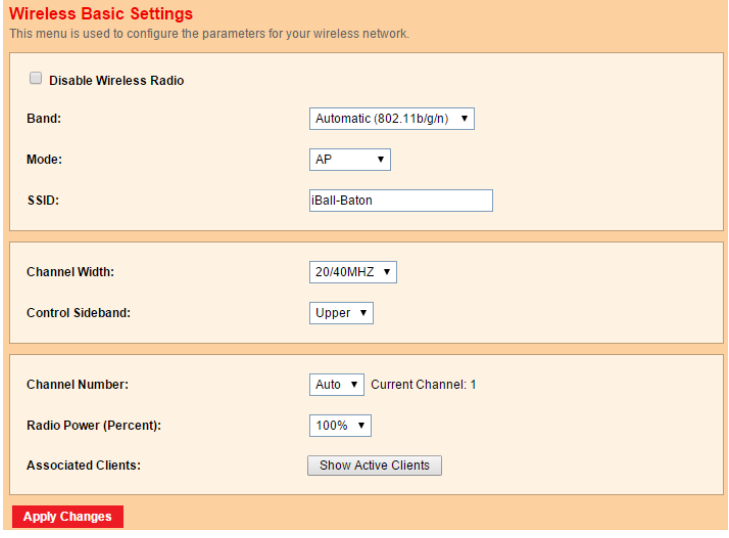
The following table describes the parameters of this page.

Field	Description
Global Address	Specify the LAN global ipv6 address. It can be assigned by ISP.
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “Other configuration” flag in RA packet.
Prefix Mode	Specify the RA feature prefix mode: “Auto”: the RA prefix will use WAN dhcp-pd prefix; “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.

5.3.3 Wireless

Wireless Basic Settings

Choose **Network Setup** > **Wireless** > **Basic Settings**, the page shown in the following figure appears. In this page, you can configure the parameters for wireless LAN clients that may connect to the modem.



The following table describes the parameters of this page:

Field	Description
Band	Choose the adapted band of the modem from the drop-down list. Automatic (802.11b/g/n) 11Mbps (802.11b) 54Mbps (802.11g) Mixed Mode (802.11b/g) 300Mbps (802.11n) 300Mbps (802.11n/g) Automatic (802.11b/g/n)
Mode	Set the working mode of the device. The mode may vary from software to software. By default, the network mode of the modem is **AP**.
SSID	Set a name for the wireless network of your device. Wireless stations associating to the modem must have the same SSID.
Channel Width	You can select **20MHZ**, **40MHZ or 20/40MHZ**.
Control Sideband	Only when choose **40MHZ** for Channel Width, you

Field	Description
	can set this parameter. You can choose **Upper** or **Lower** from the drop-down list.
Channel Number	A channel is the radio frequency used by 802.11b/g/n wireless devices. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap. Choose a channel from the drop-down list box.
Radio Power	Choose the transmission power of the radio signal. It is recommended to leave the default setting. The default setting is **100%**.
Show Active Clients	Click it to view the information of the wireless clients that are connected to the modem.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

Wireless Security

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

The following table describes the parameters of this page:

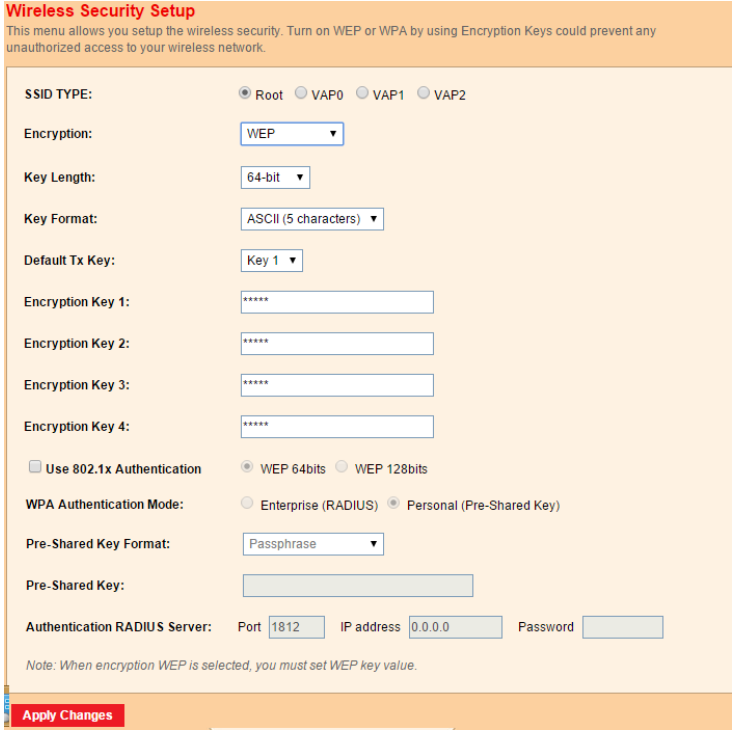
Field	Description
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)**, or **WPA2 Mixed**. ● Wired equivalent privacy (**WEP**) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (**WPA**) is a subset of the IEEE802.11i security specification draft. ● **WPA2 Mixed** is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA Authentication Mode	● Select **Personal (Pre-Shared Key)**, enter the pre-shared key in the **Pre-Shared Key** field.

Field	Description
	● Select **Enterprise (RADIUS)**, enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem. If the encryption is set to **WEP**, the modem uses 802.1 X authentication, which is Radius authentication.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

Set the **Encryption** to be **WEP**, then click **Set WEP Key**, and the following page appears.

Note:

If the encryption is set to be **WEP**, the WPS function will be disabled.



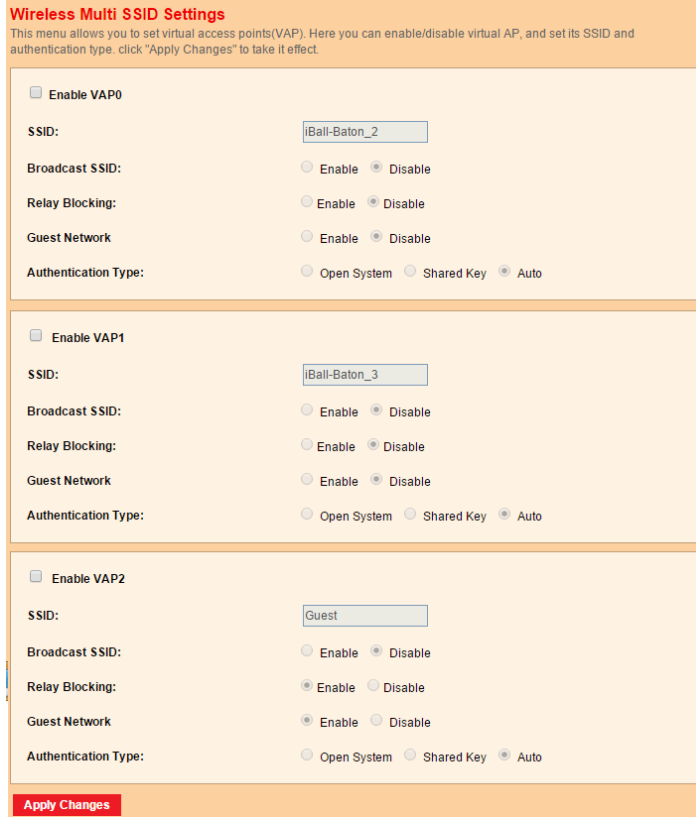
The following describes the parameters of this page:

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

Field	Description
	same encryption key for data transmission. ● If you choose **64-bit** and **ASCII (5 characters)**, enter any 5 ASCII characters. ● If you choose **64-bit** and **Hex (10 characters)**, enter any 10 hexadecimal characters. ● If you choose **128-bit** and **ASCII (13 characters)**, enter any 13 ASCII characters. ● If you choose **128-bit** and **Hex (26 characters)**, enter any 26 hexadecimal characters.

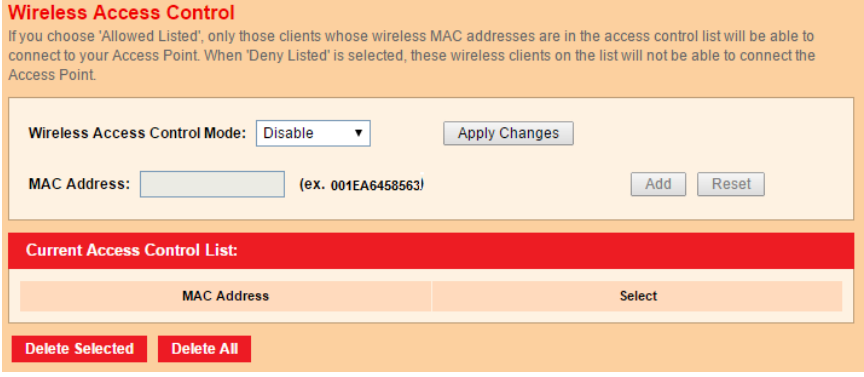
Multi SSID

Choose **Network Setup > Wireless** > **Multi SSID** and the following page appears. This page allows you to set virtual access points (VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click **Apply Changes** to take it effect.



MAC Filtering

Choose **Network Setup > Wireless** > **MAC Filtering** and the following page appears. If you choose **Allow Listed**, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When **Deny Listed** is selected, these wireless clients on the list will not be able to connect the Access Point.



Advanced

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

The following table describes parameters in this page:

Field	Description
Fragmentation Threshold (256-2346)	Set the threshold of fragmentation length. If the length of a packet is greater than the value, the packet is automatically fragmented into several packets. Because too many packets lead to low performance of the wireless network, the value of **Fragmentation Length** cannot be too small. The default value is 2346.
RTS Threshold	Set the CTS/RTS threshold. If the length of a packet is greater than the value, the router sends an RTS frame to the destination station to negotiate. After receiving the RTS frame, the wireless station responds with a Clear to Send (CTS) frame to the router, indicating that they can communicate with each other. The default value is 2346.

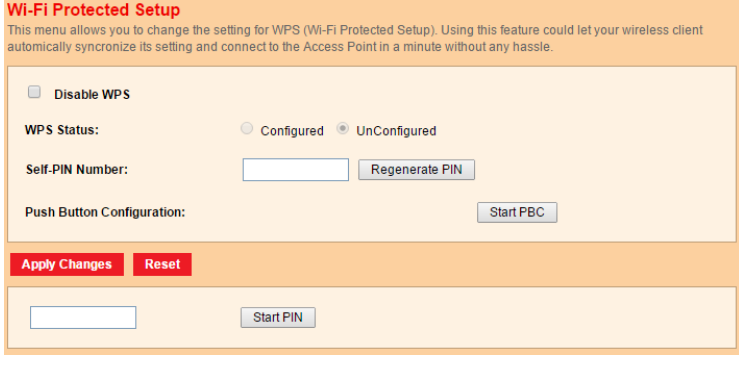
Field	Description
Data Rate	Choose the transmission rate of the wireless data from the dropdown list.
PreambleType	● **Long Preamble**: It means this card always use long preamble. ● **Short Preamble:** It means this card can support short preamble capability.
Broadcast SSID	Select whether the modem broadcasts SSID or not. You can select **Enable** or **Disable**. ● Select **Enable,** the SSID can be detected. ● Select **Disable** to hide SSID, the wireless clients cannot find the SSID. You need to enter the SSID and password of the wireless network manually.
Relay Blocking	Wireless isolation. Select **Enable**, the wireless clients that are connected to the modem cannot intercommunication.
Ethernet to Wireless Blocking	Whether the wireless network can communicate with the Ethernet network or not.
Wifi Multicast to Unicast	Enable or disable it. Multicast to unicast conversion to provide reliable transmission and reduce the loss and delay, which is necessary for multimedia applications.
Aggregation	Enable or disable it. Aggregation is a feature of the 802.11n wireless LAN standards that increases throughput by sending two or more data framesin a single transmission.
Short GI	Enable or disable it. GI is guard interval that is used to ensure that distinct transmissions do not interfere with one another. Short GI is 0.4 μs guard interval. The short guard interval results in a higher packet error rate when the delay spread of the channel exceed the guard interval and/or if timing synchronization between the transmitter and receiver is not precise.

Field	Description
WMM	Enable or disable it. WMM is a Wi-Fi Alliance interoperability certification, based on the IEEE802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for well defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones.

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

WPS

Choose **Network Setup** > **Wireless** > **WPS** and the following page appears.



There are two ways for the wireless client to establish the connection with the device through WPS.

The Device Generates PIN: Click **Regenerate PIN** to generate a new PIN, and then click **Start PBC**. In the wireless client tool, enter the PIN generated by the modem, and then start connection. The client will automatically establish the connection with the modem through the encryption mode, and you need not to enter the key.

The Wireless Client Generates PIN: Enter a PIN of the wireless client in the field, and then click **Start PIN** to establish the connection.

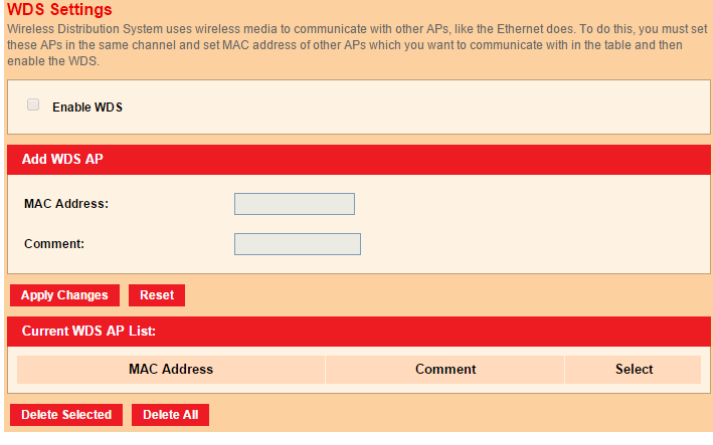
Note:

The wireless client is not able to establish the connection with iB-WRA150N2 through WPS negotiation unless it supports WPS.

WDS

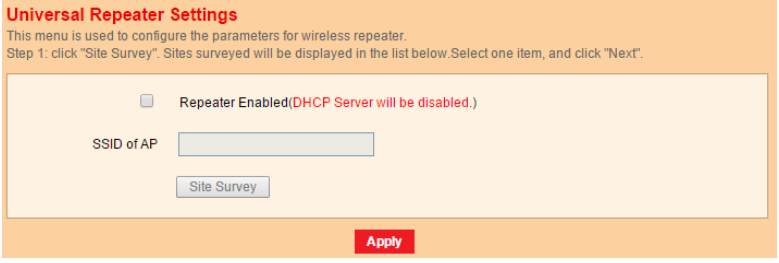
Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of wired backbone network. This function is also called wireless repeating or bridging.

Choose **Network Setup** > **Wireless** > **WDS** and the following page appears. In this page, you can enable WDS function and set ralative parameters.



Universal Repeater

Choose **Network Setup** > **Wireless** > Universal **Repeater** and the following page appears. In this page, you can set parameters for wireless repeater.



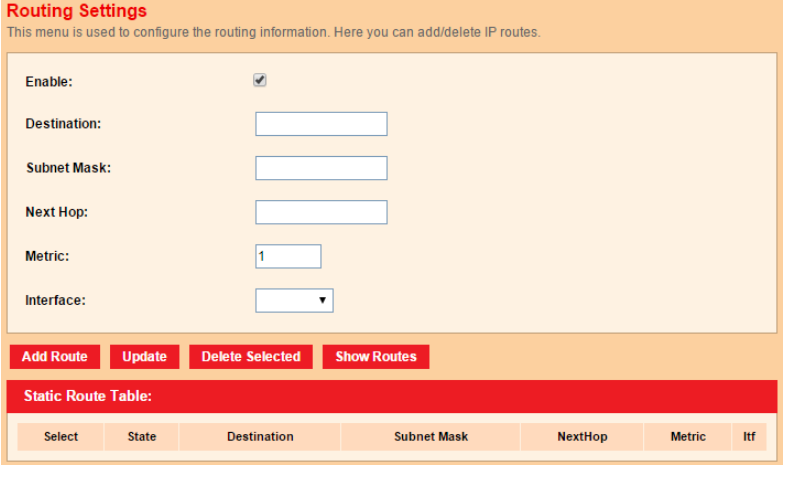
5.4 Advanced Setting

In the navigation bar, click **Advanced**. The **Advanced Settings** page that is displayed contains **Route**, **NAT**, **QoS**, **TR-069**, **Virtual Port Group, and Management.**

5.4.1 Routing

Static Route

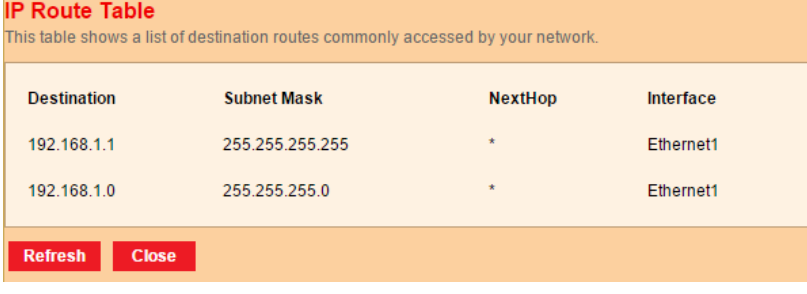
Choose Advanced Settings > **Routing** > **Static Route**, and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



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

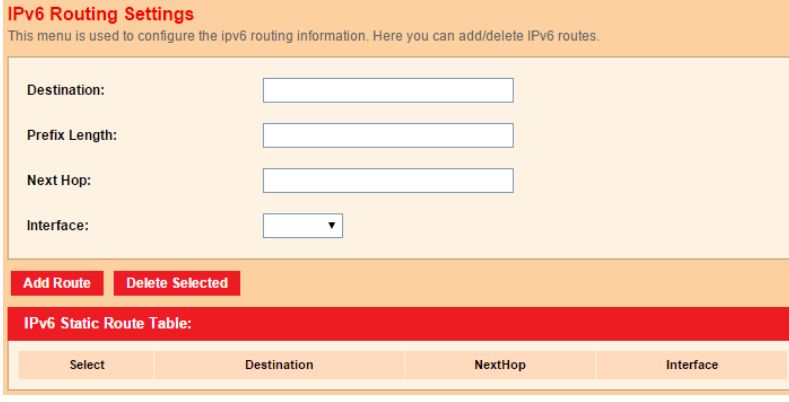
Field	Description
Enable	Select it to use static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the 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.
Delete Selected	Select a row in the **Static Route Table** and click it to delete the row.
Show Routes	Click it, the **IP Route Table** appears. You can view a list of destination routes commonly accessed by your network.
Static Route Table	A list of the previously configured static IP routes.

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



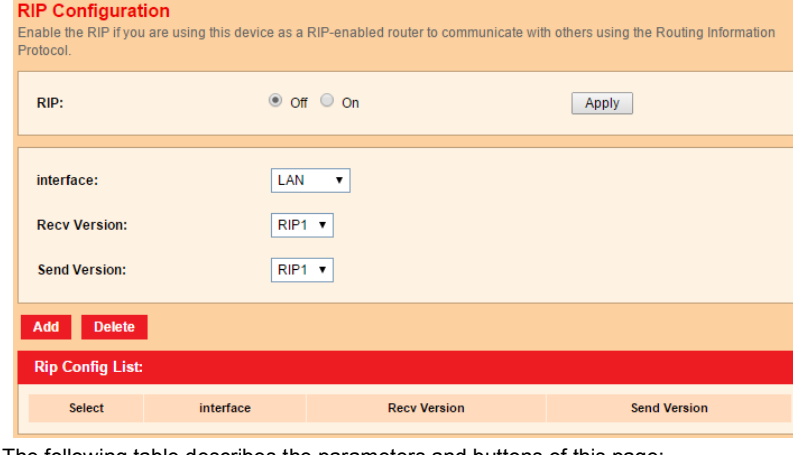
IPv6 Static Route

Choose Advanced Settings > **Routing** > **IPv6 Static Route**, and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



RIP

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



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

Field	Description
RIP	Select **Enable**, the router communicates with other

Field	Description
	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**. ● 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.

5.4.2 NAT

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, SMTP (e-mail) servers and DNS servers.

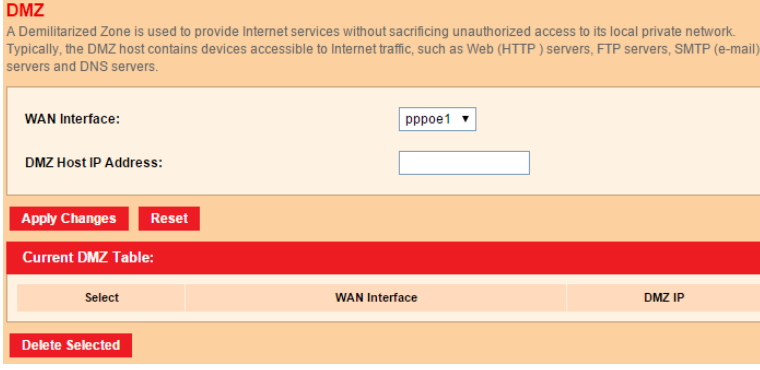
Choose Advanced Settings > **NAT** > **DMZ**, the page shown in the following figure appears.

The following describes how to configure manual DMZ.

Step 1 Select WAN interface.

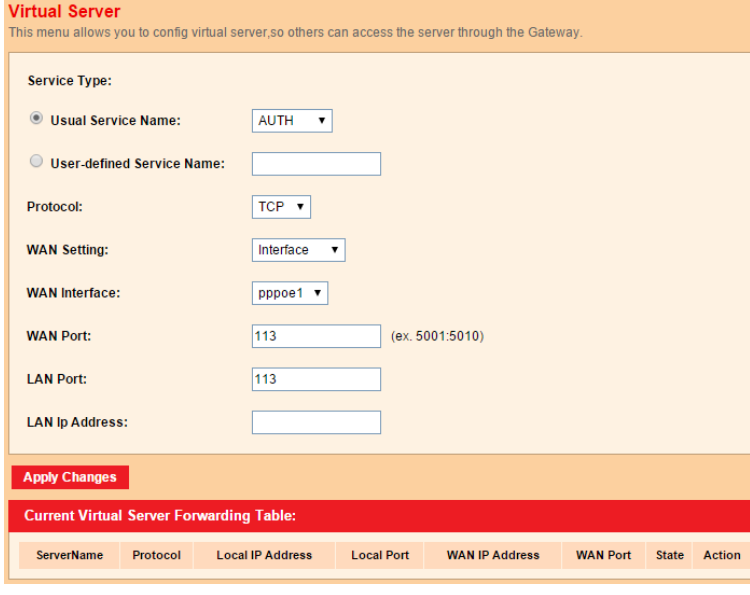
Step 2 Enter an IP address of the DMZ host.

Step 3 Click **Apply Changes** to save the settings of this page temporarily.



Virtual Server

Choose Advanced Settings > **NAT** > **Virtual Service**, and the page shown in the following figure appears.

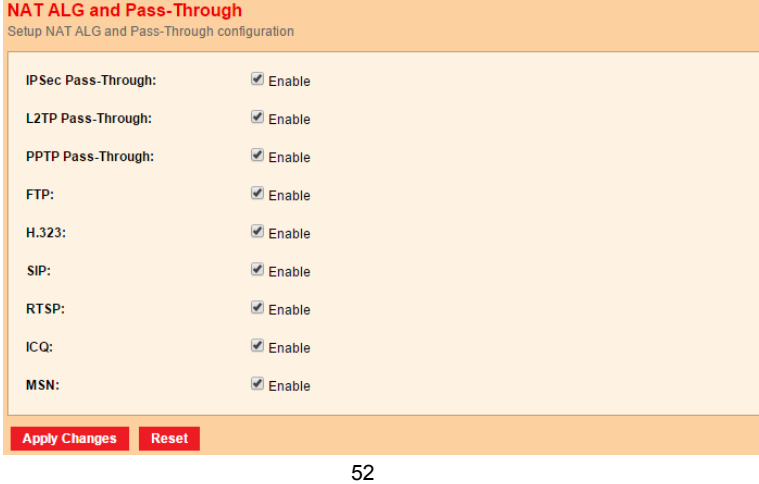


The following table describes the parameters of this page.

Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS** . You can also define a service name. ● If you select **Usual Service Name**, the corresponding parameter has the default settings. ● If you select **User-defined Service Name**, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose **TCP** or **UDP**.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the WAN interface that will apply virtual server.
WAN Port	Choose the access port on the WAN.
LAN 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.

ALG

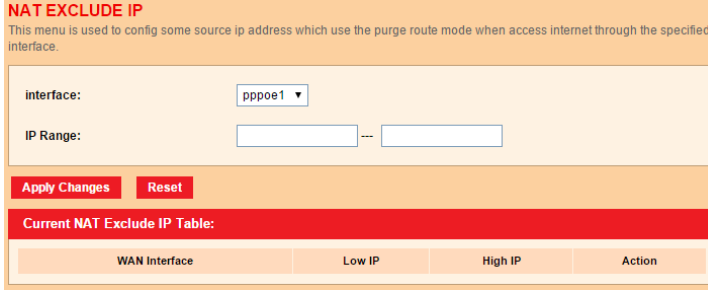
Choose Advanced S**ettings** > **NAT** > **ALG**, and the page shown in the following figure appears. Choose the NAT ALG and Pass-Through options, and then click **Apply Changes**.



NAT Exclude IP

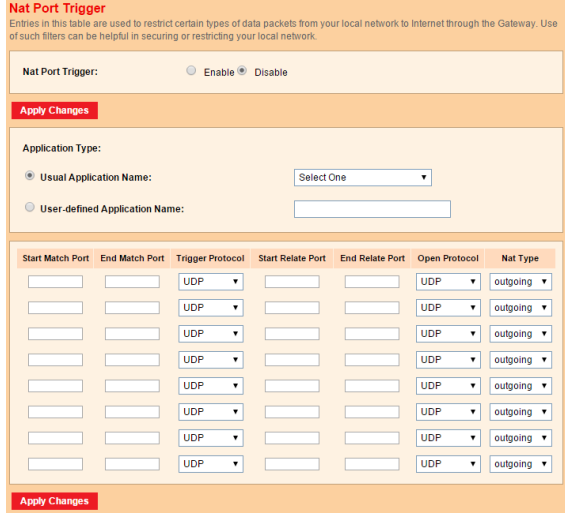
Choose Advanced **Settings**> **NAT** > **NAT Exclude IP**, and the page shown in the following figure appears.

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



Port Trigger

Choose Advanced Settings > **NAT** > **Port Trigger** and the page shown in the following figure appears.



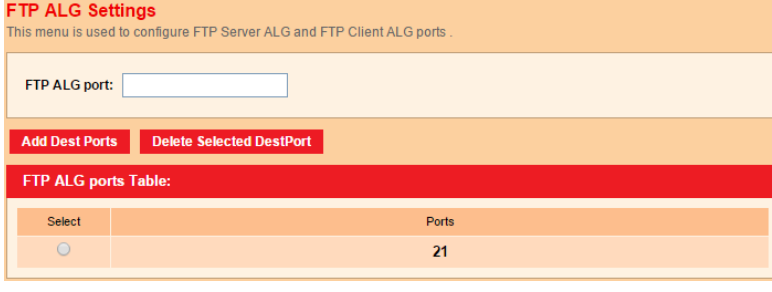
Click the **Usual Application Name** drop-down menu to choose the application you want to Setup for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

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

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

FTP ALG Port

Choose Advanced **Settings** > **NAT** > **FTP ALG Port**, the page shown in 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 FTP server 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 an FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected DestPort	Delete a selected port configuration from the list.

Nat IP Mapping

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

Choose Advanced Settings > **NAT** > **Nat IP Mapping**, the page shown in the following figure appears

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

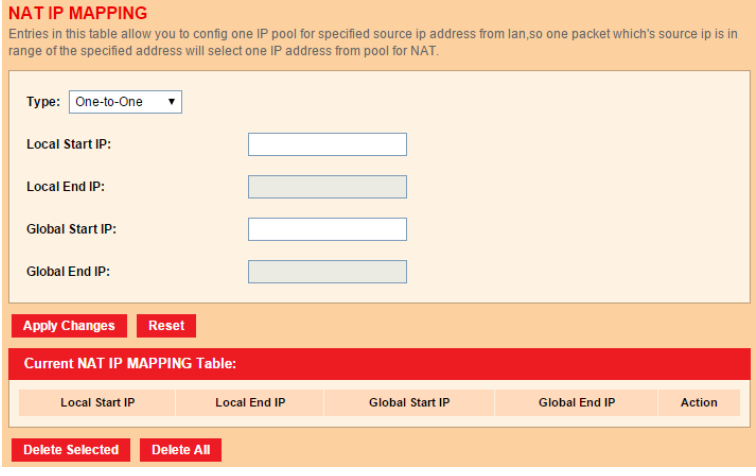


Figure 6

5.4.3 QoS

Choose Advanced Settings > **QoS** to display the submenus. You can select **QoS** or **Traffic Shaping** to do relevant settings.

5.4.4 TR-069

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

TR-069 Configuration

This menu 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: 300 seconds

Connection Request:

User Name:

Password:

Path: /tr069

Port: 7547

Debug:

ACS Certificates CPE: ◉ No ○ Yes

Show Message: ◉ Disable ○ Enable

CPE Sends GetRPC: ◉ Disable ○ Enable

Skip MReboot: ◉ Disable ○ Enable

Delay: ○ Disable ◉ Enable

Auto-Execution: ○ Disable ◉ Enable

Apply Changes | Reset

Certificate Management:

CPE Certificate Password: client | Apply | Undo

CPE Certificate: Choose File | No file chosen | Upload | Delete

CA Certificate: Choose File | No file chosen | 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.
Debug	
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable**, the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.

5.4.5 Virtual Port Group

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

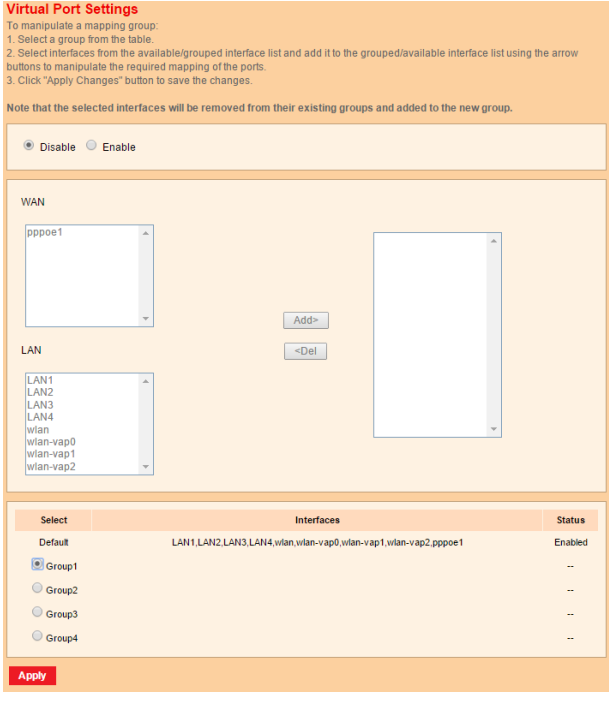


Figure 7

The procedure for manipulating a mapping group is as follows:

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

Step 2 Select a group from the table.

Step 3 Select interfaces from the WAN and LAN interface list and add them to the grouped interface list using the arrow buttons to manipulate the required mapping of the ports.

Click **Apply** to save the changes.

5.4.6 Management

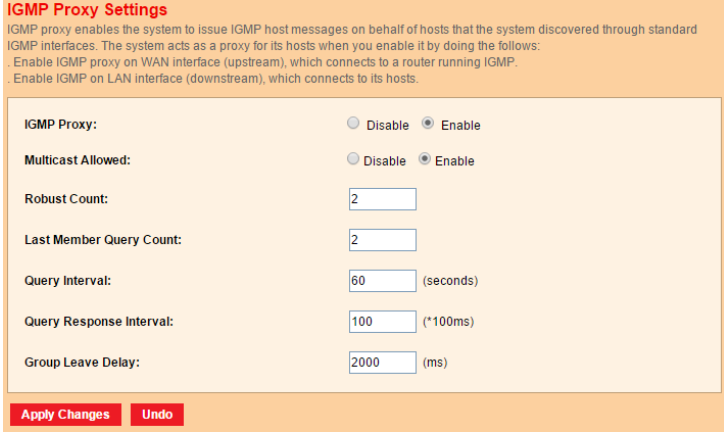
Choose Advanced Settings > **M**anagement to display the submenus. You can select **Bridge Setting**, **Client Limit**, **Tunnel**, or Half Bridge to set relevant parameters.

5.5 Access Management

5.5.1 IGMP

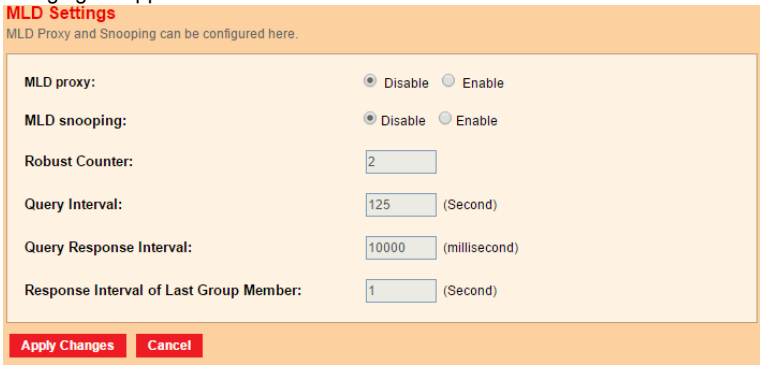
IGMP Proxy

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



MLD

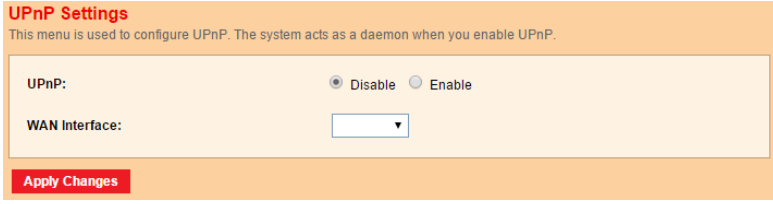
Choose **Access Management** > **IGMP** > **IGMP Proxy**, and the page shown in the following figure appears.



5.5.2 UPnP

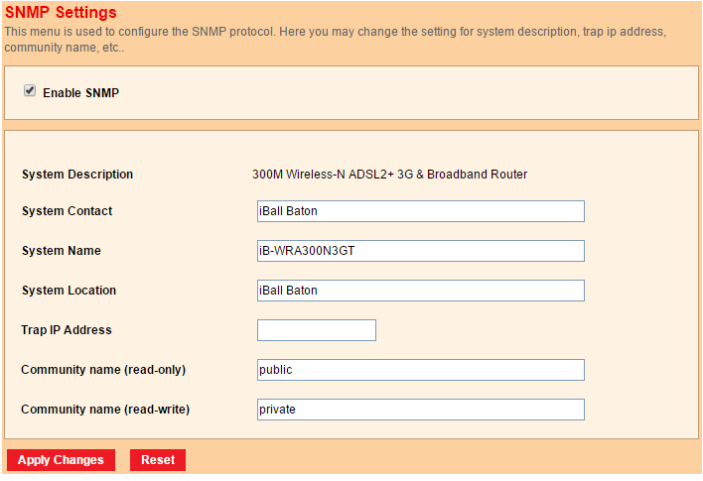
UPnP

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



5.5.3 SNMP

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



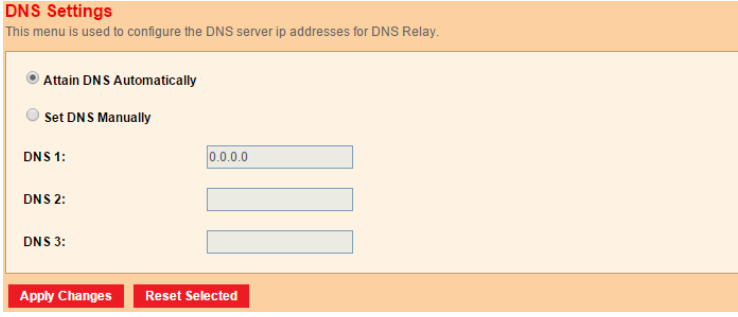
The following table describes the parameters of this page:

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

5.5.4 DNS

DNS

Choose **Access Management** > **DNS** > **DNS**, and the page shown in the following figure appears.

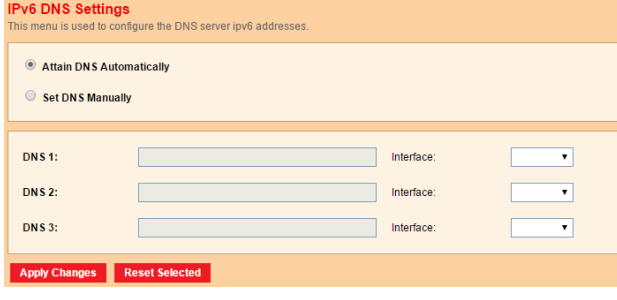


The following table describes the parameters and buttons of this page:

Field	Description
Set 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.

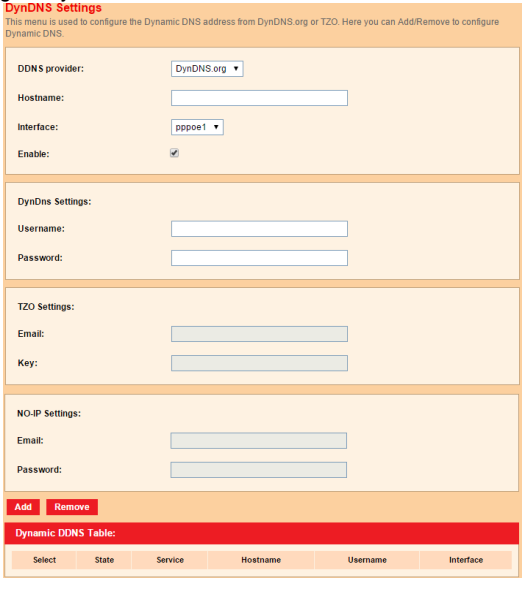
IPv6 DNS

Choose **Access Management** > **DNS** > **IPv6 DNS**, and the page shown in the following figure appears.



5.5.5 DynDNS

Choose **Access Management** > **DynDNS**, and the page shown in the following figure appears. This page is used to configure the dynamic DNS address. You can add or remove to configure dynamic DNS.



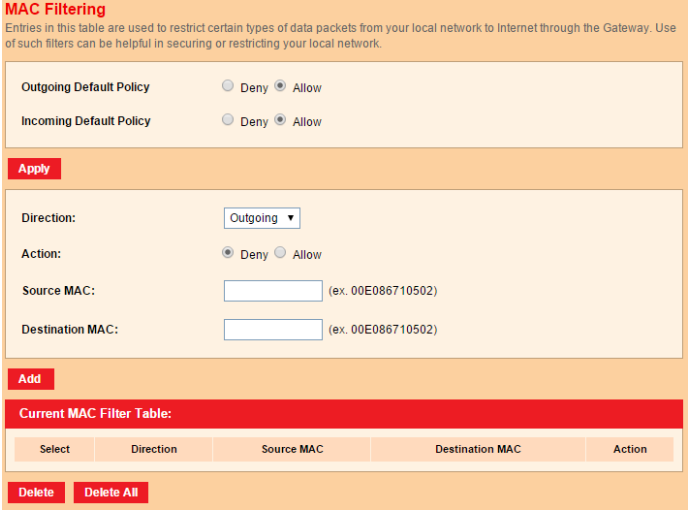
The following table describes the parameters of this page:

Field	Description
DDNS provider	Choose the DDNS provider name.
Host Name	The DDNS identifier.
Interface	The WAN interface of the router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.
Email	The email provided by DDNS provider.
Key	The key provided by DDNS provider.

5.6 Security Settings

5.6.1 MAC Filter

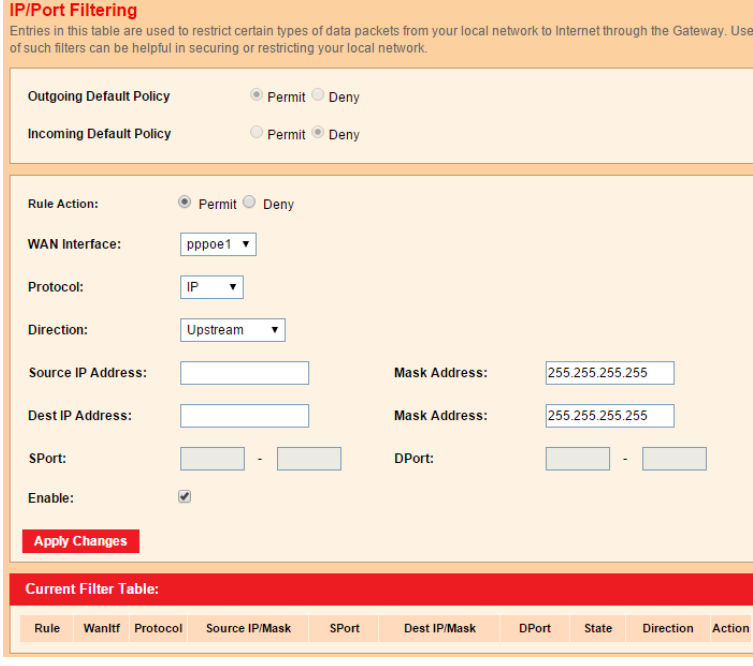
Choose **Security Settings** > **MAC Filter**, and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.



5.6.2 IP/Port Filter

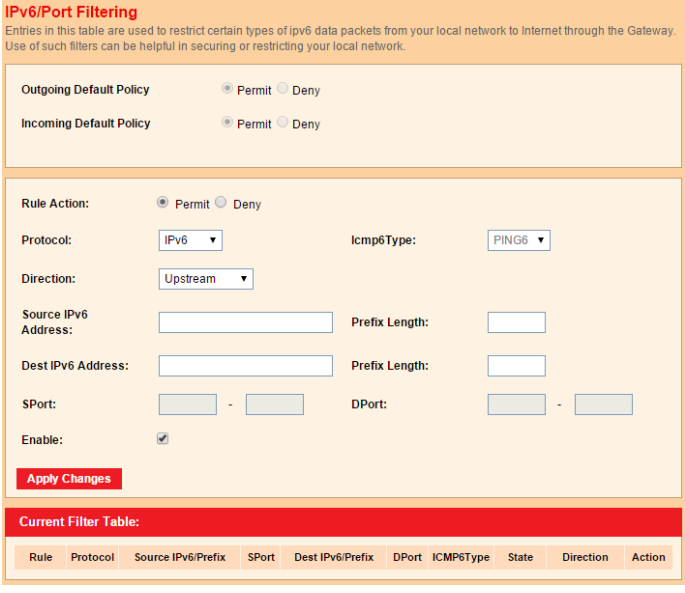
IP/Port Filter

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



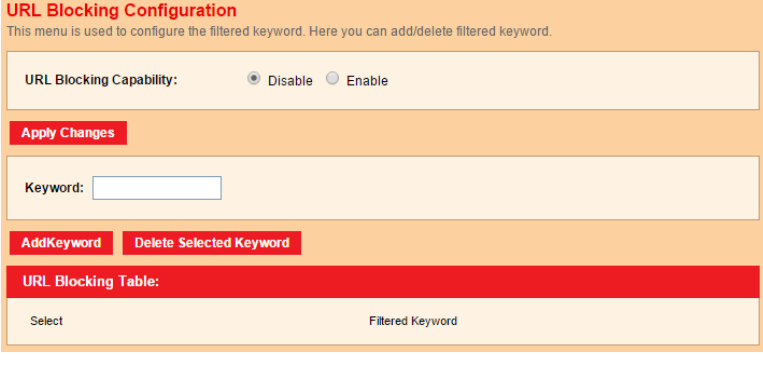
IPv6/ Port Filter

Choose **Security Settings** > **IP/Port Filter** > **IPv6/Port Filter**, and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



5.6.3 URL Filter

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



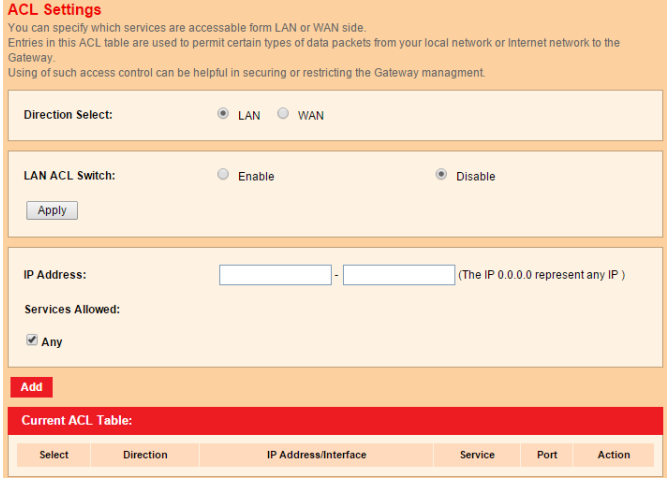
The following table describes the parameters and buttons of this page:

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 URL/keyword to the **URL/KEYWORD Blocking Table**.
URL Blocking Table	A list of the URL (s) to which access is blocked.

5.6.4 ACL

5.6.4.1 ACL

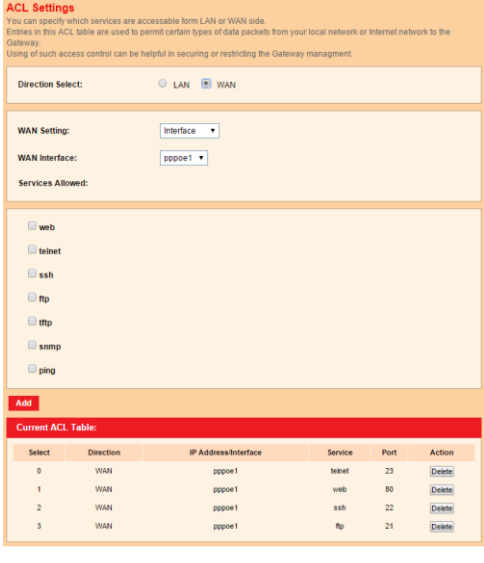
Choose **Security Settings** > **ACL**, the page shown in the following figure appears. In this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access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



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**.

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

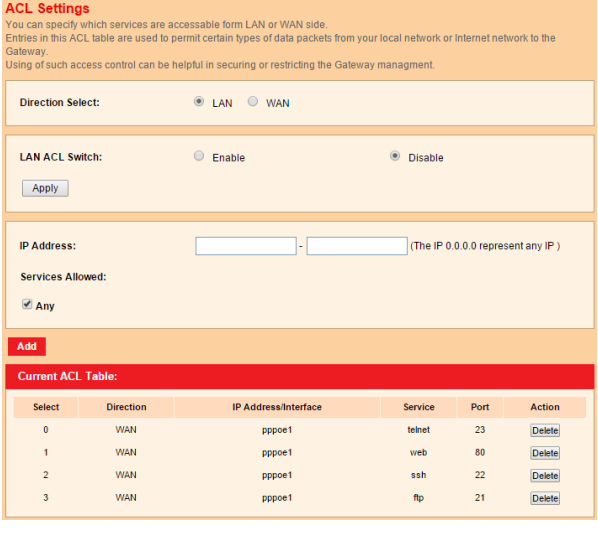


The following table describes the parameters and buttons of this page:

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.
Services Allowed	You can choose the following services from WAN: **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**.

5.6.4.2 IPv6 ACL

Choose **Security Settings** > **ACL** > **IPv6 ACL**, the page shown in the following figure appears.



5.6.5 DoS

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

Choose **Security Settings** > **DoS**, and the page shown in the following figure appears. In this page, you can prevent DoS attacks.

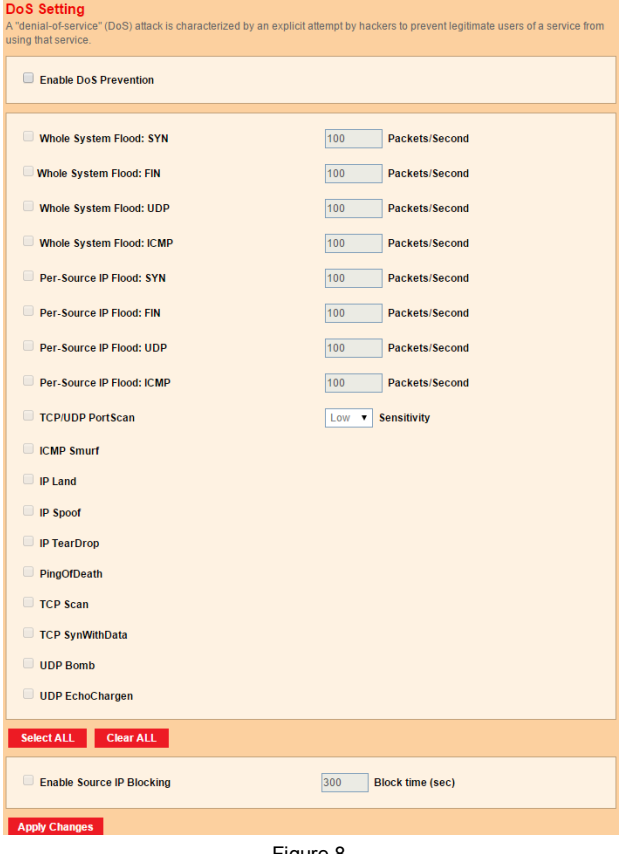


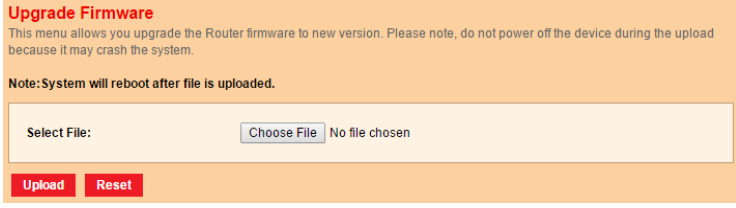
Figure 8

5.7 Maintenance

5.7.1 Update

Firmware Update

Choose **Maintenance** > **Update** > **Firmware Update**, the page shown in the following figure appears. In this page, you can upgrade the firmware of the router.

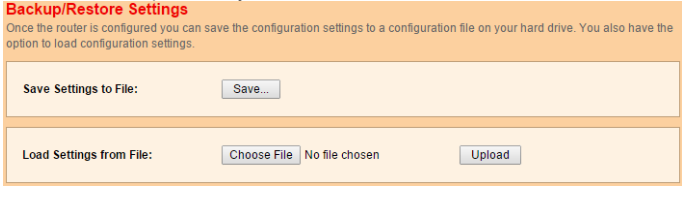


The following table describes the parameters and button of this page:

Field	Description
Select File	Click **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.

Backup/Restore

Choose **Maintenance** > **Update** > **Backup/Restore**, and the page shown in the following figure appears. You can back up the current settings to a file and restore the settings from the file that was saved previously.

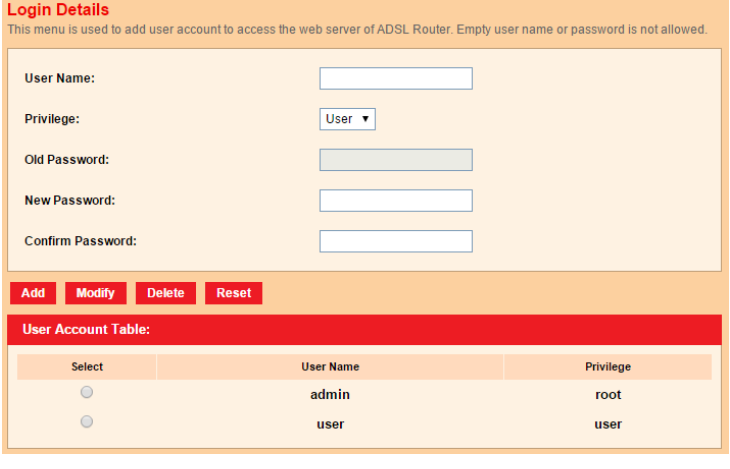


The following table describes the parameters and button of this page:

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

5.7.2 Password

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

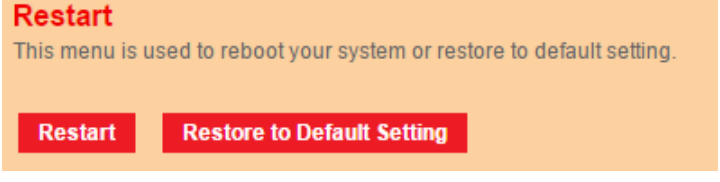


The following table describes the parameters of this page:

Field	Description
User Name	For adding a user, you can enter a user name. For changing the privilege and password of an exist user, you can select one to be modified from User Account Table.
Privilege	Choose the privilege for the account.
Old Password	Enter the old password
New Password	Enter the password to which you want to change the old password.
Confirm Password	Enter the new password again.

5.7.3 Restart

Choose **Maintenance** > **Restart**, the page shown in the following figure appears.

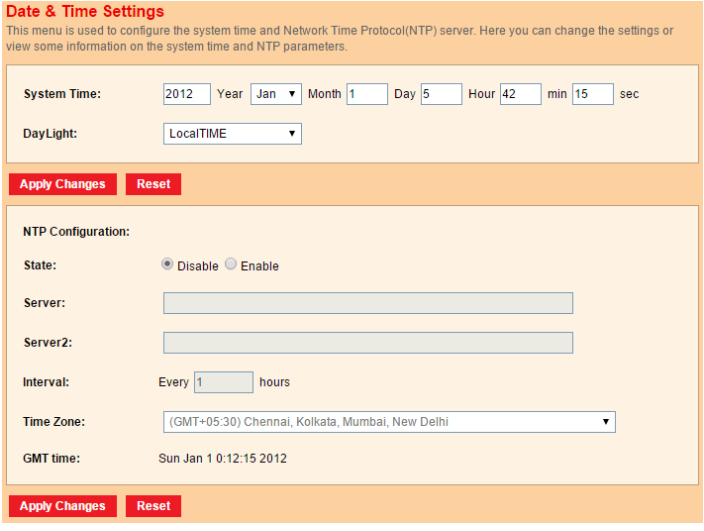


The following table describes the parameters and button of this page:

Field	Description
Restart	Click it to restart the router.
Restore to Default Setting	Click it to restore to factory default settings.

5.7.4 Time

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

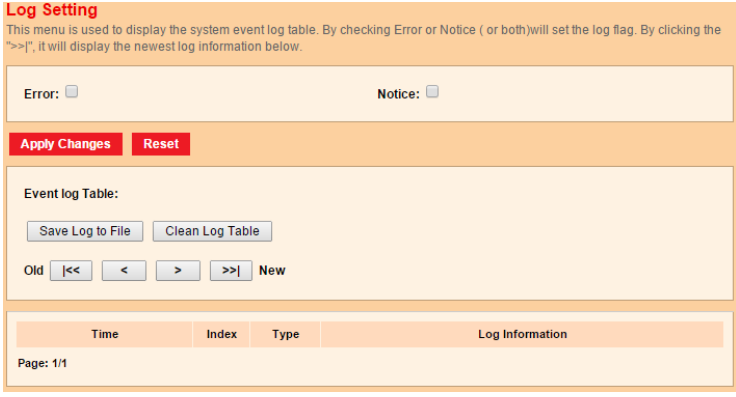


The following table describes the parameters of this page:

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

5.7.5 System Log

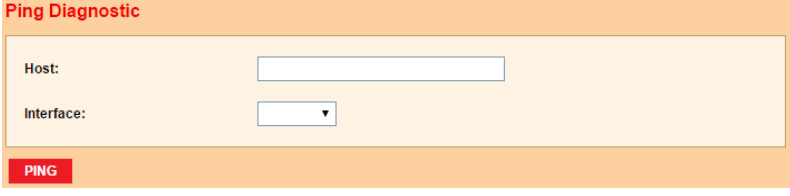
Choose **Maintenance** > **Log**, and the page shown in the following figure appears. In this page, you can enable or disable system log function and view the system log.



5.7.6 Diagnostics Tools

5.7.6.1 Ping

Choose **Diagnostics Tools** > **Ping**, and the page shown in the following figure appears.

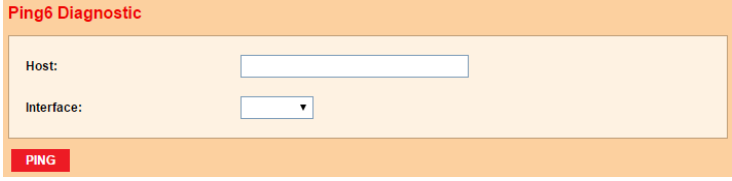


The following table describes the parameter and button of this page:

Field	Description
Host	Enter the valid IP address or domain name.
Interface	Select interface from drop-down list.
Ping	Click it to start to Ping the IP address.

5.7.6.2 Ping6

Choose **Diagnostics Tools** > **Ping6**, and the page shown in the following figure appears.

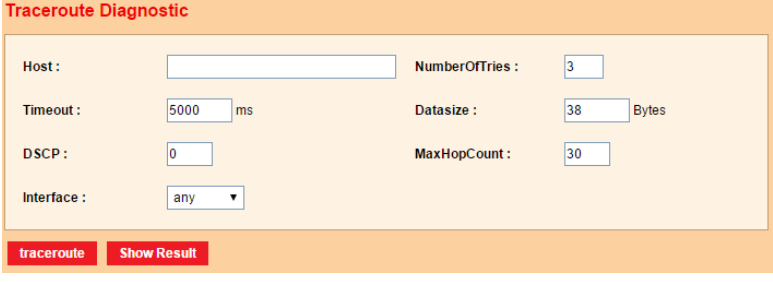


The following table describes the parameter and button of this page:

Field	Description
Host	Enter the valid IP address or domain name.
Interface	Select interface from drop-down list.
Ping	Click it to start to Ping the IP address.

5.7.6.3 Traceroute

Choose **Diagnostics Tools** > **Traceroute**, and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the Internet other side host.



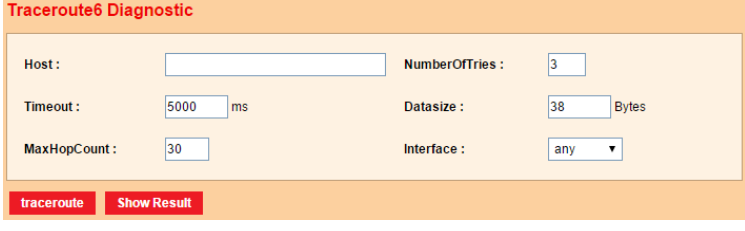
The following table describes the parameters and buttons of this page.

Field	Description
Host	Enter the destination host address for diagnosis.

NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.
traceroute	Click it to start traceroute.

5.7.6.4 Traceroute6

Choose **Diagnostics Tools** > **Traceroute6**, and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the Internet other side host.



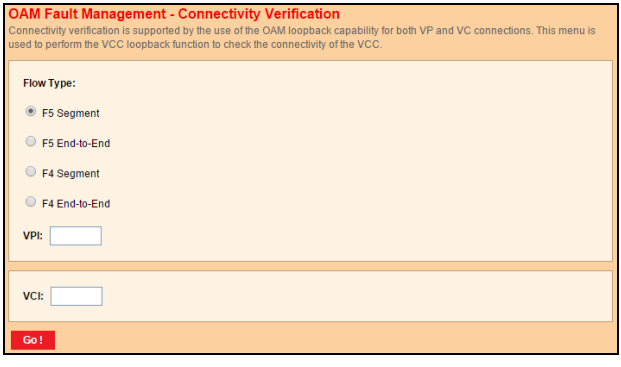
The following table describes the parameters and buttons of this page.

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
MaxHopCount	Maximum number of routes.

Interface	Select the interface.
traceroute	Click it to start traceroute.

5.7.6.5 OAM Loopback

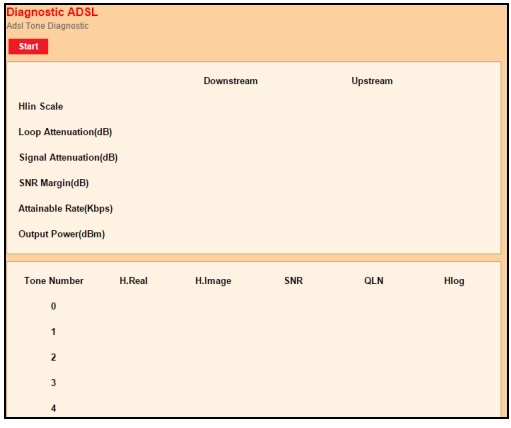
Choose **Diagnostics Tools** > **OAM Loopback**. The page shown in the following figure appears. In this page, you can use VCC loopback function to check the connectivity of the VCC. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.



Click **Go!** to start testing.

5.7.6.6 ADSL Diagnostic

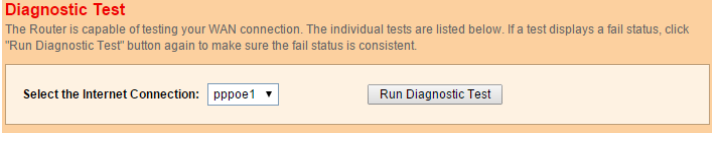
Choose **Diagnostics Tools** > **ADSL Diagnostic**. The page shown in the following figure appears. It is used for ADSL tone diagnostics.



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

5.7.6.7 Diag-Test

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



Click **Run Diagnostic Test** to start testing

Appendix A: Specifications

General	
Standards	Complies with IEEE 802.11b, IEEE 802.11g, IEEE 802.11n & IEEE 802.3, IEEE 802.3u standards
Protocols	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5,
Protocols	TCP/IP, PPPoA, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Ports	2- 10/100M Auto-Negotiation RJ45 LAN Ports (Auto MDI/MDIX) , 1- RJ11 (WAN) Port
LEDs	PWR, ADSL, Internet, WLAN, LAN ports
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps Upstream: Up to 3.5Mbps（With Annex M enabled）
WPS	WPS button
WiFi	Wi-Fi ON/OFF button
Reset button	Factory default
Safety & Emission	FCC, CE
Power	12V DC, 0.5A
System Requirement	Internet Explorer 5.20 or later, Netscape Navigator 6.0 or later Win 9x/ ME/ 2000/ XP/ Vista/Windows 7
Wireless	
Frequency Band	2.412~2.462GHz

Radio Data Rate	11n: up to 150Mbps（Automatic） 11g: 54/48/36/24/18/12/9/6Mbps（Automatic） 11b: 11/5.5/2/1Mbps（Automatic）
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK

Physical and Environment	
Working Temperature	0% ~ 40%
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40% ~ 70%
Storage Humidity	5% ~ 90% RH (non-condensing)