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

VNT814

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:	VNT814
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 a 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 200mA 50/60Hz; Output: 12V DC 500mA
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 supply in your home, 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

Getting started
Router overview

1 – ⏻ (On/Off) light

- On when the router is powered on.

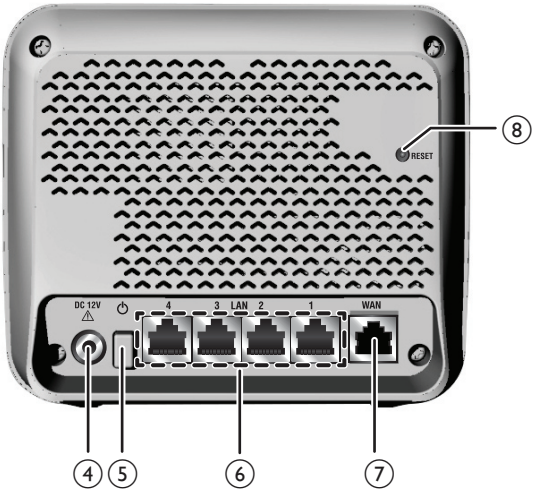
2 – WAN light

- On when the **WAN** port is connected.
- Flashes when the router receives data from the **WAN** port.

3 – L1 L2 L3 L4 lights

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

Getting started
Router overview



4 – Power jack

- Connects to the power adapter.

5 – ⏻ (On/Off) button

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

6 – LAN ports

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

7 – WAN port

- Connects to the wide area network.

8 – RESET button

- Press and hold for five seconds to reset the router to default settings.

Getting started
Plan and connect your system

The VNT814 router has four LAN ports to connect with Ethernet devices such as computers and SIP phones. Before you start setting up your system, plan it carefully. Consider the following before you start planning your system.

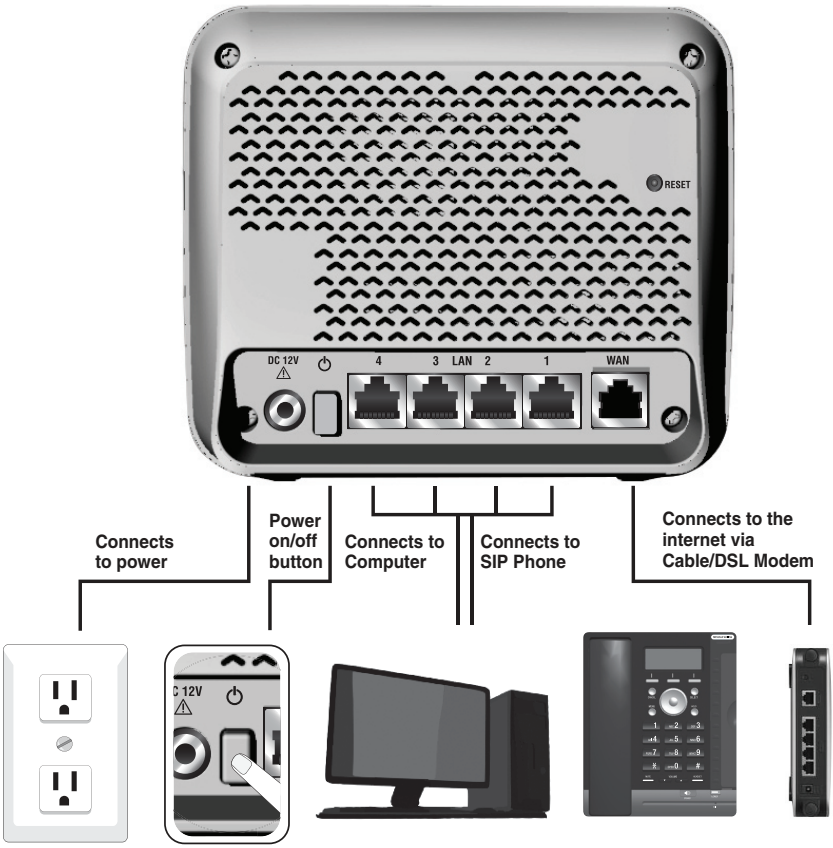
✓ Number of Ethernet device(s) you need to connect with.

✓ Number of router(s) you need.

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 ⏻ button at the back of the router. The ⏻ light will light up.

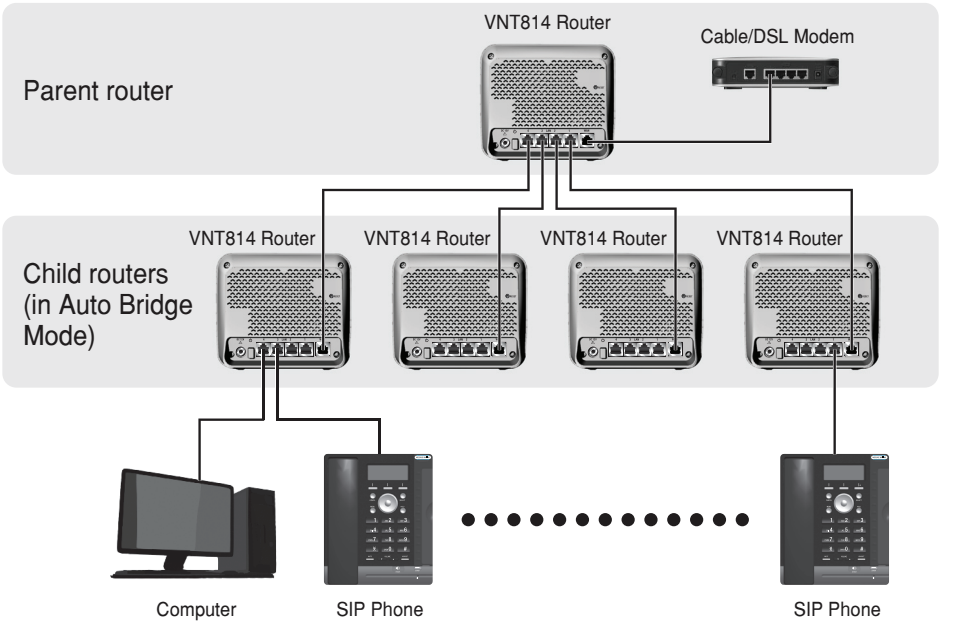


Getting started
Plan and connect your system

To connect more than four Ethernet devices, you can purchase additional VNT814 router(s), and then connect them to the parent router. See the graphic below for more details.

NOTES

- Make sure you have connected all routers and devices before you power on any router or device.
- Follow this sequence to power on the system: (1) Parent router, (2) Child routers, (3) other Ethernet devices.
- Child routers enter Auto Bridge Mode. All Ethernet devices obtain IP addresses from the parent router directly.



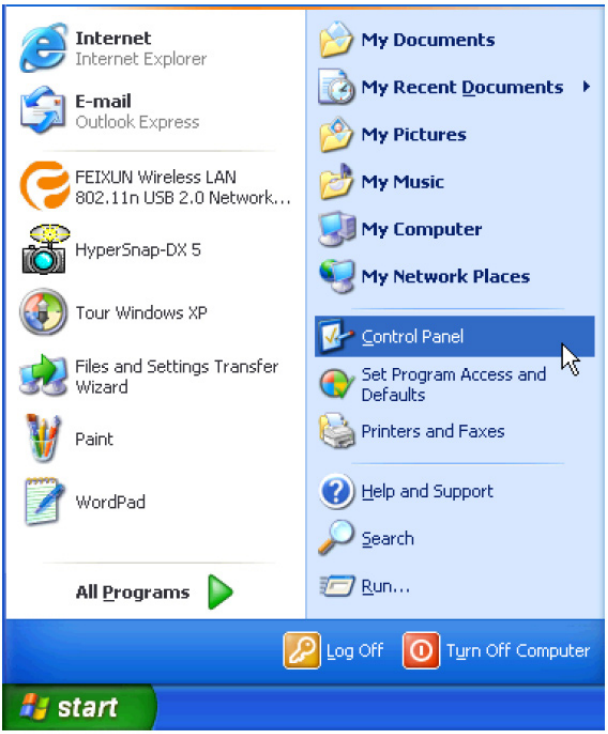
Getting started

Configure your computer network

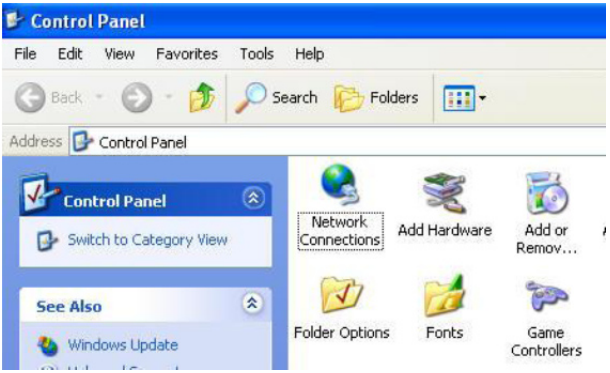
In order to view or change the settings of the VNT814 router, you need to login to the web management page of the router. Before that, connect your computer to the LAN port of the router, and then set the computer to obtain IP address automatically according to the steps below.

For Windows XP/2000

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

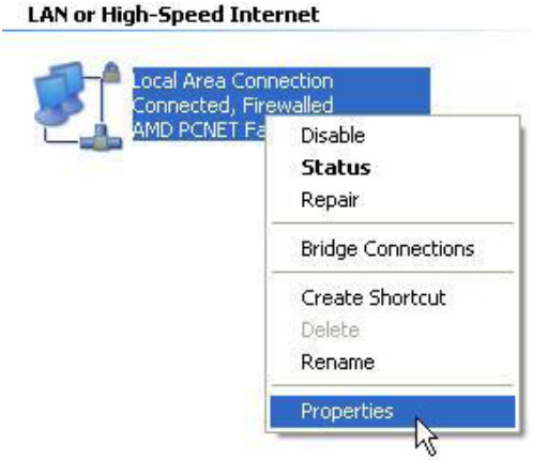


2. Double-click **Network Connections**.

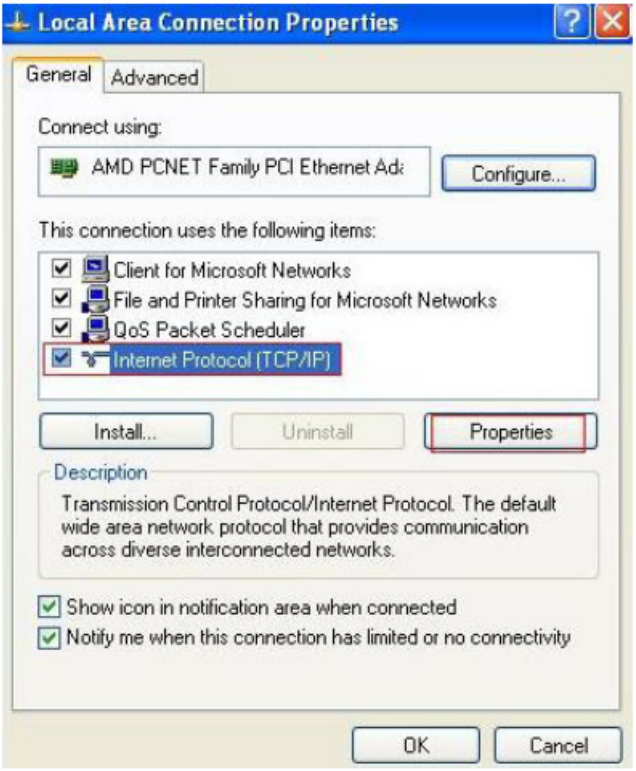


Getting started
Configure your computer network

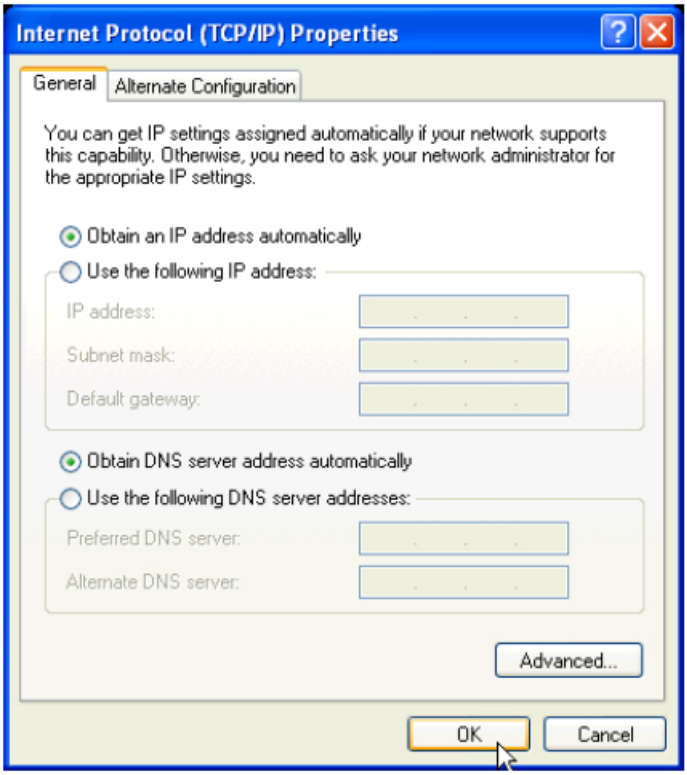
3. Right-click **Local Area Connection**, then select **Properties**.



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



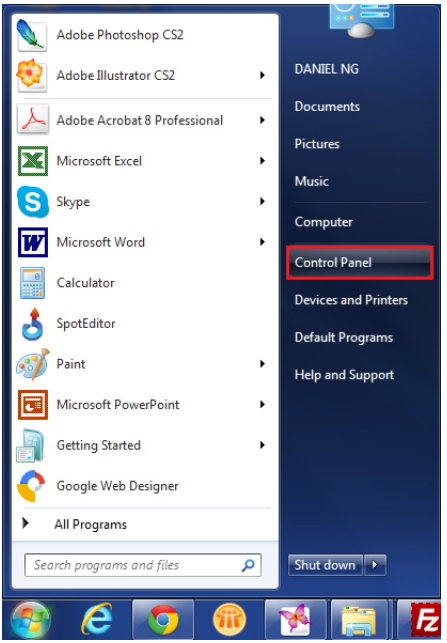
5. Select **Obtain IP address automatically** and **Obtain DNS server address automatically**, then click **OK**.



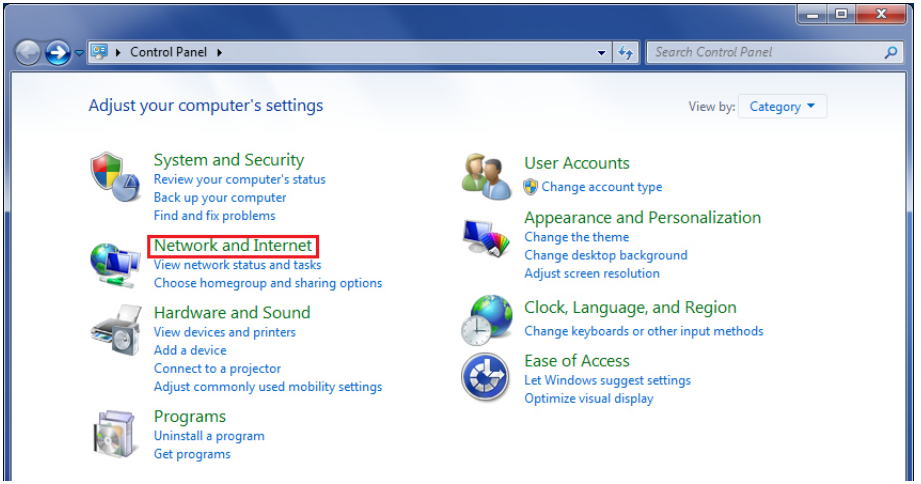
Getting started
Configure your computer network

For Windows Vista/7/8

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

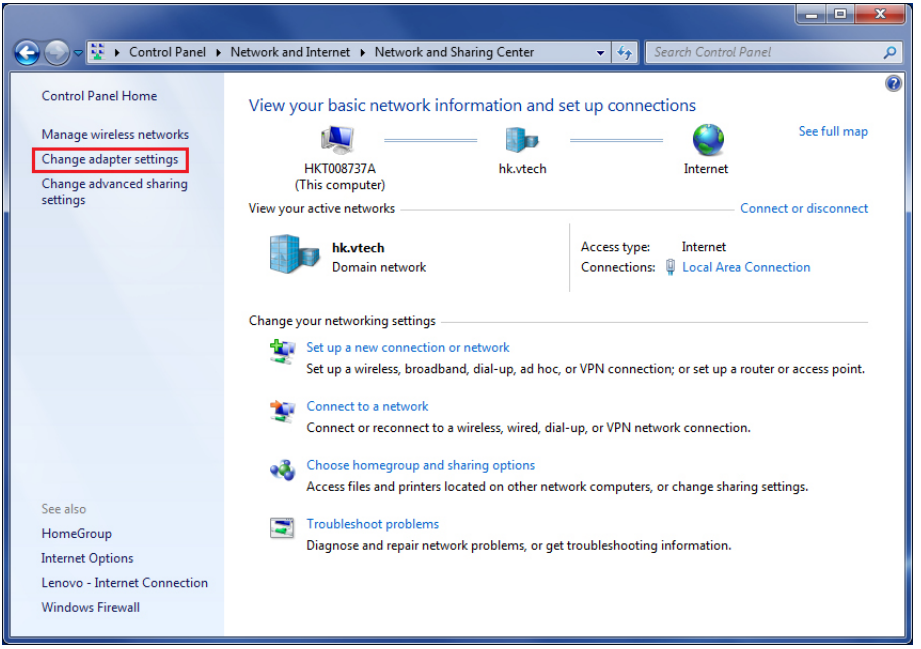


2. Click **Network and Internet**, then **Network and Sharing Center**.

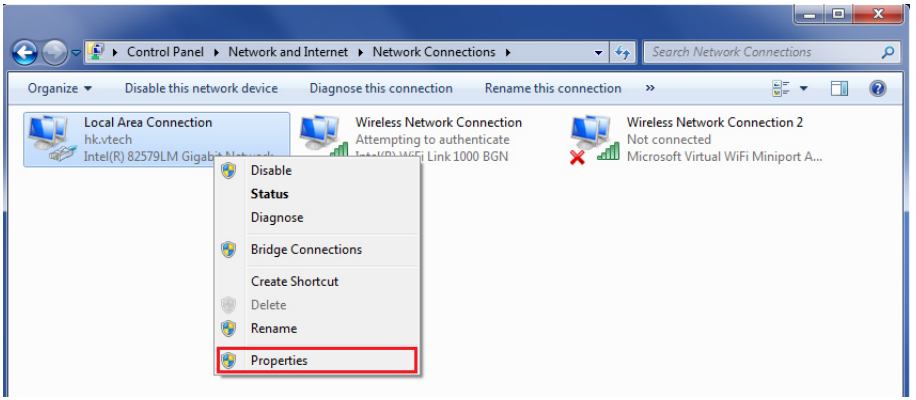


Getting started
Configure your computer network

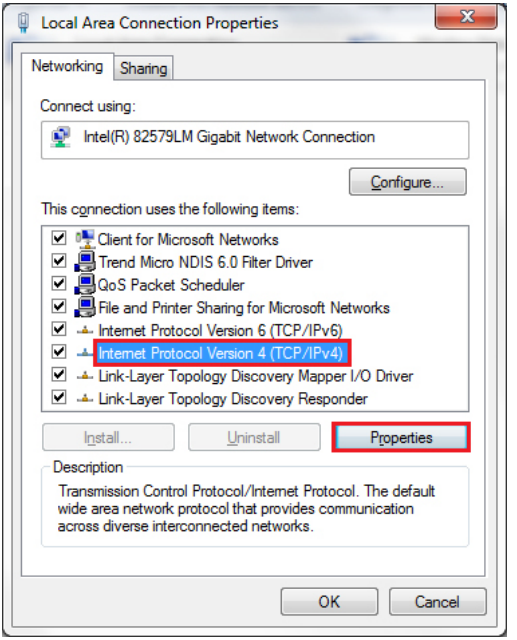
3. Click **Change adapter settings**.



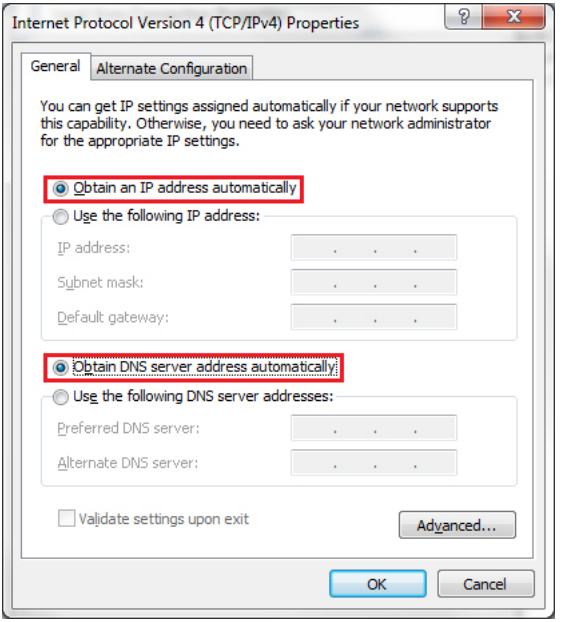
4. Right-click **Local Area Connection**, then select **Properties**.



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



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



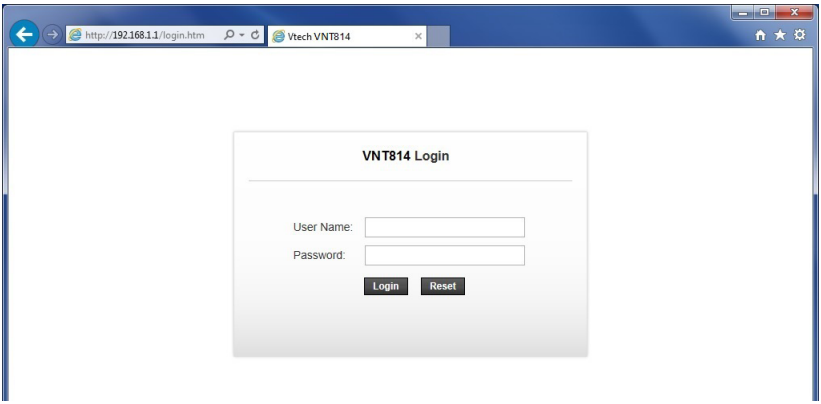
Configure your router
Login to the web management page

With your computer connected to the LAN port of the router and set to obtain IP address automatically, power on the router and you can login 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, then press **Enter**. The following login page displays.



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

	User name	Password
Administrative account	admin	admin12345
Normal user account	user	user1234

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

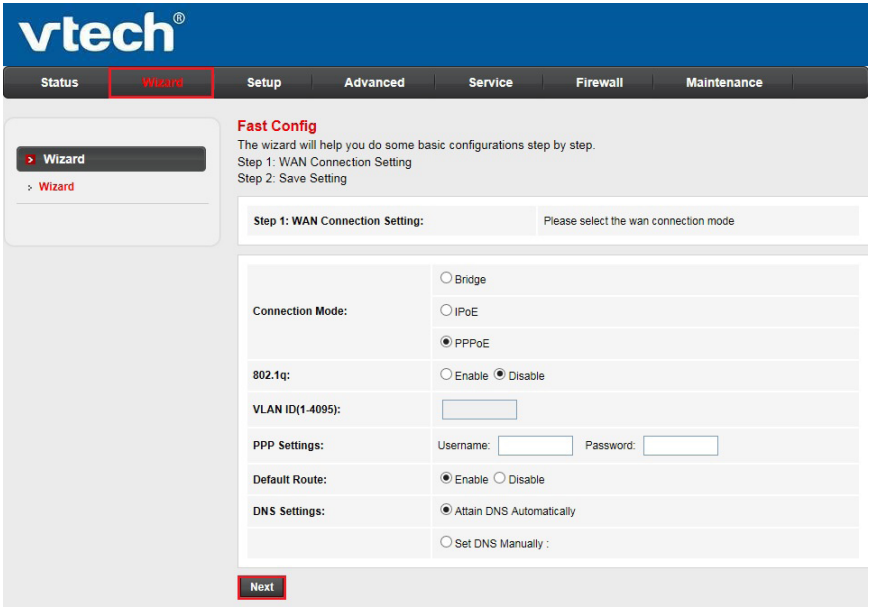
NOTE

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

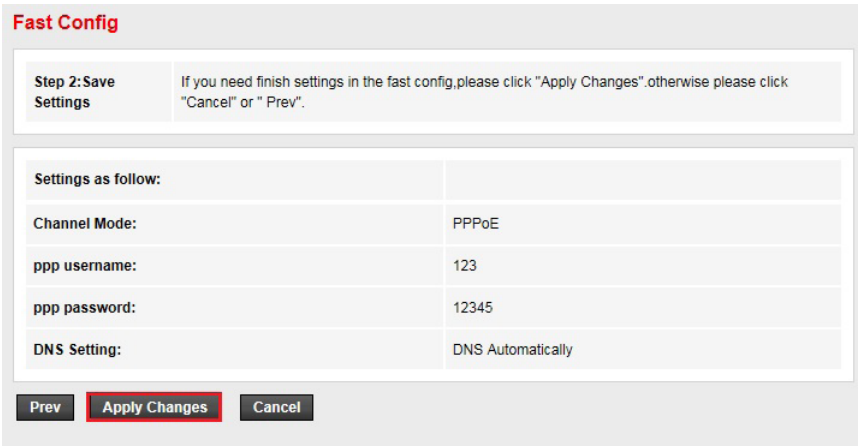
Configure your router
Fast configuration

The **Wizard** feature can guide you through the basic configurations of the router step by step.

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.
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.



Configure your router

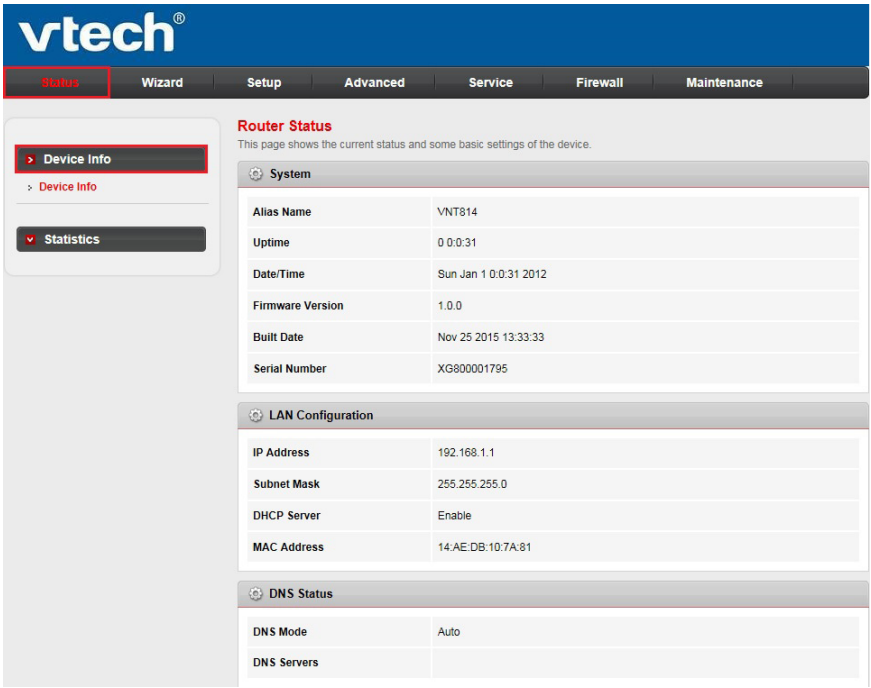
Status

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

Router status:

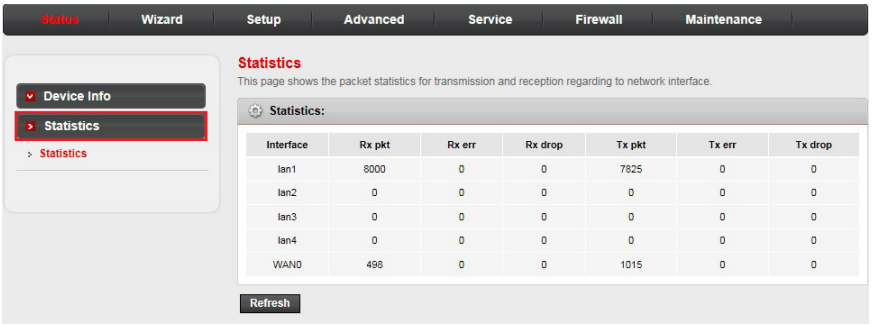
- Click the **Status** menu. The **Router Status** page under the **Device info** sub-menu in the left pane is opened automatically, displaying the basic information of the router, including system, LAN configuration, DNS status and Ethernet WAN interfaces.



Configure your router
Status

Statistics

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



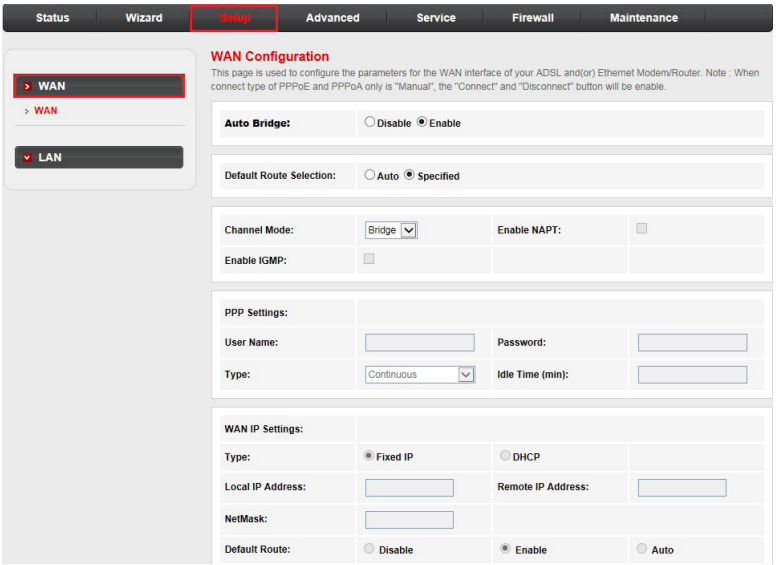
Configure your router
Setup

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 is opened automatically. You can configure the parameters for the WAN interface of your router, such as channel mode, PPP settings and WAN IP settings.



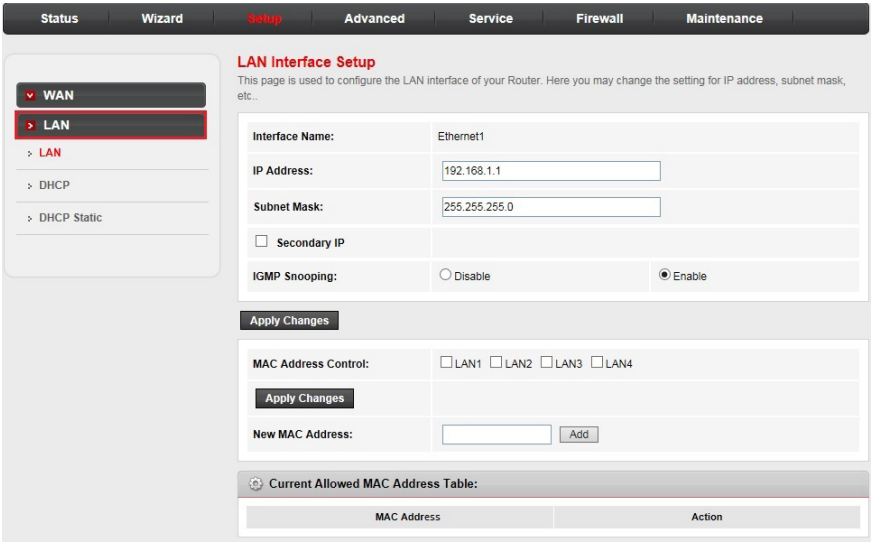
- **Auto Bridge**: Enable or disable the Auto Bridge Mode. If it is enabled, the child VNT814 router's DCHP mode will change to **DCHP Relay** automatically. See **DCHP mode** on page 17 for more details.
- **Channel mode**: It can be **Bridge**, **IPoE** or **PPPoE**.
- **Enable NAPT**: Enable or disable the NATP function.
- **Enable IGMP**: Enable or disable the IGMP function.
- **User Name**: User name of the PPP connection
- **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.

Configure your router
Setup

LAN

LAN interface setup:

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

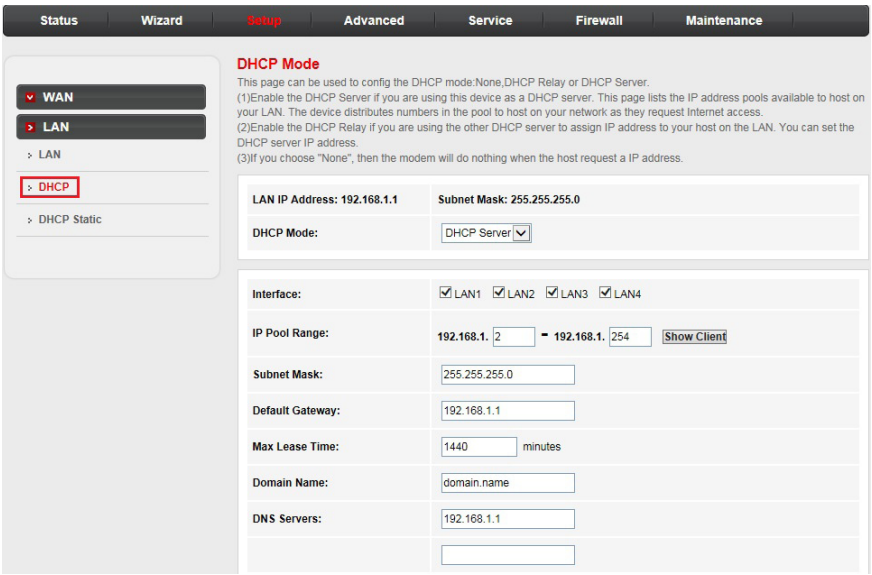


- **IP Address**: The IP address of the router's LAN interface. The default value is 192.168.1.1.
- **Subnet Mask**: The subnet mask of the router's LAN interface. The default value is 255.255.255.0.
- **Secondary IP**: If you enable the Secondary IP, you should configure another IP address and subnet mask for the LAN interface.
- **IGMP Snooping**: You can enable or disable the IGMP Snooping function by selecting the radio button.
- **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

DHCP mode:

- Click **DHCP** in the left pane. In this page, you can configure the DHCP mode of your router as **None**, **DHCP Server** or **DHCP Relay**.



- **None**: The router will do nothing when the hosts require an IP address by DHCP protocal.
- **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, gate way 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.

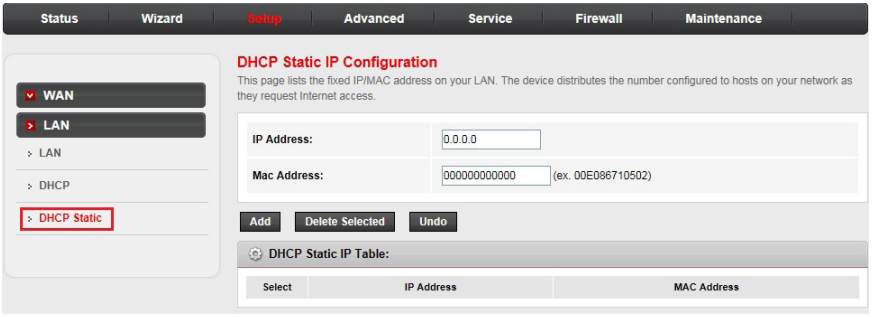
NOTES

- If you have more than four Ethernet devices and they are connected to the additional VNT814 router(s) you purchased, there is no need to change the DHCP mode setting of the child router(s). Once a child VNT814 router is connected with a parent VNT814 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 VNT814 router(s) as the child router(s), you need to set the DHCP mode to **DHCP Relay** for the VNT814 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.

Configure your router
Setup

DHCP static IP configuration:

- Click **DHCP Static** in the left pane. In 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 setup for the DHCP Server. You can manually input IP and MAC address to make a static assignment. Router searches the relevant entry in this table to assign 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 assign to the client.



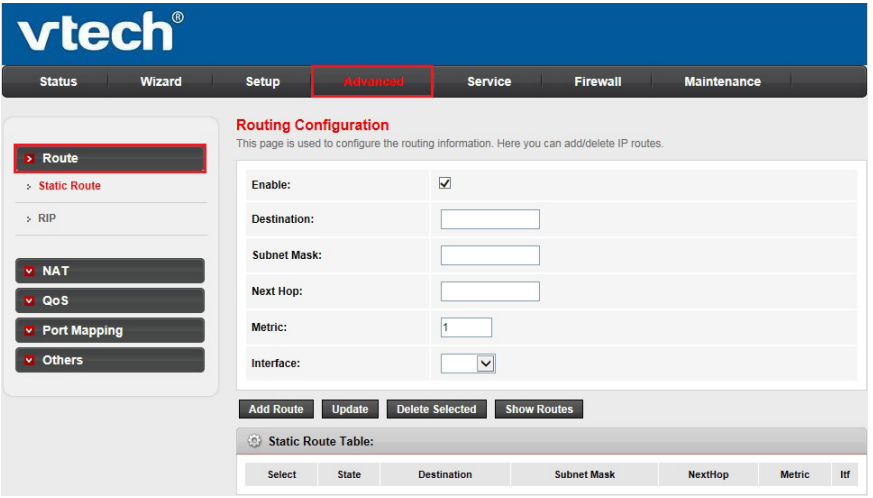
Configure your router
Advanced

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 **Static Route** page is opened automatically. You can configure the routing information such as adding and deleting IP routes.

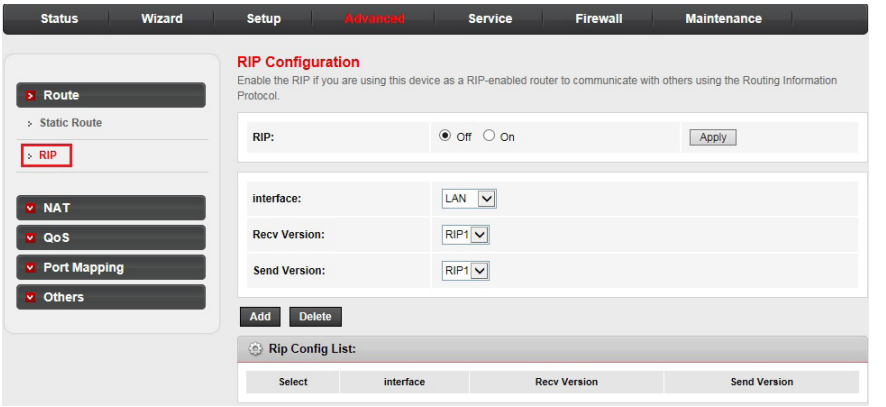


- **Destination**: This parameter specifies the IP network address of the final destination.
- **Subnet Mask**: Enter the subnet mask for this destination.
- **Next Hop**: Enter the IP address of the gateway. The gateway is an immediate neighbour of your Router that will forward the packet to the destination. 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 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

RIP configuration:

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



- **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

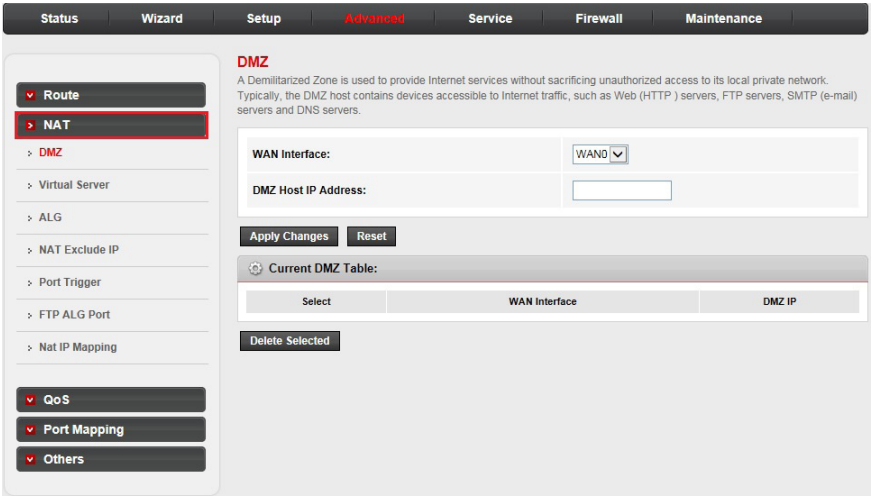
NAT

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

DMZ:

- Click the **NAT** sub-menu in the left pane. The **DMZ** page is opened automatically, where 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.

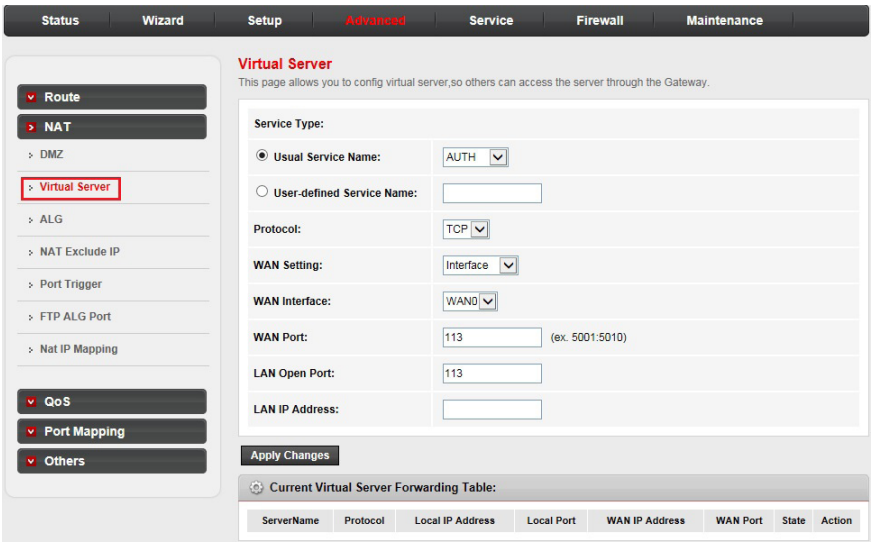


- **WAN Interface**: Select the desired WAN interface by clicking the drop-down list.
- **DMZ Host IP Address**: Enter the specified IP Address for DMZ host on the LAN side.

Configure your router
Advanced

Virtual server:

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

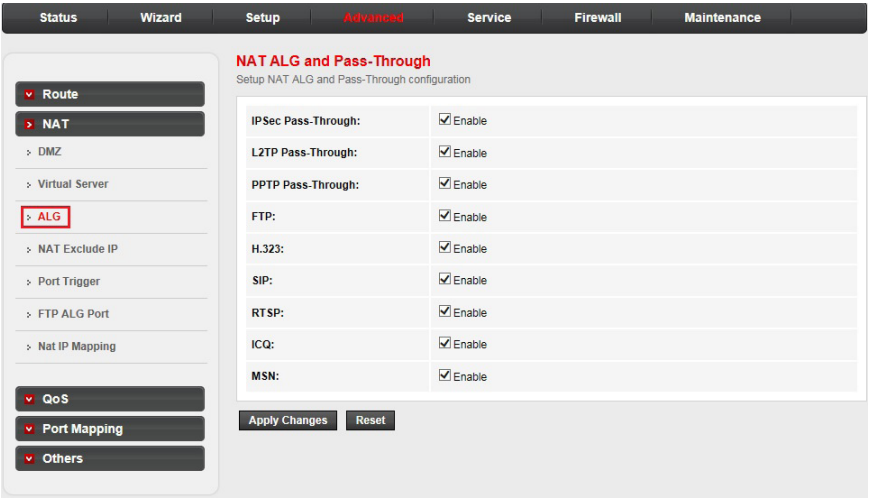


- **Usual Service Name & User-defined Service Name**: The name of this virtual server.
- **Protocol**: The protocol of this virtual server used. It can be **TCP** or **UDP**.
- **WAN Setting**: The WAN setting of this virtual server used. It can be **Interface** or **IP address**.
- **WAN Interface**: 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, you can enter the end port number the same as 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 and pass-through:

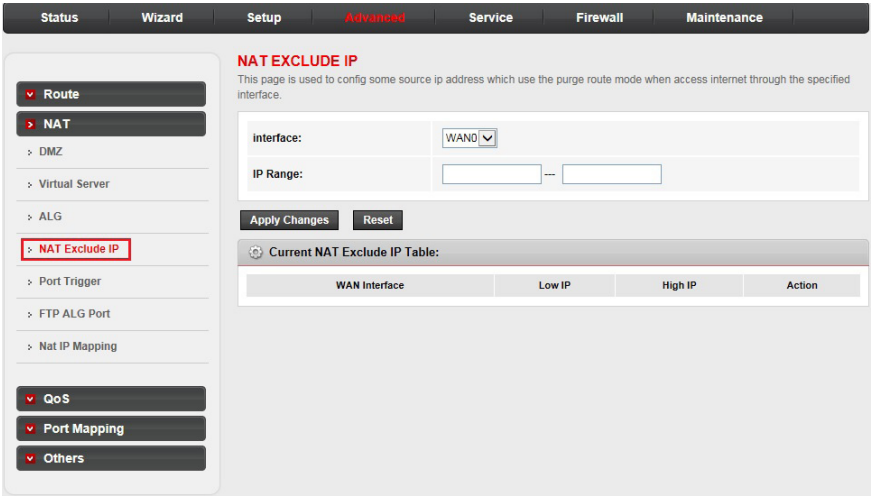
- Click **ALG** in the left pane. In this page, you can configure the Application Layer Gateway (ALG) settings such as enabling or disabling the ALG or pass-through function for each application.



Configure your router
Advanced

NAT exclude IP:

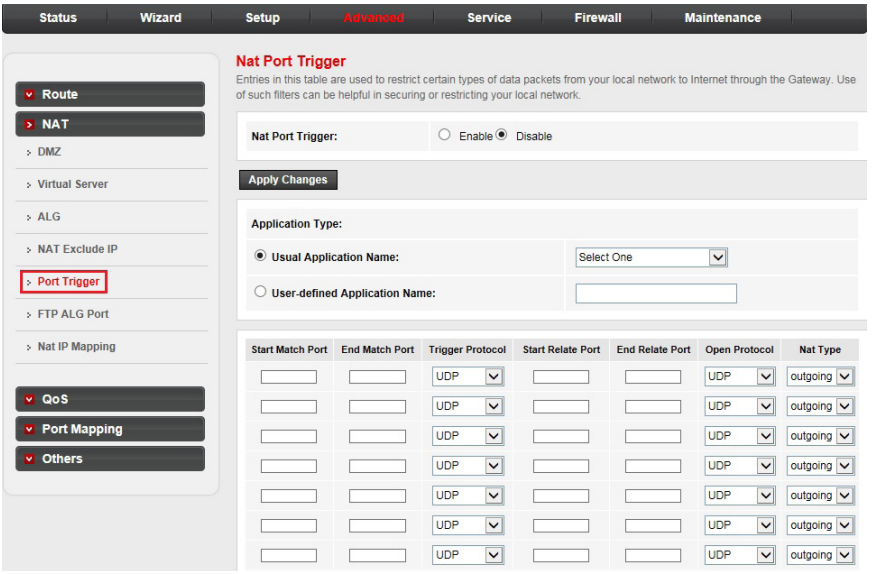
- Click **NAT Exclude IP** in the left pane. In this page, you can configure some source IP addresses which use the purge route mode when accessing the internet through the specified interface.



Configure your router
Advanced

NAT port trigger:

- Click **NAT 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. In this page, you can configure the port trigger rules.

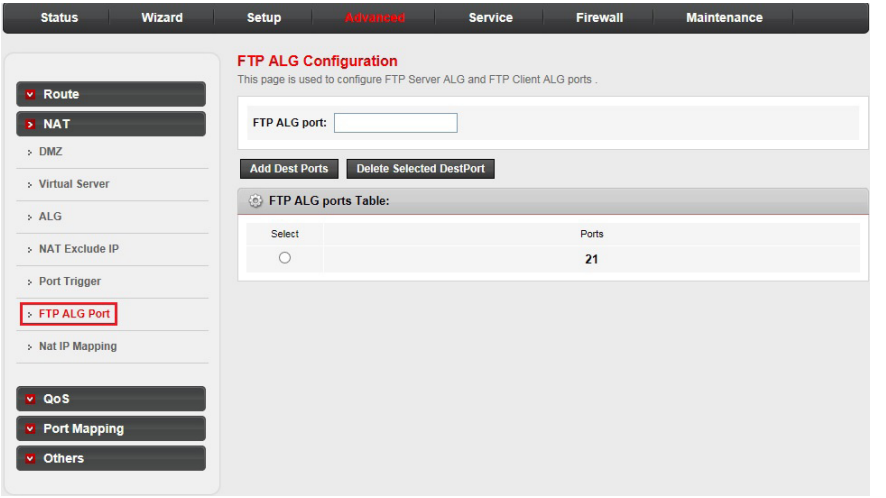


- **Nat Port Trigger**: Enable or disable the port trigger function on the device.
- **Application Type**: You can select the service from the **Usual Application Name** or define the name from **User-defined Application Name**.
- **Start Match Port** / **End Match port**: The start and end port to match.
- **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

FTP ALG configuration:

- Click **FTP ALG Port** in the left pane. In this page, you can configure the FTP server ALG and FTP client ALG ports.

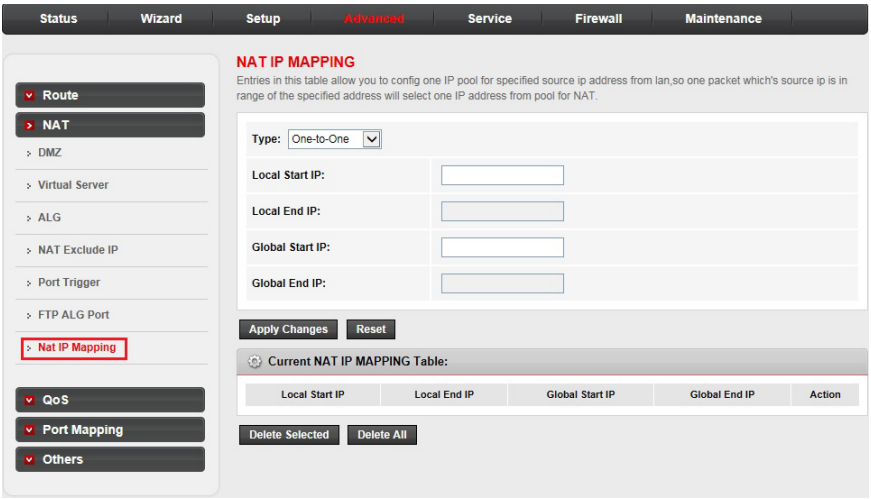


- If the FTP server listens on port 2100, you can add a FTP ALG port 2100 on the device.

Configure your router
Advanced

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 pool for NAT.



- **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.

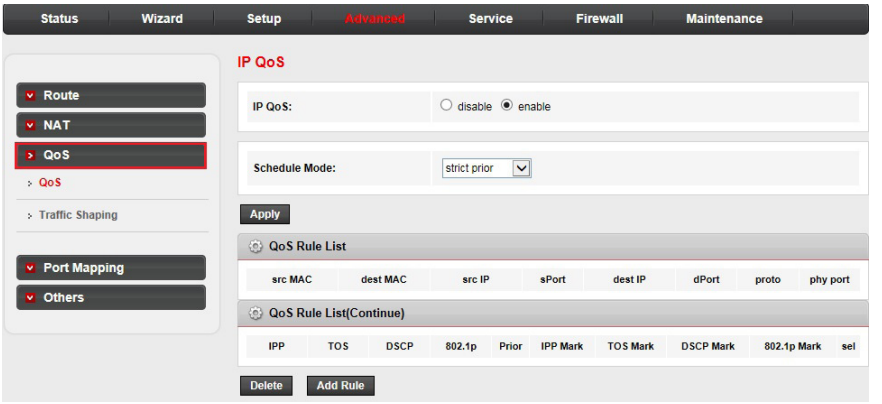
Configure your router
Advanced

QoS

Router provides a control mechanism which serves traffic with different priority. 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.

IP QoS:

- Click the **QoS** sub-menu in the left pane. The **IP QoS** page is opened automatically, where you can enable or disable the IP QoS and configure the rules if necessary.

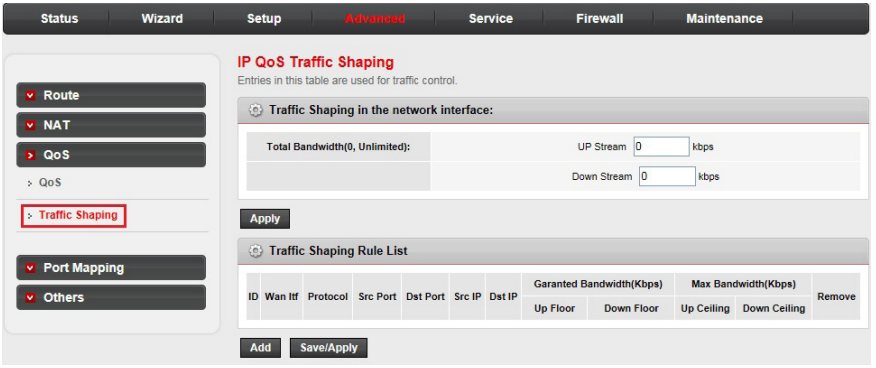


- **IP QoS**: Enable or disable the IP QoS function on the device.
- **Schedule Mode**: The schedule mode of the IP QoS function. It can be **strict prior** or **WFQ (4:3:2:1)**.
  - **Strict Prior**: Traffic with different priority will be sent by its priority. The higher priority the traffic is, the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

IP QoS traffic shaping:

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



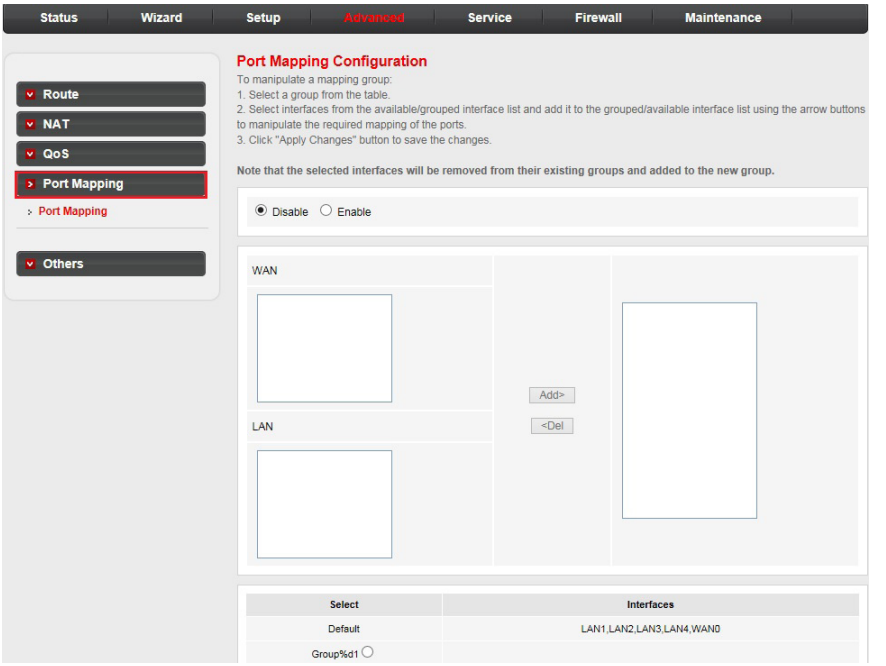
Configure your router
Advanced

Port mapping

The device 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.

Port mapping configuration:

- Click the **Port Mapping** sub-menu in the left pane. The **Port Mapping Configuration** page is opened automatically, where you can configure the mapping group.



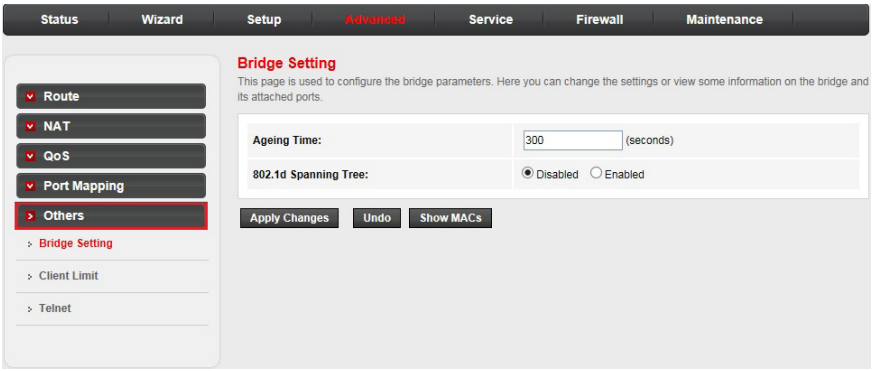
- To manipulate a mapping group:
  1. Select a group from the table, then you can see the available interface (LAN and WAN) and grouped interface list.
  2. Select interfaces from the available and grouped interface list and add it to the interface group using the **Add>** button or delete it using the **<Del** button, in order to manipulate the required mapping of the ports.
  3. Click **Apply Changes** to finish the configuration.

Configure your router
Advanced

Others

Bridge setting:

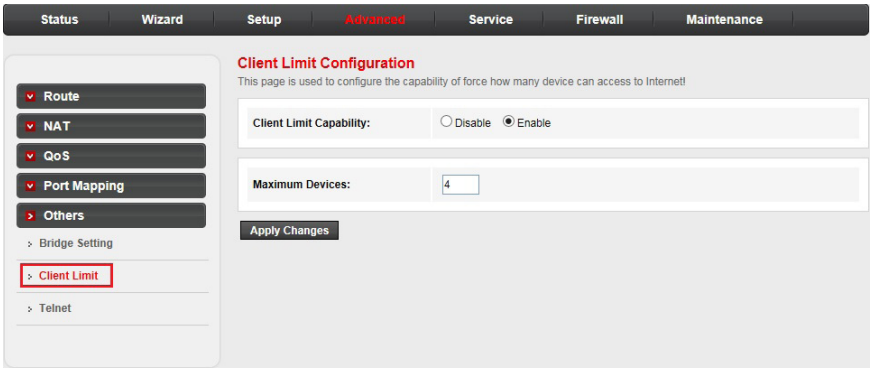
- Click the **Others** sub-menu in the left pane. The **Bridge Setting** page is opened automatically, where you can configure the bridge parameters and view the information on the bridge and its attached ports.
  Click the **Show MACs** button and you will see the current Forwarding Table of the router.



- **Ageing Time**: The time for the MAC address to age out. After the Ageing Time seconds of not having seen a frame coming from a certain address, the bridge will delete that address from the Forwarding Table.
- **802.1d Spanning Tree**: Enable or disable the spanning tree protocol.

Client limit configuration:

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

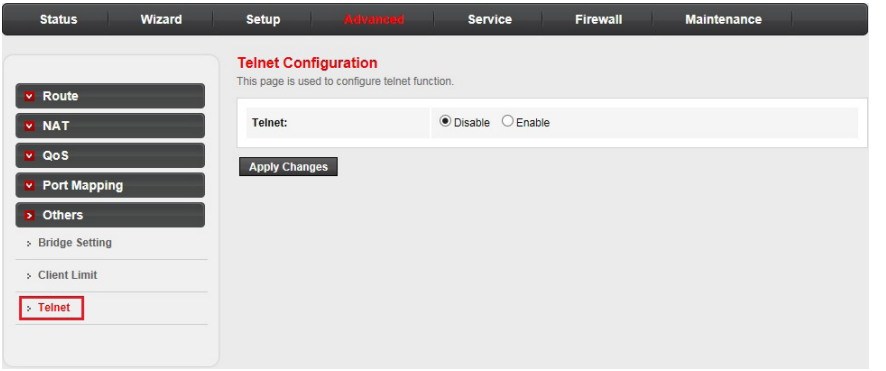


- **Client Limit Capability**: Enable or disable the client limit function.
- **Maximum Devices**: The maximum number of devices can access to the Internet.

Configure your router
Advanced

Telnet configuration:

- Click **Telnet** in the left pane. In this page, you can enable or disable the telnet function.



Configure your router
Service

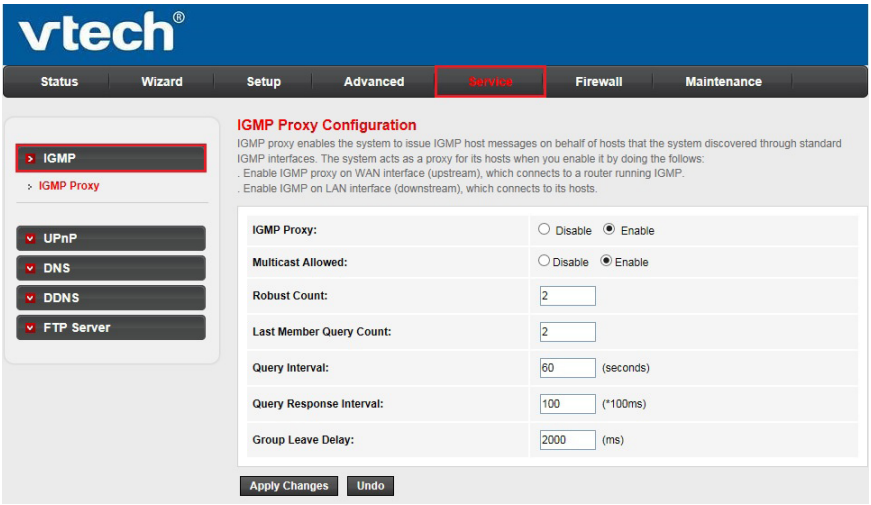
Choose the **Service** menu and you can see the next sub-menus: **IGMP**, **UPnP**, **DNS**, **DDNS** and **FTP Server**.

IGMP

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighbor routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast group. The router supports IGMP proxy that handles IGMP message. When enabled, the router will act as a proxy for a LAN host making request to join and leave multicast groups, and a multicast router sending multicast packets to multicast groups on WAN side.

IGMP proxy configuration:

- Click the **IGMP** sub-menu in the left pane. The **IGMP Proxy Configuration** page is opened automatically, where you can enable or disable the IGMP proxy function on all WAN interface, and set the parameters of the IGMP function.



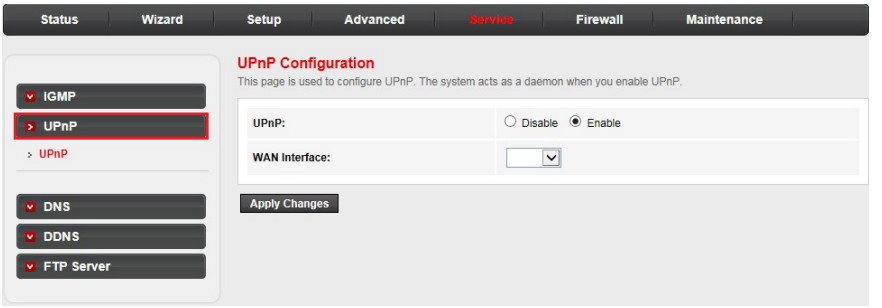
Configure your router
Service

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.

UPnP configuration:

- Click the **UPnP** sub-menu in the left pane. The **UPnP Configuration** page is opened automatically, where you can configure the UPnP.

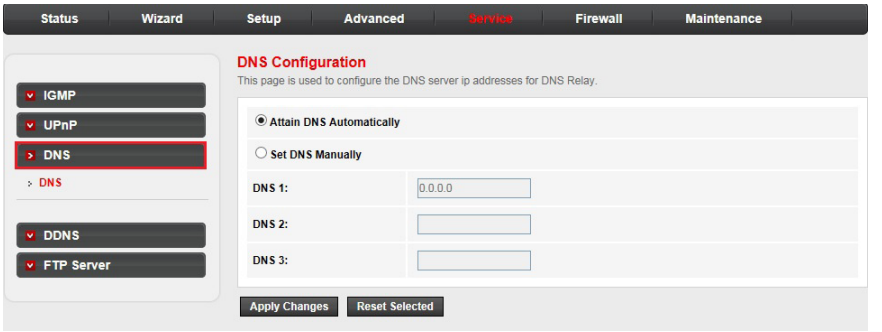


- **UPnP**: Enable or disable the UPnP function.
- **WAN Interface**: Choose which interface runs the UPnP function.

DNS

DNS configuration:

- Click the **DNS** sub-menu in the left pane. The **DNS Configuration** page is opened automatically, where you can configure the IP address of DNS server for DNS relay.



- **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.

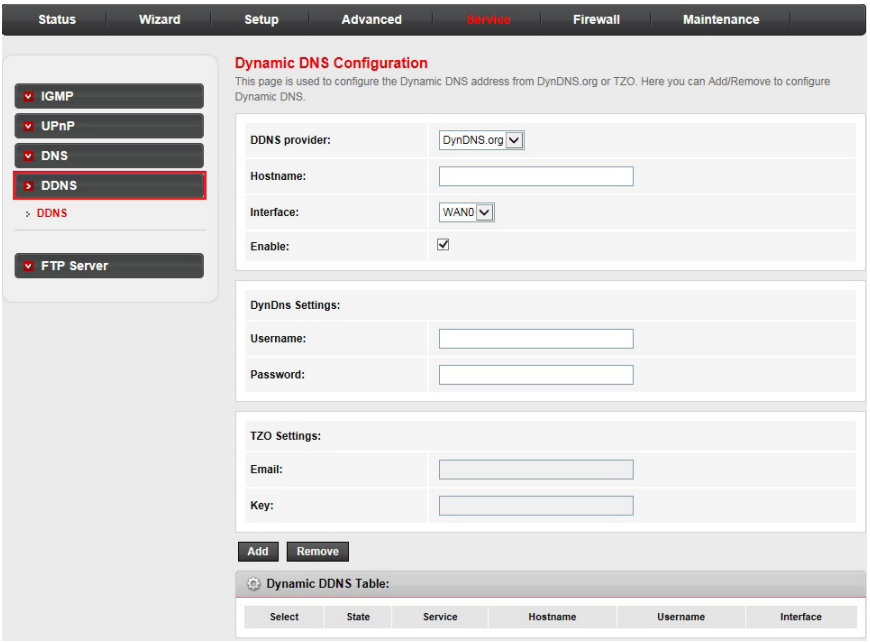
Configure your router
Service

DDNS

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

Dynamic DNS configuration:

- Click the **DDNS** sub-menu in the left pane. The **Dynamic DNS Configuration** page is opened automatically, where you can configure the DDNS settings.

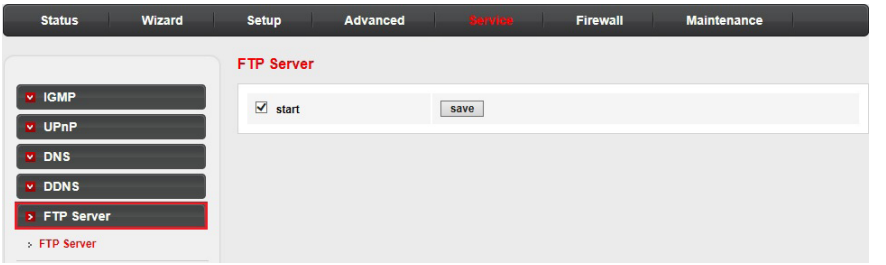


- **DDNS provider**: There are two DDNS providers to be selected in order to register your device: **DynDNS.org** and **TZO**.
- **Hostname**: Domain name to be registered with the DDNS server.
- **Interface**: The WAN interface over which your device will be accessed.
- **Enable**: Enable or disable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

FTP server

- Click the **FTP server** sub-menu in the left pane. FTP server is used for the router's back-end firmware upgrade purpose only. By default, the **start** checkbox is checked. Do not change any setting in this page.



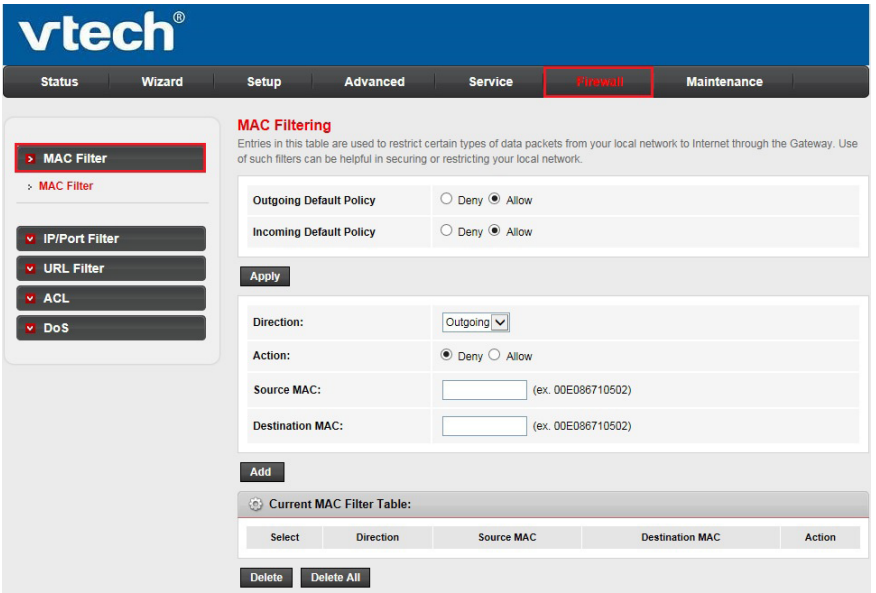
Configure your router
Firewall

Choose the **Firewall** menu and you can see the next sub-menus: **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL** and **DoS**.

MAC filter

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

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



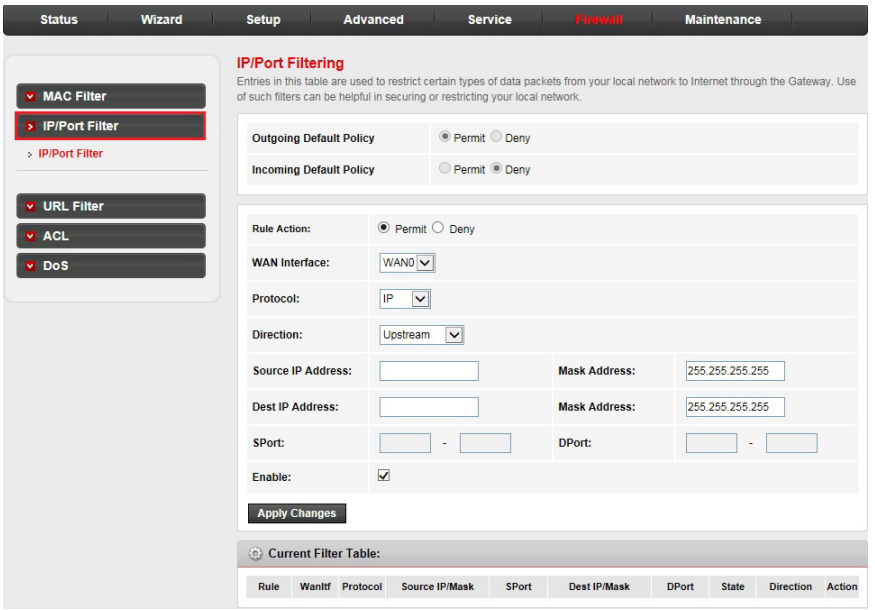
- **Outgoing/Incoming Default Policy**: The default action of outgoing/ incoming connection. It can be **Deny** or **Allow**. If the connection does not match any MAC filtering rules, the router will handle the connection with the default action you have set.
- **Direction**: The direction of the filter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

Configure your router
Firewall

IP/Port filter

IP/Port filtering:

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



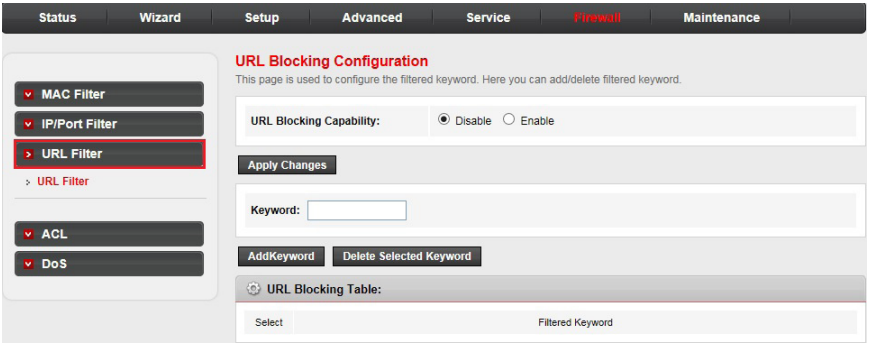
- **Rule Action**: The filter mode of this entry. It can be **Permit** or **Deny**. If the mode is **Permit**, the IP connection that matches the rule will be permitted; if the mode is **Deny**, the IP connection that matches the rule will be denied.
- **Protocol**: The protocol of this entry. It can 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. In this page, you can enable or disable the URL filtering function and add or delete the filtered keywords.



- **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.

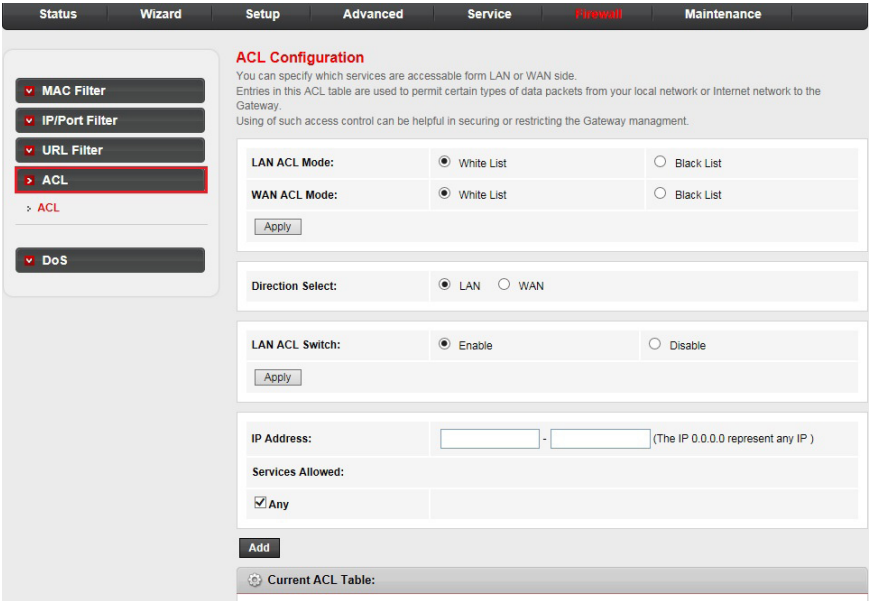
Configure your router
Firewall

ACL

The Access Control List (ACL) function is used to specify which services are accessible from LAN or WAN side.

ACL configuration:

- Click the **ACL** sub-menu in the left pane. The **ACL Configuration** page is opened automatically, where you can set the ACL entries.



- **LAN/WAN ACL Mode**: Select **White List** or **Black List** for the LAN/WAN ACL Mode.
- **Direction Select**: The direction of this ACL entry. It can be **LAN** or **WAN**.
- **LAN ACL Switch**: You can enable or disable the ACL function on LAN side. If it is disabled, all hosts on LAN side can access the services which your router provide. If it is enabled, only the hosts on the ACL list can access the specify services.
- **IP Address**: The IP address of the host. If the IP is 0.0.0.0, it means any IP.
- **Service Allowed** (LAN side): The allowed services which the host can access. It can be **any**, or any specified service such as **web**, **telnet**, **ssh**, **ftp**, **tftp** and **ping**. If you select **any**, it means the host can access all the services the router provides.

Configure your router
Firewall

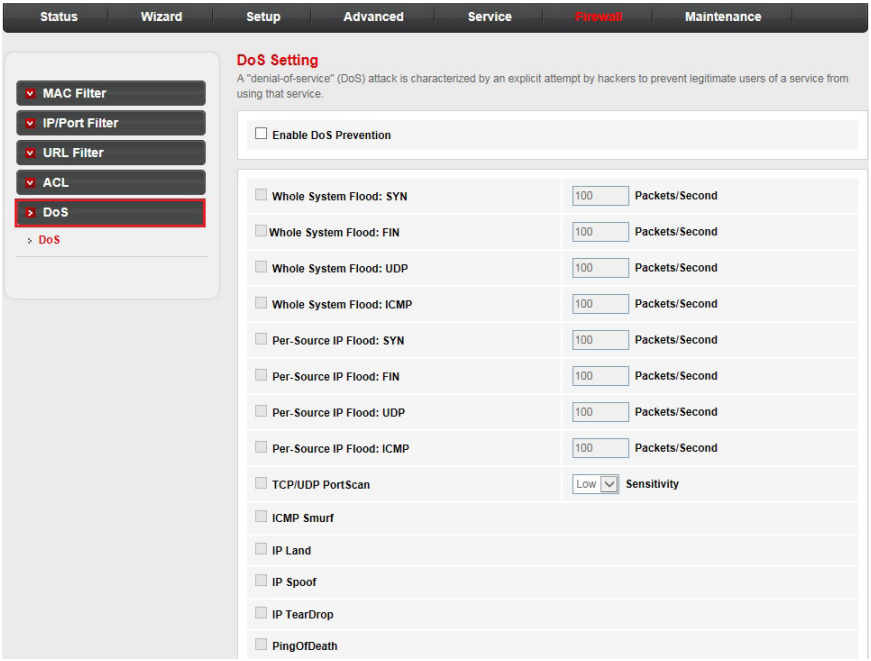
DoS

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.

DoS setting:

- Click the **DoS** sub-menu in the left pane. The **DoS setting** page is opened automatically, where you can enable or disable the DoS prevention, configure the DoS parameters and specify the hack item.



Configure your router
Maintenance

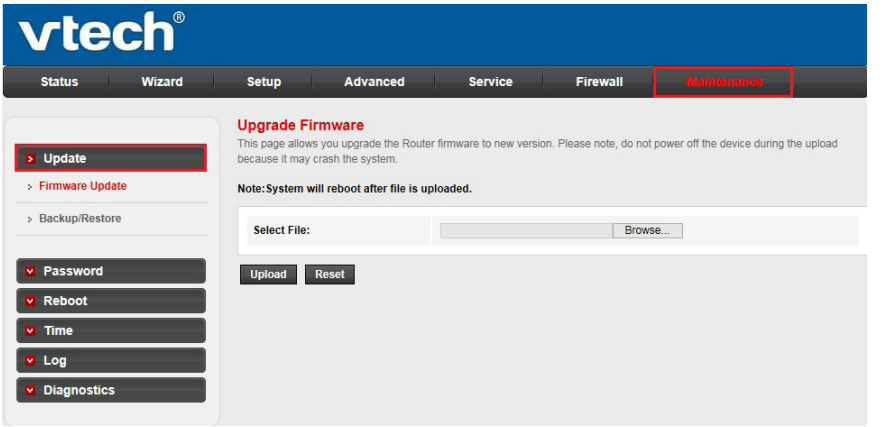
Choose the **Maintenance** menu and you can see the next sub-menus: **Update**, **Password**, **Reboot**, **Time**, **Log** and **Diagnostics**.

Update

The router supports firmware upgrade from HTTP.

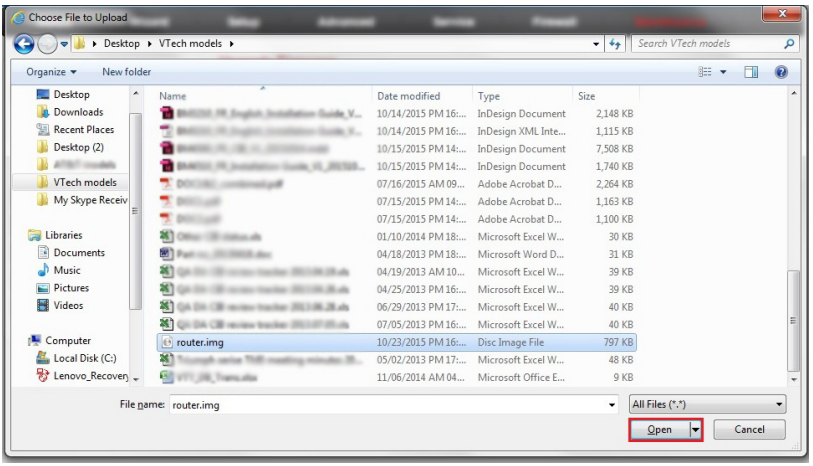
Upgrade firmware:

- Click the **Update** sub-menu in the left pane. The **Upgrade Firmware** page is opened automatically, where you can upgrade the firmware to the new version. 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.

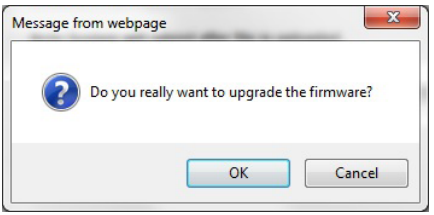


- To upgrade the router's firmware:
  1. Download a more recent firmware upgrade file.
  2. Click the **Browse...** button.
  3. Choose the update file and click **Open**.

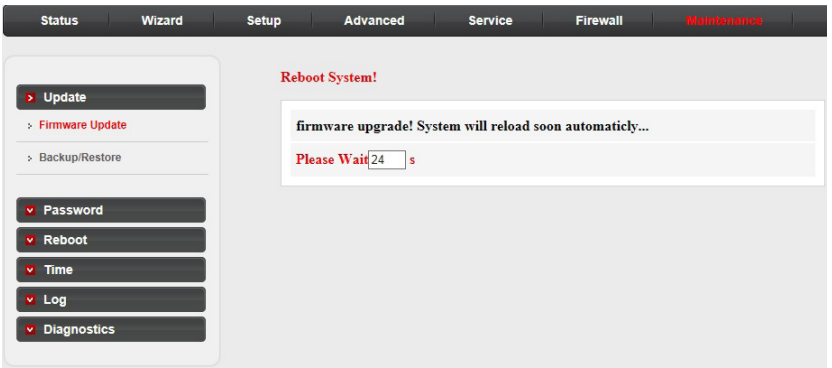
Configure your router
Maintenance



4. Click the **Upload** button.
5. A pop-up window will appear asking for confirmation of firmware upgrade. 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.



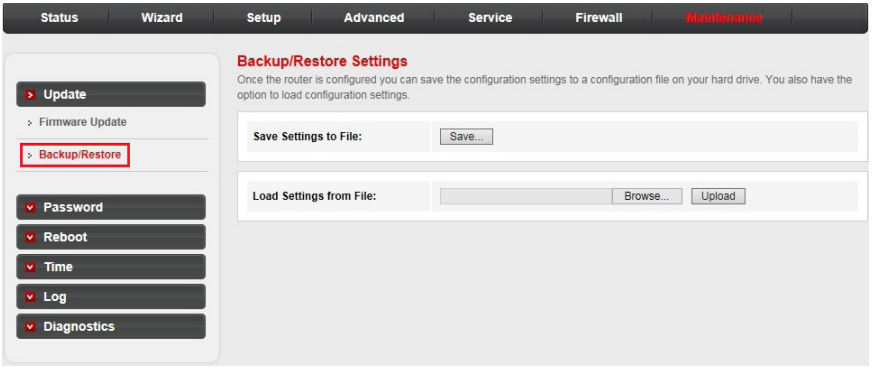
NOTES

- After the firmware is upgraded, we recommend you reset the router to default settings.
- For the router's back-end firmware upgrade purpose, please make sure the **FTP server** option is enabled under the **Service** menu. See **FTP server** on page 36 for details.

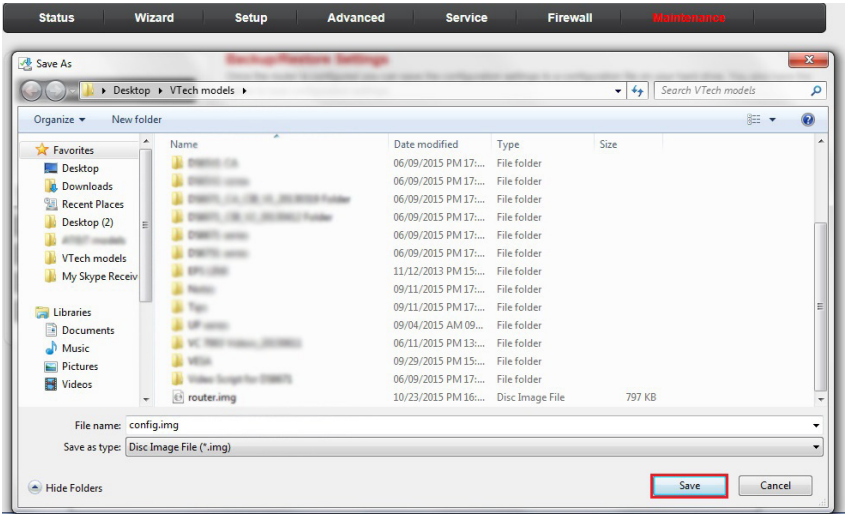
Configure your router
Maintenance

Backup/restore settings:

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



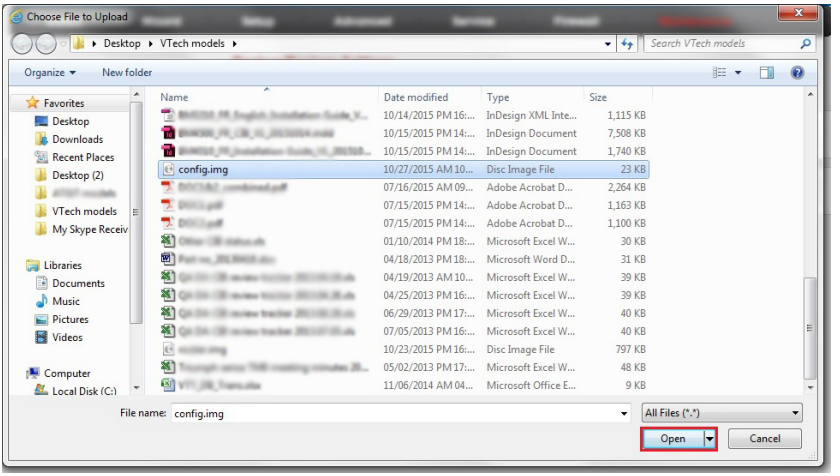
- To back up the router's current settings:
  1. Click the **Save...** button.



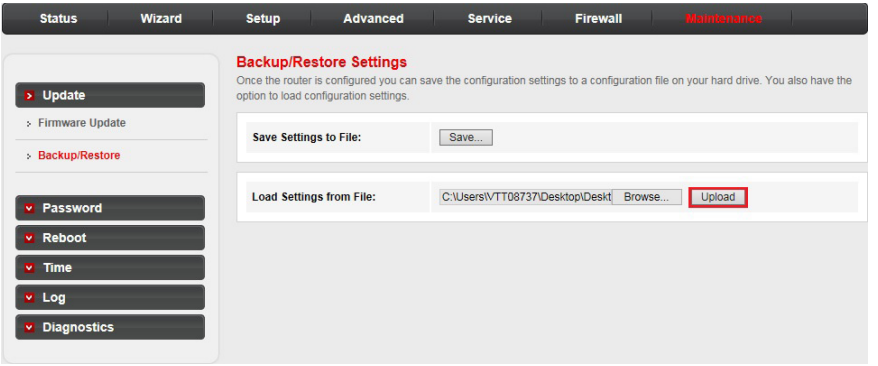
  2. Click **Save** to save the file as the appointed file.

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**.



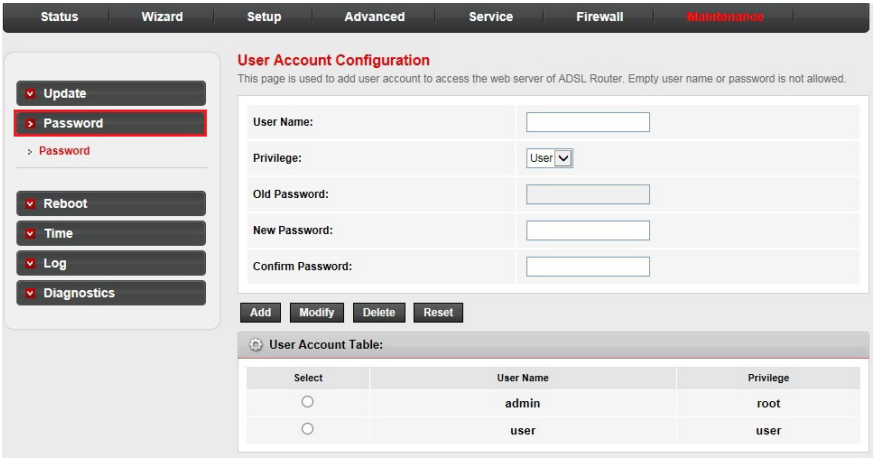
  4. A pop-up window will appear asking for confirmation of restoring the settings. Click **OK** to proceed.
  5. After the file is uploaded, the system starts a countdown and then reboots. You need to login to the web management page again.

Configure your router
Maintenance

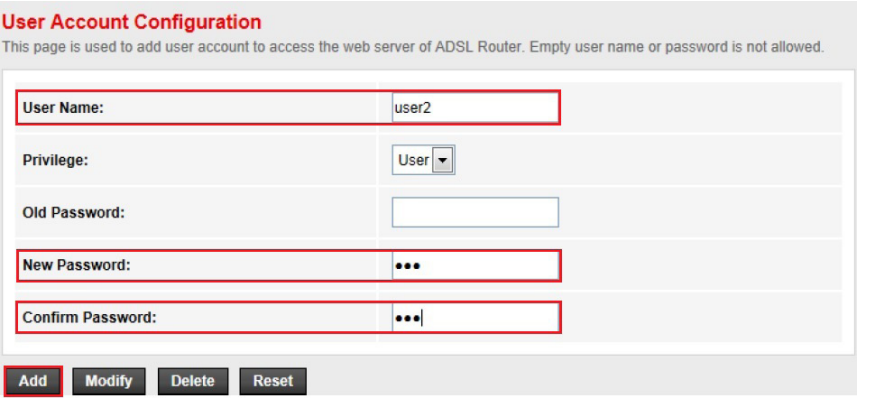
Password

User account configuration:

- Click the **Password** sub-menu in the left pane. The **User Account Configuration** page is opened automatically, where you can add user account to access the web management page and modify the password of the specified user.



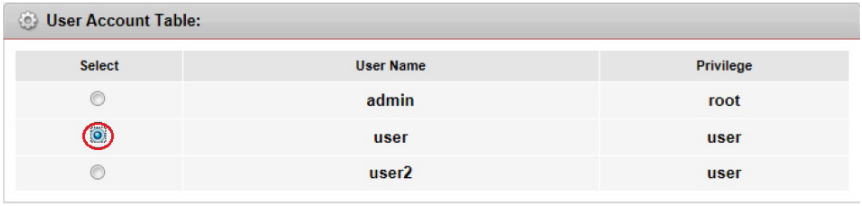
- To create an account:
  1. Type a user name in the **User Name** input box, then fill in the password in the **New Password** and **Confirm Password** input boxes.



  2. Click **Add** to create the new user account.

Configure your router
Maintenance

- To change the password of an account:
  1. Select an account which you want to change the password.



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

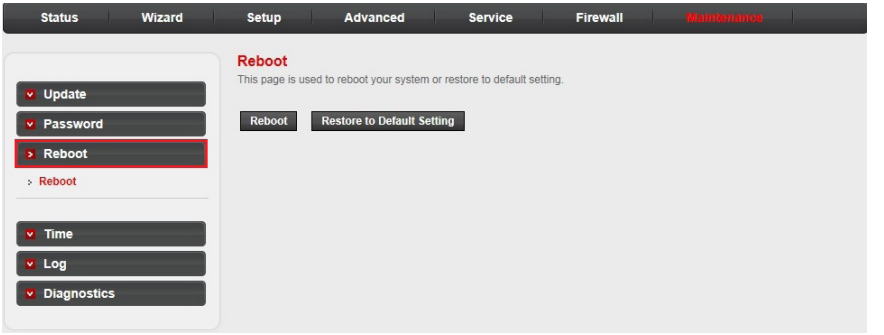
NOTE

- If you login to the web management page by administrative account, you can change the password of all accounts. The default user name is **admin** and the password is **admin12345**.

Configure your router
Maintenance

Reboot

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



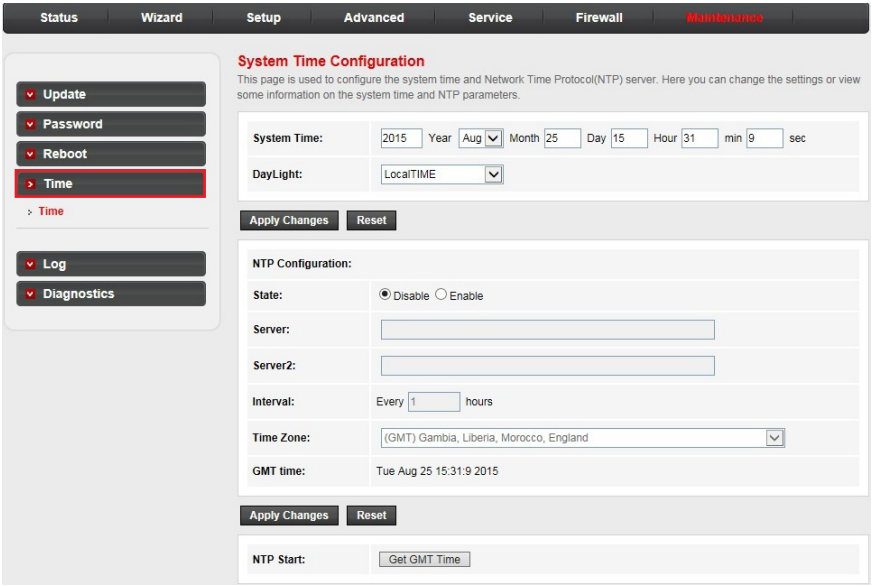
Configure your router
Maintenance

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 is opened automatically, where you can configure the system time.



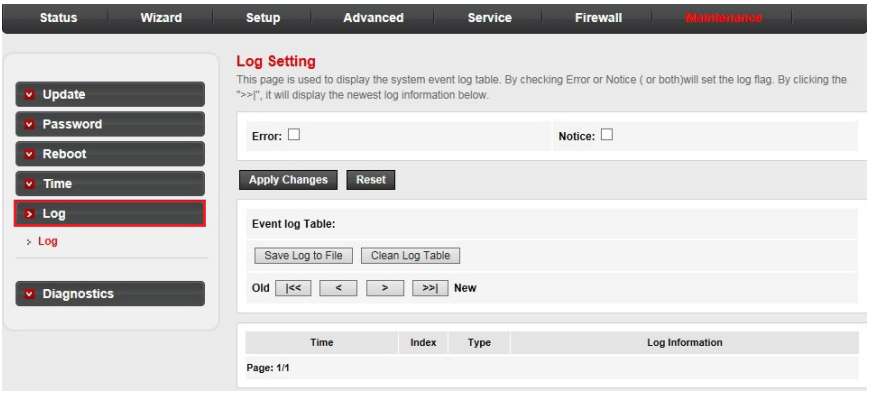
- **Server**/**Server2**: The IP address or the host name of the NTP server.
- **Interval**: The interval time of NTP function
- **Time Zone**: The time zone in which the device resides.
- When you set the NTP configuration correctly, press the button **Get GMT Time** to start the NTP function. Then, 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 is opened automatically, where you can configure the parameters of the system log and view the system log information.

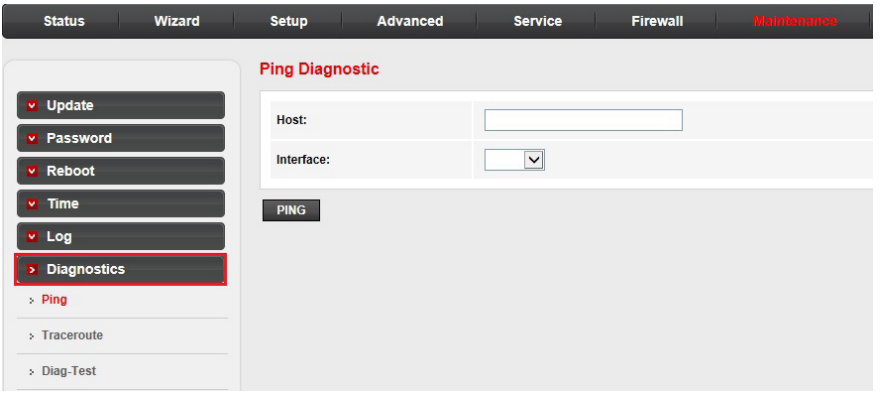


Diagnostics

The router provides several useful diagnostic tools.

Ping diagnostic:

- Click the **Diagnostics** sub-menu in the left pane. The **Ping Diagnostic** page is opened automatically, where you can use the ping command to send a message to the host you specified.

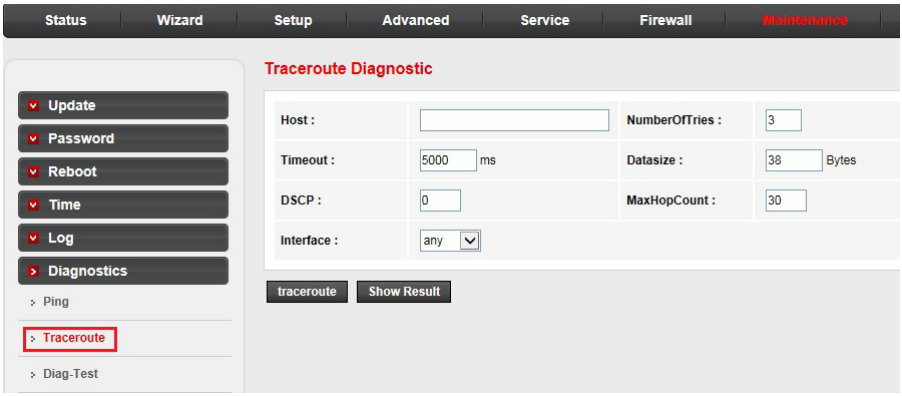


Configure your router
Maintenance

Traceroute diagnostic:

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. In this page, you can specify an IP address or host to run trace route command.



- **Host**: An IP address or host name you want to run trace route command.
- **NumberofTriers**: The number of try.
- **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.

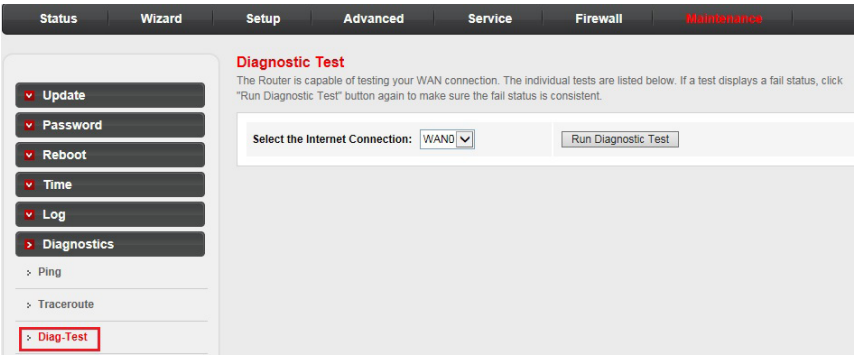
Configure your router
Maintenance

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. In 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.



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 **LAN** ports.
- Press and hold the **RESET** button for five seconds, and then wait for a few minutes for the router to restart. Observe the **WAN** light, it flashes when the router receives data.
  NOTE: After the router resets to default settings, use the default user name and password to login to the web management page.
- 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, press and hold the **RESET** button for five seconds, and then wait for a few minutes for the router to restart.

What can I do if I forgot my password?

- Restore the router to factory default settings. Then, use the default user name and password to login 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 **Plan and connect your system** on pages 3-4 for details.
- If you have more than four Ethernet devices, reset the parent router by pressing and holding the **RESET** button for five seconds, and then wait for a few minutes for the router to restart. Next, reset the child router(s) by following the same procedure.
- If you have more than four Ethernet devices and you are using an existing non-VTech router as the parent router and VNT814 router(s) as the child router(s), check if the DHCP mode of the VNT814 router(s) is set to **DHCP Relay** on the web management page, and make sure the non-VTech router has the DHCP setting enabled. See **DHCP mode** on page 17 for more details.

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 200 mA 50/60 Hz; Sortie : 12 V CC 500 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 celuici 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 nettoyants 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 50/60Hz Output: 12V DC 500mA
Network Ethernet ports	10/100 Mbps RJ-45 Port

Index

Index

Designed to fit you home.
And your life.

Document order number: 91-008806-020-100