



VB104W VDSL

User Manual

Contents

1	Safety Precautions	1
2	Overview	2
2.1	Packing List.....	2
2.2	Application	2
2.3	Features.....	3
2.4	Standards Compatibility and Compliance	4
3	Hardware Description and Installation.....	5
3.1	LEDs and Interfaces.....	5
3.2	Hardware Installation.....	7
4	PC Network Configuration and Login	10
4.1	PC Network Configuration	10
4.2	Logging in to the DSL Router	11
5	Web-based Management	12
5.1	Setup	12
5.1.1	Wizard	12
5.1.2	Internet Setup	18
5.1.3	Wireless.....	21
5.1.4	Local Network.....	26
5.1.5	Local IPv6 Network.....	30
5.1.6	Time and Date	32
5.1.7	Logout	33
5.2	Advanced.....	34
5.2.1	Advanced Wireless	34
5.2.2	ALG	41
5.2.3	Port Forwarding	41
5.2.4	DMZ	44
5.2.5	SAMBA.....	45
5.2.6	Parental Control.....	46
5.2.7	Filtering Options.....	50
5.2.8	QoS Configuration	56
5.2.9	Anti-Attack Settings	60
5.2.10	DNS	61
5.2.11	Dynamic DNS.....	61
5.2.12	Network Tools.....	63

5.2.13	Routing.....	74
5.2.14	Schedules	80
5.2.15	NAT	81
5.2.16	DLNA	82
5.2.17	IP Tunnel	82
5.2.18	Logout	87
5.3	Management	87
5.3.1	Global IPv6	87
5.3.2	System Management	88
5.3.3	Firmware Update	89
5.3.4	Access Controls	90
5.3.5	Diagnosis	96
5.3.6	Log Configuration	98
5.3.7	Logout	99
5.4	Status	100
5.4.1	Device Info	100
5.4.2	Wireless Clients	102
5.4.3	DHCP Clients	102
5.4.4	IPv6 Status	102
5.4.5	Logs	103
5.4.6	Statistics	104
5.4.7	Route Info	105
5.4.8	Logout	105
5.5	Help	105
6	Trouble Shooting	107

1 Safety Precautions

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

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. 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 heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The VB104W VDSL DSL Router integrates wireless LAN and USB service into one unit. It is designed to provide a simple and cost-effective DSL Internet connection for a private Ethernet and 802.11g/802.11b/802.11n wireless network. The Router combines high-speed DSL Internet connection, 3G WAN service, IP routing for the LAN, and wireless connectivity in one package.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The DSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network. Network and Router management is done through the web-based management interface accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

2.1 Packing List

2.2 Application

- Home gateway
- 3G Internet
- Wireless LAN
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming
- USB storage

2.3 Features

- User-friendly GUI for web configuration
- Compatible with all standard Internet applications
- Industry standard and interoperable xDSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates, compatible with IEEE 802.11b/g/n
- IP routing and bridging
- Asynchronous transfer mode (ATM) , PTM (Packet Transfer mode), and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- Web filtering
- Management and control
 - Web-based management (WBM)
 - Command line interface (CLI)
 - TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.
- Multicast listener discovery (MLD)
- Digital living network alliance (DLNA)
- Synergy advanced multipurpose bus arbiter (SAMBA)
- Internet group management protocol (IGMP)
- Application layer gateway (ALG)

2.4 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ITU G.993.1 (VDSL)
- ITU G.993.2 (VDSL2)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Installation

3.1 LEDs and Interfaces

Front Panel

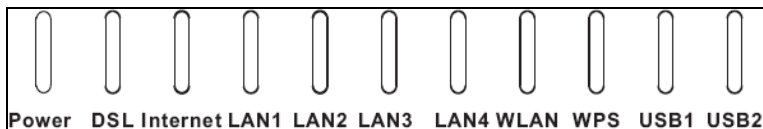


Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on.
		Off	The device is powered off.
	Red	On	Self-test fails, or failure occurs, or the device is starting.
DSL	Green	On	DSL link is established.
		Slow Blink	The DSL line is attempting to detect signals.
		Fast Blink	Signals have been detected, and the DSL line is attempting to establish link.
Internet	Green	On	Physical layer connection and IP connection is established in routing mode.
		Blink	IP connection is established, and messages are being transmitted.
		Off	IP connection or physical layer link is not established.
	Red	On	IP connection fails.
LAN 1/2/3/4	Green	On	Ethernet link is established.
		Blink	Data is being transmitted through a LAN interface.
		Off	Ethernet link is not established.
WLAN	Green	On	WLAN is enabled.

Indicator	Color	Status	Description
		Blink	Data is being transmitted by the wireless module.
		Off	WLAN is disabled.
WPS	Green	On	Negotiation is successful under Wi-Fi protected setup.
		Blink	Negotiation is in progress under Wi-Fi protected Setup.
		Off	Wi-Fi protected setup is disabled.
USB	Green	On	A USB flash disk is connected.
		Blink	Data is being transmitted.
		Off	No USB connection.

Rear Panel

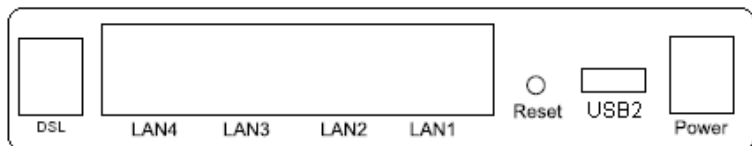


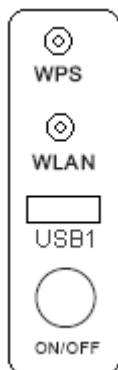
Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface connecting to a telephone set through a telephone cable
LAN1/2/3/4	Ethernet RJ-45 interfaces connecting to the Ethernet interfaces of computers or Ethernet devices
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for more than 5 seconds and then release.
USB2	USB port, for connecting USB storage devices.

Interface/Button	Description
Power	Interface connecting to the power adapter. The power adapter output is: 12V DC, 1000mA

Side Panel



Interface/Button	Description
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.
WLAN	WLAN switch, for enabling or disabling the WLAN function.
USB1	USB port, for connecting a 3G network card or other USB storage devices.
ON/OFF	Push to power on/off the device.

3.2 Hardware Installation

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

The splitter has three ports:

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

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

Note:

Use twisted-pair cables to connect the device to a Hub or switch.

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

Connection 1: Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.

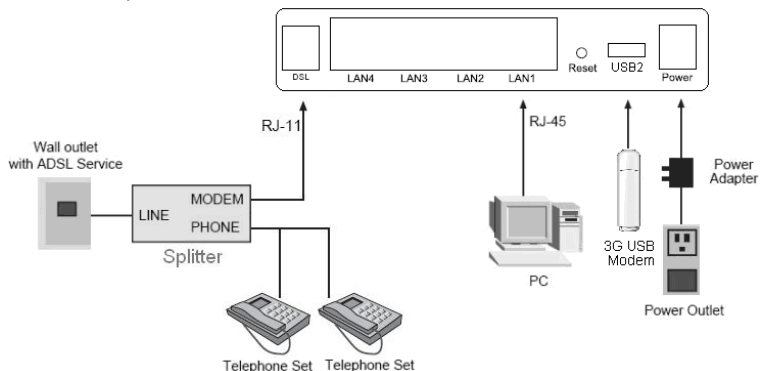


Figure 3 Connection diagram (without telephone sets before the splitter)

Connection 2: Figure 4 displays the application diagram for the connection of the device, PC, splitter and telephone sets when a telephone set is placed before the splitter.

As illustrated in the following figure, the splitter is installed close to the device.

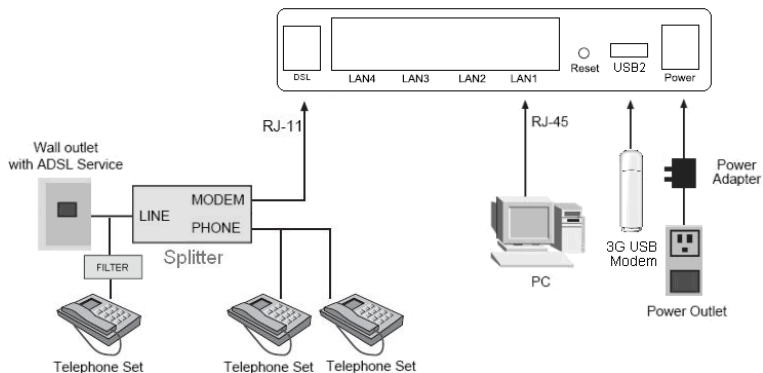


Figure 4 Connection diagram (with a telephone set before the splitter)

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. 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.

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

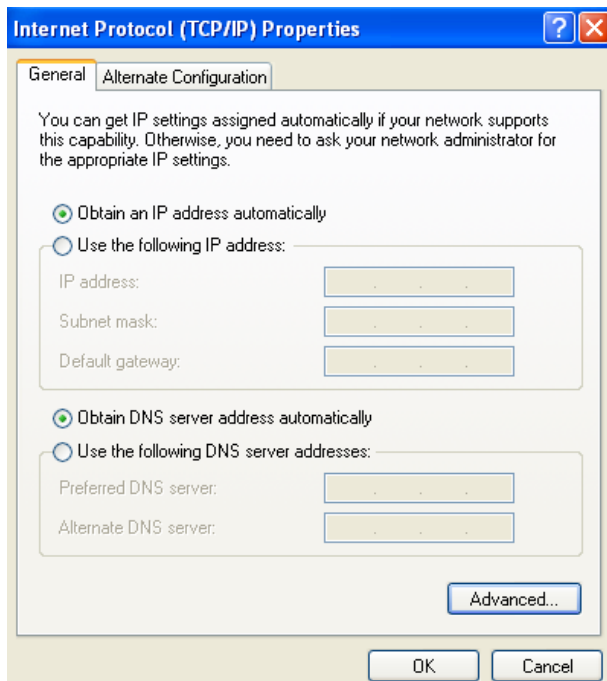


Figure 5 PC Network Configuration

TCP/IP configuration steps for Windows XP are as follows:

Step 1 Choose Start > Control Panel > Network Connections.

Right-click the Ethernet connection icon and choose **Properties**.

On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.

Select the **Obtain an IP address automatically** radio button.

Select the **Obtain DNS server address automatically** radio button.

Click **OK** to save the settings.

4.2 Logging in to the DSL Router

To log in to the DSL router, do as follows.

Step 1 Open a Web browser on your computer.

Step 2 Enter **http://192.168.1.1** (default IP address of the DSL router) in the address bar. The login page appears.

Step 3 Enter the user name and the password. The default username and password are **admin** and **admin**. The username and password of the common user are **user** and **user**. The username and password of the support account are **support** and **support**.

Step 4 You need not enter the username and the password again if you select the browser option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 5 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.

After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-based Management

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

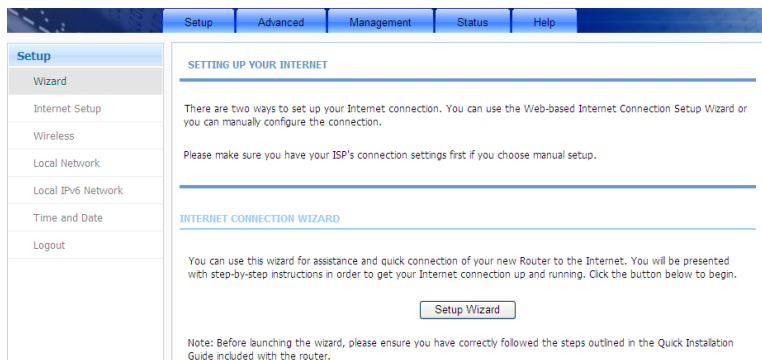
5.1 Setup

In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Internet Setup**, **Wireless**, **Local Network**, **Local IPv6 Network**, **Time and Date** and **Logout**.

5.1.1 Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe configuration parameters. When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you that you are connected to the Internet using a static or dynamic IP address, or the protocol used for communication over the Internet, such as PPPoA or PPPoE,.

Step 1 Choose **Setup > Wizard**. The page shown in the following figure appears.



Step 2 Click **Setup Wizard**. The page shown in the following figure appears.

WELCOME TO SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

- **Step 1** : Set Time and Date
- **Step 2** : Setup Internet Connection
- **Step 3** : Configure Wireless Network
- **Step 4** : Completed and Quit

Step 3 There are four steps to configure the device. Click **Next** to continue.

Step 4 Set the time and date.

STEP 1: SET TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTING

☒ **Automatically synchronize with Internet time servers**

1st NTP time server : europe.pool.ntp.org

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Time Zone : (GMT+12:00) Auckland, Wellington, Fiji

☒ **Enable Daylight Saving**

Daylight Saving Start : 2012 Year 03 Mon 11 Day 02 Hour 00 Min 00 Sec

Daylight Saving End : 2012 Year 11 Mon 04 Day 02 Hour 00 Min 00 Sec

Back Next Cancel

Step 5 Configure the Internet connection. Set the VPI and VCI.

PPPoE/ PPPoA

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **PPPoE** or **PPPoA**, the page shown in the two following figures appears.

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

DSL Mode:

Protocol:

Encapsulation Mode:

VPI: (0-255)

VCI: (32-65535)

Search Available PVC:

PPPOE/PPPOA

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

Username:

Password:

Confirm Password:

In this page, enter the user name and password as provided by your ISP.

Dynamic IP

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Dynamic IP**, the page shown in the following figure appears.

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

DSL Mode:

Protocol:

Encapsulation Mode:

VPI: (0-255)

VCI: (32-65535)

Search Available PVC:

Static IP

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Static IP**, the page shown in the following figure appears. Enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server**.

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

DSL Mode	<input type="text" value="ATM"/>
Protocol	<input type="text" value="Static IP"/>
Encapsulation Mode	<input type="text" value="LLC"/>
VPI	<input type="text" value="8"/> (0-255)
VCI	<input type="text" value="35"/> (32-65535)
Search Available PVC	<input type="button" value="Scan"/>

STATIC IP

You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS Server	<input type="text"/>

Bridge

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Bridge**, the page shown in the following figure appears.

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

DSL Mode:

Protocol:

Encapsulation Mode:

VPI: (0-255)

VCI: (32-65535)

Search Available PVC:

Note:

When you choose the **DSL Mode** as **PTM**, please refer to the configurations under **ATM** mode for corresponding Internet configurations.

Step 6 Click Next. The page shown in the following figure appears.

STEP 3: CONFIGURE WIRELESS NETWORK

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

Enable Your Wireless Network : ☒

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) :

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

Visibility Status : ☐ Visible ☒ Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

None	Security Level		Best
<input checked="" type="radio"/> None	<input type="radio"/> WEP	<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK
Security Mode: None Select this option if you do not want to activate any security features.			

Step 7 Configure the wireless network. Enter the information and click **Next**.
In this example, the **Protocol** is chosen as **PPPoE**.

STEP 4: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings.

If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	1
NTP Server 1 :	hora.ngn.rima-tde.net
NTP Server 2 :	192.168.2.100
Time Zone :	EGT
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
Username :	aaa
Password :	***
Wireless Network Name (SSID) :	vds_01
Visibility Status :	0
Encryption :	None
Pre-Shared Key :	
WEP Key :	

Step 8 Click **Apply** to save the settings.

Note:

In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.

5.1.2 Internet Setup

Choose **Setup > Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.

VB104W User Manual

Setup
Advanced
Management
Status
Help

Setup

Wizard

Internet Setup

Wireless

Local Network

Local IPv6 Network

Time and Date

Logout

INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

WAN SETUP

VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
<input type="radio"/> 8/32	0	LLC	PVC:8/32	PPPoE	1	Disconnected	<input type="radio"/>	Connect
<input type="radio"/> 8/36	0	LLC	PVC:8/36	PPPoE	1	Disconnected	<input type="radio"/>	Connect
<input type="radio"/> 8/35	0	LLC	pppoe_8_35_0_2_Int...	PPPoE	1	Disconnected	<input type="radio"/>	Connect

Add
Edit
Delete

Click **Add** in “INTERNET SETUP”. The page shown in the following figure appears.

INTERNET SETUP

This screen allows you to configure an WAN connection.

DSL MODE CONFIGURATION

DSL Mode: ATM

ATM PVC CONFIGURATION

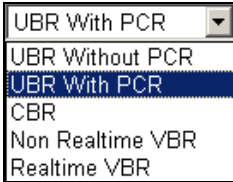
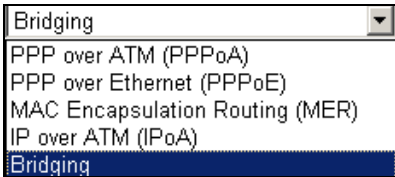
VPI: 0 (0-255)
VCI: 35 (32-65535)
Service Category: UBR With PCR
Peak Cell Rate: 0 (cells/s)
Sustainable Cell Rate: 0 (cells/s)
Maximum Burst Size: 0 (cells)

CONNECTION TYPE

Protocol: Bridging
Encapsulation Mode: LLC
802.1Q VLAN ID: 0 (0 = disable, 1 - 4094)
Priority: 0 (0 - 7)
Enable Service: ☒
Service Name: Bridging_0_7

Apply
Cancel

The following table describes the parameters in this page.

Field	Description
DSL Mode	You can select ATM or PTM .
PVC Settings	<p>VPI: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.</p> <p>VCI: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).</p>
Service Category	<p>You can select from the drop-down list.</p> 
Protocol	<p>You can select from the drop-down list.</p> 
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select LLC or VCMUX .

Click **Apply**, the page shown in the following figure appears.

INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

Default GateWay Mode ☒ Auto ☐ Manual

WAN SETUP

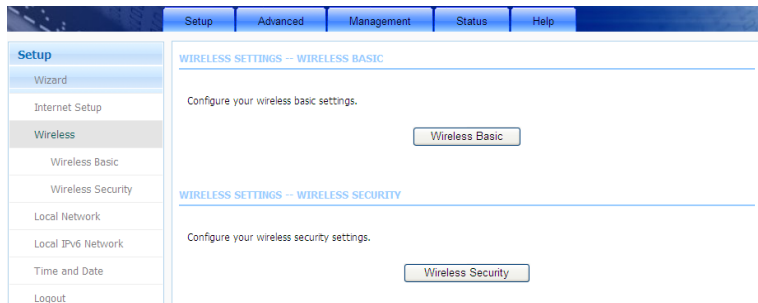
	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
<input checked="" type="radio"/>	N/A	10	LLC	PPPoE_10_1	PPPoE	1		<input checked="" type="radio"/>	-
<input type="radio"/>	0/100	0	LLC	PPPoA_0_3	PPPoA	1		<input type="radio"/>	-

To manage the existing WAN connections, select a connection from the list, and then click **Edit** or **Delete**.

5.1.3 Wireless

This section describes the wireless LAN and basic configuration. A wireless LAN can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup > Wireless**. The **Wireless** page shown in the following figure appears.



5.1.3.1 Wireless Basic

In the **Wireless** page, click **Wireless Basic**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

WIRELESS BASIC CONFIGURATION

Enable wireless ☒

AP Isolate ☒

SSID:

Visibility Status: ☒ Visible ☐ Invisible

Country:

802.11 Mode:

Band Width:

Wireless Channel:

Transmission Rate:

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
AP Isolate	Select this to turn AP isolation on.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
Visibility Status	You can select Visible or Invisible .
Country	Select the country from the drop-down list.
802.11 Mode	Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are 802.11b only , 802.11g only , 802.11n only , Mixed 802.11b/g , Mixed 802.11n/g and Mixed 802.11b/g/n .

Field	Description
Band Width	Select the appropriate band as 20M , 40M Plus , or 40M Minus from the pull-down menu.
Wireless Channel	Select the wireless channel from the pull-down menu. It is different for different country.
Transmission Rate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default is Auto .

Click **Apply** to save the settings.

5.1.3.2 Wireless Security

In the **Wireless** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.

Note:

Enable Wireless before configuring the wireless security settings in this page.
Refer to 5.1.3.1 Wireless Basic.

When the Security Mode is set as **WEP**, the following figure appears.

WIRELESS SECURITY

Wireless Security Mode : **WEP** ▼

WEP

WEP Key Length : 64 bit ▼ (length applies to all keys)

Default Tx Key : 1 ▼

WEP Key Format : HEX (10 characters) ▼

WEP Key1 : 1111111111

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication : Open ▼

Apply Cancel

The following table describes the parameters of this page.

Field	Description
WEP Key Length	Choose the WEP key length. You can choose 64-bit or 128-bit .
Default Tx Key	Choose the index of WEP Key. You can choose Key 1, 2, 3 or 4 .
WEP Key Format	<ul style="list-style-type: none"> When 64-bit key length is selected, you can choose ASCII (5 characters) or HEX (10 characters). When 128-bit key length is selected, you can choose ASCII (13 characters) or HEX (26 characters).
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is 1111111111 .
Authentication	Choose an authentication mode.

Click **Apply** to save the settings.

When the Security Mode is set as **WPA only**, **WPA2 only** or **WPA/WPA2 Mixed**, the following figure appears.

WIRELESS SECURITY

Wireless Security Mode : **WPA only**

WPA

WPA Mode : **WPA-Personal**

Encryption Mode : ☒ TKIP ☐ AES ☐ Both

Group Key Update Interval : **100** (60 - 65535)

PRE-SHARED KEY

Pre-Shared Key : (ASCII < 64, HEX = 64)

Apply

Cancel

The following table describes the parameters in this page.

Field	Description
Wireless Security Mode	<p>Configure the wireless encryption mode. You can choose None, WEP, WPA Only, WPA2 Only or WPA/WPA2 Mixed.</p> <ul style="list-style-type: none"> Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. WPA/WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. <p>Key differences between WPA and WEP are user authentication and improved data encryption.</p>
WPA Mode	<ul style="list-style-type: none"> Select Personal, and then enter the pre-shared key in the Pre-Shared Key field. Select Enterprise, and then enter the port, IP address, and password of the Radius server. You need to enter the password provided by the Radius server when the wireless client connects the modem.

Field	Description
	If the encryption is set to WEP , the modem uses 802.1 X authentication, which is Radius authentication.
Encryption Mode	When WPA /WPA2 Mixed is selected, you can select WPA encryption as AES , TKIP or Both .
Group Key Update Interval	When WPA encryption is applied, messages sent are encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.

5.1.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup > Local Network**. The **Local Network** page shown in the following figure appears.

Setup	Advanced	Management	Status	Help
Setup Wizard Internet Setup Wireless Local Network Local IPv6 Network Time and Date Logout	<div> LOCAL NETWORK </div> <p>This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.</p> <hr/> <div> ROUTER SETTINGS </div> <p>Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.</p> <p> Router IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 Domain Name : homestation <input type="checkbox"/> Enable Proxy Arp </p> <p> <input checked="" type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN IP Address : 192.168.249.1 Subnet Mask : 255.255.255.252 </p>			

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings from a PC connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP clients connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

ADD ROUTER SETTINGS

The second IP Range.

Router IP Address : 192.168.10.1
Subnet Mask : 255.255.255.0
Domain Name : gj.com
DHCP IP Address Range : 192.168.10.2 to 192.168.10.100
DHCP Lease Time : 86400 (seconds)

This page is used to configure the DHCP Server and DHCP Relay Settings. The **HCP Lease Time** is at least **600** seconds and without upper limit; **-1** means unrestricted lease time.

DHCP SETTINGS (OPTIONAL)

Use this section to configure the DHCP Relay for your network.

☐ Enable DHCP Relay

Relay IP Address :

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

☒ Enable DHCP Server

DHCP IP Address Range : to

DHCP IP Mask :

DHCP Router IP :

DHCP Lease Time : (seconds)

Use the following DNS server addresses:

☐ Enable static DNS

Preferred DNS server :

Alternate DNS server :

☒ Enable DNS Relay

Use this section to configure the DHCP Server in lan port individual:

☒ LAN Port1

☒ LAN Port2

☒ LAN Port3

☒ LAN Port4

☒ WLAN Port1

☒ WLAN Port2

☒ WLAN Port3

☒ WLAN Port4

Click **Apply** to save the settings.

The **DHCP Client Class List** section is shown as below.

DHCP CLIENT CLASS LIST

Client Class	Min Address	Max Address	DNS Address
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>			

Click **Add**, the page shown in the following figure appears.

ADD DHCP CLIENT CLASS(OPTIONAL)

Client Class Name :

Min IP Address :

Max IP Address :

DNS Address :

The **DHCP Cond Option** section is shown as below. Here you can specify the reply message (option **240~245**) the modem sends to the client. After **DHCP CLIENT CLASS** is configured, you can configure **DHCP COND OPTION**.

DHCP COND OPTION

Status	Client Class Name	Option Code	Option Value
--------	-------------------	-------------	--------------

Click **Add** to add DHCP option as shown in the following figure.

ADD DHCP OPTION(OPTIONAL)

Cond Option enable: ☐

Cond Option Client Class:

Cond Option Tag:

Cond Option Value:

Only when this function is enabled, the modem returns the content below to the client.

The **Cond Option Client Class** is the client class name of DHCP Cond Option. The **Cond Option Tag** is a part of the value in the message sent by the modem to the client. It is between **240** and **245**.

The **Cond Option Value** is a value in the message sent by the modem to the client. This value can be specified at random.

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

In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
--------	---------------	-------------	------------

Click **Add** to add static DHCP (optional). The page shown in the following figure appears.

ADD DHCP RESERVATION (OPTIONAL)

Enable : ☐

Computer Name :

IP Address :

MAC Address :

Select **Enable** to reserve the IP address for the designated PC with the configured MAC address. The **Computer Name** helps you to recognize the PC with the MAC address, for example, Father's Laptop. Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer(s).

NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time
---------------	-------------	------------	-------------

5.1.5 Local IPv6 Network

You can configure the LAN IPv6 address according to the actual application. The preset IPv6 address is fe80::1. You can use the default settings and DHCPv6 service to manage the IPv6 settings for the private network. The IPv6 address of the device is the base address used for DHCPv6. To use the device for DHCPv6 on your LAN, the IPv6 address pool used for DHCPv6 must be compatible with the IPv6 address of the device. The IPv6 address available in the DHCP IPv6 address pool changes automatically if you change the IPv6 address of the device.

Choose **Setup > Local IPv6 Network**. The page shown in the following figure appears. In this page, you can configure a static LAN IPv6 address, enable or disable DHCPv6 server and RADVD, and configure site prefix.

Setup	Advanced	Management	Status	Help
Setup Wizard Internet Setup Wireless Local Network Local IPv6 Network Time and Date Logout	<h3>IPV6 LAN SETTINGS</h3> <p>Note: Stateful DHCPv6 is supported after the IPv6 address 16-bit. For example: Interface ID range from 1 to ffff, IPv6 address range from 2111::123:123:123::1 to 2111::123:123:123::ffff.</p> <hr/> <h4>STATIC LAN IPV6 ADDRESS CONFIGURATION</h4> <p>IPv6 Interface Address <input type="text"/></p> <hr/> <h4>DHCPV6 CONFIGURATION</h4> <p>Enable DHCPv6 Server <input type="checkbox"/></p> <p>LAN address config mode <input type="radio"/> Stateless <input type="radio"/> Stateful</p> <p>Start Interface ID <input type="text"/></p> <p>End Interface ID <input type="text"/></p> <p>DHCPv6 Lease Time <input type="text"/></p> <p>Use the following DNS server addresses.</p> <p>Get DNS Servers from WAN <input type="radio"/></p> <p>Static DNS Servers <input type="radio"/></p> <p>Static IPv6 DNS Servers <input type="text"/></p> <hr/> <h4>SITE PREFIX CONFIGURATION</h4> <p>Enable RADVD <input type="checkbox"/></p> <p>Auto get prefix from WAN <input type="radio"/></p> <p>WAN interface <input type="text"/></p> <p>Static <input type="radio"/></p> <p>Site Prefix <input type="text"/></p> <p> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p>			

The following table describes the parameters in this page.

Field	Description
IPv6 Interface Address	The IPv6 address of link local gateway on the LAN side.
Enable DHCPv6 Server	Choose to enable DHCPv6 server.
LAN address config mode	Choose an IPv6 address mode. Stateless refers to stateless address auto-configuration (SLAAC) mode, and Stateful refers to dynamic host configuration protocol (DHCP) mode.
Start/ End Interface ID	IPv6 address pool range.

Field	Description
DHCPv6 Lease Time	IPv6 lease time.
Get DNS Servers from WAN	You can choose to get the IPv6 DNS server address from the WAN side.
Static DNS Servers	You can manually set the IPv6 DNS server address.
Static IPv6 DNS Servers	Input an IPv6 DNS server address.
Enable RADVD	The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
Auto get prefix from WAN	You can choose to get an IPv6 prefix from the WAN automatically.
WAN interface	You can choose to get an IPv6 prefix from the selected WAN connection.
Static	You can choose to specify an IPv6 prefix.
Site Prefix	Input an IPv6 prefix.

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

5.1.6 Time and Date

Choose **Setup > Time and Date**. The page shown in the following figure appears.

The screenshot shows the 'Time and Date' configuration page. On the left is a sidebar with a 'Setup' menu containing: Wizard, Internet Setup, Wireless, Local Network, Local IPv6 Network, Time and Date (highlighted), and Logout. The main content area has a top navigation bar with 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. Below this, the 'TIME AND DATE' section contains an introductory paragraph: 'The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.' This is followed by the 'TIME SETTING' section, which includes a checkbox for 'Automatically synchronize with Internet time servers'. Below this are two text input fields: '1st NTP time server:' (containing 'hora.ngn.rima-tde.net') and '2th NTP time server:'. The 'TIME CONFIGURATION' section shows 'Current Local Time:' as '1970-01-01 01:24' and 'Time Zone:' as a dropdown menu currently set to '(GMT-01:00) Cape Verde'. There is a checked checkbox for 'Automatically adjust clock for daylight saving changes'. At the bottom right are 'Apply' and 'Cancel' buttons.

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

Select the specific time server and the time zone from the corresponding drop-down lists.

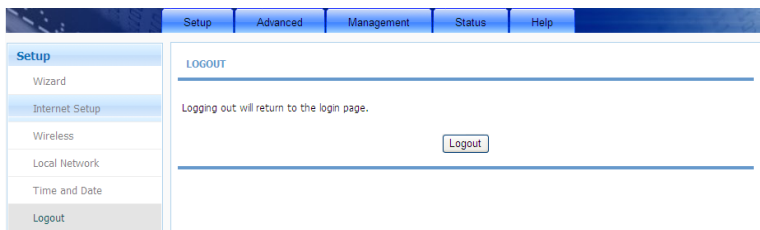
Select **Automatically adjust clock for daylight saving changes** if necessary.

Set the daylight as you want.

Click **Apply** to save the settings.

5.1.7 Logout

Choose **Setup > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



5.2 Advanced

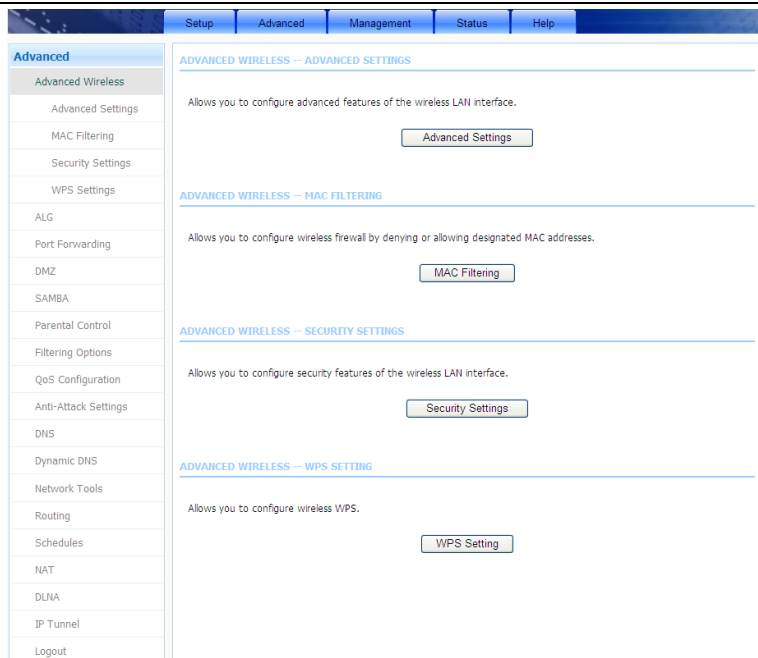
This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and troubleshoot.

In the main interface, click **Advanced** tab to enter the **Advanced** menu as shown in the following figure. The submenus are **Advanced Wireless**, **ALG**, **Port Forwarding**, **DMZ**, **SAMBA**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Anti-Attack Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, **Schedules**, **NAT**, **DLNA**, **IP Tunnel** and **Logout**.

5.2.1 Advanced Wireless

It is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **Advanced** > **Advanced Wireless**. The page shown in the following figure appears.



5.2.1.1 Advanced Settings

Select **Advanced Settings**. The page shown in the following figure appears.

ADVANCED SETTINGS

Enable wireless ☒

ADVANCED WIRELESS SETTINGS

Transmit Power : 80%
Beacon Period : 100 (20 ~ 1023)
RTS Threshold : 2346 (256 ~ 2347)
Fragmentation Threshold : 2346 (256 ~ 2346)
DTIM Interval : 10 (1 ~ 255)
Preamble Type : long

SSID

SSID : vdsi_01
Visibility Status : ☐ Visible ☒ Invisible
User Isolation : On
Disable WMM Advertise : On

GUEST/VIRTUAL ACCESS POINT-1

Enable ☐
Guest SSID : vdsi-02
Visibility Status : ☐ Visible ☒ Invisible
User Isolation : On
Disable WMM Advertise : On

GUEST/VIRTUAL ACCESS POINT-2

Enable ☐
Guest SSID : vdsi-03
Visibility Status : ☐ Visible ☒ Invisible
User Isolation : On
Disable WMM Advertise : On

GUEST/VIRTUAL ACCESS POINT-3

Enable ☐
Guest SSID : vdsi-04
Visibility Status : ☐ Visible ☒ Invisible
User Isolation : On
Disable WMM Advertise : On

Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Click **Apply** to save the settings.

5.2.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.

ACCESS CONTROL

Wireless SSID : vdsl_01

Access Control Mode : Allow

Submit Cancel

WLAN FILTER LIST

Mac	Comment	Operation
Add		

MAC address access control permits access to this route from hosts with MAC addresses contained in the WLAN Filter List.

Choose a wireless SSID, select an access control mode, and then click **Add** to add a MAC Address as shown in the following figure. Click **Apply** to finish. After adding a filter, you can edit or delete it.

ACCESS CONTROL

Wireless SSID : vdsl_01

Access Control Mode : Allow

WLAN FILTER LIST

Mac	Comment	Operation
Add		

INCOMING MAC FILTER

MAC : (xxxxxxxxxxxx)

Comment :

Apply Cancel

5.2.1.3 Security Settings

Select **Security Settings**. The VAP Configuration page appears.

VAP CONFIGURATION

WIRELESS SSID

Select SSID vds1_01 ▼

WIRELESS SECURITY

Work Mode WEP ▼

ENABLED WEP

Encryption Strength 64 bit ▼ (length applies to all keys)

Choose WEP Key 1 ▼

Key Type HEX (10 characters) ▼

WEP Key1 : 1111111111

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication Open ▼

Submit

Refresh

Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Work Mode** drop-down list. You can select **None**, **WEP**, **WPA Only**, **WPA2 Only** or **WPA/WPA2 Mixed**. The default mode is **None**. If you select **WEP**, the page shown in the following figure appears.

WIRELESS SECURITY

Work Mode WEP ▼

ENABLED WEP

Encryption Strength 64 bit ▼ (length applies to all keys)

Choose WEP Key 1 ▼

Key Type HEX (10 characters) ▼

WEP Key1 : 1111111111

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication Open ▼

Submit

Refresh

If you select **WPA Only**, **WPA2 Only** or **WPA/WPA2 Mixed**, the page shown in the following figure appears.

WIRELESS SECURITY

Work Mode:

WPA

WPA Mode:

Encryption Mode: ☒ TKIP ☐ AES ☐ Both

Group Key Update Interval: (60 - 65535)

PRE-SHARED KEY

Pre-Shared Key: (ASCII < 64, HEX = 64)

Click **Submit** to save the settings. For detailed configuration, you may refer to 5.1.3.2 Wireless Security.

5.2.1.4 WPS Settings

Select **WPS Settings**. This page is used to config WPS settings.

Note:

To configure WPS, the WLAN security mode must be WPA-PSK or WPA2-PSK mode.

WPS

The WPS condition must be WPA-PSK or WPA2-PSK security mode , and the SSID should be broadcasted.

Wireless SSID : vds1_01

WPA Mode : WPA-PSK

Pre-Shared Key : *****

WPS CONFIG

☒ Enabled WPS

Push Button : PBC

Input Station PIN : PIN

WPS Session Status :

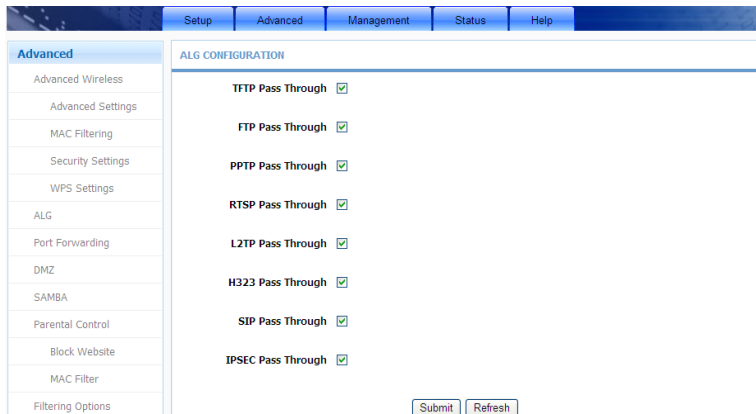
Apply Cancel

The following table describes the parameters of this page.

Field	Description
Wireless SSID	Select one SSID of the CPE.
Enabled WPS	Choose to enable WPS function to set the following parameters.
PBC	In this way, the router generates PIN. Click this button, the router will generate a PIN, and meanwhile press the WPS button on the wireless client. The wireless client automatically establishes connection with the router under encryption mode without inputting the key.
PIN	In this way, the wireless client generates PIN. Enter PIN of the wireless client in the Input Station PIN field, and then click PIN to establish the connection.
WPS Session Status	Display the session status.

5.2.2 ALG

Choose **Advanced > ALG**. The page shown in the following figure appears. In this page, you can enable passthrough of TFTP, FTP, PPTP, RTSP, L2TP, H323, SIP and IPSEC.



5.2.3 Port Forwarding

This function is used to open ports in your device and redirect data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in.

Choose **Advanced > Port Forwarding**. The page shown in the following figure appears.

SetupAdvancedManagementStatusHelp

Advanced

Advanced Wireless

ALG

Port Forwarding

DMZ

SAMBA

Parental Control

Filtering Options

QoS Configuration

Anti-Attack Settings

DNS

Dynamic DNS

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the Internal Port Start or Internal Port End is not recommended. If the External Port Start or the External Port End changes, the Internal Port Start or Internal Port End automatically changes accordingly.

PORT FORWARDING SETUP

Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
-------------	----------------	-------------------------	----------	-------------------------	-------------------	---------------	-----------

AddEditDelete

Click **Add** to add a virtual server.

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 80

WAN Connection(s) : PVC:8/32 ▼

Server Name :

☒ Select a Service : (Click to Select) ▼

☐ Custom Server :

Schedule : always ▼ [View Available Schedules](#)

Server IP Address(Host Name) : 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>

Select a service for a preset application, or enter a name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field to appoint the corresponding PC to receive forwarded packets.

Click **Apply** to save the settings. The page shown in the following figure appears. A virtual server is added.

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

PORT FORWARDING SETUP

	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
<input type="checkbox"/>	Active W...	PVC:8/32	3000/3000	tcp	3000/3000	192.168.1.10	Always	
<input type="checkbox"/>	Active W...	PVC:8/32	5670/5670	tcp	5670/5670	192.168.1.10	Always	
<input type="checkbox"/>	Active W...	PVC:8/32	7777/7777	tcp	7777/7777	192.168.1.10	Always	
<input type="checkbox"/>	Active W...	PVC:8/32	7000/7000	tcp	7000/7000	192.168.1.10	Always	

5.2.4 DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

Choose **Advanced** > **DMZ**. The page shown in the following figure appears.

Setup	Advanced	Management	Status	Help
<div> Advanced Advanced Wireless ALG Port Forwarding DMZ SAMBA Parental Control Filtering Options QoS Configuration Anti-Attack Settings DNS Dynamic DNS </div>				
<div> DMZ <hr/> <p>The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.</p> <p>Enter the computer's IP address and click "Apply" to activate the DMZ host.</p> <p>Clear the IP address field and click "Apply" to deactivate the DMZ host.</p> <hr/> DMZ HOST <hr/> <p>WAN Connection : PVC 8/32</p> <p>Enable DMZ : <input type="checkbox"/></p> <p>DMZ Host IP Address : <input type="text"/></p> <p>Apply Cancel</p> </div>				

Choose to enable DMZ, input a DMZ host ip address, and click then **Apply** to save the settings.

5.2.5 SAMBA

Select **Advanced > SAMBA**. The page shown in the following figure appears.

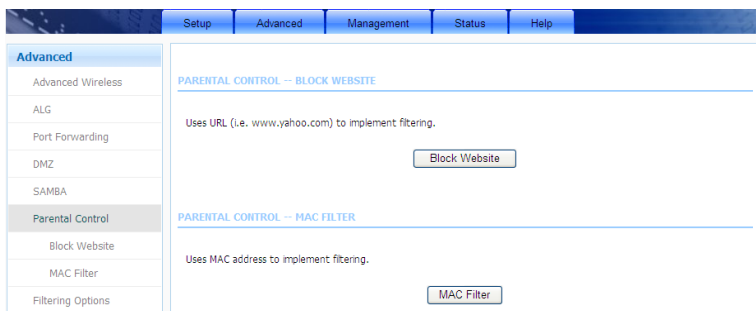
Setup	Advanced	Management	Status	Help
<div> Advanced Advanced Wireless ALG Port Forwarding DMZ SAMBA Parental Control Filtering Options QoS Configuration Anti-Attack Settings DNS Dynamic DNS Network Tools Routing Schedules </div>				
<div> SAMBA <hr/> <p>configure for Samba.</p> <hr/> SAMBA SERVER <hr/> <p>Enable SAMBA : <input type="checkbox"/></p> <p>Workgroup : Workgroup</p> <p>Netbios Name : dsl_route</p> <p>modify the password for user root</p> <p>New SMB password : *****</p> <p>Retype new SMB password : *****</p> <p>Enable USB Storage : <input checked="" type="checkbox"/></p> <p>Enable Anonymous Access : <input checked="" type="checkbox"/></p> <p>Apply Cancel</p> </div>				

The following table describes the parameters of this page.

Field	Description
Enable SAMBA	Select the check box to enable the samba service
Workgroup	Enter the name of your local area network (LAN).
Netbios Name	Enter your netbios name which is an identifier used by netbios services running on a computer.
New SMB password	Enter your samba password for user root.
Retype new SMB password	Reconfirm your samba password here.
Enable USB Storage	Select the check box to support USB storage.
Enable Anonymous Access	Select the check box to allow anonymous users access.

5.2.6 Parental Control

Choose **Advanced > Parental Control**. The **Parent Control** page shown in the following figure appears.



This page provides two useful tools for restricting the Internet access. **Block Websites** allows you to quickly create a list of all websites that you wish to stop users from accessing. **MAC Filter** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

5.2.6.1 Block Website

In the **Parental Control** page, click **Block Website**. The page shown in the following figure appears.

BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

URL	Schedule
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>	

Click **Add**. The page shown in the following figure appears.

ADD SCHEDULE RULE

URL :

☒ **Schedule :** always [View Available Schedules](#)

☐ **Manual Schedule :**

Day(s) : ☐ All Week ☒ Select Day(s)

☐ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

All Day - 24 hrs : ☐

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Enter the website in the **URL** field. Select the **Schedule** from the drop-down list, or select **Manual Schedule** and select the corresponding time and days.

Click **Apply** to add the website to the **BLOCK WEBSITE** table. The page shown in the following figure appears.

BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule
<input type="checkbox"/>	www.xxx....	Always

5.2.6.2 MAC Filter

In the **Parental Control** page, click **MAC Filter**. The page shown in the following figure appears.

BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

Mac Filtering Global Policy:

- ☒ **BLACK_LIST** --Allow all packets but **DENY** those matching any of specific rules listed
- ☐ **WHITE_LIST** --Deny all packets but **ALLOW** those matching any of specific rules listed

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule
----------	-----	----------

Choose **BLACK_LIST** or **WHITE_LIST**, and then click **Add**. The page shown in the following figure appears.

ADD SCHEDULE RULE

User Name :

☐ Current PC's MACAddress :

☒ Other MAC Address :

☒ Schedule : [View Available Schedules](#)

☐ Manual Schedule :

Day(s) : ☐ All Week ☒ Select Day(s)

☐ Sun ☐ Mon ☐ Tue ☐ Wed

☐ Thu ☐ Fri ☐ Sat

All Day - 24 hrs : ☐

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS Table**. The page shown in the following figure appears.

BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

Mac Filtering Global Policy:

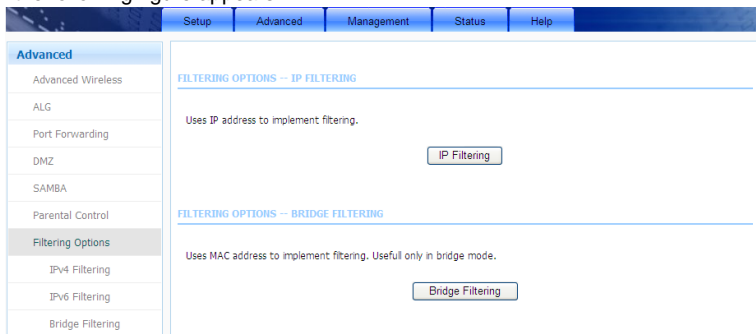
- ☒ **BLACK_LIST** --Allow all packets but **DENY** those matching any of specific rules listed
- ☐ **WHITE_LIST** --Deny all packets but **ALLOW** those matching any of specific rules listed

BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule
<input type="checkbox"/>	aa	00:22:b0:69:0d:63	Always

5.2.7 Filtering Options

Choose **Advanced > Filtering Options**. The **Filtering Options** page shown in the following figure appears.

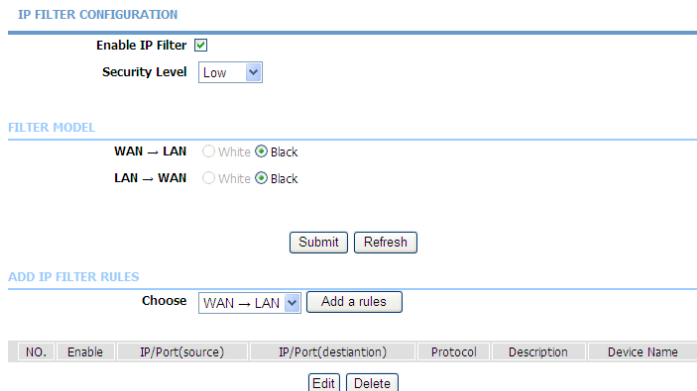


5.2.7.1 IPv4 Filtering

In the **Filtering Options** page, click **IPv4 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv4 firewall function.

Note:

The settings are applicable only when IP filter is enabled.



Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.

IP FILTER CONFIGURATION

Connection

Enable ☒

Protocol

Source IP

Source Mask

Source Port -

Destination IP

Destination Mask

Destination Port -

Description

The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv4 WAN connection.
Enable	Tick in the box to enable a filter rule.
Protocol	Choose a protocol corresponding to the rule. You may choose TCP , UDP , ICMP or TCP/UDP .
Source/ Destination IP	Original/ destination IP address.
Source/ Destination Mask	Original/ destination mask.
Source/Destination Port	Original/ end port, which is the original port range.
Description	You can describe this IPv4 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

IP FILTER CONFIGURATION

Enable IP Filter ☒

Security Level Low

FILTER MODEL

WAN → LAN ☐ White ☒ Black

LAN → WAN ☐ White ☒ Black

Submit Refresh

ADD IP FILTER RULES

Choose WAN → LAN Add a rules

NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input type="radio"/> 1	1	/	/	ICMP	Filter 1	PVC:8/32

Edit Delete

5.2.7.2 IPv6 Filtering

In the **Filtering Options** page, click **IPv6 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv6 firewall function.

Note:

The settings are applicable only when the firewall is enabled.

IP FILTER CONFIGURATION

Enable IP Filter ☒

Security Level Low

FILTER MODEL

WAN → LAN ☐ White ☒ Black

LAN → WAN ☐ White ☒ Black

Submit Refresh

ADD IP FILTER RULES

Choose WAN → LAN Add a rules

NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input type="radio"/>						

Edit Delete

Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.

IPv6 FILTER CONFIGURATION

Connection
 Enable ☒
 Protocol
 Source IP
 Source Prefix length
 Source Port -
 Destination IP
 Source Prefix length
 Destination Port -
 Description

The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv6 WAN connection.
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose TCP , UDP , ICMPv6 or TCP/UDP .
Source/ Destination IP	Original/ destination IP address
Source prefix length	Original/ destination mask
Source/Destination Port	Original/ end port, which is the original port range
Description	You can describe this IPv6 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

IP FILTER CONFIGURATION

Enable IP Filter ☒Security Level Low

FILTER MODEL

WAN → LAN ☐ White ☒ BlackLAN → WAN ☐ White ☒ BlackSubmit Refresh

ADD IP FILTER RULES

Choose WAN → LAN Add a rules

	NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input type="radio"/>	1	1	/	/	ICMP	Filter 1	PVC:8/32

Edit Delete

5.2.7.3 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page shown in the following figure appears. This page is used to configure bridge parameters. In this page, you can change the settings or view some information of the bridge and its attached ports.

BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

- ☒ **ALLOW** all packets but **DENY** those matching any of specific rules listed
- ☐ **DENY** all packets but **ALLOW** those matching any of specific rules listed

Apply Cancel

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME
---------	----------	------	------	-----	------

Add Edit Delete

As instructed in the page, choose a bridge filtering global policy as **ALLOW** or **DENY**, and then Click **Add** to add a bridge filter. The page shown in the following figure appears.

ADD BRIDGE FILTER

Protocol Type: (Click to Select) ▼

Destination MAC Address:

Source MAC Address:

User Priority: (0-7)

VlanID: (0-4095)

Frame Direction: WAN=>LAN ▼

Time schedule: always ▼ [View Available Schedules](#)

Wan interface: select all interface ▼

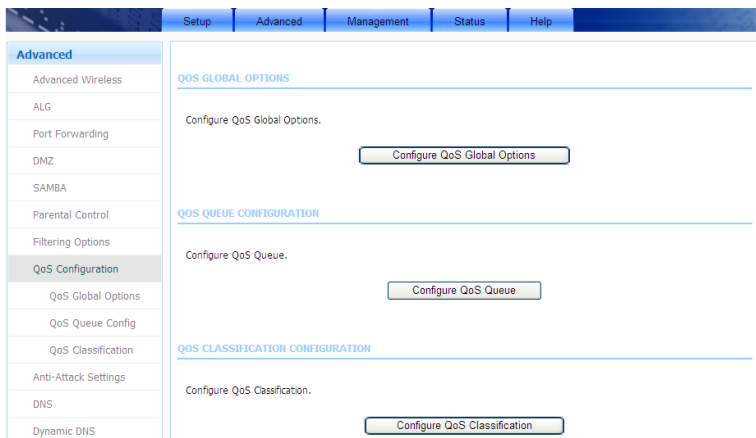
The following table describes the parameters of this page.

Field	Description
Protocol Type	Choose a third-layer protocol type for bridge filtering from the drop-down list. You may choose PPPoE , IPv4 , IPv6 , AppleTalk , IPX or NetBEUI .
Destination MAC Address	The MAC address of sendee of the message
Source MAC Address	The MAC address of sender of the message
User priority	Vlan priority.
VlanID	Vlan ID of a message.
Frame Direction	Choose the sending direction as WAN to LAN or LAN to WAN .
Time schedule	Choose the filtering strategy as always or never .
Wan interface	Set an effective interface for the bridge filtering rule.

Click **Apply** to save the settings.

5.2.8 QoS Configuration

Choose **Advanced > QoS Configuration**. The **QoS Configuration** page shown in the following figure appears.



5.2.8.1 QoS Global Options

In the **QoS Configuration** page, click **QoS Global Options**. The page shown in the following figure appears. You can tick in the checkbox and then click **Submit** to enable queuing operation.

QOS GLOBAL CONFIGURATION

Enable Queuing Operation ☐

Submit

Refresh

5.2.8.2 QoS Queue Config

In the **QoS Configuration** page, click **QoS Queue Config**. The page shown in the following figure appears. In this page, you can set QoS flow control.

QOS GLOBAL CONFIGURATION

Direction ☒ Upstream(Lan -> Wan) ☐ Downstream(Wan -> Lan)

Enable ☒

Upstream Bandwidth Kbps (0 means no limit bandwidth)

Scheduling Strategy SP (Note: Scheduling change would clear the queue configuration)

Enable DSCP/TC Mark ☐

Enable 802.1P Mark ☐

The following table describes the parameters of this page.

Field	Description
Direction	Choose Upstream queue or Downstream queue.
Enable	Tick in the box to enable queue.
Upstream Bandwidth	Total bandwidth for upstream flow
Scheduling Strategy	Scheduling algorithm of QoS queue
Enable DSCP/TC Mark	You may tick in the box to permit DSCP/TC Mark.
Enable 802.1P Mark	You may tick in the box to permit 802.1P Mark.

After setting the parameters, click **Add Queue** to add a queue.

In the above page, when **Upstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.

UPSTREAM QUEUE CONFIGURATION

Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	WAN	<input type="button" value="Delete"/>
2	UP_Q_4	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	WAN	<input type="button" value="Delete"/>
3	UP_Q_5	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	WAN	<input type="button" value="Delete"/>
4	UP_Q_6	<input checked="" type="checkbox"/>	<input type="text" value="4"/>	WAN	<input type="button" value="Delete"/>

When **Downstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.

DOWNSTREAM QUEUE CONFIGURATION

Number	Name	Enable	Precedence	Egress Interface	Operation
1	DOWN_Q_7	<input type="checkbox"/>	1	LAN	Delete
2	DOWN_Q_8	<input type="checkbox"/>	2	LAN	Delete
3	DOWN_Q_9	<input type="checkbox"/>	3	LAN	Delete
4	DOWN_Q_10	<input type="checkbox"/>	4	LAN	Delete

After modifying a queue, click **Submit** to enable the modification. Click **Refresh** to refresh the queue.

5.2.8.3 QoS Classification

In the **QoS Configuration** page, click **QoS Classification**. The page shown in the following figure appears. You can configure QoS queue rule.

QOS CLASSIFY CONFIG

LIST

Classify Number	Enable	Classify Condition	Classify Mark	Classify Queue	Operation
1	1	Source/Destination MAC address : / Ethernet Type : IPv4 VLANID : -1 802.1P : -1 Source/Destination IP address : /81.47.224.0 Source/Destination Mask : /255.255.252.0 DSCP value : Do not mark Protocol Type : Do not match Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	Edit Delete

Click **Add Classification Rule**. The page shown in the following figure appears.

QOS FLOW CLASSIFY CONFIG

Classify Type ☒ Upstream Flow Classify ☐ Downstream Flow ClassifyEnable ☐

CLASSIFY CONDITIONS

Ip Protocol Type

Input Interface

Source MAC address

Source MAC mask

802.1P

Source IPv4 address

Source subnet mask

Destination IPv4 address

Destination subnet mask

DSCP Check

Protocol Type

Source port range -

Destination port range -

CLASSIFY MATCH RESULT

Classify Queue

DSCP Mark

The following table describes the parameters of this page.

Field	Description
Classify Type	Set the QoS rule type as Upstream or Downstream .
Enable	Tick in the box to enable this QoS rule.
Ip Protocol Type	Select the protocol type IPv4 or IPv6 .
Input Interface	Based on the Classify Type, choose a WAN/LAN interface.
802.1P	Choose a matched 802.1P VLAN priority.
DSCP Check	Choose a matched DSCP type.
Protocol Type	Choose a protocol type matching with the QoS rule.

Field	Description
Source/ Destination port range	Input a source port range and a destination port range. For example, input a UDP/TCP port range.
Classify Queue	Choose a QoS queue for the rule.
DSCP Mark	Set a DSCP Mark for this QoS rule.

Click **Submit** to add the rule to the list. You may click **Edit** to modify the existing classification rule, or click **Delete** to delete it.

5.2.9 Anti-Attack Settings

Choose **Advanced > Anti-Attack Settings**. The **Anti-Attack Configuration** page shown in the following figure appears.

The screenshot shows the 'ANTI-ATTACK CONFIGURATION' page. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar is under 'Advanced' and lists various settings, with 'Anti-Attack Settings' highlighted. The main content area has the title 'ANTI-ATTACK CONFIGURATION' and contains the following settings:

- Enable Anti-Attack**: ☒
- Enable Attack Log**: ☐
- INDIVIDUAL PROTECTION SWITCH**:
 - ☒ Enable SYN Attack Protection, Max SYN Connections Per Second: 50 (Peer/Second)
 - ☒ Enable Attack Protection Function of Fraggle
 - ☒ Enable Attack Protection Function of Echo Char
 - ☒ Enable Attack Protection Function of IP Land
 - ☒ Enable Protection of Anti PortScan
- ANTI INVALID PACKETS SWITCH**:
 - ☒ TCP Flags: Set "SYN FIN"
 - ☒ TCP Flags: Set "SYN RST"
 - ☒ TCP Flags: Set "FIN RST"
 - ☒ TCP Flags: Unset "ACK", Set "FIN"
 - ☒ TCP Flags: Unset "ACK", Set "PSH"
 - ☒ TCP Flags: Unset "ACK", Set "URG"
 - ☒ TCP Flags: Unset "SYN ACK FIN RST URG PSH"
 - ☒ TCP Flags: Set "SYN ACK FIN RST URG PSH"
 - ☒ TCP Flags: Unset "PSH", Set "SYN ACK FIN RST URG"
 - ☒ TCP Flags: Unset "SYN ACK RST URG PSH", Set "FIN"
 - ☒ TCP Flags: Unset "SYN ACK RST", Set "FIN URG PSH"

At the bottom of the configuration area are 'Submit' and 'Refresh' buttons.

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

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Click **Submit** to save the settings.

5.2.10 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Advanced > DNS**. The page shown in the following figure appears.

The screenshot shows a web interface with a top navigation bar containing 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. On the left is a sidebar menu with 'Advanced' selected, and sub-items: 'Advanced Wireless', 'ALG', 'Port Forwarding', 'DMZ', 'Samba', 'Parental Control', 'Filtering Options', 'QoS Configuration', 'Anti-Attack Settings', and 'DNS'. The main content area is titled 'DNS' and includes the instruction 'Click "Apply" button to save the new configuration.' Below this is a section titled 'DNS SERVER CONFIGURATION'. It features a 'Wan Connection' dropdown menu set to 'PVC 8/32'. There are two radio button options: 'Obtain DNS server address automatically' (which is selected) and 'Use the following DNS server addresses'. The latter option has two text input fields labeled 'Preferred DNS server' and 'Alternate DNS server'. At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

If you are using the device for DHCP service on the LAN or using DNS servers on the ISP network, select **Obtain DNS server address automatically**.

If you have DNS IP addresses provided by your ISP, select **Use the following DNS server addresses**, and enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

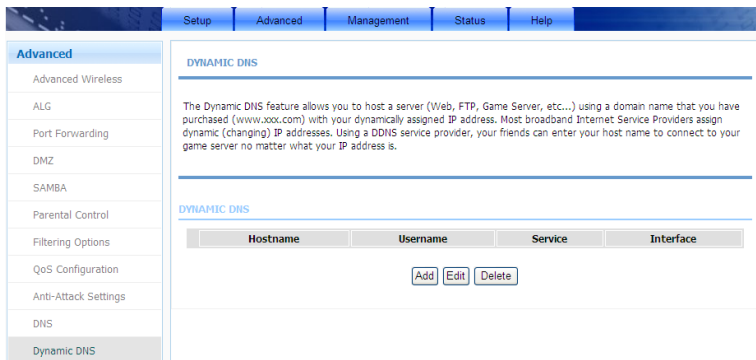
Click **Apply** to save the settings.

5.2.11 Dynamic DNS

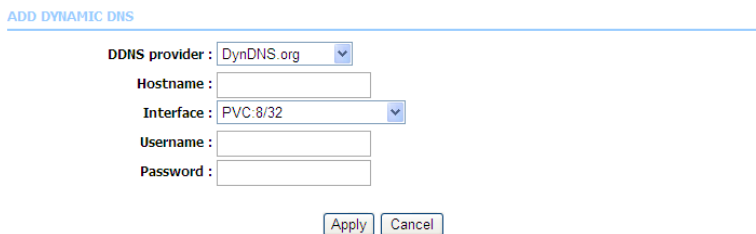
The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign

public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DynDNS.org, 3322.org and freedns.afraid.org).

Choose **Advanced > Dynamic DNS**. The page shown in the following figure appears.



Click **Add** to add dynamic DNS. The page shown in the following figure appears.



The following table describes the parameters of this page.

Field	Description
DDNS provider	Select one of the DDNS registration organizations from the down-list drop. Available servers include DynDns.org , 3322.org and freedns.afraid.org .

Field	Description
Host Name	Enter the host name that you registered with your DDNS service provider.
Username	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.

Click **Apply** to save the settings.

5.2.12 Network Tools

Choose **Advanced > Network Tools**. The page shown in the following figure appears.

Setup	Advanced	Management	Status	Help
<div> <div> Advanced Advanced Wireless ALG Port Forwarding DMZ SAMBA Parental Control Filtering Options QoS Configuration Anti-Attack Settings DNS Dynamic DNS Network Tools Port Mapping IGMP Proxy IGMP Snooping MLD Configuration UPnP ADSL SNMP TR-064 TR-069 Certificates Printer Routing Schedules NAT DLNA IP Tunnel Logout </div> <div> <p>NETWORK TOOLS -- PORT MAPPING</p> <p>Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.</p> <p>Port Mapping</p> <p>NETWORK TOOLS -- IGMP PROXY</p> <p>Transmission of identical content, such as multimedia, from a source to a number of recipients.</p> <p>IGMP Proxy</p> <p>NETWORK TOOLS -- IGMP SNOOPING</p> <p>Transmission of identical content, such as multimedia, from a source to a number of recipients.</p> <p>IGMP Snooping</p> <p>NETWORK TOOLS -- MLD CONFIGURATION</p> <p>Transmission of identical content, such as multimedia, from a source to a number of recipients.</p> <p>MLD Configuration</p> <p>NETWORK TOOLS -- UPNP</p> <p>Allows you to enable or disable UPnP.</p> <p>Upnp</p> <p>NETWORK TOOLS -- ADSL</p> <p>Allows you to configure advanced settings for ADSL.</p> <p>ADSL</p> <p>NETWORK TOOLS -- SNMP</p> <p>Network Tools -- SNMP</p> <p>SNMP</p> <p>NETWORK TOOLS -- TR-064</p> <p>Allows you to configure TR-064 protocol.</p> <p>TR-064</p> </div> </div>				

(Network Tools-1)

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

Port Mapping -- A maximum 5 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

	Group Name	Interfaces
<input type="checkbox"/>	Lan1	ethernet1,ethernet2,ethernet3,ethernet4,ra0,ra2,ra3,Bridging_0_7,
<input type="checkbox"/>	Clubwifi	ra1,

ADD PORT MAPPING

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
 2. Click "Apply" button to make the changes effective immediately.
-

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces		Available Interfaces
<div></div>	<div>-></div> <div><-</div>	<div>ethernet1 ethernet2 ethernet3 ethernet4 ra0 ra2 ra3 Bridging_0_7</div>

The procedure for creating a mapping group is as follows:

- Step 1** Enter the group name.
- Step 2** Select interfaces from the **Available Interface** list and click the <- arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.
- Step 3** Click **Apply** to save the settings.

5.2.12.2 IGMP Proxy

Choose **Advanced > Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.

IGMP PROXY

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:

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

IGMP PROXY CONFIGURATION

☐ Enable IGMP Proxy

WAN Interface : PVC:8/32

Port Binding Lan1

Apply

Cancel

IGMP TABLE

Group Address	Interface	State
---------------	-----------	-------

Refresh

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.

Click **Apply** to save the settings.

5.2.12.3 IGMP Snooping

Choose **Advanced > Network Tools** and click **IGMP Snooping**. The page shown in the following figure appears. When IGMP Snooping is enabled, the multicast data transmits through the specific LAN port which has received the request report.

IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

Enabled : ☐

LastMemberQueryInterval :

HostTimeout :

MrouterTimeout :

LeaveTimeout :

MaxGroups :

5.2.12.4 MLD Configuration

Choose **Advanced > Network Tools** and click **MLD Configuration**. The page shown in the following figure appears. This section allows you to configure the MLD setup settings of your router.

MLD SETTINGS

This section allows you to configure the MLD Setup settings of your Router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

MLD PROXY

☐ Enable Mld Proxy

WAN Connection :

MLD SNOOPING

☐ Enable Mld Snooping

The following table describes the parameters of this page.

Field	Description
Enable Mld Proxy	You can choose to enable MLD proxy.
WAN Connection	Choose an IPv6 WAN connection.
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.

5.2.12.5 UPnP

Choose **Advanced > Network Tools** and click **UPnP**. The page shown in the following figure appears.

UPnP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPnP SETUP

☐ Enable UPnP

WAN Connection :

LAN Connection :

In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

5.2.12.6 ADSL

Choose **Advanced > Network Tools** and click **ADSL**. The page shown in the following figure appears.

ADSL SETTINGS

This page is used to configure the ADSL settings of your ADSL router. You need to disable DSL before you change the ADSL mode.

ADSL SETTINGS

xDSL Mode: Auto Sync-Up

ADSL Type: ANNEX A/I/L/M

Apply

In this page, you can select a DSL mode. Normally, you can keep this factory default setting. The device negotiates the modulation mode with DSLAM. Click **Apply** to save the settings.

5.2.12.7 SNMP

Choose **Advanced > Network Tools** and click **SNMP**. The page shown in the following figure appears. In this page, you can set SNMP parameters.

SNMP CONFIGURATION

This page is used to configure the SNMP protocol.

SNMP CONFIGURATION

☐ Enable SNMP Agent

Read Community: public

Set Community: private

Trap Manager IP:

Trap Community: public

Trap Version: v2c

Apply

Cancel

Click **Apply** to save the settings.

5.2.12.8 TR-064

Choose **Advanced > Network Tools** and click **TR-064**. The page shown in the following figure appears. In this page, you can enable the **TR064** service.

TR064 CONFIGURATION

This page is used to configure the TR064 protocol.

☐ Enable TR064

Apply Cancel

5.2.12.9 TR-069

Choose **Advanced > Network Tools** and click **TR069**. The page shown in the following figure appears. In this page, you can configure the TR069 CPE.

TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

TR-069 CLIENT -- CONFIGURATION

Cwmp: ☐ Disabled ☒ Enabled

Inform: ☒ Disabled ☐ Enabled

Inform Interval: 86400

ACS URL: https://main.acs.telefonica

ACS User Name: ACS1234

ACS Password: •••••

☒ Connection Request Authentication

Connection Request User Name: ACS1234

Connection Request Password: •••••

Apply Cancel

Click **Apply** to save settings.

5.2.12.10 Certificates

Choose **Advanced > Network Tools** and click **Certificates**. The **Certificates** page shown in the following figure appears.

CERTIFICATES -- TRUSTED CA

Trusted CA certificates are used by you to verify peers' certificates.

Trusted CA

Click **Trusted CA** button to import a certificate.

CERTIFICATES -- TRUSTED CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificates can be stored. Notice you have to synchronize your time when use certificate

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action
cert	O=Grupo Telefonica/O=TME/ST=A7...	self signed certific...	Delete

Input Certificate

Note:

You can input a certificate after deleting the existing certificate.

TRUSTED CA CERTIFICATES

Enter certificate name and paste certificate content.

IMPORT CA CERTIFICATE

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
<insert Certificate here>  
-----END CERTIFICATE-----
```

Back apply Cancel

5.2.12.11 Printer

Choose **Advanced** > **Network Tools** and click **Printer**. The **Printer** page shown in the following figure appears. In this page, you can enable/disable printer support.

PRINT SERVER SETTINGS

This page allows you to enable/disable printer support.

Enable ☐

Printer Name

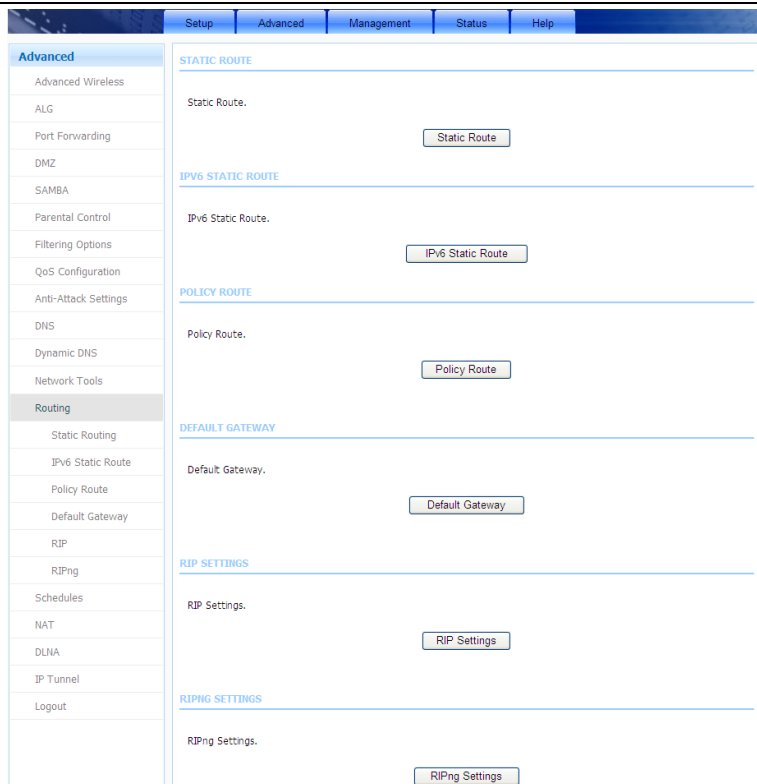
URL:

DISPLAY LIST

Manufacturer	Model	CHD	Firmware Version
<div>Apply Cancel</div>			

5.2.13 Routing

Choose **Advanced** > **Routing**. The page shown in the following figure appears.



5.2.13.1 Static Routing

Choose **Advanced > Routing** and click **Static Routing**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.

STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

Destination	Subnet Mask	Gateway	Interface
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Click **Add** to add a static route. The page shown in the following figure appears.

STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

Use Gateway IP Address :

Use Interface : ▼

The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the router.
Subnet Mask	The subnet mask of the destination IP
Use Interface	The interface name of the router output port.
Use Gateway IP Address	The gateway IP address of the router.

Click **Apply** to save the settings.

5.2.13.IPv6 Static Route

Choose **Advanced > Routing** and click **IPv6 Static Route**. The page shown in the following figure appears.

IPv6 STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

ROUTING -- IPv6 STATIC ROUTE

Status	Destination	Gateway	Interface
<div> <div>Add</div> <div>Edit</div> <div>Delete</div> </div>			

Click Add to add an IPv6 static route. The page shown in the following figure appears.

IPv6 STATIC ROUTE ADD

Enable : ☐

Destination Network Address :

Use Gateway IP Address :

Use Interface : LAN Group1 ▼

The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the static route.
Use Gateway IP Address	The gateway IP address of the static route.
Use Interface	The interface name of the static route.

5.2.13.3 Policy Route

Choose **Advanced > Routing** and click **Policy Route**. The page shown in the following figure appears. The policy route binds one WAN connection and one LAN interface.

POLICY ROUTE

Policy Route :chose one Wanconnection and one Lanconnection then bind them.

POLICY ROUTE SETUP

	WAN	LAN

Click **Add**, and the page shown in the following figure appears. Choose one WAN connection and at lease one LAN connection to bind together, and then click **Apply**.

WAN INSTANCE AND LAN INSTANCE

WAN Connection

LAN Connection

- ☐ ethernet1
- ☐ ethernet2
- ☐ ethernet3
- ☐ ethernet4
- ☐ ra0
- ☐ ra1
- ☐ ra2
- ☐ ra3

5.2.13.4 Default Gateway

Choose **Advanced > Routing** and click **Default Gateway**. The page shown in the following figure appears. You may assign a default gateway for the router to use first.

DEFAULT GATEWAY

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway OR a WAN interface. Click "Apply" button to save it.

DEFAULT GATEWAY

☒ Enable Automatic Assigned Default Gateway

☐ Use Gateway IP Address :

☐ Use Interface :

Click **Apply** to save the settings.

5.2.13.5 RIP

Choose **Advanced > Routing** and click **RIP**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.

RIP CONFIGURATION

To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

RIP

Interface	VPI/VCI	Version	Operation	Enabled	Passive
PVC:8/32	PVC:8/32	<input type="button" value="1"/>	Active	<input type="checkbox"/>	<input type="checkbox"/>
PVC:8/36	PVC:8/36	<input type="button" value="1"/>	Active	<input type="checkbox"/>	<input type="checkbox"/>
pppoe_8_35_0_2_Internet	PVC:8/35	<input type="button" value="1"/>	Active	<input type="checkbox"/>	<input type="checkbox"/>
Lan1	-	<input type="button" value="1"/>	Active	<input type="checkbox"/>	<input type="checkbox"/>

If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

5.2.13.6 RIPng

Choose **Advanced** > **Routing** and click **RIPng**. The page shown in the following figure appears. You can enable or disable dynamic routing of an IPv6 interface after establishing an IPv6 PVC connection.

RIPNG CONFIGURATION

To activate RIPng for the interface, place a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIPng based on the configuration.

RIPNG

Interface	VPI/VCI	Enabled

5.2.14 Schedules

Choose **Advanced** > **Schedules**. The page shown in the following figure appears.

SCHEDULES

Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

SCHEDULE RULES

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time

Click **Add** to add schedule rule. The page shown in the following figure appears.

ADD SCHEDULE RULE

Name :

Day(s) : ☐ All Week ☒ Select Day(s)

☐ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

All Day - 24 hrs : ☐

Start Time : : (hour:minute, 24 hour time)
 End Time : : (hour:minute, 24 hour time)

Click **Apply** to save the settings.

5.2.15 NAT

Choose **Advanced > NAT**. The page shown in the following figure appears. Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are unidirectional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts

NAT

Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.

NAT TABLES

Name	Internal IP Address	External IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

Click **Add** to set a NAT set in the following page. For IP type, you can choose single IP or IP range. Click **Apply** to save and enable the setting.

NAT SETTINGS

Entry Name :

Internal IP Type : ▼

Internal IP Address :

External IP Type : ▼

External IP Address :

5.2.16 DLNA

Choose **Advanced** > **DLNA**. The page shown in the following figure appears. In this page, you can choose to enable DLNA, and then click **Apply**.

DLNA

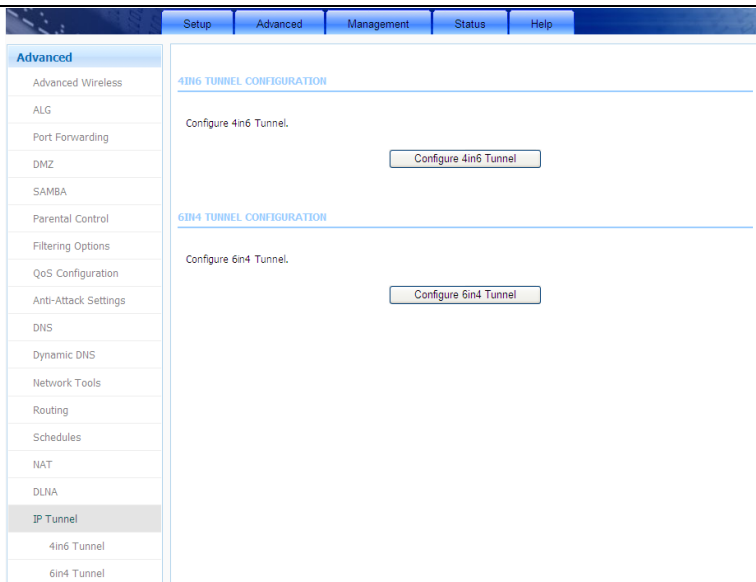
You can Enable or Disable DLNA here.

DLNA SETTING

Enable DLNA : ☒

5.2.17 IP Tunnel

Choose **Advanced** > **IP Tunnel**. The page shown in the following figure appears.



5.2.17.1 4in6 Tunnel

Choose **Advanced > IP Tunnel** and then click **4in6 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv4 penetration through IPv6 network. When only IPv6 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.

IP TUNNEL CONFIGURATION

Network topology in IPv4/v6 Internet, some only run IPv6 protocol stack P routers form the pure IPv6 backbone. However, due to the large IPv4 applications will be a period of time is still widely used, so the need for pure IPv6 backbone network to IPv4 stack border access.

IPTUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>					

DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism	Dynamic	RemoteIPv6Address	ConnStatus	Select
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>				

Click **Add** below the table **IPTUNNEL** to add tunnel items. The page shown in the following figure appears.

ADD TUNNEL ITEMS

Tunnel Name:
 Tunnel Mode: 4in6
 Wan Interface:
 Lan Interface: LAN:br0

The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.
Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **DS-Lite IPv4 over IPv6 Tunnel List** to add a DS-Lite item, which is a 4in6 tunnel. The page shown in the following figure appears.

Mechanism: DualStackLite ▾

Dynamic: 0 ▾

RemoteIPv6Address:

Apply Cancel

The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is DS-Lite, which is 4in6 tunnel.
Dynamic	Set the obtaining mode of remote IPv6 addresses. You can select 0 or 1 .
RemoteIPv6Address	Set the remote end IPv6 address of the tunnel.

Click **Apply** to enable the settings.

5.2.17.26in4 Tunnel

Choose **Advanced > IP Tunnel** and then click **6in4 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv6 penetration through IPv4 network. When only IPv4 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.

IP TUNNEL CONFIGURATION

6rd is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of Internet service providers.

It is derived from 6to4, a preexisting mechanism to transfer IPv6 packets over the IPv4 network, with the significant change that it operates entirely within the end-user's ISP's network, thus avoiding the major architectural problems inherent in the original design of 6to4.

IP TUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
-------------	------	---------------	---------------	-----------	---------

Add Edit Delete

IPv6 RAPID DEPLOYMENT

Mechanism	Dynamic	IPv4MaskLen	Prefix	BorderRelayAddress	ConnStatus	Select
-----------	---------	-------------	--------	--------------------	------------	--------

Add Edit Delete

Click **Add** below the table **IPTUNNEL** to add tunnel items. The page shown in the following figure appears.

ADD TUNNEL ITEMS

Tunnel Name:

Tunnel Mode: 6in4 ▼

Wan Interface: PVC: 8/32 ▼

Lan Interface: LAN: br0 ▼

The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.
Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **IPv6 Rapid Deployment** to add a 6RD item, which is a 6in4 tunnel. The page shown in the following figure appears.

IPv6 RAPID DEPLOYMENT LIST

Mechanism: Ipv6RapidDeployment ▼

Dynamic: 0 ▼

IPv4MaskLen:

Prefix:

BorderRelayAddress:

The following table describes the parameters of this page.

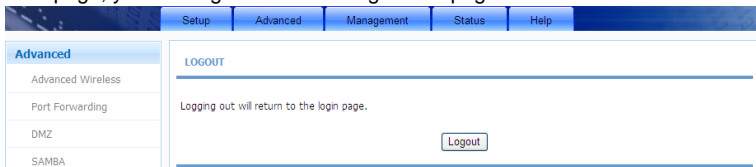
Field	Description
Mechanism	The tunnel type is 6RD, which is a 6in4 tunnel.
Dynamic	Set the obtaining mode of Border Relay Address.

IPv4MaskLen	Set the subnet mask digits of the IPv4 address of the local WAN interface.
Prefix	Set the IPv6 prefix of the 6RD tunnel.
BorderRelayAddress	Set the Border Relay IPv4 address at the remote end.

Click **Apply** to enable the settings.

5.2.18 Logout

Choose **Advanced** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

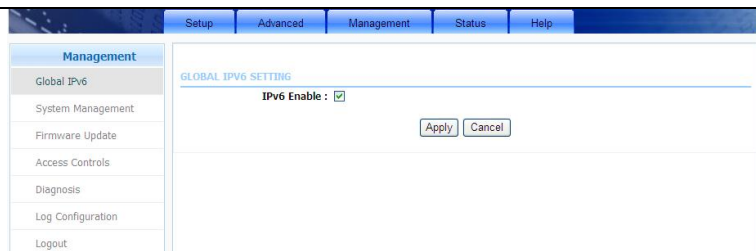


5.3 Management

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure. The submenus are **Global IPv6**, **System Management**, **Firmware Update**, **Access Controls**, **Diagnosis**, **Log Configuration** and **Logout**.

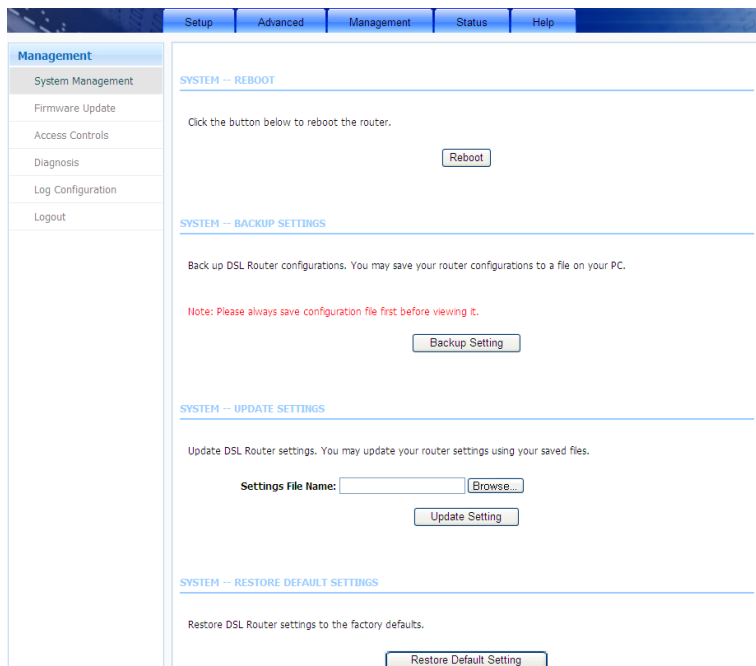
5.3.1 Global IPv6

Choose **Management** > **Global IPv6**. The page shown in the following figure appears. You can choose to IPv6 function.



5.3.2 System Management

Choose **Management > System Management**. The page shown in the following figure appears.



In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.

The buttons in this page are described as follows.

Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
Update setting	Click Browse to select the configuration file of device and then click Update Settings to begin updating the device configuration.
Restore Default Setting	Click this button to reset the device to default settings.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

5.3.3 Firmware Update

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

Management

- Global IPv6
- System Management
- Firmware Update**
- Access Controls
- Diagnosis
- Log Configuration
- Logout

FIRMWARE UPDATE

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

FIRMWARE UPDATE

Current Firmware Version: 1.1.0

Current Firmware Date: 08/01/2012-12:43:09

Select File:

Clear Config: ☐

To update the firmware, take the following steps.

Step 1 Click **Browse...** to locate the file.

Step 2 Select **Clear Config** to clear the current configuration and restore the default.

Step 3 Click **Update Firmware** to copy the file.

The device loads the file and reboots automatically.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

5.3.4 Access Controls

Choose **Management > Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **User Management**, **Local Access Control**, **Remote Access Control** and **IP Address**.

The screenshot shows the 'Access Controls' page in the VB104W User Manual. The page has a sidebar menu on the left with the following items: Management, Global IPv6, System Management, Firmware Update, Access Controls (highlighted), User Management, Local Access Control, Remote Access Control, IP Address, Diagnosis, Log Configuration, and Logout. The main content area is divided into four sections, each with a title and a description, and a button to access the configuration page.

- ACCOUNT PASSWORD**: Manage DSL Router user accounts. Button: Account Password
- SERVICES**: A Service Control List ("SQL") enables or disables services from being used. Button: Services
- IP ADDRESS**: Permits access to local management services. Button: IP Address
- ENABLE IPV6 FORWARDING**: Enable IPv6 Forwarding : ☒. Buttons: Apply, Cancel

5.3.4.1 Account Password

In the **Access Controls** page, click **Account Password**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.

ACCOUNT PASSWORD

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. This user name can not be used in local.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username:	<input type="text" value="1234"/>
New Username:	<input type="text" value="1234"/>
Current Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out:	<input type="text" value="29"/>	(5 ~ 30 minutes)
--------------------	---------------------------------	------------------

You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

Select the **Username** from the drop-down list. You can select **1234** (subject to different models), **user** or **support**.

Enter the current and new passwords and confirm the new password to change the password. Click **Apply** to apply the settings.

Web Idle Time Out is the idle duration of user interfaces. After this duration, you need to login to the router again for operation.

5.3.4.2 Services

In the **Access Controls** page, click **Services**. The page shown in the following figure appears.

SERVICES

A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROL – SERVICES

Select WAN Connections PVC: 8/36

IPv4 TABLE

Service	LAN	WAN	WAN Access Destination Host(IP / Mask : Port)		
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 21
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 80
ICMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 0
SSH	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 22
TELNET	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 23
TFTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 69
DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 53
TR069	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	/ 0.0.0.0	: 7547

Apply

Cancel

In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

Select the management services that you want to enable or disable on the LAN or WAN interface. Click **Apply** to apply the settings.

Note:

If you disable HTTP service, you cannot access the configuration page of the device any more.

5.3.4.3 Local Access Control

Under the **Access Controls** menu, click **Local Access Control**. The page shown in the following figure appears. This page allows you to enable or disable LAN management services. For example, if the Telnet service is enabled on port 23, the remote host can access the router by Telnet through port 23.

LOCAL ACCESS CONTROL

Enable Local Access ☒

Choose A Connection LAN1

Service	Enable	Source IP	Source Mask	Protocol	Port
FTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	21
HTTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	80
ICMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	ICMP	0
SNMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	1050
SSH	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	22
TELNET	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	23
TFTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	69
DNS	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	53
TR069	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	7547

5.3.4.4 Remote Access Control

Under the **Access Controls** menu, click **Remote Access Control**. The page shown in the following figure appears. This page allows you to enable or disable WAN management services. You may refer to 5.3.4.3 Local Access Control.

REMOTE ACCESS CONTROL

Choose A Connection PVC:8/32

Service	Enable	Source IP	Source Mask	Protocol	Destination Port
FTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	21
HTTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	80
ICMP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	ICMP	0
SNMP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	161
SSH	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	22
TELNET	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	23
TFTP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	69
DNS	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	53
TR069	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	7547

Submit

Refresh

5.3.4.5 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.

IP ADDRESS

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Enter the IP address of the management station permitted to access the local management services, and click "Apply".

ACCESS CONTROL -- IP ADDRESSES

☐ Enable Access Control Mode

IP

Add

Delete

In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

Note:

If you enable the ACL, ensure that IP address of the host is in the ACL list.

To add an IP address to the IP list, click **Add**. The page shown in the following figure appears.

IP ADDRESS

IP Address :

Apply

Cancel

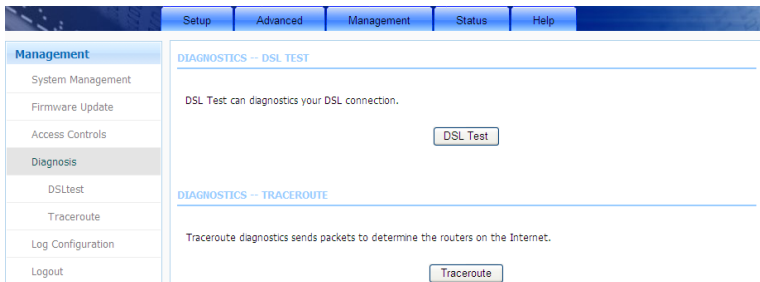
Click **Apply** to apply the settings, and then choose **Enable Access Control Mode** to enable ACL.

5.3.4.6 Enable IPv6 Forwarding

In the **Access Controls** page, you can also choose to enable IPv6 Forwarding. Click **Apply** to enable the setting.

5.3.5 Diagnosis

Choose **Management > Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test** and **Traceroute**.



5.3.5.1 DSL Test

In the **Diagnosis** page, click **DSL Test**. The page shown in the following figure appears. In this page, you can test your DSL connection.

DIAGNOSTICS

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

WAN Connection PVC: 8/32

Click **Run Diagnostic Tests**. After testing, the following figure appears.

DIAGNOSTICS

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

WAN Connection PVC: 8/32

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your LAN 1 Connection	FAIL
Test your LAN 2 Connection	FAIL
Test your LAN 3 Connection	FAIL
Test your LAN 4 Connection	PASS
Test your Wireless Connection	PASS

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

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

TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER

Ping Default Gateway	FAIL
Ping Primary Domain Name Server	FAIL

5.3.5.2 Traceroute

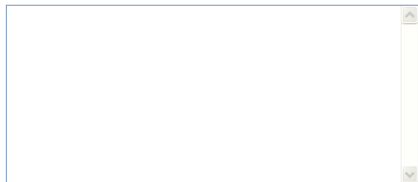
In the **Diagnostics** page, click **Traceroute**. The page shown in the following figure appears. In this page, you can determine the routers on the Internet by sending packets.

TRACEROUTE DIAGNOSIS

Traceroute diagnostics sends packets to determine the routers on the Internet..

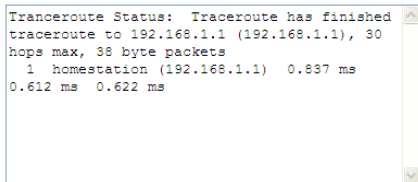
Host :	<input type="text" value="192.168.1.1"/>	
Max TTL :	<input type="text" value="30"/>	(1-128)
Wait times :	<input type="text" value="5"/>	(2-60s)
<div><input type="button" value="Traceroute"/> <input type="button" value="Stop"/></div>		

RESULT



Click **Traceroute** to begin diagnosis. After finish, the page shown in the following figure appears.

RESULT



5.3.6 Log Configuration

Choose **Management > Log Configuration**. The **System Log** page shown in the following figure appears.

Management

- Global IPv6
- System Management
- Firmware Update
- Access Controls
- Diagnosis
- Log Configuration**
- Logout

SYSTEM LOG

If the log mode is enabled, the system will begin to log all the selected events. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

SYSTEM LOG -- CONFIGURATION

☐ Enable Log

Mode : Local

Server IP Address :

Server UDP Port :

This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. In this page, you can enable or disable the system log function.

To log the events, take the following steps.

- Step 1** Select **Enable Log** check box.
- Step 2** Select the display mode from the **Mode** drop-down list.
- Step 3** Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.
- Step 4** Click **Apply** to apply the settings.
- Step 5** Click **View System Log** to view the detail information of system log.

5.3.7 Logout

Choose **Management > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

Management

- System Management
- Firmware Update
- Access Controls
- Diagnosis
- Log Configuration
- Logout**

LOGOUT

Logging out will return to the login page.

5.4 Status

In the main interface, click **Status** tab to enter the **Status** menu as shown in the following figure. The submenus are **Device Info**, **Wireless Clients**, **DHCP Clients**, **IPv6 Status**, **Logs**, **Statistics**, **Route Info** and **Logout**. You can view the system information and monitor performance.

5.4.1 Device Info

Choose **Status > Device Info**. The page shown in the following figure appears.

Setup	Advanced	Management	Status	Help
-------	----------	------------	--------	------

Status

Device Info
Wireless Clients
DHCP Clients
IPv6 Status
Logs
Statistics
Route Info
Logout

DEVICE INFO

This information reflects the current status of your all connection.

SYSTEM INFO

Modem Name :	HG
Serial Number :	001ee332bb11
Time and Date :	1969-12-31 23:53
HardwareVersion :	HG_BH_R2A
SoftwareVersion :	HG_BH_V1.2
Firmware Version :	1.1.0
System Up Time :	00:53:16

INTERNET INFO

Internet Connection Status : PVC 8/32

Internet Connection Status:	Disconnected
Wan service type:	Internet_TR069
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Downstream Line Rate (Kbps):	21566
Upstream Line Rate (Kbps):	1004
Data Time Counter (Second):	N/A

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	IP Address
N/A	PVC:8/32	PPPOE	Disable	
N/A	PVC:8/36	PPPOE	Disable	
N/A	pppoe_8_35_0_2_Internet	PPPOE	Disable	
N/A	Bridging_0_7	BRIDGE	Disable	

WIRELESS INFO

select wireless : vdsl_01

MAC Address:	00:1E:E3:32:BB:1C
Status:	Enable
Network Name (SSID):	vdsl_01
Visibility:	Hide
Security Mode:	WPA

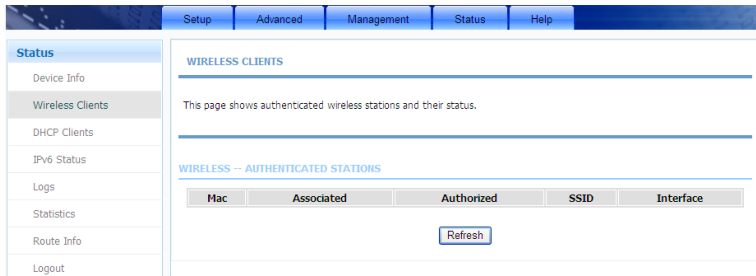
LOCAL NETWORK INFO

MAC Address:	00:1e:e3:32:bb:11
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

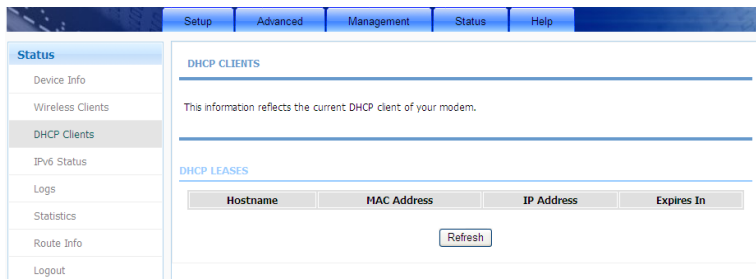
5.4.2 Wireless Clients

Choose **Status > Wireless Clients**. The page shown in the following figure appears. The page displays authenticated wireless stations and their statuses.



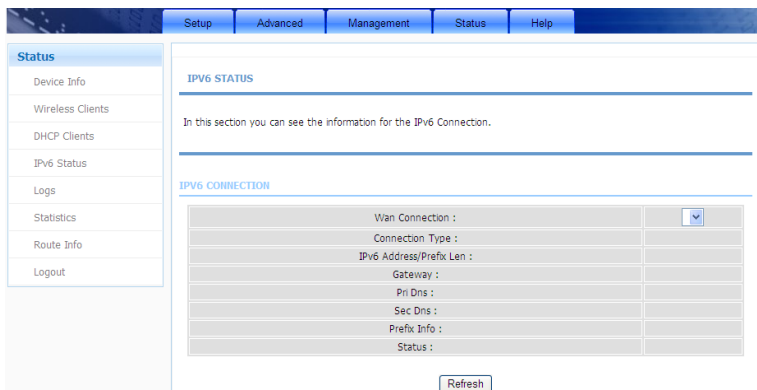
5.4.3 DHCP Clients

Choose **Status > DHCP Clients**. The page shown in the following figure appears. This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).



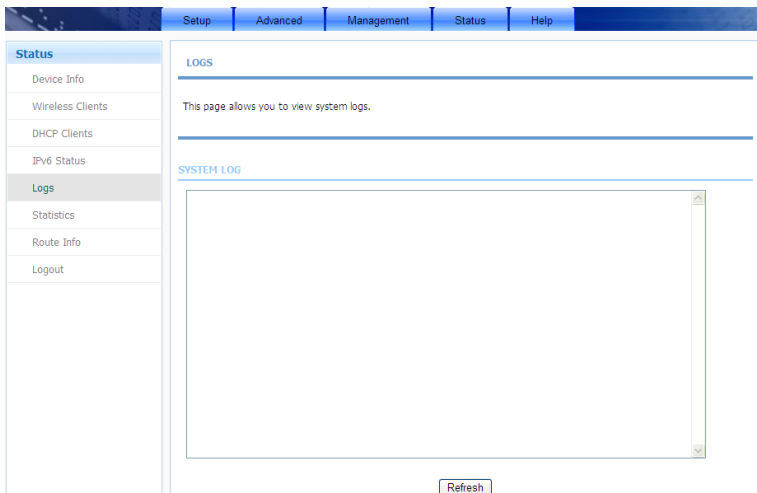
5.4.4 IPv6 Status

Choose **Status > IPv6 Status**. The page shown in the following figure appears. This page displays the IPv6 connection information.



5.4.5 Logs

Choose **Status > Logs**. The page shown in the following figure appears. This page lists the system log. Click **Refresh** to refresh the system log shown in the table.



5.4.6 Statistics

Choose **Status > Statistics**. The page shown in the following figure appears. This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.

Setup | **Advanced** | **Management** | **Status** | **Help**

Status

- Device Info
- Wireless Clients
- DHCP Clients
- IPv6 Status
- Logs
- Statistics**
- Route Info
- Logout

DEVICE INFO

This information reflects the current status of your all connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN4	160114	1316	0	0	1871615	2350	0	0
vdsl_01	24664	224	0		0	11	0	0
vdsl_02	0	0	0		0	0	0	0
vdsl_03	0	0	0		0	0	0	0
vdsl_04	0	0	0		0	0	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
PVC:8/32	PVC:8/32	PPPOE								
PVC:8/36	PVC:8/36	PPPOE								
pppoe_8...	PVC:8/35	PPPOE								
Bridging...	PVC:0/35	BRIDGE								

ADSL

Mode:	G.992.3_Annex_A		
Type:	Interleave		
Line Coding:	Enable		
Status:	Disabled		
Up Time:			
	Downstream	Upstream	
SNR Margin (0.1dB):	80	95	
Attenuation (0.1dB):	40	20	
Output Power (dBm):			
Attainable Rate (Kbps):	23080	1112	
Rate (Kbps):	21566	1004	
D (interleave depth):	0	0	
Delay (msec):	0	0	
Data Counter:	2669	<input type="button" value="Clear"/>	62 <input type="button" value="Clear"/>
HEC Errors:	0	0	
OCF Errors:	0	0	
LCD Errors:	0	0	
CRC Errors:	0	0	
FEC Errors:	5	0	
Total ES	0	1	
Total Frames	2669	62	

5.4.7 Route Info

Choose **Status > Route Info**. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.

The screenshot shows the 'Route Info' page. At the top is a navigation bar with tabs: Setup, Advanced, Management, Status (selected), and Help. On the left is a sidebar menu with options: Status (selected), Device Info, Wireless Clients, DHCP Clients, IPv6 Status, Logs, Statistics, Route Info (highlighted), and Logout. The main content area is titled 'ROUTE INFO' and contains the following text: 'Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect)'. Below this is a section titled 'DEVICE INFO -- ROUTE' containing a table of routes.

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.249.0	0.0.0.0	255.255.255.252	U	0	0	br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	br1

5.4.8 Logout

Choose **Status > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

The screenshot shows the 'Logout' page. The navigation bar and sidebar menu are identical to the previous page. The main content area is titled 'LOGOUT' and contains the text: 'Logging out will return to the login page.' Below this text is a button labeled 'Logout'.

5.5 Help

In the main interface, click **Help** tab to enter the **Help** menu as shown in the following figure. This section provides detailed configuration information for the device. Click a wanted link to view corresponding information.

	Setup	Advanced	Management	Status	Help
Help					
Menu					
Setup					
Advanced					
Management					
Status					
Logout					

HELP MENU

- [Setup](#)
- [Advanced](#)
- [Management](#)
- [Status](#)

SETUP HELP

- [Wizard](#)
- [Internet Setup](#)
- [Wireless](#)
- [Local Network](#)
- [Time and Date](#)

ADVANCED HELP

- [Advanced Wireless](#)
- [Port Forwarding](#)
- [DMZ](#)
- [Parental Control](#)
- [Filtering Options](#)
- [Firewall Settings](#)
- [DNS](#)
- [DDNS](#)
- [Network Tools](#)
- [Routing](#)
- [Schedules](#)

MANAGEMENT HELP

- [System Management](#)
- [Firmware Update](#)
- [Access Controls](#)
- [Diagnosis](#)
- [Log Configuration](#)

STATUS HELP

- [Device Info](#)
- [Wireless Clients](#)
- [DHCP Clients](#)
- [Logs](#)
- [Statistics](#)
- [Route Info](#)

6 Trouble Shooting

Question	Answer
Why are all the indicators off?	<ul style="list-style-type: none"> ● Check the connection between the power adapter and the power socket. ● Check whether the power switch is turned on.
Why the LAN indicator is off?	<p>Check the following:</p> <ul style="list-style-type: none"> ● The connection between the device and your PC, hub or switch ● The running status of the computer, hub, or switch
Why is the DSL indicator not on?	Check the connection between the DSL 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?	<p>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.</p> <ul style="list-style-type: none"> ● Administrator username/password: 1234/1234 (subject to different models). ● Common username/password: user/user. ● ISP technician username/password: support/support.