

Go to
businessphones.vtech.com
to register your product for
enhanced warranty support and
the latest VTech product news.

VNT832
4-Port Ethernet Router



vtech[®]

User's manual



Congratulations

on your purchase of this VTech product. Before using this product, please read the **Important safety information**.

This user's manual provides you with the complete installation, setup and operation instructions.

For customer service or product information, visit our website at **businessphones.vtech.com** or call **1 (888) 370-2006**.

Model number: VNT832

Type: 4-Port Ethernet Router

Serial number: _____

Purchase date: _____

Place of purchase: _____

Both the model and serial numbers of your VTech product can be found on the bottom of the router.

Save your sales receipt and original packaging in case it is necessary to return your router for warranty service.

Important Safety Information

When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury, including the following:

1. Read and understand all instructions.
2. Do not use this product near water such as near a bath tub, wash bowl, kitchen sink, laundry tub or swimming pool, or in a wet basement or shower.
3. Do not place this product on an unstable table, shelf, stand or other unstable surfaces.
4. CAUTION: Use only the adapters included with this product. Incorrect adapter polarity or voltage can seriously damage the product.
Power adapter: Input 100–240V AC 500mA 50/60Hz; Output: 12V DC 1000mA.
5. The power adapters are intended to be correctly oriented in a vertical or floor mount position. The prongs are not designed to hold the plug in place if it is plugged into a ceiling, under-the-table or cabinet outlet.
6. For pluggable equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.
7. Unplug this product from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
8. Do not cut off the power adapters to replace them with other plugs, as this causes a hazardous situation.
9. Do not allow anything to rest on the power cords. Do not install this product where the cords may be walked on or crimped.
10. This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supplied at the premises, consult your dealer or local power company.
11. Do not overload wall outlets or use an extension cord.
12. This product should not be placed in any area where proper ventilation is not provided. Slots and openings in the back or bottom of this product are provided for ventilation. To protect them from overheating, these openings must not be blocked by placing the product on a soft surface such as a bed, sofa or rug. This product should never be placed near or over a radiator or heat register.
13. Never push objects of any kind into this product through the slots because they may touch dangerous voltage points or create a short circuit. Never spill liquid of any kind on the product.
14. To reduce the risk of electric shock, do not disassemble this product, but take it to an authorized service facility. Opening or removing parts of the product other than specified access doors may expose you to dangerous voltages or other risks. Incorrect reassembling can cause electric shock when the product is subsequently used.
15. Periodically examine all components for damage.

SAVE THESE INSTRUCTIONS

Important Safety Information

Electromagnetic fields (EMF)

This VTech product complies with all standards regarding electromagnetic fields (EMF). If handled properly and according to the instructions in this user's manual, the product is safe to be used based on scientific evidence available today.

Parts checklist

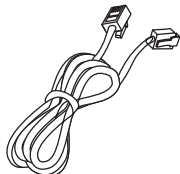
Your router package contains the following items. Save your sales receipt and original packaging in the event warranty service is necessary.



Abridged user's manual



Router



Ethernet cable



Power adapter

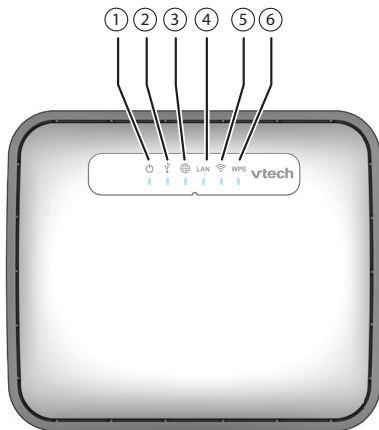
Table of Contents

Important Safety Information ...	i	
Parts checklist.....	ii	
Getting started	3	
Router Overview.....	3	
Connect your system	5	
Configure your computer network	6	
For Windows XP/2000	6	
For Windows Vista/7/8	9	
Connecting wireless devices.....	12	
Manual connection.....	12	
Using WPS.....	12	
Configure your router	13	
Log in to the web management page	13	
Web management page overview	14	
Fast configuration	15	
Status	16	
Device info: Wireless Router Status	16	
Statistics	17	
Setup.....	18	
WAN: WAN Configuration.....	18	
LAN: LAN Interface Setup	20	
LAN: DHCP mode:.....	21	
LAN: DHCP Static IP Configuration.....	23	
WLAN: Wireless Basic Settings.....	24	
WLAN: Wireless Security Setup	25	
WLAN: Wireless Multiple BSSID Setup	27	
WLAN: Wireless Access Control	28	
WLAN: Wireless Advanced Settings.....	29	
WLAN: Wi-Fi Protected Setup ..	31	
WLAN: WDS Settings	32	
Advanced.....	33	
Route: Routing configuration	33	
Route: RIP Configuration.....	34	
NAT: DMZ	35	
NAT: Virtual server.....	36	
NAT: ALG	37	
NAT: NAT port trigger	38	
NAT: NAT IP mapping	39	
QoS: IP QoS.....	40	
QoS: IP QoS traffic shaping:.....	41	
Port Mapping Configuration	42	
Others: Bridge Setting.....	43	
Others: Client limit configuration.....	44	
Others: Telnet.....	44	
Service	45	
UPnP	45	
DNS Configuration	46	

Dynamic DNS Configuration.....	47
USB Storage	48
Firewall	49
MAC filter.....	49
IP/Port filter.....	50
URL filter.....	52
DoS.....	53
Maintenance	54
Update: Upgrade firmware	54
Update: Backup/restore settings:	56
Password: User account configuration.....	58
Reboot.....	60
Time.....	61
Log: Log setting.....	62
Diagnostics: Ping	62
Diagnostics: Traceroute	63
Diagnostics: Diagnostic test.....	64
Appendix.....	65
Frequently asked questions	65
FCC part 15	66
For cETL compliance only	67
Mesures de sécurité importantes.....	67
For cETL compliance only	68
Limited Warranty.....	69
Technical specifications.....	71

Getting started

Router Overview



1- **On/Off light**

- On when the router is powered on.

2- **USB light**

- On when there is a device connected to the USB port.
- Flashes when the USB port receives data
- Off when no device is connected to the USB port.

3- **WAN light**

- On when the Internet connectivity is established as the **WAN** port is connected to Internet.

4- **LAN light**

- On when any **LAN** port is connected.
- Flashes when any **LAN** port receives data.

5- **Wi-Fi light**

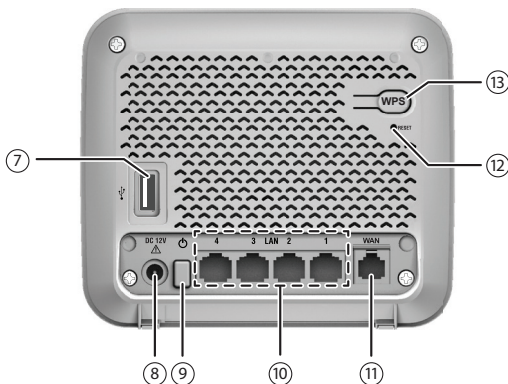
- On when the Wi-Fi is turned on.
- Off when the Wi-Fi is turned off.

6- **WPS light**

- On when WPS is in progress.
- Off when the WPS is not in progress.

Getting started

Router Overview



7–USB port

- Connects to USB device for file sharing.

8–Power jack

- Connects to the power adapter.

9– On/Off button

- Press to power on the router.
- Press once again to power it off.

10–LAN ports

- Connect to Ethernet devices such as computers and SIP phones.

11–WAN port

- Connects to the wide area network.

12–RESET button

- Press and hold (using a narrow-pointed object) to reset the router to default settings.

13–WPS button

- After turning on the Wi-Fi, press and hold for 10 seconds to start the Wireless Protected Setup (WPS).



Getting started

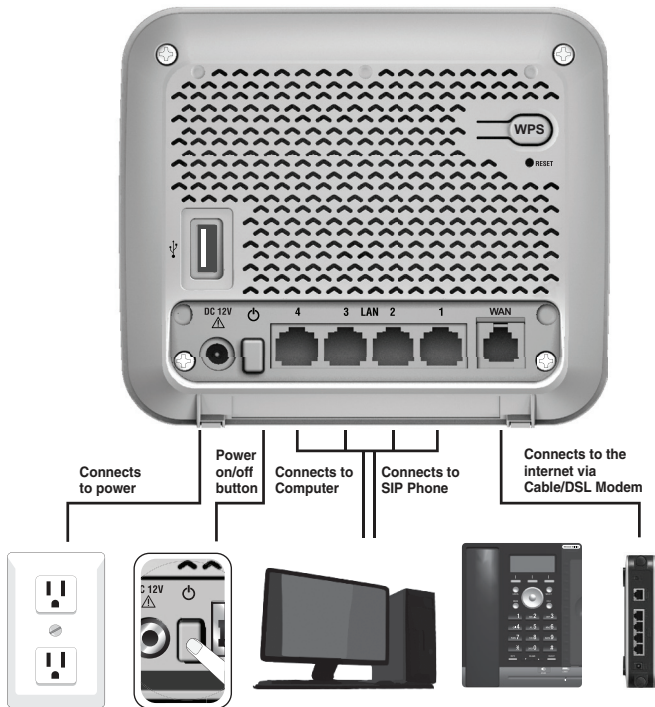
Connect your system

The VNT832 router has four LAN ports for connecting Ethernet devices such as computers and SIP phones. Before you start setting up your system, plan it carefully. Consider the number of Ethernet device(s) you need to connect before you start planning your system.

NOTES

- Use only the adapter provided.
- Make sure the electrical outlet is not controlled by a wall switch.
- The adapter is intended to be correctly oriented in a vertical or floor mount position. The prongs are not designed to hold the plug in place if it is plugged into a ceiling, under-the-table or cabinet outlet.

To power on, press the  button at the back of the router. The  light will turn on.



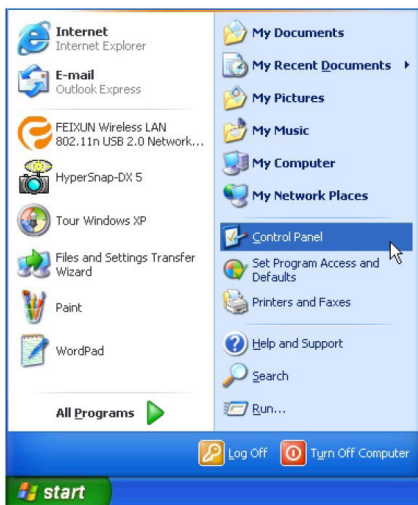
Getting Started

Configure your computer network

In order to view or change the settings of the VNT832 router, you need to login to the web management page of the router. Before that, connect your computer to the LAN port of the router, and then set the computer to obtain IP address automatically according to the steps below.

For Windows XP/2000

1. Click **Start**, then open the **Control Panel**.



2. Double-click **Network Connections**.



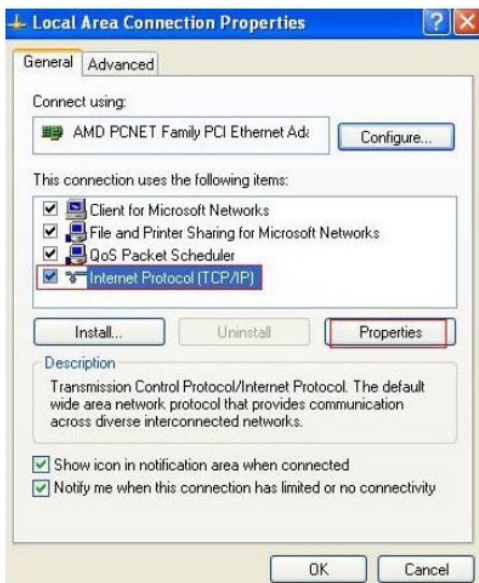
Getting Started

Configure your computer network

3. Right-click **Local Area Connection**, and then select **Properties**.



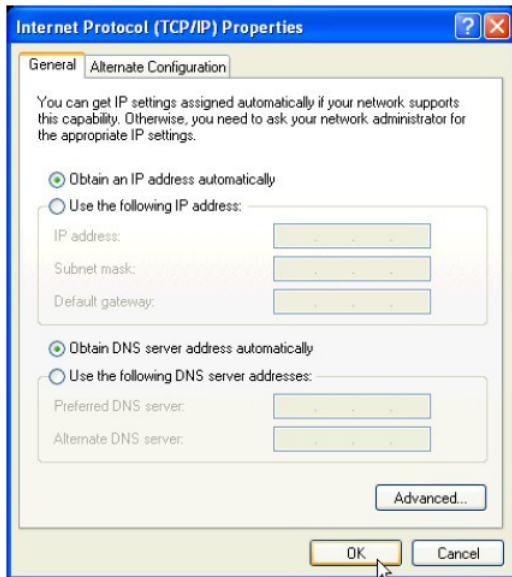
4. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.



Getting Started

Configure your computer network

5. Select **Obtain IP address automatically** and **Obtain DNS server address automatically**, and then click **OK**.

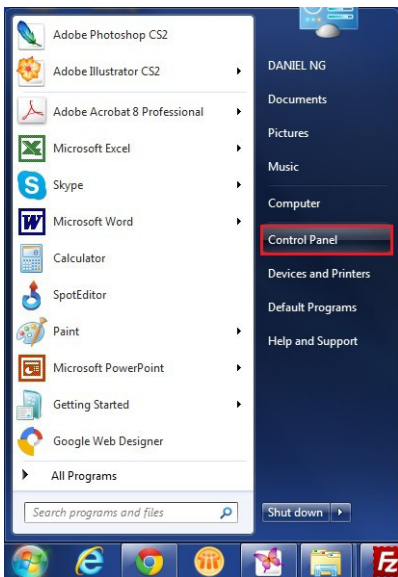


Getting Started

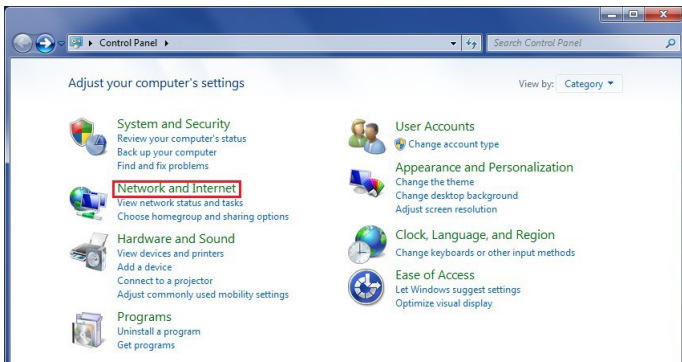
Configure your computer network

For Windows Vista/7/8

1. Click **Start**, and then open the **Control Panel**.



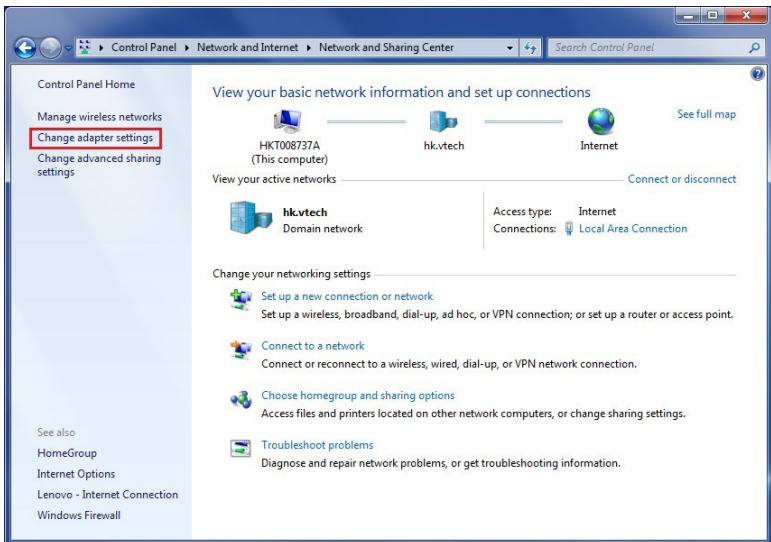
2. Click **Network and Internet**, and then **Network and Sharing Center**.



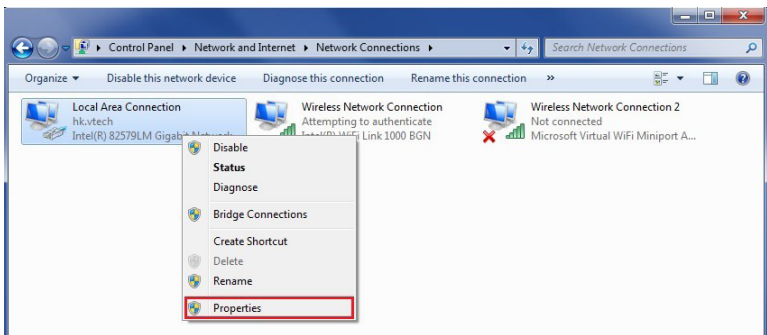
Getting Started

Configure your computer network

3. Click **Change adapter settings**.



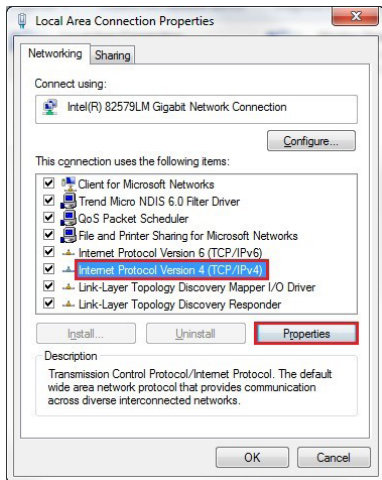
4. Right-click **Local Area Connection**, and then select **Properties**.



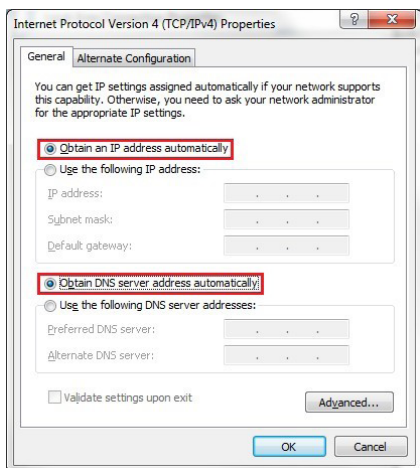
Getting Started

Configure your computer network

5. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.



6. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then click **OK**.



Getting Started

Connecting wireless devices

Before you connect wireless devices to the router, you should run the fast configuration Wizard. See “Fast configuration” on page 15.

You can connect wireless devices manually or by using WPS, which is fast and convenient.

Manual connection

1. On your wireless device, open your Network or Wi-Fi settings and find the list of available Wi-Fi networks.
2. Find the network name (SSID) for your VNT832 router. If you have trouble identifying the SSID, it is printed on the label on the bottom of the router.
3. On your device, select the network and enter the Wi-Fi password, which is also printed on the label on the bottom of the router.
4. On your device, click Connect.

Using WPS

1. On the router, press and hold the Wi-Fi/WPS button for 10 seconds.
The WPS light on the front panel turns on, and you will have two minutes to complete the rest of this procedure.
2. On your device, find your WPS settings and turn WPS on.
Your device will connect to the network. If your device requests a WPS PIN, the WPS PIN is printed on the label on the bottom of the router.

To configure additional WPS settings for the router, see “WLAN: Wi-Fi Protected Setup” on page 31.

Configure your router

Log in to the web management page

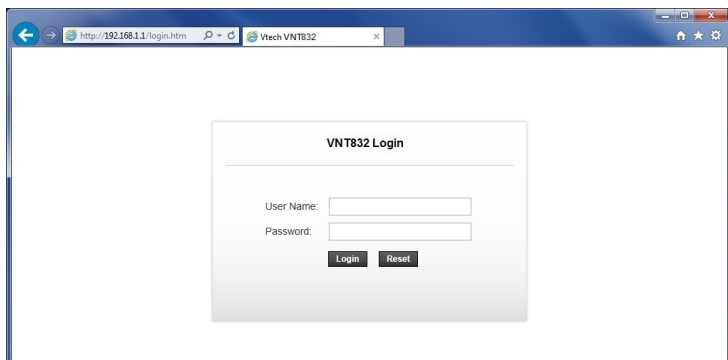
With your computer connected to a LAN port of the router and set to obtain an IP address automatically, power on the router. You can log in to the web management page to browse the router settings and change them if necessary.



TIP

- Before you browse the web management page, check your browser's network setting. Make sure you do not use a proxy server for LAN setting.

1. Open a web browser on your computer.
2. Type **http://192.168.1.1** in the address bar, and then press **Enter**. The following login page displays.



3. Enter the default user name and password for the administrative account as shown below. The user name and password are case-sensitive.

Username: **admin**

Password: **12345**

4. Click **Login** to enter the web management page of the router.



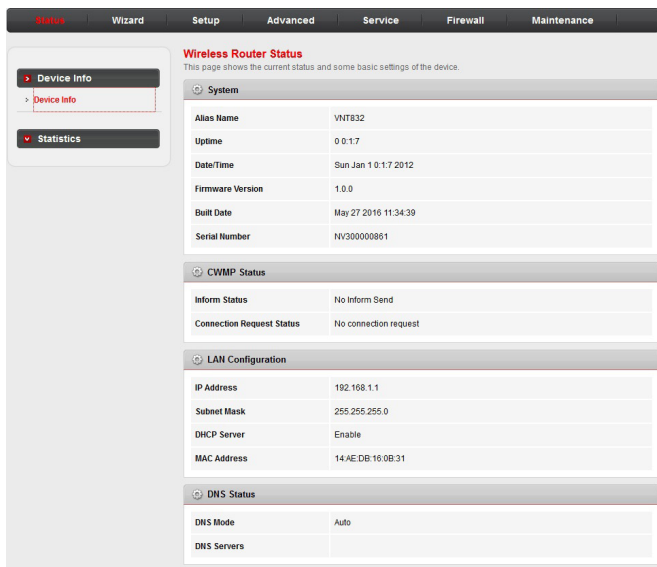
NOTE

- Both administrative account and normal user account can view the router settings. To change the settings, you must login using an administrative account.

Configure your router

Web management page overview

After you logged in to the web management page, you can do the configurations of your router here. You will see the menus for **Status**, **Wizard**, **Setup**, **Advanced**, **Service**, **Firewall**, and **Maintenance**.



The screenshot displays the router's web management interface. At the top, there is a navigation bar with tabs for Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance. The 'Status' tab is selected. On the left side, there is a sidebar menu with 'Device Info' and 'Statistics' options. The main content area is titled 'Wireless Router Status' and includes a sub-header 'System'. Below this, there are several sections: 'System' (with fields for Alias Name, Uptime, Date/Time, Firmware Version, Built Date, and Serial Number), 'CWMP Status' (with Inform Status and Connection Request Status), 'LAN Configuration' (with IP Address, Subnet Mask, DHCP Server, and MAC Address), and 'DNS Status' (with DNS Mode and DNS Servers).

System	
Alias Name	WRT832
Uptime	0 0:17
Date/Time	Sun Jan 1 0:17:2012
Firmware Version	1.0.0
Built Date	May 27 2016 11:34:39
Serial Number	NY300000861

CWMP Status	
Inform Status	No Inform Send
Connection Request Status	No connection request

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	14:AE:DB:16:0B:31

DNS Status	
DNS Mode	Auto
DNS Servers	

- **STATUS:** Allows you to view the information and statistics of the router.
- **WIZARD:** Allows you to start the fast configuration Wizard.
- **SETUP:** Allows you to configure the basic functions of the router.
- **ADVANCED:** Allows you to configure the advanced functions of the router.
- **SERVICE:** Allows you to configure extended network features.
- **FIREWALL:** Allows you to secure your router from unauthorized devices and/or services.
- **MAINTENANCE:** Allows you to manage firmware updates, passwords, network time, and diagnostics.

Configure your router

Fast configuration

The **Wizard** feature can guide you through the basic configuration of the router step by step. After running the Wizard you can close the web management page and then start connecting devices to the router.

1. Click the **Wizard** menu to start the fast configuration.
2. Select or input the information on the page as appropriate to configure the WAN settings. Click **Next** to proceed.

The screenshot shows the 'Fast Config' wizard interface. The top navigation bar includes 'Status', 'Wizard', 'Setup', 'Advanced', 'Service', 'Firewall', and 'Maintenance'. The left sidebar has a 'Wizard' menu. The main content area is titled 'Fast Config' and contains the following text: 'The wizard will help you do some basic configurations step by step. Step 1: WAN Connection Setting, Step 2: WLAN Connection Setting, Step 3: Save Setting.' Below this is a form for 'Step 1: WAN Connection Setting:'. The form includes a title 'Please select the wan connection mode' and several configuration options: 'Connection Mode' with radio buttons for Bridge, IPoE, and PPPoE (selected); '802.1q' with radio buttons for Enable and Disable (selected); 'VLAN ID(1-4095):' with an empty text input field; 'PPP Settings:' with 'Username:' and 'Password:' text input fields; 'Default Route:' with radio buttons for Enable and Disable (selected); and 'DNS Settings:' with radio buttons for 'Attain DNS Automatically' (selected) and 'Set DNS Manually:'. A 'Next' button is located at the bottom of the form.

3. Preview the settings and click **Apply Changes** to save the settings. Otherwise, click **Prev** to return to the previous page or click **Cancel** to cancel the fast configuration.

The screenshot shows the 'Fast Config' wizard interface at the 'Step 3: Save Settings' stage. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'Fast Config' and contains the following text: 'Step 3: Save Settings. If you need finish settings in the fast config, please click "Apply Changes"; otherwise please click "Cancel" or "Prev".' Below this is a table showing the 'Settings as follow:'. The table has two columns and the following rows: 'Channel Mode: PPPoE', 'IP Protocol: Ipv4', 'ppp username: admin', 'ppp password: admin12345', 'DNS Setting: DNS Automatically', and 'WLAN: Enable'. At the bottom of the form are three buttons: 'Prev', 'Apply Changes' (highlighted with a red box), and 'Cancel'.

Configure your router

Status

The **Status** menu allows you to view the information and statistics of the router. Choose this menu and you can see the next sub-menus: **Device info** and **Statistics**.

Device info: Wireless Router Status

Click the **Status** menu. The **Wireless Router Status** page under the **Device info** sub-menu in the left pane opens, displaying the basic information of the router, including system, LAN configuration, DNS status and Ethernet WAN interfaces.

The screenshot shows a web interface for a wireless router. At the top, there is a navigation bar with tabs: Status (highlighted in red), Wizard, Setup, Advanced, Service, Firewall, and Maintenance. On the left side, there is a sidebar menu with 'Device Info' (expanded) and 'Statistics'. The main content area is titled 'Wireless Router Status' and contains several sections:

- System**: A table showing system information.

Alias Name	VNT832
Uptime	0 d 1.7
Date/Time	Sun Jan 1 0:17:2012
Firmware Version	1.0.0
Built Date	May 27 2016 11:34:39
Serial Number	NV300000861
- CWMP Status**: A table showing CWMP status.

Inform Status	No Inform Send
Connection Request Status	No connection request
- LAN Configuration**: A table showing LAN configuration.

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	14:AE:DB:16:0B:31
- DNS Status**: A table showing DNS status.

DNS Mode	Auto
DNS Servers	
- Ethernet WAN Interfaces**: A table showing Ethernet WAN interfaces.

Interface	Droute	Protocol	IP Address	Gateway	Status
WAN0	On	PoE	0.0.0.0	0.0.0.0	down

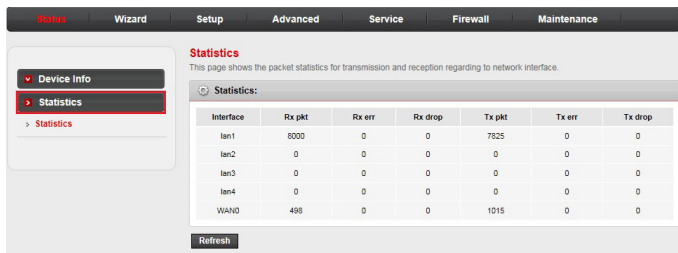
At the bottom of the main content area, there is a 'Refresh' button.

Configure your router

Status

Statistics

Click the **Statistics** sub-menu. The page displays the packet statistics for transmission and reception regarding network interface.



The screenshot shows the router's configuration interface with the 'Statistics' sub-menu selected. The main content area displays a table of statistics for various network interfaces. The table has seven columns: Interface, Rx pkt, Rx err, Rx drop, Tx pkt, Tx err, and Tx drop. The data is as follows:

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
lan1	8000	0	0	7825	0	0
lan2	0	0	0	0	0	0
lan3	0	0	0	0	0	0
lan4	0	0	0	0	0	0
WAN0	498	0	0	1015	0	0

Below the table is a 'Refresh' button. The left sidebar shows a menu with 'Device Info' and 'Statistics' (highlighted with a red box). The top navigation bar includes 'Status', 'Wizard', 'Setup', 'Advanced', 'Service', 'Firewall', and 'Maintenance'.

Configure your router

Setup

The **Setup** menu allows you to configure the functions of the router. Choose this menu and you can see the next sub-menus: **WAN** and **LAN**.

WAN: WAN Configuration

Click the **Setup** menu. The **WAN Configuration** page under the WAN sub-menu in the left pane opens. You can configure the parameters for the WAN interface of your router, such as channel mode, PPP settings and WAN IP settings.

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

Auto Bridge: Disable Enable

Default Route Selection: Auto Specified

Channel Mode: Enable NAPT:

PPP Settings:

User Name: Password:

Type: Idle Time (min):

WAN IP Settings:

Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

NetMask:

Default Route: Disable Enable Auto

Unnumbered:

Connect Disconnect Add Modify Delete Undo Refresh

WAN Interfaces Table:

Select	Inf	Mode	NAPT	IGMP	DRoute	IP Addr	Remote IP	NetMask	User Name	Status	Edit
<input type="checkbox"/>	WAN0	PoE	On	Off	On	0.0.0.0	0.0.0.0	0.0.0.0	---	down	

- **Auto Bridge:** Enable or disable the Auto Bridge Mode. If it is enabled, the child VNT832 router's DHCP mode will change to DHCP Relay automatically. See **DHCP mode** on page 21 for more details.
- **Default Route Selection:** Auto, Specified.

Configure your router

Setup

- **Channel mode:** It can be **Bridge**, **IPoE** or **PPPoE**.
- **Enable NAPT:** Enable or disable the NATP function.
- **PPP User Name:** User name of the PPP connection
- **PPP Password:** Password of the PPP connection.
- **Type** (PPP settings): **Continuous**, **Manual** or **Connect On Demand**.
- **Idle Time (min):** The idle time of the PPP connection when the type is Connect On Demand.
- **Type** (WAN IP settings): **Fixed** or **DHCP**.
- **Local IP address:** The IP address of the router.
- **Remote IP address:** The gateway's IP address of the router.
- **NetMask:** The subnet mask of the router.
- **Default Route:** The mode of the default route of the router.
- **Unnumbered:** Enable or disable IP unnumbered interface mode.

Configure your router

Setup

LAN: LAN Interface Setup

Click the **LAN** sub-menu in the left pane. The **LAN Interface Setup** page opens. You can configure the LAN interface of your router, such as changing the setting for IP address and subnet mask.

The screenshot shows the router's configuration page for the LAN interface. At the top, there are navigation tabs: Status, Wizard, Setup (highlighted), Advanced, Service, Firewall, and Maintenance. On the left, a sidebar menu shows options for WAN, LAN (highlighted), LAN, DHCP, DHCP Static, and WLAN. The main content area is titled "LAN Interface Setup" and includes a description: "This page is used to configure the LAN interface of your Router. Here you may change the setting for IP address, subnet mask, etc." The configuration fields are as follows:

- Interface Name: Ethernet1
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Secondary IP:

Below these fields is an "Apply Changes" button. Further down, there is a "MAC Address Control" section with checkboxes for LAN1, LAN2, LAN3, LAN4, and WLAN. An "Apply Changes" button is also present here. Below that is a "New MAC Address" section with an input field and an "Add" button. At the bottom, there is a "Current Allowed MAC Address Table" section with a table header containing "MAC Addr" and "Action".

- **IP Address:** The IP address of the router's LAN interface. The default value is 192.168.1.1.
- **Subnet Mask:** The subnet mask of the router's LAN interface. The default value is 255.255.255.0.
- **Secondary IP:** If you enable the Secondary IP, you should configure another IP address and subnet mask for the LAN interface.
- **MAC Address Control:** Select the LAN interface on which you want to run MAC Address Control.
- **New MAC Address:** You can add a new MAC address.
- The **Current Allowed MAC Address Table** shows the current allowed MAC address list.

Configure your router

Setup

LAN: DHCP mode:

Click **DHCP** in the left pane. The **DHCP Mode** page opens. On this page, you can configure the DHCP mode of your router as **None**, **DHCP Server** or **DHCP Relay**.

DHCP Mode

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

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode:

IP Pool Range: 192.168.1.2 - 192.168.1.254

Subnet Mask:

Default Gateway:

Max Lease Time: minutes

Domain Name:

DNS Servers:

- **DHCP Mode:** Select one of the DHCP modes described below:
 - **None:** The router will do nothing when the hosts require an IP address by DHCP protocol.
 - **DHCP Server:** DHCP Server is used to configure correct TCP/IP protocol related parameters for the computer on you local network. If you enable the DHCP Server function, you can make the DHCP Server automatically configure the TCP/IP protocol parameters (such as IP address, subnet mask, gateway and DNS servers) for the computer on you local network.
 - **DHCP Relay:** DHCP Relay is used if you are using the other DHCP Server to assign IP address to your Ethernet devices on the LAN. You can set the DHCP Server's IP address.

Configure your router

Setup

NOTES

- If you have more than four Ethernet devices and they are connected to the additional VNT832 router(s) you purchased, there is no need to change the DHCP mode setting of the child router(s). Once a child VNT832 router is connected with a parent VNT832 router, the child router enters Auto Bridge Mode, and all Ethernet devices obtain IP addresses from the parent router directly. See **Plan and connect your system** on page 4 for more details.
- If you have more than four Ethernet devices and you are using an existing non-VTech router as the parent router and VNT832 router(s) as the child router(s), you need to set the DHCP mode to **DHCP Relay** for the VNT832 router(s) manually and make sure the non-VTech router has the DHCP setting enabled, so that all Ethernet devices obtain IP addresses from the parent router directly.
- **IP Pool Range:** Enter the range of assignable IP addresses.
- **Subnet Mask:** The subnet mask of the router's LAN interface. The default value is 255.255.255.0.
- **Default Gateway:** Enter the IP address of the default gateway.
- **Max Lease Time:** Set the lease time for assigned IP addresses. When the lease time expires, the router may assign a new address for the client.
- **Domain Name:** Enter the domain name for the router.
- **DNS Servers:** Enter addresses for up to three DNS servers.

Configure your router

Setup

LAN: DHCP Static IP Configuration

In the left pane, click **DHCP Static**. The **DHCP Static IP Configuration** page opens. On this page, you can set the DHCP address reservation rules. The DHCP Static IP table shows the reserved IP address and MAC address that have been set up for the DHCP Server.

The screenshot shows the router's configuration page for DHCP Static IP. The top navigation bar includes Status, Wizard, Setup (highlighted), Advanced, Service, Firewall, and Maintenance. The left sidebar has a tree view with WAN, LAN, DHCP, DHCP Static (highlighted with a red box), and WLAN. The main content area is titled 'DHCP Static IP Configuration' and contains a description: 'This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.' Below this are two input fields: 'IP Address' with the value '0.0.0.0' and 'Mac Address' with the value '000000000000' (with an example '(ex. 00E986710502)'). There are three buttons: 'Add', 'Delete Selected', and 'Undo'. At the bottom, there is a table titled 'DHCP Static IP Table' with columns for 'Select', 'IP Address', and 'MAC Address'.

- **IP Address:** Manually input an IP address to add a static assignment.
- **Mac Address:** Manually input a MAC address to add a static assignment.
- Click **Add** to add the static IP and associated MAC address to the Static IP table. The router searches the relevant entry in this table to assign an IP address according to the client's MAC address. If the router cannot find a corresponding static entry, it will choose an unallocated IP address from DHCP pool assigned to the client.

Configure your router

Setup

WLAN: Wireless Basic Settings

In the left pane, click **WLAN**. The **Wireless Basic Settings** page opens. On this page, you can configure the router if you plan to use the wireless LAN (Wi-Fi) features.

Wireless Basic Settings
This page is used to configure the parameters for your wireless network.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP

SSID: YTECH8320B31

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: Auto Current Channel: 0

Radio Power (Percent): 100%

Associated Clients: Show Active Clients

Apply Changes

- **Disable Wireless LAN Interface:** Click to disable wireless functionality.
- **Band:** Select the wireless band standard: 2.4 GHz (B), 2.4 GHz (G), 2.4 GHz (B+G), 2.4 GHz (N), 2.4 GHz (G+N), 2.4 GHz (B+G+N)
- **SSID:** If necessary, edit the Server Set Identifier (SSID), that is, the Wi-Fi network name
- **Channel Width:** Select your preferred bandwidth: 20MHz, 40MHz, 20/40MHz. The lower bandwidth works best in busy Wi-Fi environments, and offers increased range.
- **Control Sideband:** When channel width is set to 40MHz, select the band to be used as the secondary channel: Upper, Lower. For channel numbers up to 7, select Lower; for channels up to 11, select Upper.

Configure your router

Setup

- **Channel Number:** Select the channel the router uses for Wi-Fi: Auto, 5,6,7,8,9,10,11. Unless you have specific requirements to use a specific channel, leave this setting at Auto.
- **Radio Power (Percent):** Select the power level of the Wi-Fi radio transmitter: 100, 80, 50, 25, 10 percent. Unless you have issues with signal strength and range, you should leave this setting at default.
- **Associated Clients:** Click the **Show Active Clients** button to display the Active Wireless Client Table. This table lists the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

WLAN: Wireless Security Setup

In the left pane, click **Security**. The **Wireless Security Setup** page opens. This page allows you to prevent any unauthorized access to your wireless network.

The screenshot shows the router's configuration page for Wireless Security Setup. The top navigation bar includes Status, Wizard, Setup (highlighted), Advanced, Service, Firewall, and Maintenance. The left sidebar shows a tree view with WAN, LAN, and WLAN sections. Under WLAN, there are sub-items: Basic, Security (highlighted with a red box), MBSSID, Access Control List, Advanced, WPS, and WDS. The main content area is titled "Wireless Security Setup" and includes a sub-header: "This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network." The configuration fields are as follows:

- SSID TYPE:** Radio buttons for Root (selected), VAP0, VAP1, VAP2, and VAP3.
- Encryption:** A dropdown menu set to "WPA2 Mixed".
- Use 802.1x Authentication:** A checkbox that is unchecked.
- WPA Authentication Mode:** Radio buttons for Enterprise (RADIUS) and Personal (Pre-Shared Key) (selected).
- Pre-Shared Key Format:** A dropdown menu set to "Passphrase".
- Pre-Shared Key:** A text input field containing "*****".
- Authentication RADIUS Server:** Fields for Port (1812), IP address (0.0.0.0), and Password.

A note at the bottom states: "Note: When encryption WEP is selected, you must set WEP key value." An "Apply Changes" button is located at the bottom left of the main content area.

Configure your router

Setup

- **SSID Type:** Root, VAP0, VAP1, VAP2, VAP3. Selecting Virtual Access Points VAP0 to VAP3 disables the security settings on this page. You must configure Virtual Access Points and VAP security on the MBSSID page.
- **Encryption:** Select the encryption type: WPA2 Mixed, WPA2(TKIP) WPA2(AES), WPA(AES), WPA(TKIP), WEP, None. None is not recommended except for certain configuration or troubleshooting situations.
 - If you select WEP you must configure key length, key format, default Tx key, and encryption keys 1 to 4 (use the same number of characters for each key).
- **Use 802.1x Authentication Mode:** Select the authentication mode: Enterprise (RADIUS) or Personal (Pre-Shared Key). Select Enterprise (RADIUS) if using an external RADIUS server to authenticate clients.
- **Pre-Shared Key Format:** Select the pre-shared key format: Passphrase or Hex (64 characters). Passphrase can contain a–z, A–Z, 0–9, and symbols. Hex can contain 0–9, and upper case letters A–F.
- **Pre-Shared Key:** Enter the key for WPA or WEP authentication, from 8 to 63 characters.
- **Authentication RADIUS Server:** Enter the RADIUS server settings if using the RADIUS server for wireless client authentication. Port, IP address, Password

Configure your router

Setup

WLAN: Wireless Multiple BSSID Setup

In the left pane, click **MBSSID**. The **Wireless Multiple BSSID Setup** page opens. This page allows you to set four virtual access points (VAP0 to VAP3).

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

Enable VAP0

SSID:

Broadcast SSID: Enable Disable

Relay Blocking: Enable Disable

Authentication Type: Open System Shared Key Auto

Enable VAP1

SSID:

Broadcast SSID: Enable Disable

Relay Blocking: Enable Disable

Authentication Type: Open System Shared Key Auto

Enable VAP2

SSID:

Broadcast SSID: Enable Disable

Relay Blocking: Enable Disable

Authentication Type: Open System Shared Key Auto

Enable VAP3

SSID:

Broadcast SSID: Enable Disable

Relay Blocking: Enable Disable

Authentication Type: Open System Shared Key Auto

- **Enable VAP n :** Enable the virtual access point (VAP).
- **SSID:** Edit the SSID for the enabled VAP.
- **Broadcast SSID:** Set whether the router broadcasts the SSID: Enable, Disable. When enabled, wireless clients can display the SSID in their list of available networks.

Configure your router

Setup

- **Relay Blocking:** Set whether wireless clients using the same VAP are visible (and potentially have access) to each other: Enable, Disable
- **Authentication Type:** Select the authentication type: Open System, Shared Key, Auto

WLAN: Wireless Access Control

In the left pane, click **Access Control List**. The **Wireless Access Control** page opens. On this page, you can specify which clients can connect to your access point, based on device MAC addresses.

The screenshot shows the router's configuration page for Wireless Access Control. At the top, there are tabs for Status, Wizard, Setup (selected), Advanced, Service, Firewall, and Maintenance. On the left, a sidebar menu lists various settings: WAN, LAN, WLAN, Basic, Security, MBSSID, Access Control List (highlighted with a red box), Advanced, WPS, and WDS. The main content area is titled 'Wireless Access Control' and includes a help text: 'If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.' Below this, there is a 'Wireless Access Control Mode' dropdown menu set to 'Disable' and an 'Apply Changes' button. A 'MAC Address' input field contains the example '00E086710502', with 'Add' and 'Reset' buttons to its right. A section titled 'Current Access Control List' contains a table with two columns: 'MAC Address' and 'Select'. Below the table are 'Delete Selected' and 'Delete All' buttons.

- **Wireless Access Control Mode:** Select the mode for device access control: Disable, Allow Listed, Deny Listed.
- **MAC Address:** If **Allow Listed** or **Deny Listed** are selected, enter a MAC address for each client you want to allow or deny access to the network. Click **Add** after entering each MAC address.

Click **Apply Changes** to apply the new control mode.

Configure your router

Setup

WLAN: Wireless Advanced Settings

In the left pane, click **Advanced**. The **Wireless Advanced Settings** page opens. Unless you are a technically advanced user with special requirements for your wireless network, you should not have to change these settings.

Wireless Advanced Settings

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

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

Apply Changes

- **Authentication Type:** Open System, Shared Key, Auto
- **Fragment Threshold:** Sets the maximum packet size (maximum transmission unit, or MTU) before data is fragmented into multiple packets to accommodate devices in the transmission path that have lower MTU settings: 256–2346. Adjusting the threshold may correct a high packet error rate, although low settings can reduce performance over a wireless network.
- **RTS Threshold:** Sets the size of Mac protocol data unit (MPDU) below which a Request to Send/Clear to Send handshake between ADSL modem and router will not be performed: 0–2347 (bytes).
- **Beacon Interval:** Set the frequency of a beacon broadcast by the access point to synchronize the wireless network: 20–1024 ms

Configure your router

Setup

- **DTIM Interval:** Set the frequency of the Delivery Traffic Indication Message (DTIM): 1–255. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access point clients will awaken to receive the broadcast and multicast messages.
- **Data Rate:** Set the data transmission rate: Auto, 1–54M, MCS0–15. Leaving this setting at Auto will ensure the fastest available data rate, with automatic fallback to the best possible rate when the access point and client maximum speeds differ.
- **Preamble Rate:** Set the type of the Cyclic Redundancy Check (used for synchronizing router and clients, and detecting data transmission errors): Long Preamble, Short Preamble. In general, Long Preamble is compatible with older and newer devices. Long Preamble can be effective when there is network interference or signal strength is low. Short Preamble can improve performance if clients support the Short Preamble type.
- **Broadcast SSID:** Enabled, Disabled
- **Relay Blocking:** Enabled, Disabled
- **Ethernet to Wireless Blocking:** Enabled, Disabled.
- **Wifi Multicast to Unicast:** Enable this setting to have the router switch from multicast media (one media stream to multiple clients) streaming to unicast (multiple one-to-one sessions to multiple clients) streaming: Enabled, Disabled
- **Aggregation:** Enables or disables Aggregated MAC Protocol Data Unit (AMPDU), which can improve network performance in busy Wi-Fi environments : Enabled, Disabled. Overall, though, it can hamper performance when Wi-Fi signal is strong and few clients are connected.
- **Short GI:** Enables or disables short Guard Interval (GI): Enabled, Disabled. Short GI can increase the data rate by about 10% in certain environments, and when using 802.11n and 802.11ac only.

Configure your router

Setup

WLAN: Wi-Fi Protected Setup

In the left pane, click **WPS**. The **Wi-Fi Protected Setup** page opens. WPS is a convenient method for wireless clients to connect to the network.

The screenshot shows the router's web interface. At the top, there are tabs for Status, Wizard, Setup (highlighted in red), Advanced, Service, Firewall, and Maintenance. On the left, a navigation menu lists WAN, LAN, WLAN, Basic, Security, MBSSID, Access Control List, Advanced, WPS (highlighted with a red box), and WDS. The main content area is titled "Wi-Fi Protected Setup" and includes a sub-header: "This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle." Below this, there are several sections: "Disable WPS" with a checkbox; "WPS Status" with radio buttons for "Configured" and "UnConfigured"; "Self-PIN Number" with a text input field containing "13774240" and a "Regenerate PIN" button; "Push Button Configuration" with a "Start PBC" button; and "Start PIN" with a "Start PIN" button. At the bottom of the main area are "Apply Changes" and "Reset" buttons.

- **Disable WPS:** Click to disable Wi-Fi Protected Setup. Other methods of authentication will apply, such as entering a WPA2 passphrase.
- **WPS Status:** Configured, Unconfigured.
- **Self-PIN Number:** Set the 8-digit PIN that must be entered for clients to connect. The default PIN is provided on the label on the bottom of the router.
- **Push Button Configuration:** Click the PBC button to start Wi-Fi Protected Setup. You have two minutes to find the available wireless network on your device and connect to the router (you may also need to enter the PIN).
- **Start PIN:** Enter the client device's WPS PIN. After saving the client-generated WPS PIN, the client device can discover this router (some devices will display "WPS available" with the network name) in its list of detected networks. You can then easily connect to the router on your client device.

Configure your router

Setup

WLAN: WDS Settings

In the left pane, click **WDS**. The **WDS Settings** page opens. Wireless Distribution System (WDS) uses wireless media to communicate with other access points. In this way, you can expand the reach of your wireless network. On this page, you can enable WDS and add MAC addresses of the other devices/access points the router will communicate with.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

Add WDS AP

MAC Address:

Comment:

Apply Changes **Reset**

Current WDS AP List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected **Delete All**

- **Enable WDS:** Click to enable WDS.
- **MAC Address:** Enter the MAC address of another device that will be another access point connected to the router.
- **Comment:** Enter any notes about the access point device name or location.

Click **Apply Changes** to add the new access point to the WDS AP list.

Configure your router

Advanced

The Advanced menu allows you to configure the advanced functions of the router. Choose this menu and you can see the next sub-menus: **Route**, **NAT**, **QoS**, **Port Mapping**, **Others**.

Route: Routing configuration

Click the **Route** sub-menu in the left pane. The **Routing Configuration** page opens. On this page, you can enable static routes, configure routing information, and add and delete IP routes.

Routing Configuration
This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

Add Route Update Delete Selected Show Routes

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	If
--------	-------	-------------	-------------	---------	--------	----

- **Destination:** Specifies the IP network address of the final destination.
- **Subnet Mask:** Enter the subnet mask for this destination.
- **Next Hop:** Enter the IP address of the gateway. The gateway is an immediate neighbour of your Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.
- **Metric:** Metric represents the cost of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number needs not to be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
- **Interface:** The WAN interface to which a static route is to be applied.
- The **Static Route Table** shows the current static route entries.

Configure your router

Advanced

Route: RIP Configuration

Click **RIP** in the left pane. The **RIP Configuration** page opens. Routing Information Protocol (RIP) is an internet protocol you can setup to share routing table information with other routing devices. On this page, you can configure the RIP settings such as enabling or disabling the RIP function.

The screenshot shows the 'RIP Configuration' page in a router's web interface. The top navigation bar includes 'Status', 'Wizard', 'Setup', 'Advanced' (highlighted), 'Service', 'Firewall', and 'Maintenance'. The left sidebar has a tree view with 'Route' expanded, showing 'Static Route' and 'RIP' (highlighted with a red box). Below 'Route' are buttons for 'NAT', 'QoS', 'Port Mapping', and 'Others'. The main content area is titled 'RIP Configuration' and contains the following elements:

- A sub-header: 'RIP Configuration' with a description: 'Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.'
- A 'RIP:' section with radio buttons for 'Off' (selected) and 'On', and an 'Apply' button.
- An 'Interface:' section with a dropdown menu set to 'LAN'.
- A 'Recv Version:' section with a dropdown menu set to 'RIP1'.
- A 'Send Version:' section with a dropdown menu set to 'RIP1'.
- 'Add' and 'Delete' buttons.
- A 'Rip Config List:' section with a table:

Select	interface	Recv Version	Send Version
--------	-----------	--------------	--------------

- **RIP:** Enable or disable the RIP function of the router.
- **Interface:** The interface on which you want to enable RIP.
- **Recv Version:** Indicates the RIP version in which information must be passed to the device it can be accepted into its routing table.
- **Send Version:** Indicates the RIP version this interface will use when it sends its route information to the other device.
- The **RIP Config List** shows the current RIP setting of the device.

Configure your router

Advanced

NAT: DMZ

You can set up the Network Address Translation (NAT) function in the **NAT** sub-menu.

Click the **NAT** sub-menu in the left pane. The **DMZ** page opens. On this page, you can configure the DMZ settings.

A Demilitarized Zone (DMZ) is a host between a private local network and the outside public network. Users of the public network outside the company can access the DMZ host. It allows you to expose one network user to the internet for some special-purpose services such as internet gaming or video conferencing. DMZ hosting forwards all the ports at the same time to one computer. You should assign a static IP address to the destination computer before you use this feature.

DMZ

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

DMZ Host IP Address:

Apply Changes **Reset**

Current DMZ Table:

Select	WAN Interface	DMZ IP
--------	---------------	--------

Delete Selected

- **DMZ Host IP Address:** Enter the specified IP Address for DMZ host on the LAN side.

Configure your router

Advanced

NAT: Virtual server

Click **Virtual Server** in the left pane. The **Virtual Server** page opens. This page allows you to configure the virtual server so that others can access the server through the Gateway.

The screenshot shows the 'Virtual Server' configuration page. The top navigation bar includes 'Status', 'Wizard', 'Setup', 'Advanced' (highlighted), 'Service', 'Firewall', and 'Maintenance'. The left sidebar has a tree view with 'Route', 'NAT' (expanded), 'DMZ', 'Virtual Server' (highlighted with a red box), 'ALG', 'Port Trigger', 'Nat IP Mapping', 'QoS', 'Port Mapping', and 'Others'. The main content area is titled 'Virtual Server' and contains the following fields:

- Service Type:** Radio buttons for 'Usual Service Name' (selected) and 'User-defined Service Name'.
- Usual Service Name:** Dropdown menu with 'AUTH' selected.
- Protocol:** Dropdown menu with 'TCP' selected.
- WAN Setting:** Dropdown menu with 'Interface' selected.
- WAN Interface:** Dropdown menu with 'WAN0' selected.
- WAN Port:** Text input field with '113' and '(ex. 5001:5010)'.
- LAN Open Port:** Text input field with '113'.
- LAN IP Address:** Text input field.

Below the fields is an 'Apply Changes' button. At the bottom, there is a section for the 'Current Virtual Server Forwarding Table' with a table header:

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

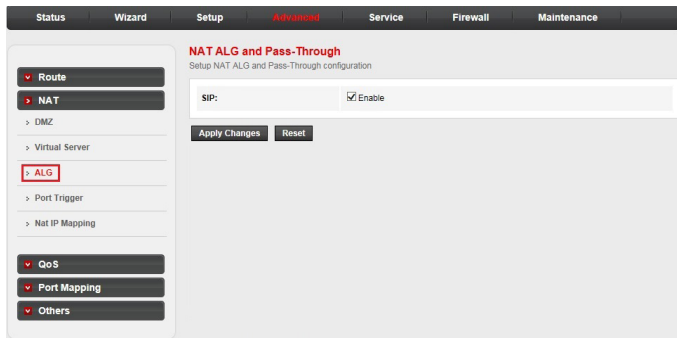
- **Usual Service Name & User-defined Service Name:** The name of this virtual server.
- **Protocol:** The protocol of this virtual server used: TCP or UDP.
- **WAN Setting:** The WAN setting of this virtual server used: Interface or IP address.
- **WAN Interface:** The interface on which the virtual server used on WAN side.
- **WAN Port:** The open port on WAN side. It can be either a single port or a port range.
- **LAN Open Port:** Enter the specific start and end port number you want to forward. If it is one port only, enter the same end port and start port number. For example, if you want to set the FTP virtual server, set the start and end port number to 21.
- **LAN IP Address:** The IP address of the host which provides the service on LAN side.
- The **Current Virtual Server Forwarding Table** displays the information about the virtual servers you established.

Configure your router

Advanced

NAT: ALG

Click **ALG** in the left pane. The **NAT ALG and Pass-Through** page opens. On this page, you can configure the Application Layer Gateway (ALG) setting.



- **SIP:** Enable.

Configure your router

Advanced

NAT: NAT port trigger

Click **Port Trigger** in the left pane. Port trigger is used to restrict certain types of data packets from your local network to the internet. Use of such filters can be helpful in securing and restricting your local network. On this page, you can configure the port trigger rules.

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

Nat Port Trigger: Enable Disable

Apply Changes

Application Type:

Usual Application Name:

User-defined Application Name:

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

Apply Changes

- **Nat Port Trigger:** Enable or disable the port trigger function on the device.
- **Application Type:** Select the service from the **Usual Application Name** or define the name from **User-defined Application Name**.
- **Start Match Port / End Match port:** The start and end port to match.
- **Trigger Protocol:** The protocol to trigger the rule. It can be **TCP**, **UDP** or **TCP/UDP**.
- **Start Relate Port / End Relate Port:** The start and end relate port.
- **Open Protocol:** It can be **TCP**, **UDP** or **TCP/UDP**.
- **NAT Type:** It can be **outgoing** or **incoming**.

Configure your router

Advanced

NAT: NAT IP mapping

Click **Nat IP Mapping** in the left pane. NAT IP mapping allows you to configure one IP pool for specified source IP address from LAN, so a packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.

The screenshot shows the NAT IP Mapping configuration page. At the top, there are tabs for Status, Wizard, Setup, Advanced (selected), Service, Firewall, and Maintenance. On the left, a navigation menu includes Route, NAT (selected), DMZ, Virtual Server, ALG, Port Trigger, Nat IP Mapping (highlighted), QoS, Port Mapping, and Others. The main content area is titled "NAT IP MAPPING" and contains a description: "Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT." Below the description, there are four input fields for "Local Start IP", "Local End IP", "Global Start IP", and "Global End IP", each with a dropdown menu set to "One-to-One". There are "Apply Changes" and "Reset" buttons. Below the form is a table titled "Current NAT IP MAPPING Table" with columns for "Local Start IP", "Local End IP", "Global Start IP", "Global End IP", and "Action". At the bottom of the table are "Delete Selected" and "Delete All" buttons.

- **Type:** The type of this mapping rule. It can be **One-to-One**, **Many-to-One**, **Many-to-Many** or **One-to-Many**.
 - **One-to-One:** One local IP will be mapped to one global IP.
 - **Many-to-One:** The IP between Local Start IP and Local End IP will be mapped to a global IP.
 - **Many-to-Many:** The IP between Local Start IP and Local End IP will be mapped to the IP between Global Start IP and Global End IP.
 - **One-to-Many:** One local IP will be mapped to any of the IP between Global Start IP and Global End IP.
- **Local Start IP:** A local IP address.
- **Local End IP:** A local IP address.
- **Global Start IP:** A global IP address used for NAT.
- **Global End IP:** A global IP address used for NAT.

Configure your router

Advanced

QoS: IP QoS

The router provides a control mechanism that serves traffic with different priorities. The traffic is classified by criteria. A classification rule contains three configuration blocks: Quality of Service (QoS) policy, schedule mode and traffic rule. The QoS policy enables you to classify packet on the basis of various fields in the packet. The schedule mode enables you to configure which priority queue you want to use. The traffic rule enables you to assign the precedence or add marker for different streams.

To configure IP QoS, click the **QoS** sub-menu in the left pane. The **IP QoS** page opens. On this page, you can enable or disable the IP QoS and configure the rules if necessary.

The screenshot shows the IP QoS configuration page. The top navigation bar includes tabs for Status, Wizard, Setup, **Advanced**, Service, Firewall, and Maintenance. The left sidebar menu has options for Route, NAT, **QoS**, Traffic Shaping, Port Mapping, and Others. The main content area is titled "IP QoS" and contains the following elements:

- IP QoS:** A radio button interface to enable or disable the function. The "enable" option is selected.
- Schedule Mode:** A dropdown menu currently set to "strict prior".
- Apply** button.
- QoS Rule List** table with columns: src MAC, dest MAC, src IP, sPort, dest IP, dPort, proto, phy port.
- QoS Rule List(Continue)** table with columns: IPP, TOS, DSCP, 802.1p, Prior, IPP Mark, TOS Mark, DSCP Mark, 802.1p Mark, sel.
- Delete** and **Add Rule** buttons at the bottom.

- **IP QoS:** Enable or disable the IP QoS function on the device.
- **Schedule Mode:** The schedule mode of the IP QoS function. It can be **strict prior** or **WFQ (4:3:2:1)**.
 - **Strict Prior:** Traffic with different priority will be sent by its priority. The higher priority the traffic is, the higher priority the traffic will be sent out.
 - **WFQ (4:3:2:1):** Traffic with different priority will be sent in proportion of its priority. The four priority traffic will be sent out in proportion to 4:3:2:1.

Configure your router

Advanced

QoS: IP QoS traffic shaping:

Click **Traffic Shaping** in the left pane. The **IP QoS Traffic Shaping** page opens. The tables on this page are used for traffic control. You can add traffic shaping rules in the list.

The screenshot shows the 'Advanced' configuration page for IP QoS Traffic Shaping. The top navigation bar includes 'Status', 'Wizard', 'Setup', 'Advanced' (highlighted), 'Service', 'Firewall', and 'Maintenance'. On the left, a sidebar menu lists 'Route', 'NAT', 'QoS', 'QoS' (sub-item), 'Traffic Shaping' (highlighted with a red box), 'Port Mapping', and 'Others'. The main content area is titled 'IP QoS Traffic Shaping' and contains the following sections:

- IP QoS Traffic Shaping**
Entries in this table are used for traffic control.
- Traffic Shaping in the network interface:**
A table with columns for 'Total Bandwidth(0, Unlimited):', 'UP Stream', and 'Down Stream'. The 'UP Stream' and 'Down Stream' columns each have an input field with '0' and a unit of 'kbps'.
- Apply** button.
- Traffic Shaping Rule List**
A table with columns: ID, Wan If, Protocol, Src Port, Dst Port, Src IP, Dst IP, Guaranteed Bandwidth(Kbps) (sub-columns: Up Floor, Down Floor), Max Bandwidth(Kbps) (sub-columns: Up Ceiling, Down Ceiling), and Remove.
- Add** and **Save/Apply** buttons.

Configure your router

Advanced

Port Mapping Configuration

The router provides multiple interface groups and supports up to five interface groups including one default group. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the device can isolate traffic from group to group for some applications. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.

Click the **Port Mapping** sub-menu in the left pane. The **Port Mapping Configuration** page opens.

The screenshot shows the 'Port Mapping Configuration' page. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, **Advanced**, Service, Firewall, and Maintenance. On the left, a sidebar menu is visible with categories: Route, NAT, QoS, **Port Mapping** (selected), and Others. The main content area is titled 'Port Mapping Configuration' and includes instructions: 'To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports. 3. Click "Apply Changes" button to save the changes.' Below the instructions, there is a note: 'Note that the selected interfaces will be removed from their existing groups and added to the new group.' A radio button selection is present with 'Disable' selected and 'Enable' unselected. The main configuration area is divided into two sections: 'WAN' and 'LAN'. Each section contains a large empty box representing the interface list. Between these sections are two buttons: 'Add>' and '<Del'. At the bottom, there is a table with two columns: 'Select' and 'Interfaces'. The 'Select' column has a 'Default' row with a radio button next to it. The 'Interfaces' column lists 'LAN1, LAN2, LAN3, LAN4, WAN0'. Below the table, there is a label 'Group#id1' followed by a radio button.

To manipulate a mapping group:

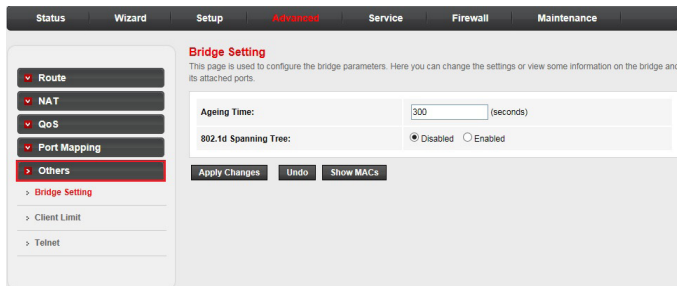
1. Select a group from the table, then you can see the available interface (LAN and WAN) and grouped interface list.
2. Select interfaces from the available and grouped interface list and add them to the interface group using the **Add>** button or delete them using the **<Del** button.
3. Click **Apply Changes** to finish the configuration.

Configure your router

Advanced

Others: Bridge Setting

Click the **Others** sub-menu in the left pane. The **Bridge Setting** page opens. Here you can configure the bridge parameters and view the information on the bridge and its attached ports.



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

Click the **Show MACs** button and you will see the current Forwarding Table of the router.

- **Ageing Time:** The time for the MAC address to age out. If a frame does not come from a certain MAC address within the Ageing Time, the bridge will delete that address from the Forwarding Table.
- **802.1d Spanning Tree:** Enable or disable the spanning tree protocol.

Configure your router

Advanced

Others: Client limit configuration

Click **Client Limit** in the left pane. The **Client Limit Configuration** page opens. On this page, you can enable or disable the client limit function and set the maximum number of device that can access the internet.

The screenshot shows the 'Client Limit Configuration' page. At the top, there are navigation tabs: Status, Wizard, Setup, Advanced (highlighted), Service, Firewall, and Maintenance. On the left, a sidebar menu lists various settings: Route, NAT, QoS, Port Mapping, Others, Bridge Setting, Client Limit (highlighted with a red box), and Telnet. The main content area is titled 'Client Limit Configuration' and includes a subtitle: 'This page is used to configure the capability of force how many device can access to Internet!'. Below this, there are two main configuration sections. The first is 'Client Limit Capability', which has radio buttons for 'Disable' and 'Enable', with 'Enable' selected. The second is 'Maximum Devices', which has a text input field containing the number '4'. At the bottom of the configuration area, there is an 'Apply Changes' button.

- **Client Limit Capability:** Enable or disable the client limit function.
- **Maximum Devices:** The maximum number of devices can access to the Internet.

Others: Telnet

Click **Telnet** in the left pane. The **Telnet Configuration** page opens. On this page, you can enable or disable the Telnet function.

The screenshot shows the 'Telnet Configuration' page. At the top, there are navigation tabs: Status, Wizard, Setup, Advanced (highlighted), Service, Firewall, and Maintenance. On the left, a sidebar menu lists various settings: Route, NAT, QoS, Port Mapping, Others, Bridge Setting, Client Limit, and Telnet (highlighted with a red box). The main content area is titled 'Telnet Configuration' and includes a subtitle: 'This page is used to configure telnet function.'. Below this, there is a 'Telnet:' section with radio buttons for 'Disable' and 'Enable', with 'Disable' selected. At the bottom of the configuration area, there is an 'Apply Changes' button.

Configure your router

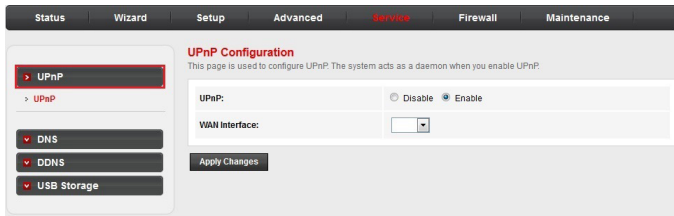
Service

Choose the **Service** menu and you can see the next sub-menus: **UPnP**, **DNS**, **DDNS** and **USB Storage**.

UPnP

Universal Plug and Play networking protocol (UPnP) is a feature that requires the operating system to support the UPnP application. LAN hosts can request a specific port translation on router by UPnP, so the external hosts can access the resources on the internal hosts when needed.

Click the **UPnP** sub-menu in the left pane. The **UPnP Configuration** page opens. On this page, you can configure the Universal Plug and Play networking protocol.



- **UPnP:** Enable or disable the UPnP function.
- **WAN Interface:** Choose which interface runs the UPnP function.

Configure your router

Service

DNS Configuration

Click the **DNS** sub-menu in the left pane. The **DNS Configuration** page opens. On this page, you can configure the IP address of the DNS server for DNS relay.

The screenshot shows the router's configuration interface. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service (highlighted in red), Firewall, and Maintenance. On the left side, there is a sidebar menu with options: UPnP, DNS (highlighted with a red border), DDNS, and USB Storage. The main content area is titled "DNS Configuration" and includes a subtitle: "This page is used to configure the DNS server ip addresses for DNS Relay." There are two radio button options: "Attain DNS Automatically" (selected) and "Set DNS Manually". Below these options are three input fields for DNS server addresses, labeled "DNS 1:", "DNS 2:", and "DNS 3:". The "DNS 1:" field contains the value "0.0.0.0". At the bottom of the configuration area, there are two buttons: "Apply Changes" and "Reset Selected".

- **Attain DNS Automatically:** The device will use the DNS servers which are obtained by the WAN interface via the auto-configuration mechanism.
- **Set DNS Manually:** Configure the DNS IP address manually.

Configure your router

Service

Dynamic DNS Configuration

Dynamic Domain Name Server (DDNS) allows you to point a hostname to a dynamic or static IP address or URL.

Click the **DDNS** sub-menu in the left pane. The **Dynamic DNS Configuration** page opens. On this page, you can configure the DDNS settings.

The screenshot shows the 'Dynamic DNS Configuration' page. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service (highlighted in red), Firewall, and Maintenance. On the left, a sidebar menu has 'DDNS' highlighted in red. The main content area is titled 'Dynamic DNS Configuration' and includes a sub-header: 'This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.' Below this are several form sections: 'DDNS provider:' with a dropdown menu set to 'DynDNS.org'; 'Hostname:' with a text input field; 'Interface:' with a dropdown menu set to 'WAN0'; and 'Enable:' with a checked checkbox. There are also sections for 'DynDns Settings:' with 'Username:' and 'Password:' text input fields, and 'TZO Settings:' with 'Email:' and 'Key:' text input fields. At the bottom, there are 'Add' and 'Remove' buttons, and a table titled 'Dynamic DDNS Table:' with columns for 'Select', 'State', 'Service', 'Hostname', 'Username', and 'Interface'.

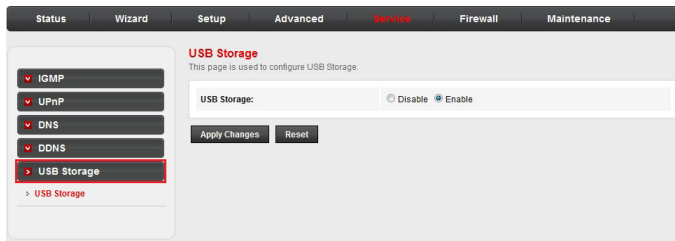
- **DDNS provider:** There are two DDNS providers to be selected in order to register your device: **DynDNS.org** and **TZO**.
- **Hostname:** Domain name to be registered with the DDNS server.
- **Interface:** The WAN interface over which your device will be accessed.
- **Enable:** Enable or disable the registration account for the DDNS server.
- **Username:** User name assigned by the DDNS provider.
- **Password:** Password assigned by the DDNS provider.

Configure your router

Service

USB Storage

Click the **USB Storage** sub-menu in the left pane. The **USB Storage** page opens. On this page, you can enable or disable USB functionality.



Once enabled, you can connect a USB drive to the router and share files (via FTP) between devices connected to the network.

To share files on a connected USB drive:

1. In the address field of your web browser, enter **ftp://** followed by the IP address of the router (usually **192.168.1.1**).
2. Log in to the router using your administrator account username and password.
The top-level folder of your USB drive should appear in your browser.
3. From there, you can navigate to and access the desired files and folders on your USB drive.

NOTE

- In order to upload and download files, use your preferred FTP client.

Configure your router

Firewall

The **Firewall** menu includes the following sub-menus: **MAC Filter**, **IP/Port Filter**, **URL Filter** and **DoS**.

MAC filter

In order to manage your local network better, you can use the MAC address filter function to control internet access.

Click the **MAC Filter** sub-menu in the left pane. The **MAC Filtering** page opens. On this page, you can set the MAC filtering rules.

vtech

Status Wizard Setup Advanced Service **Firewall** Maintenance

MAC Filter

> MAC Filter

IP/Port Filter

URL Filter

DoS

MAC Filtering

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

Outgoing Default Policy Deny Allow

Incoming Default Policy Deny Allow

Apply

Direction:

Action: Deny Allow

Source MAC: (ex. D0E086710502)

Destination MAC: (ex. D0E086710502)

Add

Current MAC Filter Table:

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

Delete Delete All

- **Outgoing/Incoming Default Policy:** The default action of outgoing/incoming connection. It can be **Deny** or **Allow**. If the connection does not match any MAC filtering rules, the router will handle the connection with the default action you have set.
- **Direction:** The direction of the filter entry (**Outgoing** or **Incoming**).
- **Action:** The action of the filter entry. It can be **Deny** or **Allow**. If the action is **Deny**, the connection matching the filter rule will be denied; if the action is **Allow**, the connection matching the filter rule will be allowed.

Configure your router

Firewall

- **Source MAC:** The source MAC address of the filter entry. An empty field means it matches any source MAC address.
- **Destination MAC:** The destination MAC address of the filter entry. An empty field means it matches any destination MAC address.
- The **Current MAC Filter Table** shows the current MAC filtering rules. You can delete the entry on the list.

IP/Port filter

Click the **IP/Port Filter** sub-menu in the left pane. The **IP/Port Filtering** page opens. On this page, you can set the IP/Port filter rules to secure or restrict your local network. The default actions of the outgoing and incoming connection are shown on the top of the page.

The screenshot shows the router's configuration page for IP/Port Filtering. At the top, there are navigation tabs: Status, Wizard, Setup, Advanced, Service, Firewall (selected), and Maintenance. On the left, a sidebar contains menu items: MAC Filter, IP/Port Filter (selected), IP/Port Filter (sub-item), URL Filter, and DoS. The main content area is titled 'IP/Port Filtering' and includes a descriptive paragraph: 'Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.'

Configuration options include:

- Outgoing Default Policy: Permit Deny
- Incoming Default Policy: Permit Deny
- Rule Action: Permit Deny
- WAN Interface: WAND
- Protocol: IP
- Direction: Upstream
- Source IP Address: [] Mask Address: 255.255.255.255
- Dest IP Address: [] Mask Address: 255.255.255.255
- SPort: [] - [] DPort: [] - []
- Enable:

An 'Apply Changes' button is located below the configuration fields. At the bottom, there is a 'Current Filter Table' section with a table header:

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

- **Rule Action:** The filter mode of this entry. It can be **Permit** or **Deny**. If the mode is **Permit**, the IP connection that matches the rule will be permitted; if the mode is **Deny**, the IP connection that matches the rule will be denied.

Configure your router

Firewall

IP/Port filtering (continued):

- **Protocol:** The protocol of this entry. It can be **IP**, **ICMP**, **TCP** or **UDP**.
- **Direction:** The direction of this entry. It can be **Upstream** or **Downstream**.
- **Source IP Address/ Mask Address:** The source IP address and mask address of the entry.
- **Dest IP Address/ Mask Address:** The destination IP address and mask address of the entry.
- **SPort:** If the protocol is TCP or UDP, you should set the source port of the entry. It can be a single port or a port range.
- **DPort:** If the protocol is TCP or UDP, you should set the destination port of the entry. It can be a single port or a port range.
- **Enable:** Enable or disable this filter entry.
- The **Current Filter table** shows the current filter rules. You can enable or disable or delete the filter entry.

Configure your router

Firewall

URL filter

In order to manage the site control of your local LAN client, you can use the URL filtering function to specify which site(s) cannot be accessed.

Click the **URL Filter** sub-menu in the left pane. The **URL Blocking Configuration** page opens. On this page, you can enable or disable the URL filtering function and add or delete the filtered keywords.

The screenshot shows the router's configuration page for URL blocking. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall (selected), and Maintenance. On the left, a sidebar menu includes MAC Filter, IP/Port Filter, URL Filter (highlighted with a red border), and DoS. The main content area is titled "URL Blocking Configuration" and contains the following elements: a sub-header "URL Blocking Configuration" with a description "This page is used to configure the filtered keyword. Here you can add/delete filtered keyword."; a "URL Blocking Capability:" section with radio buttons for "Disable" (selected) and "Enable"; an "Apply Changes" button; a "Keyword:" input field; "AddKeyword" and "Delete Selected Keyword" buttons; and a "URL Blocking Table:" section with a table header containing "Select" and "Filtered Keyword" columns.

- **URL Blocking Capability:** Enable or disable the URL filtering function. If it is enabled, the access to the site which matches the keyword will be blocked by the router; if it is disabled, nothing will be done.
- **Keyword:** The keyword of the site you want to block.
- The **URL Blocking Table** shows the current URL filtering entry. You can delete the selected entry.

Configure your router

Firewall

DoS

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

The router provides a protection of DoS attack.

Click the **DoS** sub-menu in the left pane. The **DoS setting** page opens. On this page, you can enable or disable the DoS prevention, configure the DoS parameters and specify the hack item.

DoS Setting

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

Enable DoS Prevention

<input type="checkbox"/> Whole System Flood: SYN	100	Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	100	Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	100	Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	100	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	100	Packets/Second
<input type="checkbox"/> TCP/UDP PortScan	Low	Sensitivity
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		

Configure your router

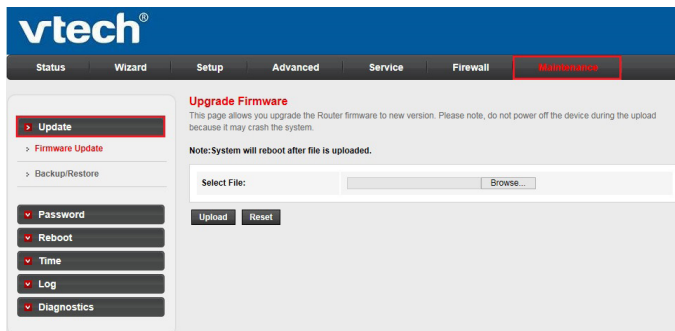
Maintenance

Choose the **Maintenance** menu and you can see the next sub-menus: **Update**, **Password**, **Reboot**, **Time**, **Log** and **Diagnostics**.

Update: Upgrade firmware

The router supports firmware upgrade from HTTP.

Click the **Update** sub-menu in the left pane. The **Upgrade Firmware** page opens. On this page, you can upgrade the router firmware. Make sure the firmware or ROM file you want to use is on the local hard drive of your computer. Click **Browse** to find the local hard drive and locate the firmware or ROM file to be used for upgrade.



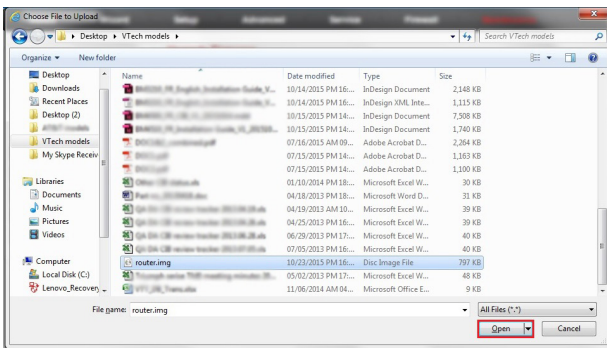
To upgrade the router's firmware:

1. Download a more recent firmware upgrade file.
2. Click the **Browse...** button.
3. Choose the update file and click **Open**.

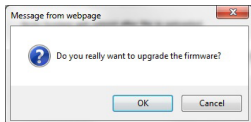
Configure your router

Maintenance

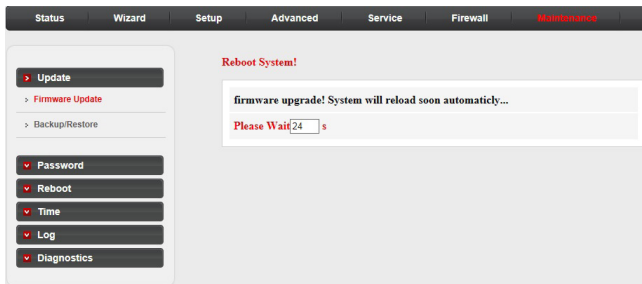
4. Click the **Upload** button.



5. When the confirmation message appears, click **OK** to proceed.



6. After the firmware file is uploaded, the system starts a 30-second countdown and then reboots. You need to login to the web management page again.



NOTES

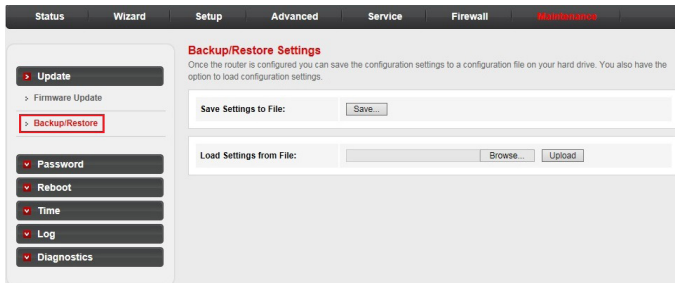
- After the firmware is upgraded, we recommend resetting the router to default settings.
- For the router's back-end firmware upgrade, ensure the FTP server option is enabled under the Service menu. See FTP server on page 36 for details.

Configure your router

Maintenance

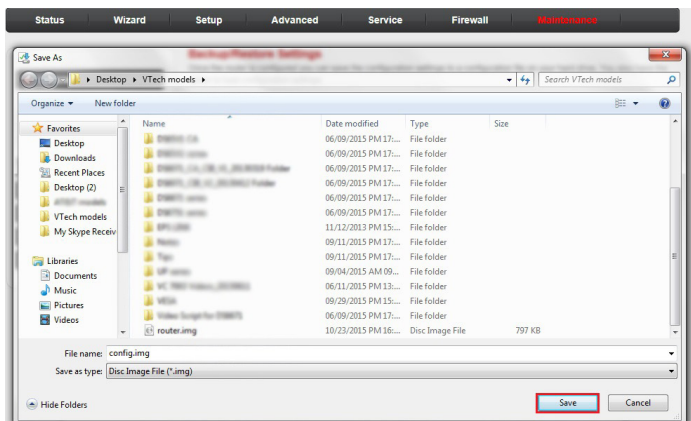
Update: Backup/restore settings:

Click **Backup/Restore** in the left pane. The **Backup/Restore Settings** page opens. On this page, you can save the current configuration settings to a file or restore the settings from a configuration file.



To back up the router's current settings:

1. Click the **Save...** button.
2. Click **Save** to save the file as the appointed file.

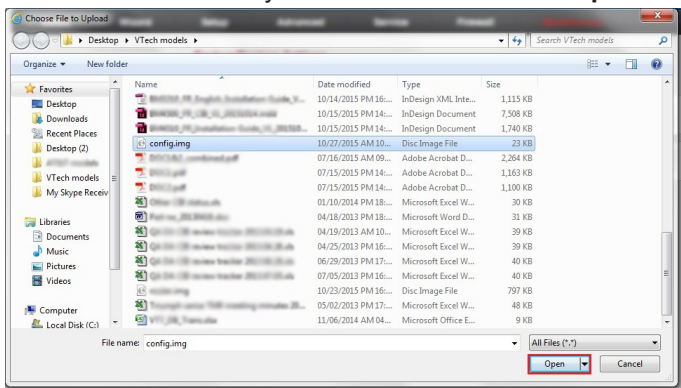


Configure your router

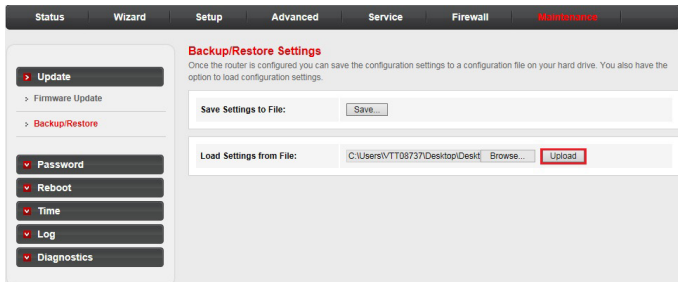
Maintenance

To restore the router's current settings:

1. Click the **Browse...** button.
2. Choose the file which you have saved and click **Open**.



3. Click **Upload**.



4. A pop-up window will appear asking for confirmation of restoring the settings. Click **OK** to proceed.
5. After the file is uploaded, the system starts a countdown and then reboots. You need to login to the web management page again.

Configure your router

Maintenance

Password: User account configuration

Click the **Password** sub-menu in the left pane. The **User Account Configuration** page opens. On this page, you can add a user account to access the web management page and modify the password of the specified user.

The screenshot shows the router's web management interface. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). On the left side, there is a sidebar menu with options: Update, Password (highlighted in red), Reboot, Time, Log, and Diagnostics. The main content area is titled "User Account Configuration" and contains a form with the following fields: User Name (input box), Privilege (dropdown menu showing "User"), Old Password (input box), New Password (input box), and Confirm Password (input box). Below the form are buttons for Add, Modify, Delete, and Reset. At the bottom, there is a "User Account Table" with the following data:

Select	User Name	Privilege
<input type="radio"/>	admin	root
<input type="radio"/>	user	user

To create an account:

1. Type a user name in the **User Name** input box, and then enter a password in the **New Password** and **Confirm Password** input boxes.
2. Click **Add** to create the new user account.

This is a close-up view of the "User Account Configuration" form. The fields are filled out as follows: User Name: user2; Privilege: User; Old Password: (empty); New Password: ***; Confirm Password: ***. The "Add" button is highlighted with a red box.

Configure your router

Maintenance

To change the password of an account:

1. Select an account for which you want to change the password.

User Account Table:		
Select	User Name	Privilege
<input type="radio"/>	admin	root
<input checked="" type="radio"/>	user	user
<input type="radio"/>	user2	user

2. Fill in the **Old Password**, **New Password** and **Confirm Password** input boxes, and then click **Modify** to save it.

NOTE

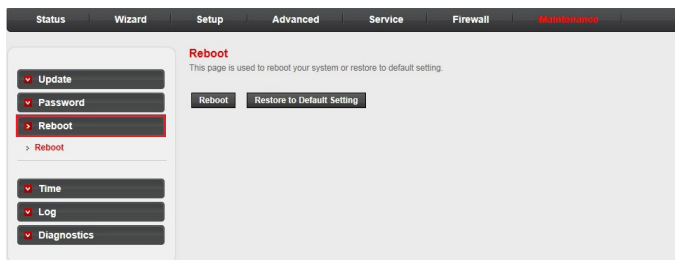
- If you login to the web management page with an administrative account, you can change the password of all accounts. The default user name is **admin** and the password is **12345**.

Configure your router

Maintenance

Reboot

Click the **Reboot** sub-menu in the left pane. The **Reboot** page opens. On this page, you can reboot your system or restore the router to default settings.



Configure your router

Maintenance

Time

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time with the public SNTP server.

System time configuration:

Click the **Time** sub-menu in the left pane. The **System Time Configuration** page opens. On this page, you can configure the system time.

The screenshot shows the 'System Time Configuration' page. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). On the left, a sidebar menu contains: Update, Password, Reboot, Time (highlighted with a red border), Log, and Diagnostics. The main content area is titled 'System Time Configuration' and includes a sub-header: 'This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.'

The configuration fields are as follows:

- System Time:** 2015 Year, Aug Month, 25 Day, 15 Hour, 31 min, 9 sec
- DayLight:** LocalTIME
- Buttons:** Apply Changes, Reset
- NTP Configuration:**
 - State:** Disable Enable
 - Server:** [Empty text box]
 - Server2:** [Empty text box]
 - Interval:** Every 1 hours
 - Time Zone:** (GMT) Gambia, Liberia, Morocco, England
 - GMT time:** Tue Aug 25 15:31:9 2015
- Buttons:** Apply Changes, Reset
- NTP Start:** [Get GMT Time]

- **Server/Server2:** The IP address or the host name of the NTP server.
- **Interval:** The interval time of NTP function
- **Time Zone:** The time zone in which the device resides.
- When you set the NTP configuration correctly, press the button **Get GMT Time** to start the NTP function. Then, you can see the GMT time obtained from NTP server.

Configure your router

Maintenance

Log: Log setting

Click the **Log** sub-menu in the left pane. The **Log Setting** page opens. On this page, you can configure the parameters of the system log and view the system log information.

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

Diagnostics: Ping

The router provides several useful diagnostic tools.

Click the **Diagnostics** sub-menu in the left pane. The **Ping Diagnostic** page opens. On this page, you can use the ping command to send a message to the host you specified.

The screenshot shows the 'Ping Diagnostic' page. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). On the left, a sidebar contains menu items: Update, Password, Reboot, Time, Log, Diagnostics (highlighted in red), Ping, Traceroute, and Diag-Test. The main content area is titled 'Ping Diagnostic' and includes a 'Host:' label with an input field. Below it is an 'Interface:' label with a dropdown menu. At the bottom, there is a 'PING' button.

Configure your router

Maintenance

Diagnostics: Traceroute

The router provides a trace route command to measure the route path and transit time of packets across an Internet Protocol (IP) network.

Click **Traceroute** in the left pane. The **Traceroute Diagnostic** page opens. On this page, you can specify an IP address or host to run trace route command.

The screenshot shows the 'Traceroute Diagnostic' configuration page. The navigation bar includes tabs for Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). The left sidebar menu shows options like Update, Password, Reboot, Time, Log, Diagnostics (expanded), Ping, Traceroute (highlighted with a red box), and Diag-Test. The main configuration area includes fields for Host, NumberOfTries (3), Timeout (5000 ms), Datasize (38 Bytes), DSCP (0), MaxHopCount (30), and Interface (any). Buttons for 'traceroute' and 'Show Result' are at the bottom.

- **Host:** An IP address or host name you want to run trace route command.
- **NumberOfTries:** The number of tries.
- **Timeout:** The time for the trace route command timeout.
- **Datasize:** Data size of the trace route packet.
- **DSCP:** The value of DSCP.
- **MaxHopCount:** The maximum hop count.
- **Interface:** The interface to which the trace route is to be applied.

Configure your router

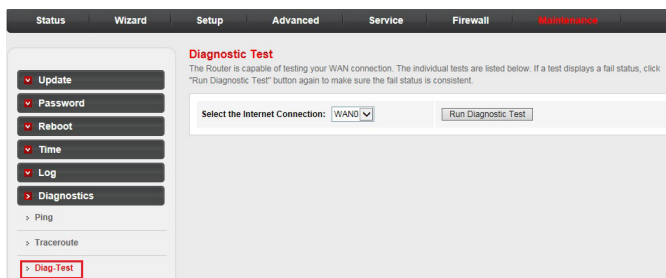
Maintenance

Diagnostics: Diagnostic test

The Diagnostic Test allows you to test your DSL connection of the physical layer and protocol layer for both LAN and WAN sides.

Click **Diag-Test** in the left pane. The **Diagnostic Test** page opens. On this page, you can select an interface to run the diagnostic test.

Click the **Run Diagnostic Test** button to start the test. The test result will display after several minutes.




The screenshot shows the router's web interface. At the top, there is a navigation bar with tabs: Status, Wizard, Setup, Advanced, Service, Firewall, and Maintenance (highlighted in red). On the left side, there is a sidebar menu with the following items: Update, Password, Reboot, Time, Log, Diagnostics (expanded), Ping, Traceroute, and Diag-Test (highlighted with a red box). The main content area is titled "Diagnostic Test" and contains the following text: "The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent." Below this text, there is a form with a label "Select the Internet Connection:" followed by a dropdown menu showing "WAN0" and a "Run Diagnostic Test" button.

Appendix


Frequently asked questions

Below are the questions most frequently asked about the router. If you cannot find the answer to your question, visit our website at businessphones.vtech.com or call **1 (888) 370-2006** for customer service.

My router does not work.

- Make sure you install the router properly, and the electrical outlet is not controlled by a wall switch.
- Make sure the router is powered on and the  light is on.

My router cannot load data from the Internet.

- Make sure you connect the WAN port properly. DO NOT mix up the WAN port with the LAN ports.
- Disconnect and then reconnect the power adapter, and then wait for a while for the router to restart. Observe the  WAN light; it flashes when the router receives data.
- Disconnect the Ethernet cable from the router and connect it to a different router. If there is no signal on that router either, the problem is in your wiring or local service. Contact your Internet service provider.
- Your Ethernet cable might be defective. Try installing a new one.

How do I restore my router to its factory default settings?

- When the router is powered on, use a narrow-pointed object to press and hold the Reset button, and then wait for a while for the router to restart.

NOTE

- After the router resets to default settings, use the default user name and password to login to the web management page.

What can I do if I forgot my password?

- Restore the router to factory default settings. After the router restarts, use the default user name and password to log in to the web management page.

What can I do if my Ethernet devices cannot obtain IP addresses?

- Make sure you install the router and connect it with your Ethernet devices properly. See “Connect your system” on page 5 for details.
- If you have more than four Ethernet devices, use a narrow-pointed object to press and hold the Reset button, and then wait for a while for the router to restart.

Appendix

FCC part 15

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

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

WARNING: Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian requirement: CAN ICES-3 (B)/NMB-3(B)

Appendix

For cETL compliance only

Mesures de sécurité importantes

Lorsque vous utilisez votre appareil, vous devriez toujours suivre certaines mesures de précaution de base afin de réduire les risques d'incendie, d'électrocution et de blessures corporelles, dont ceux qui suivent :

Information relative à la sécurité

1. Lisez et comprenez bien toutes les instructions.
2. N'utilisez pas cet appareil près de l'eau ni de toute autre source d'humidité, par exemple, près d'une baignoire, cuve à lessive, évier de cuisine, dans un sous-sol humide ni près d'une piscine, dans un soussol humide ou une douche.
3. Ne déposez pas ce téléphone sur un chariot, support ou table chancelants. L'appareil pourrait tomber et être sérieusement endommagé.
4. **MISE EN GARDE** : N'utilisez que les adaptateurs inclus avec ce produit. L'utilisation d'un adaptateur dont la polarité ou la tension serait inadéquate risque d'endommager sérieusement le produit et mettre votre sécurité en péril.
Adaptateur : Entrée 100-240V CA 800 mA 50/60 Hz; Sortie : 12 V CC 2000 mA
5. Lorsqu'ils sont branchés dans une prise de courant, les adaptateurs secteur ont été conçus pour être orientés correctement, soit à la verticale ou au plancher. Les broches n'ont pas été conçues pour supporter le poids du bloc d'alimentation et le maintenir en place si celui-ci est branché dans une prise au plafond, sous une table ou dans un meuble.
6. Pour les PRODUITS À BRANCHER À UNE PRISE DE COURANT, la prise de courant doit être installée près du produit, afin d'assurer une accessibilité sécuritaire à la prise de courant.
7. Débranchez ce produit de la prise de courant avant de procéder au nettoyage. N'utilisez pas de nettoyeurs en aérosols. Utilisez un chiffon humide pour le nettoyer.
8. Ne coupez pas les cordons d'alimentation pour remplacer les fiches, car ceci peut présenter un danger potentiel.
9. Ne laissez aucun objet reposer ni appuyer sur le cordon d'alimentation. N'installez pas cet appareil dans un endroit où l'on risque d'écraser le cordon d'alimentation ou de le piétiner.
10. Ne faites fonctionner cet appareil qu'avec le type d'alimentation indiqué sur l'étiquette. Si vous ne connaissez pas le type d'alimentation que vous possédez à votre domicile, consultez votre marchand ou votre compagnie locale d'électricité.
11. Ne surchargez pas les prises de courant murales ni les rallonges électriques.
12. Les trous et ouvertures du boîtier, situés à l'arrière de l'appareil ou sous celui-ci, servent à aérer l'appareil. Pour l'empêcher de surchauffer, ne bloquez sous aucun prétexte ces ouvertures et n'empêchez pas l'aération adéquate de l'appareil en le plaçant sur un lit, divan, tapis ou toute autre surface similaire. De même, ne le positionnez pas à proximité ni au-dessus d'une source de chaleur ou d'un calorifère. De plus, ne placez pas l'appareil dans un endroit avant de vous assurer qu'il y ait une bonne circulation d'air.
13. N'enfoncez jamais d'objets à travers les ouvertures de cet appareil, car ils pourraient entrer en contact avec des points de tension dangereux ou causer des courts-circuits qui peuvent dégénérer en incendies ou en risques d'électrocution. Ne renversez jamais de liquide dans ce produit.
14. Afin de réduire les risques d'électrocution, ne démontez pas cet appareil, mais apportez-le dans un centre de service autorisé. L'ouverture du boîtier ou le retrait de toutes pièces que contient cet appareil, à l'exception de l'accès autorisé à certaines portes ou ouvertures, risque de vous exposer à des points de tension dangereux ou d'autres dangers. Un remontage incorrect peut par la suite présenter des risques d'électrocution.
15. Examinez les composantes afin de vérifier si celles-ci ne sont pas endommagées.

CONSERVEZ CES INSTRUCTIONS

Appendix

For cETL compliance only

Champs électromagnétiques (EMF)

Ce produit de VTech est conforme à toutes les normes se rapportant aux champs électromagnétiques (EMF) standard. Si vous le manipulez correctement en suivant les instructions de ce guide, son utilisation sera sécuritaire pendant de nombreuses années, selon les meilleures évidences scientifiques dont nous disposons aujourd'hui.

Appendix

Limited Warranty

1. What does this limited warranty cover?

The manufacturer of this VTech product warrants to the holder of a valid proof of purchase (“CONSUMER” or “you”) that the product and all accessories provided in the sales package (“PRODUCT”) are free from defects in material and workmanship, pursuant to the following terms and conditions, when installed and used normally and in accordance with the PRODUCT operating instructions. This limited warranty extends only to the CONSUMER for products purchased and used in the United States of America and Canada.

2. What will VTech do if the PRODUCT is not free from defects in materials and workmanship during the limited warranty period (“materially defective PRODUCT”)?

During the limited warranty period, VTech’s authorized service representative will repair or replace at VTech’s option, without charge, a materially defective PRODUCT. If we repair the PRODUCT, we may use new or refurbished replacement parts. If we choose to replace the PRODUCT, we may replace it with a new or refurbished PRODUCT of the same or similar design. We will retain defective parts, modules, or equipment. Repair or replacement of the PRODUCT, at VTech’s option, is your exclusive remedy. VTech will return repaired or replacement products to you in working condition. You should expect the repair or replacement to take approximately 30 days.

3. How long is the limited warranty period?

The limited warranty period for the PRODUCT extends for TWO (2) YEARS from the date of purchase. If VTech repairs or replaces a materially defective PRODUCT under the terms of this limited warranty, this limited warranty also applies to repaired or replacement PRODUCT for a period of either (a) 90 days from the date the repaired or replacement PRODUCT is shipped to you or (b) the time remaining on the original two-year limited warranty; whichever is longer.

4. What is not covered by this limited warranty?

This limited warranty does not cover:

- PRODUCT that has been subjected to misuse, accident, shipping or other physical damage, improper installation, abnormal operation or handling, neglect, inundation, fire, water, or other liquid intrusion; or
- PRODUCT that has been damaged due to repair, alteration, or modification by anyone other than an authorized service representative of VTech; or
- PRODUCT to the extent that the problem experienced is caused by signal conditions, network reliability or cable or antenna systems; or
- PRODUCT to the extent that the problem is caused by use with non-VTech accessories; or
- PRODUCT whose warranty/quality stickers, PRODUCT serial number plates or electronic serial numbers have been removed, altered or rendered illegible; or
- PRODUCT purchased, used, serviced, or shipped for repair from outside the United States of America or Canada, or used for commercial or institutional purposes (including but not limited to products used for rental purposes); or
- PRODUCT returned without a valid proof of purchase (see item 6 on the next page); or
- Charges for installation or setup, adjustment of customer controls, and installation or repair of systems outside the unit.

Appendix

Limited Warranty

5. How do you get warranty service?

To obtain warranty service, visit businessphones.vtech.com or call 1 (888) 370-2006.

NOTE: Before calling for service, please review the user's manual; a check of the PRODUCT's controls and features may save you a service call.

Except as provided by applicable law, you assume the risk of loss or damage during transit and transportation and are responsible for delivery or handling charges incurred in the transport of the PRODUCT(s) to the service location. VTech will return repaired or replaced PRODUCT under this limited warranty to you. Transportation, delivery or handling charges are prepaid. VTech assumes no risk for damage or loss of the PRODUCT in transit. If the PRODUCT failure is not covered by this limited warranty, or proof of purchase does not meet the terms of this limited warranty, VTech will notify you and will request that you authorize the cost of repair prior to any further repair activity. You must pay for the cost of repair and return shipping costs for the repair of products that are not covered by this limited warranty.

6. What must you return with the PRODUCT to get warranty service?

You must:

- Return the entire original package and contents including the PRODUCT to the VTech service location along with a description of the malfunction or difficulty; and
- Include a "valid proof of purchase" (sales receipt) identifying the PRODUCT purchased (PRODUCT model) and the date of purchase or receipt; and
- Provide your name, complete and correct mailing address, and telephone number.

7. Other limitations

This warranty is the complete and exclusive agreement between you and VTech. It supersedes all other written or oral communications related to this PRODUCT. VTech provides no other warranties for this PRODUCT. The warranty exclusively describes all of VTech's responsibilities regarding the PRODUCT. There are no other express warranties. No one is authorized to make modifications to this limited warranty and you should not rely on any such modification.

State/Provincial Law rights: This warranty gives you specific legal rights, and you may also have other rights which vary from state to state or province to province.

Limitations: Implied warranties, including those of fitness for a particular purpose and merchantability (an unwritten warranty that the PRODUCT is fit for ordinary use) are limited to one year from date of purchase. Some states/provinces do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. In no event shall VTech be liable for any indirect, special, incidental, consequential, or similar damages (including, but not limited to lost profits or revenue, inability to use the PRODUCT or other associated equipment, the cost of substitute equipment, and claims by third parties) resulting from the use of this PRODUCT. Some states/provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Please retain your original sales receipt as proof of purchase.

Appendix

Technical specifications

Operating temperature	34°F - 104°F 0°C - 40°C
Power requirements	Input: 100-240V AC 500mA 50/60Hz Output: 12V DC 1000mA
Network Ethernet ports	10/100 Mbps RJ-45 Ports

The Wi-Fi CERTIFIED™ Logo is a certification mark of Wi-Fi Alliance®.

VTECH COMMUNICATIONS LTD.

A member of THE VTECH GROUP OF COMPANIES.

Distributed in the U.S.A. by VTech Communications Inc., Beaverton, Oregon 97008.

VTech is a registered trademark of VTech Holdings Limited.

Copyright © 2016 for VTECH COMMUNICATIONS LTD. All rights reserved.

Version 1, 12/16