

VB204W

User Manual

Table of 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.....	8
4	PC Network Configuration and Login	9
4.1	PC Network Configuration	9
4.2	Logging in to the DSL Router	10
5	Web-based Management.....	12
5.1	Setup	12
5.1.1	Wizard.....	12
5.1.2	Internet Setup.....	20
5.1.3	Wireless	23
5.1.4	Local Network.....	27
5.1.5	Local IPv6 Network.....	32
5.1.6	Time and Date.....	35
5.1.7	Logout	35
5.2	Advanced.....	36
5.2.1	Advanced Wireless.....	37
5.2.2	ALG.....	44
5.2.3	Port Forwarding.....	45
5.2.4	DMZ	47
5.2.5	SAMBA.....	48
5.2.6	Parental Control	49
5.2.7	Filtering Options	52
5.2.8	QoS Configuration.....	57
5.2.9	Anti-Attack Settings	61
5.2.10	DNS	63
5.2.11	Dynamic DNS.....	64

5.2.12	Network Tools	66
5.2.13	Routing	76
5.2.14	NAT	81
5.2.15	FTPD	81
5.2.16	FTPD Account	82
5.2.17	Logout	83
5.3	Management	84
5.3.1	System Management	84
5.3.2	Firmware Update	85
5.3.3	Access Controls	86
5.3.4	Diagnosis	92
5.3.5	Log Configuration	Error! Bookmark not defined.
5.3.6	Logout	95
5.4	Status	96
5.4.1	Device Info	97
5.4.2	Wireless Clients	97
5.4.3	DHCP Clients	98
5.4.4	IPv6 Status	Error! Bookmark not defined.
5.4.5	Logs	98
5.4.6	Statistics	99
5.4.7	Route Info	100
5.4.8	Logout	101
5.5	Help	102
6	Trouble Shooting	103

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 VB204W VDSL Wi-Fi Router integrates 802.11n Wireless, LAN and USB service into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11g/802.11b/802.11n wireless network. The Router combines a high-speed xDSL Internet connection, 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 xDSL 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

- 1 x VB204W
- 1 x power adapter
- 1 x telephone cables (RJ-11, more than 1.8m)
- 1 x Ethernet cable (RJ-45, more than 1.8m)

2.2 Application

- Home gateway
- Wireless LAN
- 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 G993.2 (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

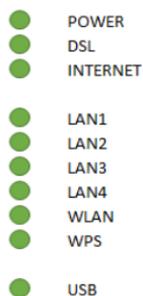


Figure 1 Front panel

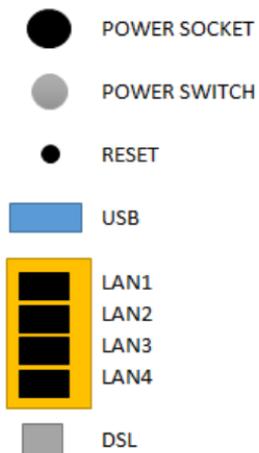
The following table describes the indicators on the front panel.

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.

VB204W User Manual

Indicator	Color	Status	Description
	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.
		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 3G network card or USB flash disk is connected.
		Blink	Data is being transmitted.
		Off	No USB connection.

Rear Panel



VB204W User Manual

Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
Power Socket	Interface connecting to the power adapter. The power adapter output is: 12V DC, 2000mA
Power Switch	Press to turn on or off
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.
USB	USB port, for connecting USB storage devices.
LAN1/2/3/4	Ethernet RJ-45 interfaces connecting to the Ethernet interfaces of computers or Ethernet devices
DSL	RJ-11 interface connecting to a telephone set through a telephone cable

Top 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.

3.2 Hardware Installation

- Step 1** Connect the **DSL** port of the device to the socket installed by Chorus
- Step 2** Connect a **LAN** port of the device to the network card of the PC through an Ethernet cable.

Note:

If connecting to ADSL service, make sure ADSL Filters are used.

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

Installing a telephone without using either a Splitter or filter will lead to failure of xDSL connection, or failure of Internet access, or slow connection speed. If you really need to add a telephone set, you must add a microfilter or Central Splitter.

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. The VB204W 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.

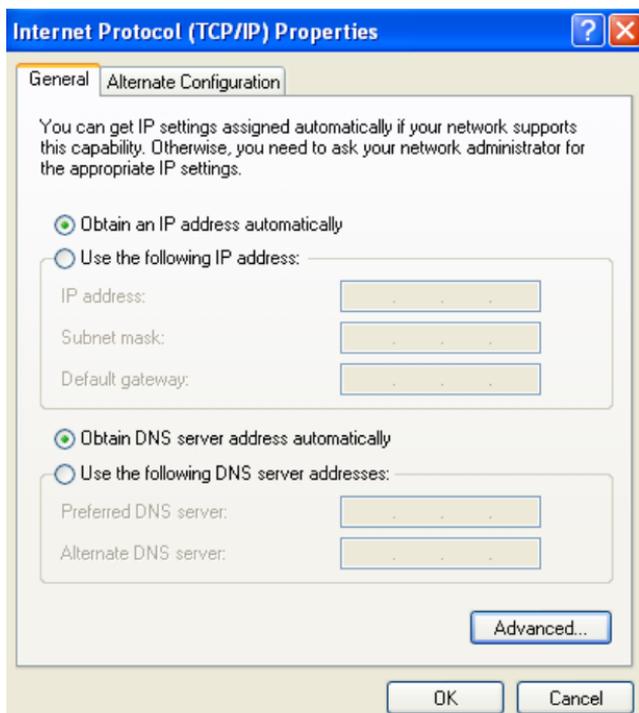


Figure 3 PC Network Configuration

VB204W User Manual

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

- Step 1** Choose Start > Control Panel > Network Connections.
- Step 1** Right-click the Ethernet connection icon and choose **Properties**.
- Step 2** On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.
- Step 3** Select the **Obtain an IP address automatically** radio button.
- Step 4** Select the **Obtain DNS server address automatically** radio button.
- Step 5** 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**. You need not enter the username and the password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.
- Step 4** Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.



Input username and password

Language English ▾

UserName admin ▾

Password

Login

Copyright © Energy Imports Systems, Inc.

Figure 4 Logging in to the DSL Router

After logging in to the DSL router as a admin 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 VB204W, which allows you to configure and control all of 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**, **2.4G 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,.

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

VB204W User Manual

The screenshot shows the router's web interface with a navigation menu on the left and a main content area. The navigation menu includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The 'Setup' menu is expanded, showing 'Wizard' (highlighted), 'Internet Setup', '2.4G Wireless', 'Local Network', 'Local IPv6 Network', 'Time and Date', and 'Logout'. The main content area is titled 'SETTING UP YOUR INTERNET' and contains the following text:

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

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

The screenshot shows the router's web interface with the 'Setup Wizard' page. The navigation menu is the same as in the previous screenshot. The main content area is titled 'WELCOME TO SETUP WIZARD' and contains the following text:

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

VB204W User Manual

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

Step 1 Set the time and date.

The screenshot shows the configuration interface for the VB204W device. At the top, there are navigation tabs: Setup, Advanced, Management, Status, and Help. On the left, a sidebar menu lists various setup options: Setup, Wizard, Internet Setup, 2.4G Wireless, Local Network, Local IPv6 Network, Time and Date, and Logout. The main content area is titled 'STEP 1: SET TIME AND DATE' and contains the following configuration options:

TIME SETTING

Automatically synchronize with Internet time servers

1st NTP time server : 0.nz.pool.ntp.org

2nd NTP time server : 1.nz.pool.ntp.org

TIME CONFIGURATION

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

Enable Daylight Saving

Daylight Saving Start : 2015 Year 03 Mon 11 Day 02 Hour 00 Min 00 Sec

Daylight Saving End : 2015 Year 11 Mon 04 Day 02 Hour 00 Min 00 Sec

Buttons: Back, Next, Cancel

Step 2 Configure the Internet connection:

VDSL Connection

Select Other for Country and PTM as DSL Mode, set VLAN ID as 10 and enter the user name and password as provided by your ISP :

STEP 2: SETUP INTERNET CONNECTION

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

Country :	<input type="text" value="Other"/>	
Internet Service Provider :	<input type="text" value="Other"/>	
WAN Mode :	<input type="text" value="DSL"/>	
DSL Mode :	<input type="text" value="PTM"/>	
Protocol :	<input type="text" value="PPPoE"/>	
802.1Q VLAN ID :	<input type="text" value="10"/>	(0 = disable, 1 - 4094)
Priority :	<input type="text" value="0"/>	(0 - 7)

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 :	<input type="text" value="user@isp.co.nz"/>
Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>

ADSL Connection

Select Other for Country and ATM as DSL Mode, set Protocol as PPPoA, set VPI to 0 and VCI to 100. Finally enter the user name and password as provided by your ISP :

STEP 2: SETUP INTERNET CONNECTION

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

Country :	<input type="text" value="Other"/>	▼
Internet Service Provider :	<input type="text" value="Other"/>	▼
WAN Mode :	<input type="text" value="DSL"/>	▼
DSL Mode :	<input type="text" value="ATM"/>	▼
Protocol :	<input type="text" value="PPPoA"/>	▼
Encapsulation Mode :	<input type="text" value="LLC"/>	▼
VPI :	<input type="text" value="0"/>	(0-255)
VCI :	<input type="text" value="100"/>	(32-65535)
Search Available PVC :	<input type="button" value="Scan"/>	

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 :	<input type="text" value="user@isp.co.nz"/>
Password :	<input type="password" value="....."/>
Confirm Password :	<input type="password" value="..... "/>
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Cancel"/>	

Bridge

When you choose the **DSL Mode** as **PTM** 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.

Country :	<input type="text" value="Other"/>	▼
Internet Service Provider :	<input type="text" value="Other"/>	▼
WAN Mode :	<input type="text" value="DSL"/>	▼
DSL Mode :	<input type="text" value="PTM"/>	▼
Protocol :	<input type="text" value="Bridge"/>	▼
802.1Q VLAN ID :	<input type="text" value="10"/>	(0 = disable, 1 - 4094)
Priority :	<input type="text" value="0"/>	(0 - 7)

Note:

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

VB204W User Manual

Step 3 Configure the wireless network. Enter the information and click **Next**. In this example, the Network name is 'vdsi_01' with no security.

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	<i>Security Level</i>		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 4 Click **Apply** to save the settings.

STEP 4: SAVE AND APPLY CHANGES

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.

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 :	0.nz.pool.ntp.org
NTP Server 2 :	1.nz.pool.ntp.org
Time Zone :	NZT
Daylight Saving Time :	1
Protocol :	PPPoE
802.1Q VLAN ID :	10
Priority :	0
Username :	user@isp.co.nz
Password :	****
SSID (2.4G):	vdc1_01
Visibility Status :	Invisible
Encryption :	None
Pre-Shared Key :	N/A
WEP Key :	N/A

Back Finish Cancel

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.

INTERNET SETUP

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

Default GateWay Mode Auto Manual

DSL CONFIG

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	Action
<input checked="" type="radio"/>	N/A	10	LLC	D_PPPoE_10_1	PPPoE	1		<input type="radio"/>	-	-
<input checked="" type="radio"/>	0/100	0	VCMUX	D_PPPoA_0_2	PPPoA	1		<input type="radio"/>	-	-

The 2 WAN Configurations that are already set up are the most common in New Zealand. You should only need to edit these to change the PPP Username and password if needed. PPPoE Protocol is the WAN connection required for VDSL, and PPPoA Protocol is the WAN connection required for ADSL connections. To manage the existing WAN connections, select a connection from the list, and then click **Edit** or **Delete**.

VB204W User Manual

INTERNET SETUP

This screen allows you to configure an WAN connection.

DSL MODE CONFIGURATION

DSL Mode :

CONNECTION TYPE

Protocol :

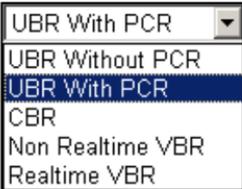
802.1Q VLAN ID : (0 = disable, 1 - 4094)

Priority : (0 - 7)

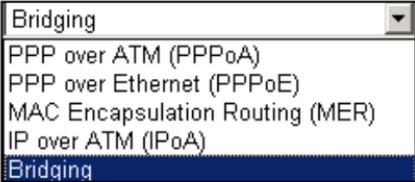
Enable Service :

Service Name :

The following table describes the parameters in this page.

Field	Description
DSL Mode	You can select ATM or PTM .
PVC Settings	VPI : The virtual path between two points in an ATM network, and its valid value is from 0 to 255 . 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).
Service Category	You can select from the drop-down list. 
Protocol	You can select from the drop-down list.

VB204W User Manual

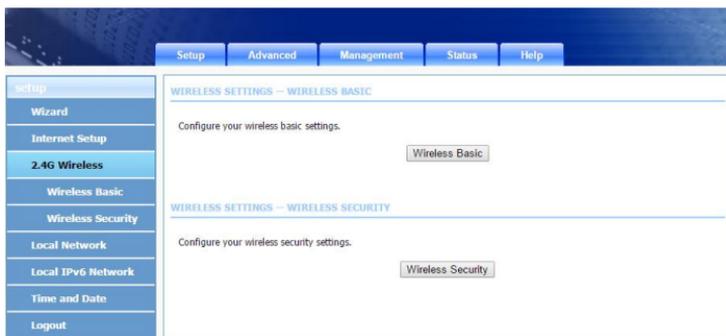
Field	Description
	
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select LLC or VCMUX .

Click **Apply**.

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.

VB204W User Manual

WIRELESS BASIC CONFIGURATION

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS BASIC CONFIGURATION

Enable Wireless :

AP Isolate :

SSID :

Visibility Status : Visible Invisible

Continent/Country :

802.11 Mode :

Band Width :

Wireless Channel :

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 .

VB204W User Manual

Field	Description
Band Width	Select the appropriate band as 20M , 40M , or 20M/40M from the pull-down menu.
Wireless Channel	Select the wireless channel from the pull-down menu.
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 **WPA2** or **WPA/WPA2 Mixed**, the following figure appears.

VB204W User Manual

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

Wireless Security Mode :

WPA2 ONLY

WPA Mode :

Encryption Mode :

Group Key Update Interval : (60 - 65535)

PRE-SHARED KEY

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

The following table describes the parameters in this page.

Field	Description
Wireless Security Mode	<p>Configure the wireless encryption mode. You can choose None, WPA2 or WPA/WPA2 Mixed.</p> <ul style="list-style-type: none">● 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.
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

Field	Description
	to enter the password provided by the Radius server when the wireless client connects the modem.
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.

VB204W User Manual

LOCAL NETWORK

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.

ROUTER SETTINGS

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.

Router IP Address :
Subnet Mask :
Domain Name :

Configure the second IP Address and Subnet Mask for LAN

IP Address :
Subnet Mask :

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.

VB204W User Manual

This page is used to configure the DHCP Server and DHCP Relay Settings. The **DHCP Lease Time** is set to **86400** seconds by default. The IP range and lease time can be set in this section:

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 Lease Time : (seconds [time not allowed less than

600s])

Use the following DNS server addresses:

Enable DNS Relay :

Preferred DNS server :

Alternate DNS server :

Click **Apply** to save the settings.

VB204W User Manual

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

DHCP CLIENT CLASS LIST

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

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 Conditional 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 CONDITIONAL OPTION

Status	Client Class Name	Option Code	Option Value
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

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

ADD DHCP OPTION(OPTIONAL)

Conditional Option Enable :

Conditional Option Client Class :

Conditional Option Tag :

Conditional Option Value :

Figure 5

VB204W User Manual

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

The **Conditional Option Client Class** is the client class name of DHCP Conditional Option.

The **Conditional 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 **Conditional 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
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

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.

VB204W User Manual

IPv6 LAN SETTINGS

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.

IPv6 ADDRESS

IPv6 Address :

RADVD CONFIGURATION

Enable RADVD :
RADVD DNSLL :

DHCPV6 CONFIGURATION

Enable DHCPv6 Server :
LAN Address Config Mode : Stateless Stateful
Start Interface ID :
End Interface ID :
DHCPv6 Lease Time :
DHCPv6 Valid Time :

IPv6 DNS Mode : From WAN Manual
WAN Interface :
Primary DNS :
Secondary DNS :

PREFIX CONFIGURATION

Get Prefix Mode : From WAN Manual
WAN Interface :
Site Prefix : /64

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.

VB204W User Manual

Field	Description
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.
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.

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 : 0.nz.pool.ntp.org

2nd NTP time server : 1.nz.pool.ntp.org

TIME CONFIGURATION

Current Local Time : 2015-08-27 15:34

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

Enable Daylight Saving

Daylight Saving Start : 9 Mon 4 No. 0 The day of week(0~6) 02 Hour

Daylight Saving End : 4 Mon 1 No. 0 The day of week(0~6) 02 Hour

Apply Cancel

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.

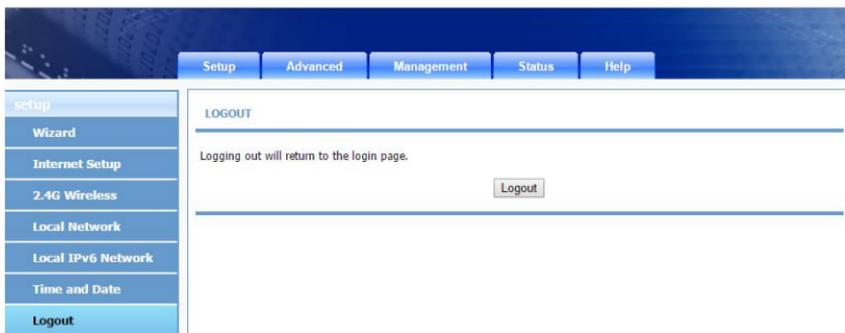
Set the daylight as you want.

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.

VB204W User Manual



5.2 Advanced

VB204W User Manual

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**, **Porttrigger**, **DMZ**, **SAMBA**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Anti-Attack Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, **NAT**, **FTP Setting**, **FTP Account** 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.

The screenshot shows a web interface with a top navigation bar containing tabs for Setup, Advanced, Management, Status, and Help. A left sidebar lists various configuration options, with '2.4G Advanced Wireless' selected. The main content area is titled 'ADVANCED WIRELESS -- ADVANCED SETTINGS' and contains a description: 'Allows you to configure advanced features of the wireless LAN interface.' Below this is a button labeled 'Advanced Settings'. The next section is 'ADVANCED WIRELESS -- MAC FILTERING', described as 'Allows you to configure wireless firewall by denying or allowing designated MAC addresses.', with a 'MAC Filtering' button. The third section is 'ADVANCED WIRELESS -- SECURITY SETTINGS', described as 'Allows you to configure security features of the wireless LAN interface.', with a 'Security Settings' button. The fourth section is 'ADVANCED WIRELESS -- WPS SETTING', described as 'Allows you to configure wireless WPS.', with a 'WPS Setting' button. The final section is 'ADVANCED WIRELESS -- WDS SETTING', which is currently empty.

5.2.1.1 **Advanced Settings**

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

VB204W User Manual

ADVANCED SETTINGS

These options are for users who wish to change the behavior of their 802.11g wireless radio from the standard setting. It is not recommended to modify these settings from the factory defaults. Incorrect settings may affect your wireless performance. The default settings usually provide the best wireless performance in most environments.

WIRELESS ENABLE

Enable Wireless :

ADVANCED WIRELESS SETTINGS

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

SSID

SSID : vds_01
Visibility Status : Visible Invisible
User Isolation : Off ▼
Disable WMM Advertise : On ▼
Max Clients : 16 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable :
Guest SSID : Energy Imports VB204W
Visibility Status : Visible Invisible
User Isolation : Off ▼
Disable WMM Advertise : On ▼
Max Clients : 32 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable :
Guest SSID : Energy Imports VB204W
Visibility Status : Visible Invisible
User Isolation : Off ▼
Disable WMM Advertise : On ▼
Max Clients : 32 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable :
Guest SSID : Energy Imports VB204W
Visibility Status : Visible Invisible
User Isolation : Off ▼
Disable WMM Advertise : On ▼
Max Clients : 32 (1 ~ 32)

Apply Cancel

VB204W User Manual

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

If you enable the MAC Address Access Control mode, hosts with MAC addresses contained in the access control list are allowed to access to the router.

ACCESS CONTROL -- MAC ADDRESSES

Wireless SSID :

Access Control Mode :

WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="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.

VB204W User Manual

ACCESS CONTROL

If you enable the MAC Address Access Control mode, hosts with MAC addresses contained in the access control list are allowed to access to the router.

ACCESS CONTROL -- MAC ADDRESSES

Wireless SSID : ▼
Access Control Mode : ▼

WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="Add"/>		

INCOMING MAC FILTER

MAC : (xx:xx:xx:xx:xx:xx)
Comment :

5.2.1.3 Security Settings

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

VB204W User Manual

WIRELESS SECURITY

WIRELESS SSID

Select SSID :

WIRELESS SECURITY

Security Mode :

WPA2 ONLY

WPA Mode :

Encryption Mode :

Group Key Update Interval : (60 - 65535)

PRE-SHARED KEY

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

Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Security Mode** drop-down list. You can select **WPA2 Only** or **WPA/WPA2 Mixed**. The default mode is **None**.

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

WIRELESS SECURITY

Security Mode :

WPA2 ONLY

WPA Mode :

Encryption Mode :

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 :

WPA Mode : WPA2-PSK

Pre-Shared Key : *****

WI-FI PROTECTED SETUP CONFIG

Enabled WPS :

Device PIN :

Generate Pin Status:

Push Button :

Input Station PIN :

WPS Session Status :

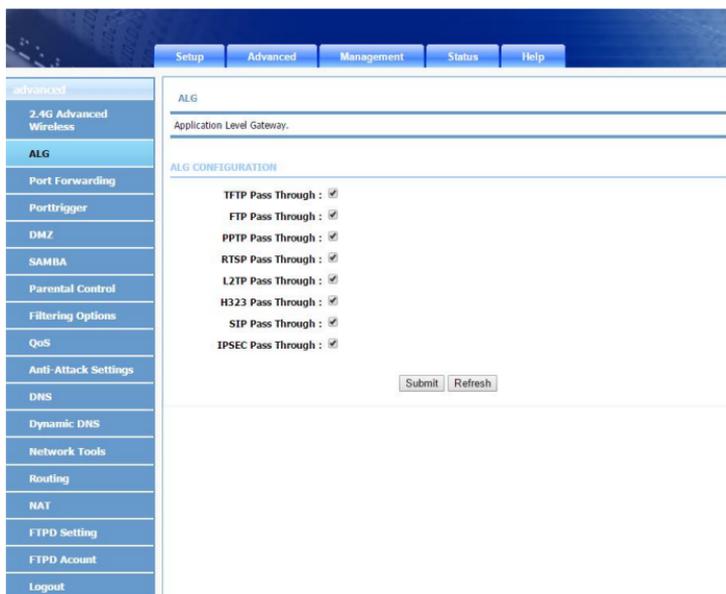
The following table describes the parameters of this page.

Field	Description
Wireless SSID	Select one SSID of the CPE.
Enabled WPS	Choose to enable WPS function to set the following parameters.

Field	Description
Push Button	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.
Input Station 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.

The screenshot shows the 'PORT FORWARDING' configuration page. The navigation tabs at the top are 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar contains a list of settings: 'advanced', '2-4G Advanced Wireless', 'ALG', 'Port Forwarding' (highlighted), 'Porttrigger', 'DMZ', 'SAMBA', 'Parental Control', 'Filtering Options', 'QoS', 'Anti-Attack Settings', 'DNS', 'Dynamic DNS', 'Network Tools', 'Routing', 'NAT', 'FTPD Setting', 'FTPD Account', and 'Logout'.

The main content area is titled 'PORT FORWARDING' and contains the following text:

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 16 entries can be configured for each WAN connection.

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.

Below the text is the 'PORT FORWARDING SETUP' section, which features a table with the following columns: Server Name, Wan Connection, External Port Start/End, Protocol, Internal Port, Server IP Address, Schedule Rule, and Remote IP. Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

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

PORT FORWARDING SETUP

WAN Connection(s) : D_PPPoE_10_1 ▼

Server Name :

Schedule : always ▼

Server IP Address(Host Name) : 192.168.1.

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

Type in a Server name in the **Server name** field.

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

Enter a Start and end Port on the **External Port**.

Enter the **Internal Port** you want this traffic directed to.

Enter the **Remote IP** of the LAN device you want the traffic directed to.

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

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.

The screenshot shows the DMZ configuration page in a DSL Router's web interface. The interface has a blue header with navigation tabs: Setup, Advanced, Management, Status, and Help. A left sidebar lists various configuration options, with DMZ highlighted. The main content area is titled 'DMZ' and contains the following text:

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.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ HOST

WAN Connection :

Enable DMZ :

DMZ Host IP Address :

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.

The screenshot shows the SAMBA configuration page. The sidebar on the left lists various network settings, with 'SAMBA' selected. The main content area has a top navigation bar with 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. Below this, the 'SAMBA' configuration is displayed. It includes a 'SAMBA SERVER' section with the following options:

- Enable SAMBA:**
- Workgroup:** Workgroup
- Netbios Name:** El_router
- Enable USB Storage:**
- Enable Anonymous Access:**

There are also password fields for 'New SMB password' and 'Retype new SMB password', and 'Apply' and 'Cancel' buttons at the bottom.

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

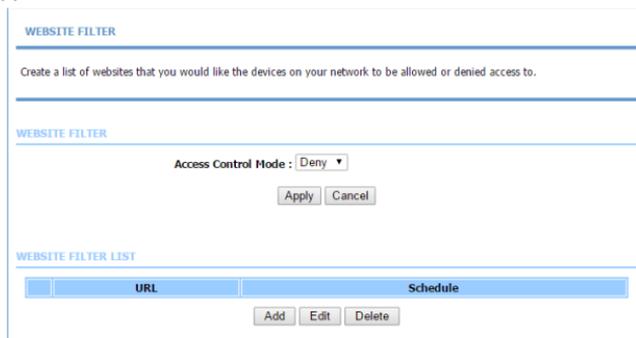
Choose **Advanced > Parental Control**. The **Parent Control** page shown in the following figure appears.



This page provides two useful tools for restricting the Internet access. **Filter 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 **Website Filter**. The page shown in the following figure appears.



VB204W User Manual

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

ADD SCHEDULE RULE

URL :

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 **WEBSITE FILTER** table. The page shown in the following figure appears.

WEBSITE FILTER LIST

	URL	Schedule
<input type="checkbox"/>	xxx.co.n...	Sun,Mon,Tue,Wed,Thu,Fri,Sat, time 00:00 00:00

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

Apply Cancel

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

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 : d0:50:99:52:f2:10

Other MAC Address :

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)

Apply Cancel

Enter the use name with no spaces 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

Apply Cancel

BLOCK MAC ADDRESS--BLACKLIST

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

Add Edit Delete

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.

IP FILTER CONFIGURATION

Enable IP Filter

Security Level

FILTER MODEL

WAN → LAN White Black

LAN → WAN White Black

ADD IP FILTER RULES

Choose

NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name

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

FILTER MODEL

WAN --> LAN White Black
 LAN --> WAN White Black

ADD IP FILTER RULES

Choose

	NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input checked="" type="radio"/>	1	1	/	/	TCP		D_PPPE_10_1

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

FILTER MODEL

WAN → LAN White Black

LAN → WAN White Black

ADD IP FILTER RULES

Choose

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

FILTER MODEL

WAN → LAN White Black

LAN → WAN White Black

ADD IP FILTER RULES

Choose

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

5.2.8 QoS Configuration

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

The screenshot shows the 'QoS Configuration' page. At the top, there are tabs for 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar contains a list of menu items: 'advanced', '2-4G Advanced Wireless', 'ALG', 'Port Forwarding', 'Porttrigger', 'DMZ', 'SAMBA', 'Parental Control', 'Filtering Options', 'QoS' (highlighted), 'Anti-Attack Settings', 'DNS', 'Dynamic DNS', 'Network Tools', 'Routing', 'NAT', 'FTPD Setting', 'FTPD Account', and 'Logout'.

The main content area is titled 'QUALITY OF SERVICE' and contains the following configuration options:

- Configuration of classification table for IP QoS.**
- QoS:** Enable Disable
- QoS QUEUE**
- Direction:** Upstream (LAN -> WAN) Downstream (WAN -> LAN)
- Queue Enable:** Enable Disable
- Bandwidth:** Kbps (0 means no limit bandwidth)
- Discipline:** WRR Strict Priority
- WRR weight:** Highest: High: Medium: Low:
(all sum should be less or equal than 100)
- Enable DSCP ReMark:**
- Enable 802.1p ReMark:**
- Buttons:** Save, Cancel
- QoS CLASSIFICATION RULES**
- Table:**

#	Enable	Rule	Action	Edit	Drop
Add a Rule					

5.2.8.1 QoS Queue Config

In the **QoS Configuration** page, click Tick **Enable**. Fill out the details.

VB204W User Manual

QOS QUEUE

Direction : Upstream (LAN -> WAN) Downstream (WAN -> LAN)

Queue Enable : Enable Disable

Bandwidth : Kbps (0 means no limit bandwidth)

Discipline : WRR Strict Priority

WRR weight : Highest: High: Medium: Low:
(all sum should be less or equal than 100)

Enable DSCP ReMark :

Enable 802.1p ReMark :

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 **Save** to add a queue.

5.2.8.2 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

Add Classification Rule

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	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

ADD QOS CLASSIFICATION RULES

RULE

Classify Type : Upstream Flow Classify

Actions Enable Disable

Application :

Physical Ports :

Destination MAC Address :

Destination IP Address :

Destination Subnet Mask :

Destination Port Range : ~

Source MAC Address :

Source IP Address :

Source Subnet Mask :

Source Port Range : ~

Protocol :

Vlan ID :

DSCP :

Queue # :

ACTIONS

DSCP Remark :

802.1p Remark :

Queue # :

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 .

Field	Description
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.
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 displays the 'Anti-Attack Settings' page in the VB204W web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various configuration categories, with 'Anti-Attack Settings' selected. The main content area is titled 'ANTI-ATTACK' and contains the following sections:

- ANTI-ATTACK COFIGURATION:**
 - 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 Fraglen
 - Enable Attack Protection Function of Echo Charpen
 - 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 page, there 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.

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 (DyndDNS.org, 3322.org and freedns.afraid.org).

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

The screenshot shows a web interface with a top navigation bar containing buttons for Setup, Advanced, Management, Status, and Help. On the left is a vertical sidebar menu with the following items: advanced, 2.4G Advanced Wireless, ALG, Port Forwarding, Porttrigger, DMZ, SAMBA, Parental Control, Filtering Options, QoS, Anti-Attack Settings, DNS, Dynamic DNS (highlighted), and Network Tools. The main content area is titled 'DYNAMIC DNS' and contains the following text:

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Below the text is a table with the following columns: Hostname, Username, Service, and Interface. Underneath the table are three buttons: Add, Edit, and Delete.

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

ADD DYNAMIC DNS

DDNS provider :

Hostname :

Interface :

Username :

Password :

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 .
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
advanced					
2.4G Advanced Wireless					
ALG					
Port Forwarding					
Porttrigger					
DMZ					
SAMBA					
Parental Control					
Filtering Options					
QoS					
Anti-Attack Settings					
DNS					
Dynamic DNS					
Network Tools					
Port Mapping					
IGMP Proxy					
IGMP Snooping					
MLD Configuration					
UPnP					
DSL					
SNMP					
TR-069					
Printer					
Routing					
NAT					
FTPD Setting					
FTPD Account					
Logout					

NETWORK TOOLS -- PORT MAPPING
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.
Port Mapping
NETWORK TOOLS -- IGMP PROXY
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Proxy
NETWORK TOOLS -- IGMP SNOOPING
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Snooping
NETWORK TOOLS -- MLD CONFIGURATION
Transmission of identical content, such as multimedia, from a source to a number of recipients.
MLD Configuration
NETWORK TOOLS -- UPNP
Allows you to enable or disable UPnP.
Upnp
NETWORK TOOLS -- DSL
Allows you to configure advanced settings for DSL.
DSL
NETWORK TOOLS -- SNMP
Network Tools - SNMP
SNMP
NETWORK TOOLS -- PRINTER
Allows you to manage printer .
printer

(Network Tools-1)

5.2.12.1 Port Mapping

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

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.

PORT MAPPING SETUP

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

Click **Add** to add port mapping. The page shown in the following figure appears.

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

ethernet1
ethernet2
ethernet3
ethernet4
ra0
ra1
ra2
ra3

->
<-

Apply Cancel

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.

VB204W User Manual

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

WAN Interface : D_PPPoE_10_1 ▼

IGMP Version : IGMP V3 ▼

Enable IGMP Proxy :

LAN Connection : Lan1 ▼

Enable FastLeaving :

General Query Interval : 150 (seconds)

General Query Response Interval : 20 (1~255)(*100 milliseconds)

Group Query Interval : 325 (seconds)

Group Query Response Interval : 20 (1~255)(*100 milliseconds)

Group Query Count : 3

Last Member Query Interval : 1 (seconds)

Last Member Query Count : 1

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.



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 DSL

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

DSL SETTINGS

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

DSL SETTINGS

xDSL Mode : Auto Sync-Up ▼

xDSL Type : ANNEX A/I/J/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.

TR064 CONFIGURATION

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 : 28800

ACS URL : http://acs.energyimports.

ACS Username : cpe

ACS Password :

Connection Request Authentication

Connection Request User Name : admin

Connection Request Password :

Apply Cancel

Click **Apply** to save settings.

5.2.12.10 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	CMD	Firmware Version
--------------	-------	-----	------------------

5.2.13 Routing

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

The screenshot displays the 'Routing' configuration page in the VB204W web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various configuration categories, with 'Routing' selected. The main content area is divided into sections:

- STATIC ROUTE**: Contains a 'Static Route' button.
- IPv6 STATIC ROUTE**: Contains an 'IPv6 Static Route' button.
- POLICY ROUTE**: Contains a 'Policy Route' button.
- RIP SETTINGS**: Contains a 'RIP Settings' button.
- RIPNG SETTINGS**: Contains a 'RIPng Settings' button.

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.

VB204W User Manual

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

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.

5.2.13.2 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
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

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 least one LAN connection to bind together, and then click **Apply**.

POLICY ROUTE

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

POLICY ROUTE SETUP

	WAN	LAN

WAN INSTANCE AND LAN INSTANCE

WAN Connection :

- LAN Connection :
- ethernet1
 - ethernet2
 - ethernet3
 - ethernet4
 - ra0
 - ra1
 - ra2
 - ra3

5.2.13.4 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	Dynamic Route	Direction
D_PPPE_10_1	OFF ▼	Active ▼
D_PPPE_0_2	OFF ▼	Active ▼
Lan1	OFF ▼	Active ▼

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.

5.2.13.5 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 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 : ▼

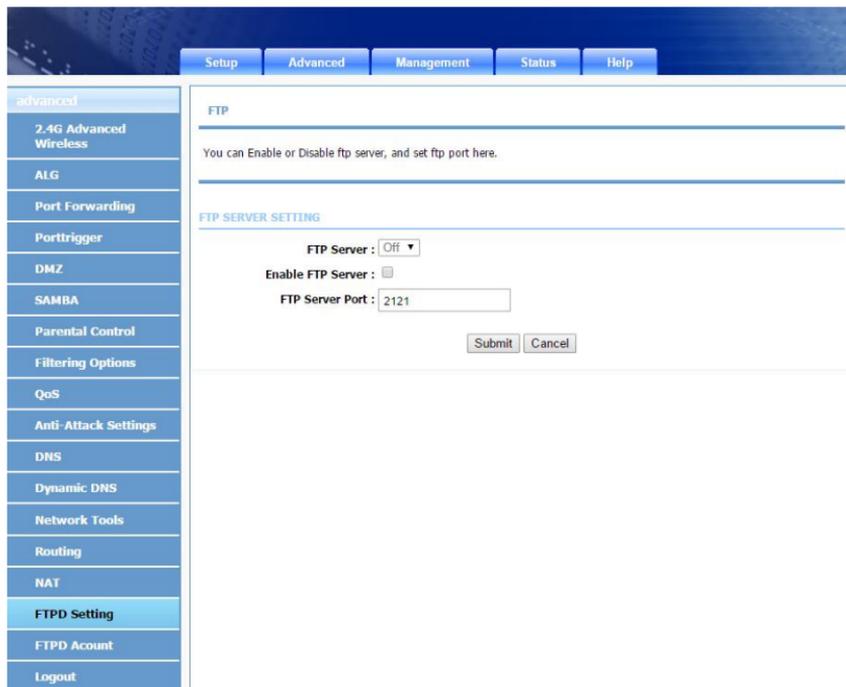
Internal IP Address :

External IP Type : ▼

External IP Address :

5.2.15 FTPD

Choose **Advanced** > **FTPD Setting**. The page shown in the following figure appears. This page is used to configure the FTP Server and Port for the SAMBA share. Enable the FTP Server and enter the port required



5.2.16 FTPD Account

Choose **Advanced > FTPD Account**. The page shown in the following figure appears. This page is used to configure the FTP Server account login details and access restrictions.

The screenshot shows the 'Advanced' configuration page for 'FTP User Manage'. The left sidebar lists various settings, with 'FTPD Account' selected. The main content area includes a title 'FTP', a description 'You can manage ftp user information here, such as username, password, and rights.', and a form for adding a new user. The form has fields for 'Username' (containing 'user') and 'Password' (masked with dots). Below these are checkboxes for 'Rights': 'View', 'Upload', and 'Download'. At the bottom of the form are 'Append' and 'Refresh' buttons. Below the form is an 'ACCOUNT TABLE' with the following structure:

No.	User	Password	Rights			Operation
			View	Upload	Download	

5.2.17 Logout

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

LOGOUT

Logging out will return to the login page.

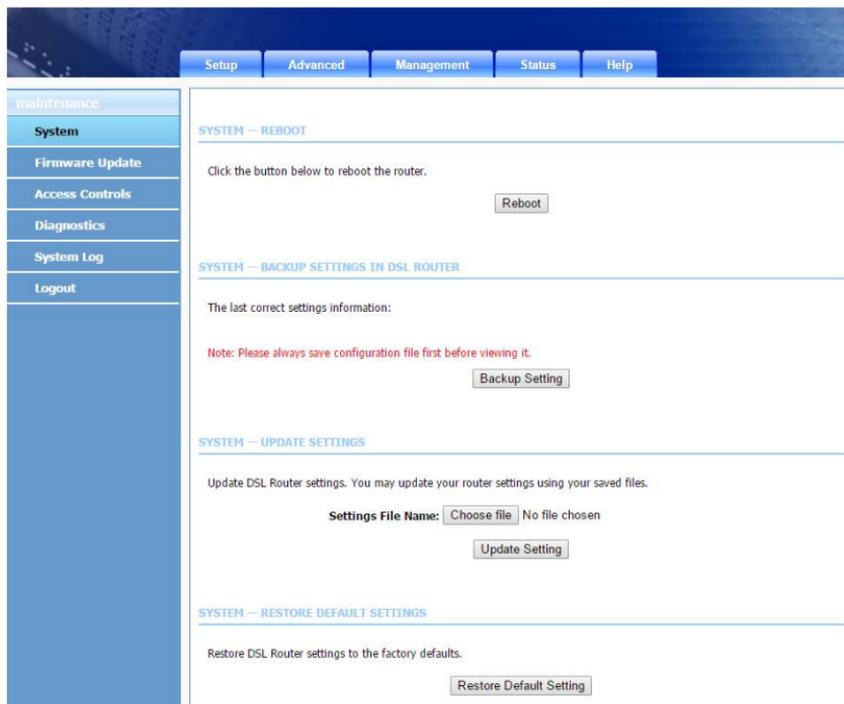
Logout

5.3 Management

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

5.3.1 System Management

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



The screenshot displays the 'Management' tab selected in the top navigation bar. The left sidebar shows a 'maintenance' menu with sub-items: System, Firmware Update, Access Controls, Diagnostics, System Log, and Logout. The main content area is divided into three sections:

- SYSTEM -- REBOOT**: Contains the instruction 'Click the button below to reboot the router.' and a 'Reboot' button.
- SYSTEM -- BACKUP SETTINGS IN DSL ROUTER**: Contains the instruction 'The last correct settings information:', a red note 'Note: Please always save configuration file first before viewing it.', and a 'Backup Setting' button.
- SYSTEM -- UPDATE SETTINGS**: Contains the instruction 'Update DSL Router settings. You may update your router settings using your saved files.', a 'Settings File Name:' label with a 'Choose file' button and 'No file chosen' text, and an 'Update Setting' button.
- SYSTEM -- RESTORE DEFAULT SETTINGS**: Contains the instruction 'Restore DSL Router settings to the factory defaults.' and a 'Restore Default Setting' button.

VB204W User Manual

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.

5.3.2 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.

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

maintenance
System
Firmware Update
Access Controls
Diagnostics
System Log
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 : GUN4.NT216A-C-EI-R1B010-NZ.EN_2T2R-EI

Current Firmware Date : 06/17/2015-08:10:05

Select File : No file chosen

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.

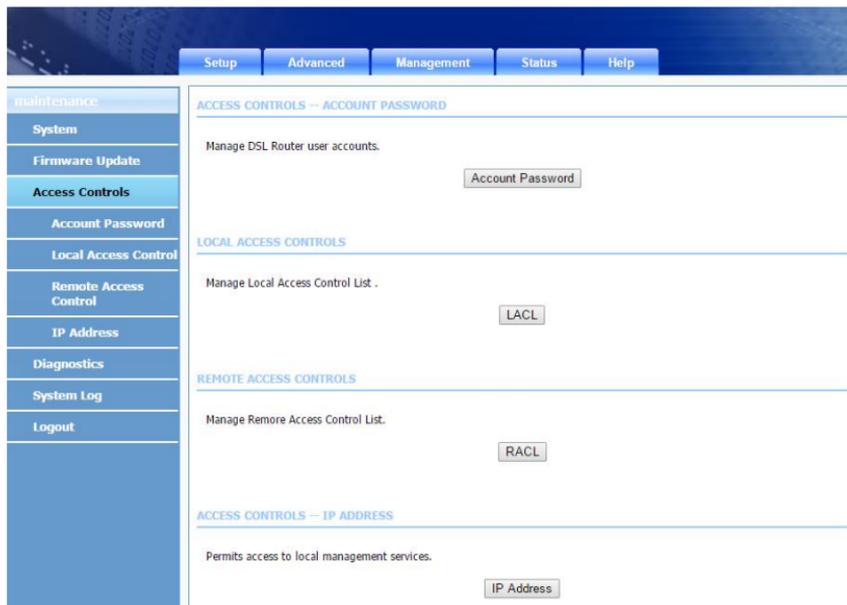
The device loads the file and reboots automatically.

Note:

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

5.3.3 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**.



5.3.3.1 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.

VB204W User Manual

ACCOUNT PASSWORD

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

The user name "admin" will have full access to the Web-based management interface.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

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="admin"/>
New Username :	<input type="text" value="admin"/>
Current Password :	<input type="password"/>
New Password :	<input type="password"/>
Confirm Password :	<input type="password"/>
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

WEB IDLE TIME OUT SETTINGS

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

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 **admin** or **user**. 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.

5.3.3.2 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

You can set a service control list (SCL) to enable or disable services from being used.

LOCAL ACCESS CONTROL -- SERVICES

Enable Local Access :

Choose A Connection : Lan1 ▾

IPv4 ACL

Service	Enable	Source IP	Source Mask	Protocol	Port
FTP	<input 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	-
SNMP	<input 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 checked="" 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 type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	7547

IPv6 ACL

Service	Enable	Source IP	Protocol	Port
HTTP	<input checked="" type="checkbox"/>	:::0	TCP	80
TR069	<input checked="" type="checkbox"/>	:::0	TCP	7547
ICMPv6	<input checked="" type="checkbox"/>	:::0	ICMPv6	-

Submit Refresh

5.3.3.3 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 5.3.3.22 Local Access Control.

REMOTE ACCESS CONTROL

You can set a service control list (SCL) to enable or disable services from being used.

REMOTE ACCESS CONTROL -- SERVICES

Choose A Connection

IPv4 ACL

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

5.3.3.4 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
<input type="button" value="Add"/> <input type="button" value="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.

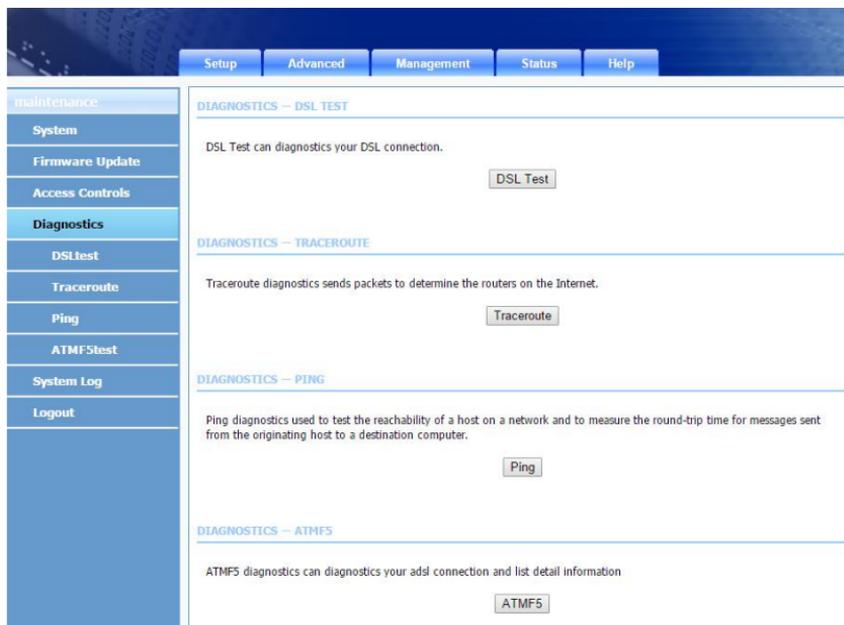
IP ADDRESS

IP Address :

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

5.3.4 Diagnosis

Choose **Management > Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test Traceroute, Ping and ATM5test**.



5.3.4.1 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.

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

5.3.4.2 Traceroute

In the **Diagnosis** 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.

Protocol :	IPv4 ▾
WAN Connction :	D_PPpoe_10_1 ▾
Host :	www.google.co.nz
Max TTL :	30 (1-64)
Wait times :	5000 (>1ms)
<input type="button" value="Traceroute"/> <input type="button" value="Stop"/>	

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

RESULT

```
Traceroute Status: Traceroute is running...
traceroute: warning: www.google.co.nz has
multiple addresses; using 119.224.142.46
ttraceroute to www.google.co.nz
(119.224.142.46), 30 hops max, 38 byte
packets
```

5.3.4.3 Ping

In the **Diagnosis** page, click **Ping**. The page shown in the following figure appears. In this page, you can determine if the IP or URL responds on the Internet by sending packets.

RESULT

```
Host: www.google.co.nz
Ping status: finish
Success times: 5
Failed times: 0
Response time: max 6 ms , min 4 ms , avg 4 ms
```

PING DIAGNOSIS

Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Protocol : IPv4 ▾

Host : www.google.co.nz

Number of retries : 5

Timeout : 1

Packet Size : 56

WAN Connection : D_PPPE_10_1 ▾

Ping...

5.3.5 System Log

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

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 :

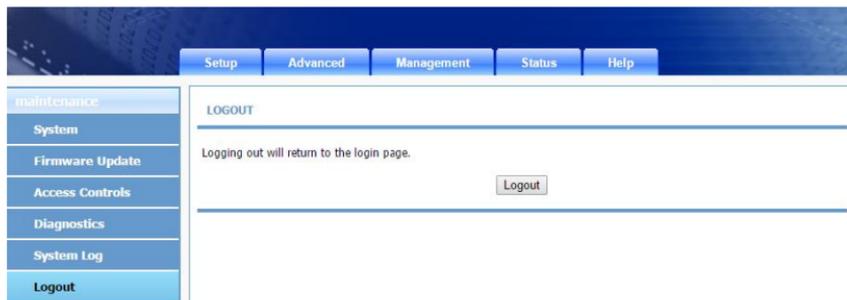
This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. In this page, you can enable or disable the system log function.

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.

5.3.6 Logout

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

The screenshot shows the router's status page with a navigation menu at the top (Setup, Advanced, Management, Status, Help) and a left sidebar (status, Device Info, Wireless Clients, DHCP Clients, Logs, Statistics, Route Info, Logout). The main content area is titled 'DEVICE INFO' and contains the following sections:

DEVICE INFO

This information reflects the current status of your all connection.

SYSTEM INFO

Modem Name :	VB204W
Serial Number :	001122334455
Time and Date :	2015-08-27 17:25
HardwareVersion :	GUN4.NT216A-C
Firmware Version :	GUN4.NT216A-C-EI-R1B010-NZ.EN_2T2R-EI
System Up Time :	46:47:11

INTERNET INFO

Internet Connection Status :

IP Protocol:

Internet Connection Status:	Connected
Wan service type:	Internet_TR069
IP Address:	119.224.94.234
Sub Mask:	255.255.255.255
Default Gateway:	101.98.0.94
DNS Server:	202.180.64.10,202.180.64.11

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP
N/A	D_PPPoE_10_1	PPPoE	Disable
0/100	D_PPPoA_0_2	PPPoA	Disable

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.

status

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

WIRELESS CLIENTS

This page shows authenticated wireless stations and their status.

WIRELESS -- AUTHENTICATED STATIONS

Mac	Associated	Authorized
C0:BD:D1:AE:DE:E1	Connected	WPA2
5C:0A:5B:4B:34:FB	Connected	WPA2
5C:F8:A1:B1:3D:66	Connected	WPA2
88:C9:D0:F2:91:19	Connected	WPA2
64:20:0C:82:5F:78	Connected	WPA2
F4:09:D8:C4:84:F7	Connected	WPA2
80:E6:50:6C:00:3B	Connected	WPA2
C4:8E:8F:8A:8B:17	Connected	WPA2

Refresh

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 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.

The screenshot shows the VB204W web interface. At the top, there are navigation tabs: Setup, Advanced, Management, Status, and Help. The left sidebar has a 'Status' section with sub-items: Device Info, Wireless Clients, DHCP Clients, Logs (highlighted), Statistics, Route Info, and Logout. The main content area is titled 'LOGS' and contains the text: 'This page allows you to view system logs.' Below this is a 'SYSTEM LOG' section with a scrollable text area containing the following log entries:

```

Manufacturer: Energy Imports
ProductClass: VB204W
SerialNumber: 001122334455
IP: 192.168.1.1
HWVer: GUN4.WT216A-C
SWVer: GUN4.WT216A-C-EI-R1B010-NZ-EN_2T2R-EI

Para:[] Result:[0] CPE periodically inform to ACS!
2015-08-26 15:47:55 [6] syslog: Accessor:[ACS] Method:[GetNoti] Para:[]
Result:[00000000]
2015-08-26 15:52:43 [5] syslog: Accessor:[CPE] Method:[INFORM] Para:[]
Result:[0] CPE periodically inform to ACS!
2015-08-26 15:52:44 [6] syslog: Accessor:[ACS] Method:[GetNoti] Para:[]
Result:[00000000]
2015-08-26 16:00:18 [5] syslog: Accessor:[CPE] Method:[INFORM] Para:[]
Result:[0] CPE periodically inform to ACS!
2015-08-26 16:00:18 [6] syslog: Accessor:[ACS] Method:[GetNoti] Para:[]
Result:[00000000]
2015-08-26 16:14:37 [5] syslog: Accessor:[CPE] Method:[INFORM] Para:[]
Result:[0] CPE periodically inform to ACS!

```

Below the log text area is a 'Refresh' button.

5.4.5 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.

The screenshot shows the configuration interface with a top navigation bar containing 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. On the left is a sidebar menu with 'status' at the top and sub-items: 'Device Info', 'Wireless Clients', 'DHCP Clients', 'Logs', 'Statistics', 'Route Info' (highlighted), and 'Logout'. The main content area is titled 'ROUTE INFO' and contains the text: 'Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect)'. Below this is a sub-header 'DEVICE INFO -- ROUTE' followed by a table:

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
119.47.114.165	101.98.0.94	255.255.255.255	UGH	0	0	ppp0
101.98.9.16	101.98.0.94	255.255.255.255	UGH	0	0	ppp0
101.98.0.94	0.0.0.0	255.255.255.255	UH	0	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	0	eth0
0.0.0.0	101.98.0.94	0.0.0.0	UG	0	0	ppp0

5.4.7 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 configuration interface with the same top navigation bar. The sidebar menu has 'Logout' highlighted. 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.

The screenshot displays the user interface of the VB204W device. At the top, there is a navigation bar with five tabs: Setup, Advanced, Management, Status, and Help. The Help tab is currently selected. On the left side, there is a vertical menu with the following items: Menu, Setup, Advanced, Management, Status, and Logout. The main content area is titled 'HELP MENU' and contains three sections of links:

- HELP MENU**
 - [Setup](#)
 - [Advanced](#)
 - [Management](#)
 - [Status](#)
- SETUP HELP**
 - [Wizard](#)
 - [Internet Setup](#)
 - [Wireless Setup](#)
 - [Local Network](#)
 - [Local IPv6 Network](#)
 - [Time and Date](#)
- ADVANCED HELP**
 - [2.4G Advanced Wireless](#)
 - [ALG](#)
 - [Port Forwarding](#)
 - [DMZ](#)
 - [SMB](#)
 - [Parental Control](#)
 - [Filtering Options](#)
 - [QoS](#)
 - [DNS](#)
 - [Anti-Attack](#)
 - [DDNS](#)
 - [Network Tools](#)
 - [Routing](#)
 - [NAT](#)
 - [FTPD Setting](#)
 - [FTPD Account](#)
- MANAGEMENT HELP**
 - [System](#)

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 DSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why do 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: admin/admin ● Common username/password: user/user.