H108N V2.1

Configuration Manual

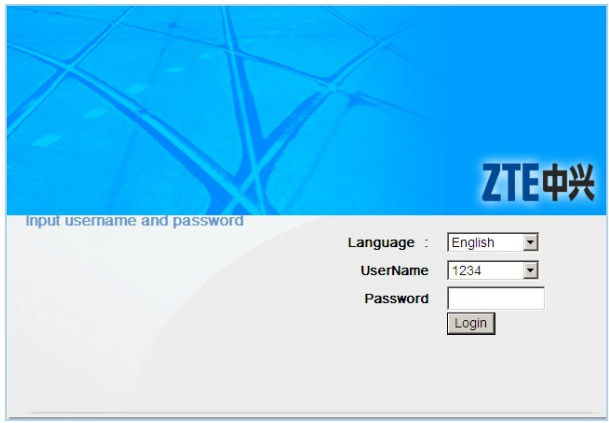
Contents

1 Accessing the Device

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

Step 1 Open your browser and enter this address: http://192.168.1.1:8000.

Step 2 The **Login** page shown in the following figure appears. Enter the password and click **Login**. The user name and password of the super user are **1234** and **1234**.



2 Setup section

In the main interface, click **Setup** tab to enter the **Setup** menu as follow. In the following pages we will discuss about the use of each function.

2.1 Wizard

The H108N V2.1 is customized with the configuration for your internet provider (check the operator logo printed on the case of the router). In this way you don't have to worry because it should work automatically.

May you wish to configure it by yourself, the **Wizard** enables fast and easy configuration of Internet connection and other important parameters. The following sections describe the configuration of those parameters.

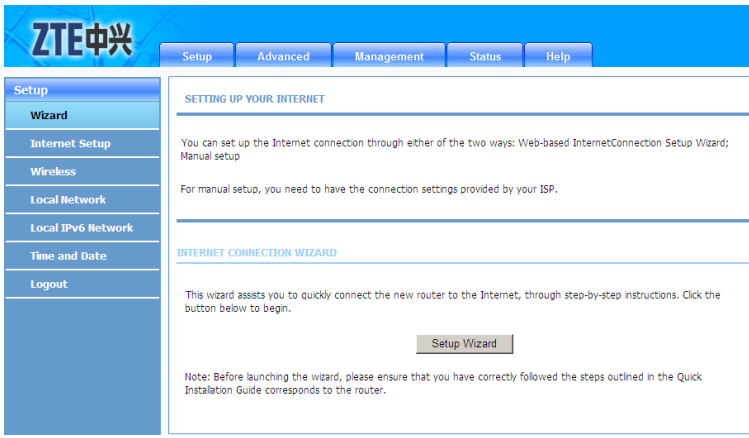
When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Technical information about the

properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

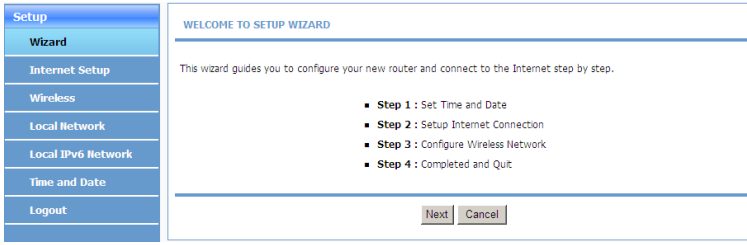
Note:

The next chapter “Internet Setup” describes the scenarios for Movistar Internet Provider in Spain, including the configuration values itself. If this is your case we recommend you jump ahead to the chapter.

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

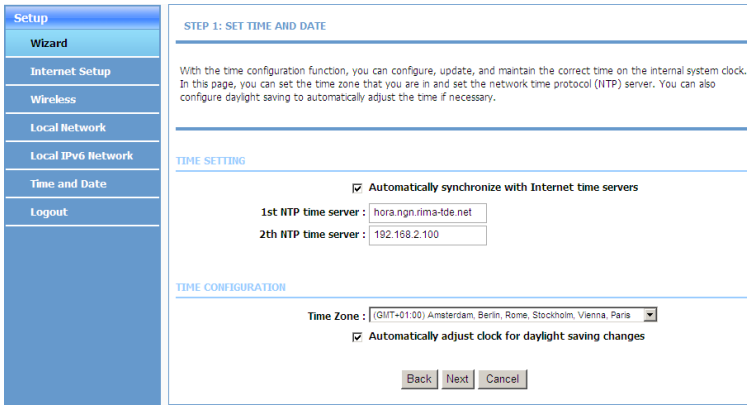


Click **Setup Wizard**. The page shown in the following figure appears.



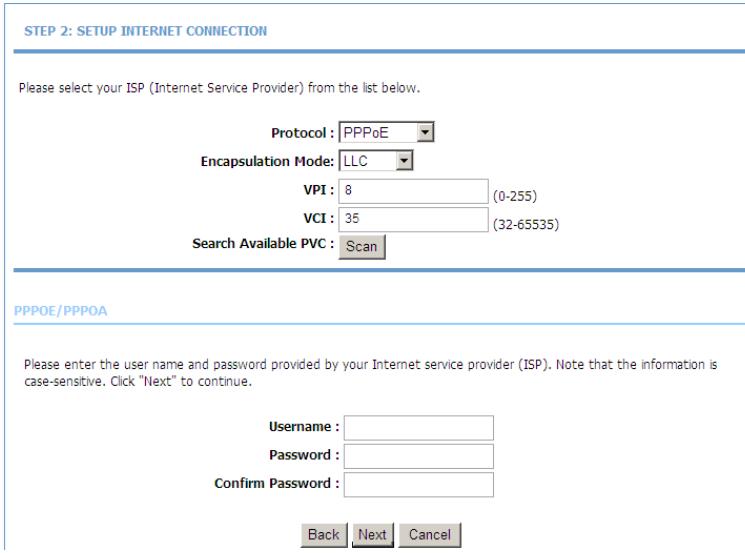
There are 4 steps to configure the device. Click **Next** to continue.

Step 1 Set the time and date in this page. After setting, click **Next**.

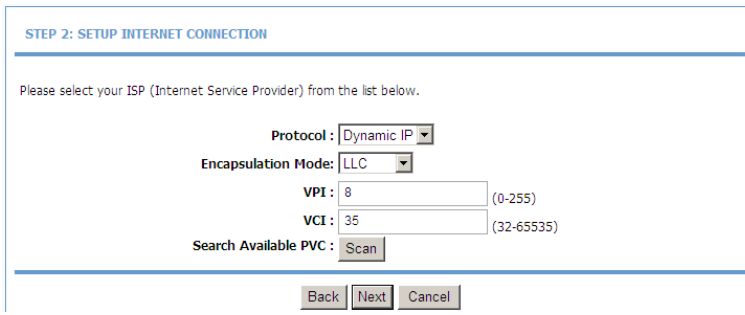


Step 2 Configure the Internet connection in this page.

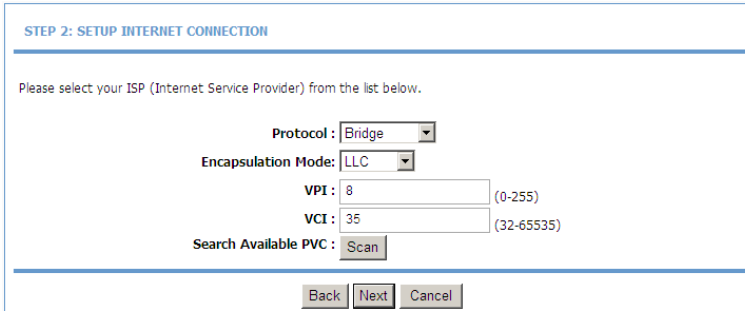
(A) If the internet service you subscribed is **PPPoE** or **PPPoA**, choose the **Protocol** as following figure appears**.** Set the VPI and VCI. Enter the user name and password provided by your ISP.



(B) If the internet service you subscribed is **Static IP** or **Dynamic IP,** choose the **Protocol** as following figure appears (this will match to the MER+LLC protocol). The page shown in the following figure appears. For Static IP enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server** provided by your ISP.

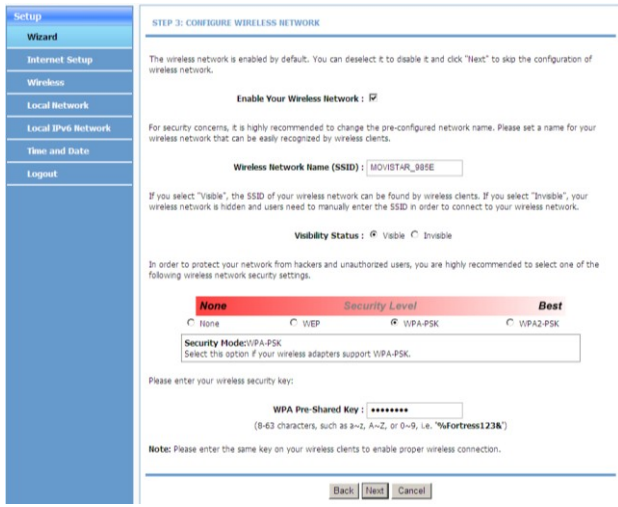


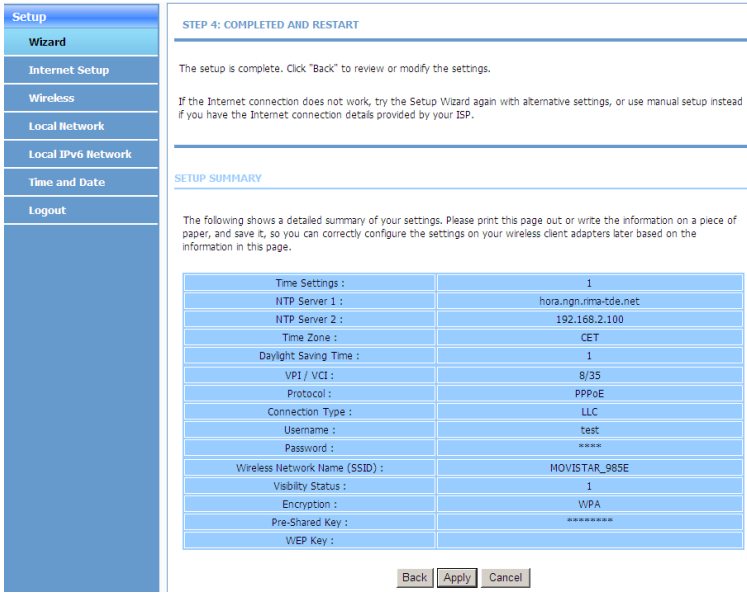
(C) If the protocol is set to be **Bridge**, the page shown in the following figure appears.



Click **Next**. The page shown in the following page appears.

Step 3 Configure the wireless network. Enter the information and click **Next**.





Step 4 Click **Apply** to save the settings.

Note:

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

2.2 Internet Setup

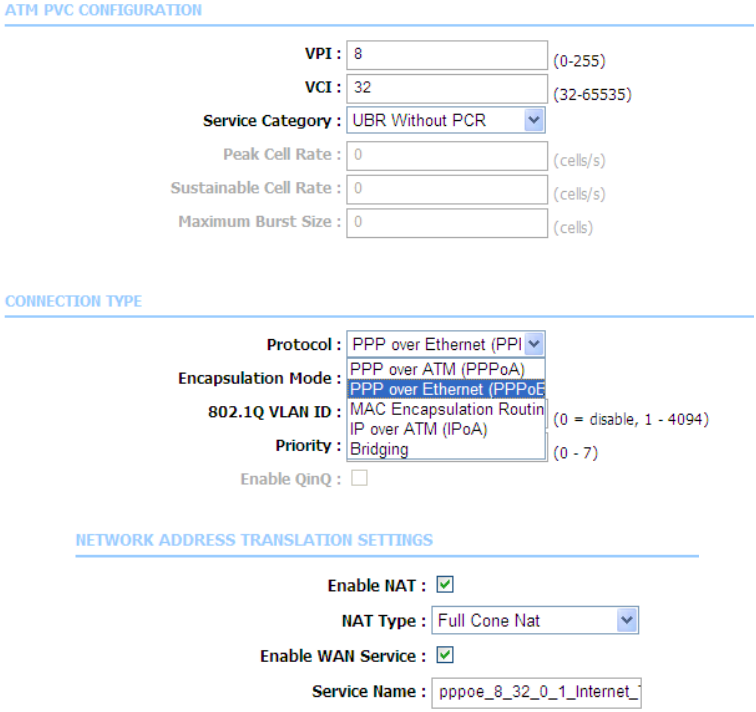
2.2.1 Configuration for multi-device with dynamic IP

Multiuser configuration allows you to create a network of multiple computers, mobile phones, or tablets, with access to the Internet from all of them.

With dynamic addressing, the router will get the IP address required to access Internet dynamically, each time you connect, during the time that the connection remains active. The next time you log in, you will be assigned a different IP address.

The advantage of this configuration is the security as to make use of NAT (Network Address Translation) the private addresses of the computers on your LAN are not visible from the outside internet, but translated into a single public IP and valid from the Internet.

In management GUI, it can be set on **Setup->Internet Setup**:



Here is the WAN configuration to set in **Setup->Internet Setup** for the WAN1 connection ("connectivity default"):

- VPI and VCI each: 8/32
- Service Category (QoS): UBR without PCR
- Connection Type: PPPoE
- Encapsulation mode: LLC
- PPPoE Username: adslppp@telefonicanetpa
- PPPoE Password: adslppp
- NAT enabled.

Then refer to the **Advanced** section:

- **Advanced -> QoS Configuration**: these rules are already configured from factory named as UP_Q_3 and traffic priority is given in the order of this list:
  - Traffic to the ACS: 80.58.63.192/255.255.255.192.
  - Traffic for public NGN: 81.47.224.0/255.255.252.0.
- **Advanced -> Routing -> RIP**: rules for 8/32 are turned off.

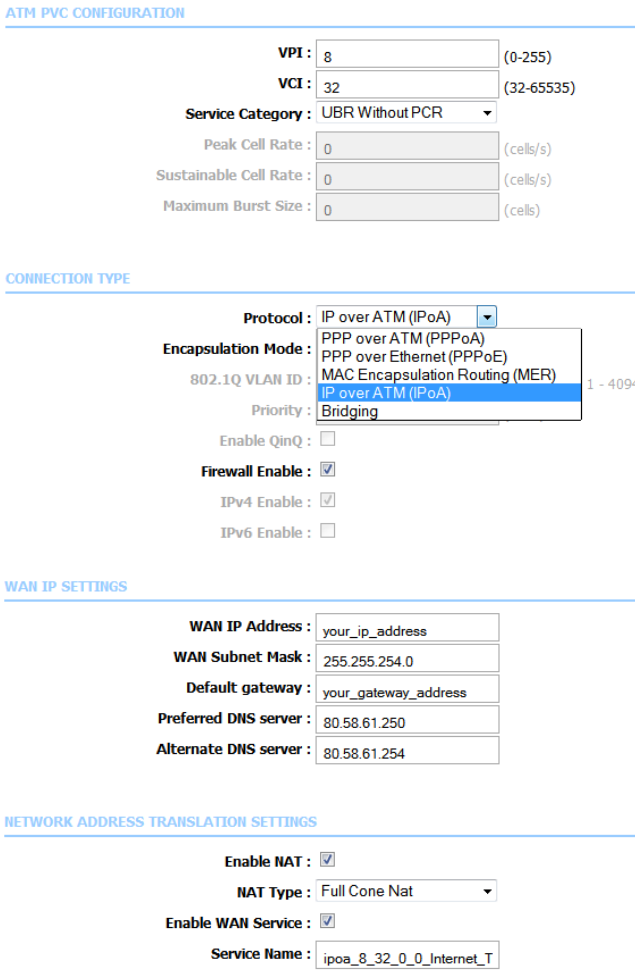
Finally refer to the **Management -> Access Controls -> Services**, find the WAN connection 8/32, and configure the following protection in the table:

- Allow ICMP traffic from WAN for all IP address (zero).
- Allow FTP, TELNET, HTTP (23, 21, 8000) traffic from WAN for these IP:
  - IP add = 193.152.37.192,80.58.63.128
  - Masks = 255.255.255.240,255.255.255.128
- Deny all other WAN traffic

2.2.2 Configuration for multi-device with static IP

This configuration mode differs from the previous in that your router is assigned a fixed IP address through which you will always access Internet.

In management GUI, it can be set on **Setup->Internet Setup**:



Here is the WAN configuration to set in **Setup->Internet Setup** for the WAN1 connection ("connectivity default"):

- VPI and VCI each: 8/32
- Service Category (QoS): UBR without PCR

- Connection Type: IPoA (also called static, RFC 2684, formerly 1483)
- Encapsulation mode: LLC
- WAN IP address: provided by your operator
- WAN subnet mask: provided by your operator
- Default gateway: provided by your operator
- Preferred DNS server: by your operator (Movistar is 80.58.61.250)
- Alternate DNS server: by your operator (Movistar is 80.58.61.254)
- NAT enabled.

Then refer to the **Advanced** section (same config as last chapter):

- **Advanced -> QoS Configuration**: these rules are already configured from factory named as UP_Q_3 and traffic priority is given in the order of this list:
  - Traffic to the ACS: 80.58.63.192/255.255.255.192.
  - Traffic for public NGN: 81.47.224.0/255.255.252.0.
- **Advanced -> Routing -> RIP**: rules for 8/32 are turned off.

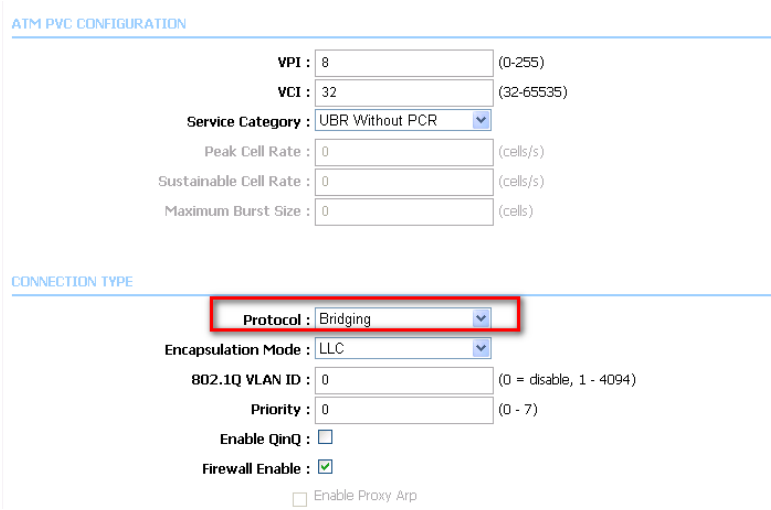
Finally refer to the **Management -> Access Controls -> Services**, find the WAN connection 8/32, and configure the following protection in the table (same config as last chapter):

- Allow ICMP traffic from WAN for all IP address (zero).
- Allow FTP, TELNET, HTTP (23, 21, 8000) traffic from WAN for these IP:
  - IP add = 193.152.37.192,80.58.63.128
  - Masks = 255.255.255.240,255.255.255.128
- Deny all other WAN traffic

2.2.3 Configuration for standalone device with dynamic IP

With standalone setup only one PC can be directly connected to the Internet, as it does not use NAT. It is strongly recommended to use some kind of protection on the computer: firewall and antivirus.

In this scenario, the router will transparently work in bridge mode, so your PC will need to establish manually the PPPoE connection with your Internet Provider (ISP). In management GUI, it can be set on **Setup->Internet Setup**:



Here is the WAN configuration to set in **Setup->Internet Setup** for the WAN1 connection ("connectivity default"):

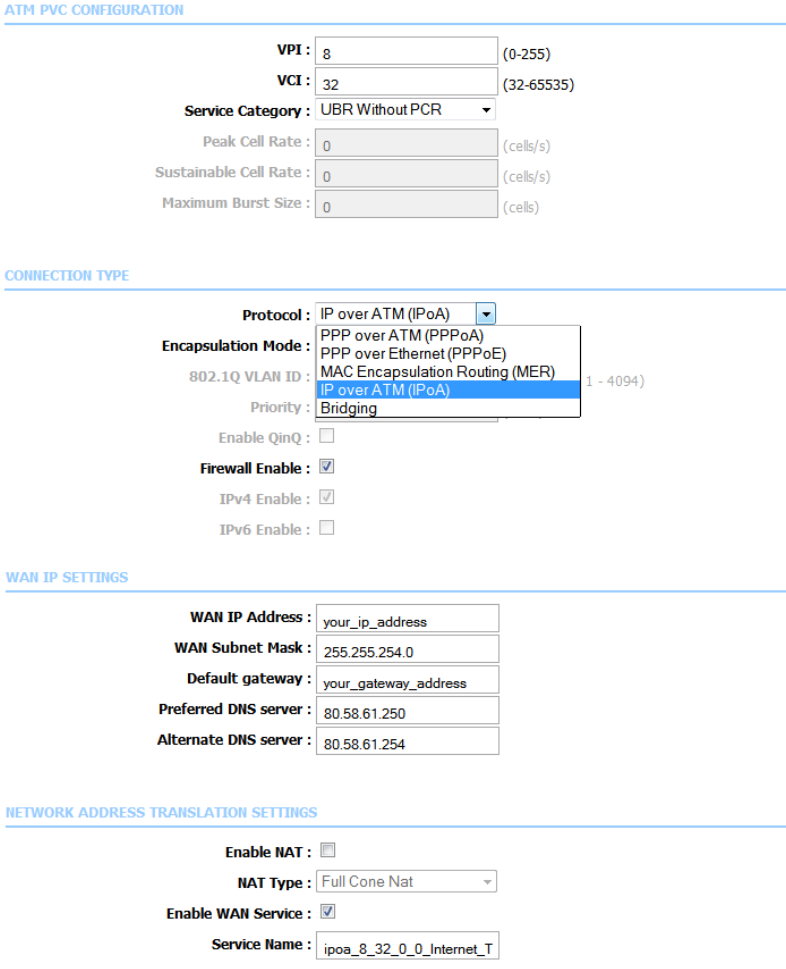
- VPI and VCI each: 8/32
- Service Category (QoS): UBR without PCR
- Connection Type: bridging
- Encapsulation mode: LLC
- NAT disabled.

2.2.4 Configuration for standalone device with static IP

With standalone setup only one PC can be directly connected to the Internet, as it does not use NAT. It is strongly recommended to use some kind of protection on the computer: firewall and antivirus.

In the WAN side, the router will get a public IP for management. In the LAN side, the router's DHCP will provide to your PC a unique IP configured in the pool, that will be the public line.

This configuration can be set on **Setup->Internet Setup**:



Here is the WAN configuration to set in **Setup->Internet Setup** for the WAN1 connection ("connectivity default"):

- VPI and VCI each: 8/32
- Service Category (QoS): UBR without PCR
- Connection Type: IPoA (also called static, RFC 2684, formerly 1483)
- Encapsulation mode: LLC
- WAN IP address: provided by your operator (management IP)
- WAN subnet mask: provided by your operator
- Default gateway: provided by your operator
- Preferred DNS server: by your operator (Movistar is 80.58.61.250)
- Alternate DNS server: by your operator (Movistar is 80.58.61.254)
- NAT disabled.

In the **Setup->Local Network**, find the section "DHCP settings":

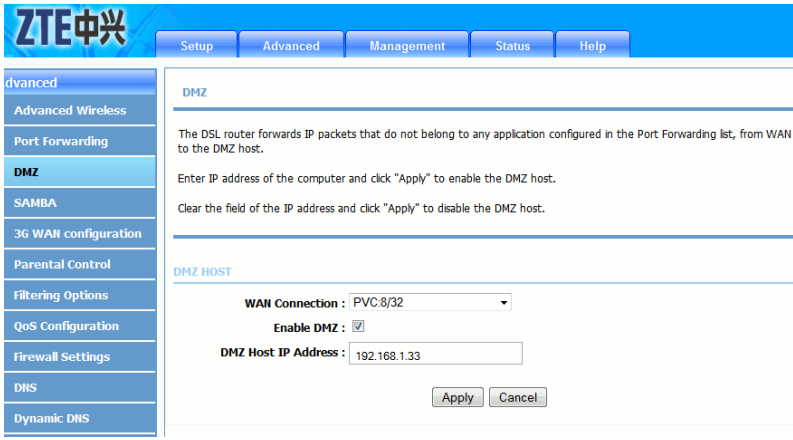
- DHCP IP Address Range = [Start] = [End] = provided by your operator
- DHCP IP mask = 255.255.255.252
- DHCP gateway IP = first static address of the public WAN

Then refer to the **Advanced -> Routing -> RIP** and ensure rules for 8/32 are turned off.

2.2.5 Configuration for standalone device (generic)

Based on your default factory configuration you can emulate the "standalone" scenario with much easier configuration. Simply use the DMZ to expose your computer to internet.

Refer to section **Advanced > DMZ**:

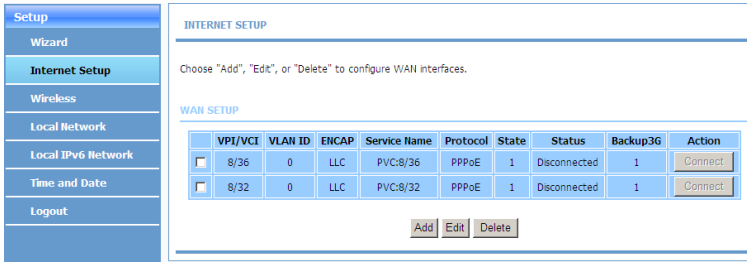


- Select your connection VCI/VPI (probably 8/32). You can review the list of connections in Setup > Internet Setup. The list will display which one is connected.
- Select enable DMZ (de-militarized zone)
- Enter the IP of the computer or device that you want to expose to internet as standalone system.
- Click **Apply**.
- On your computer you don't need to take any action. It will have full bi-directional communication with Internet. It is recommended to install a firewall and antivirus software for basic protection.

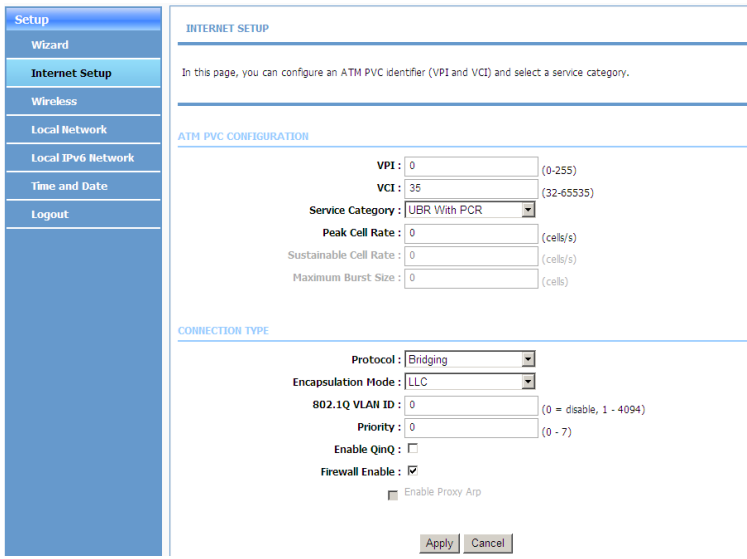
2.2.6 Generic Configuration

The H108N V2.1 is customized with the configuration for your internet provider (check the operator logo printed on the case of the router). In this way you don't have to worry because it should work automatically.

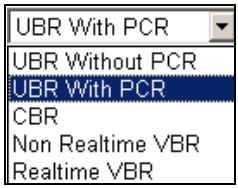
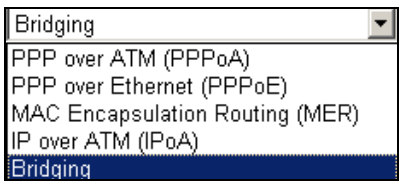
However, you can access and modify manually the configuration in the section **Setup** > **Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.



Click **Add** and the page shown as the following figure appears.



The following table describes the parameters in the previous page.

Field	Description
PVC Settings	**VPI**: The virtual path between two points in an ATM network and its valid value is from **0** to **255**. **VCI**: The virtual channel between two points in an ATM network, ranging from **32** to **65535** (0 to 31 is reserved for local management of ATM traffic).
Service Category	You can select from the drop-down list. 
Protocol	You can select from the drop-down list.  Please see the explanation note bellow this table for more advanced information.
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.

Regarding the “protocols” available:

Bridging: the device will become a simple switch/bridge with five ports (4 ETH + 1 DSL), and the traffic is repeated as-is to any port.

- Your PC(s) will need to have public address/es, and also require an external remote gateway. Your network will be public and externally routable.
- Most internet providers (but not all) can support this kind of traffic on their network (DSLAMs), or even allow you to have more than one public IP address.
- All routing functions of the H108N are turned off just for this “pure bridging mode”, so NAT is not possible here.
- If your internet provider requires a PPPoE session, but you want to configure the router in “bridging mode”, you will need to establish the connection from your PC(s) manually.

MER (MAC Encapsulated Routing): equivalent to the above, the device will also bridge the traffic “MAC packets” to the DSL port, but it will encapsulate it first for the VC. For this reason it often has other equivalent names:

- “Ethernet encapsulation” or “IPoEoATM”
- “RFC1483 or RFC2684”
- “RFC1483 or RFC2684 bridged” (no “IP” here)

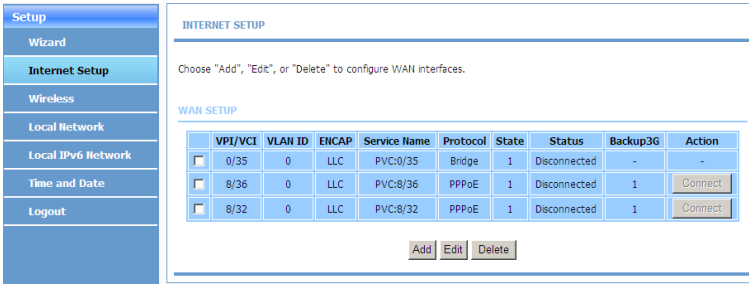
IPoA (IP over ATM): the device will route the traffic (IP packets), and encapsulate it for sending over your DSL line (ATM). For this reason it has other equivalent names:

- “RFC1483 or RFC2684 bridged IP”
- “RFC1483 or RFC2684 routed”

For the two latter protocols, the RFC2684 allows your router to perform bridging on the WAN side while routing on the LAN side (thus NAT).

Finally, the **PPPoE** and **PPPoA** match the two latter protocols, but the router will establish a PPP session to deliver the traffic to the right gateway.

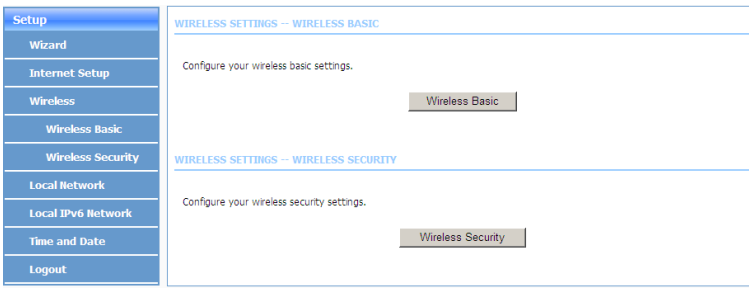
Click **Apply** to make the settings take effect and the page is shown as the following figure appears.



2.3 Wireless

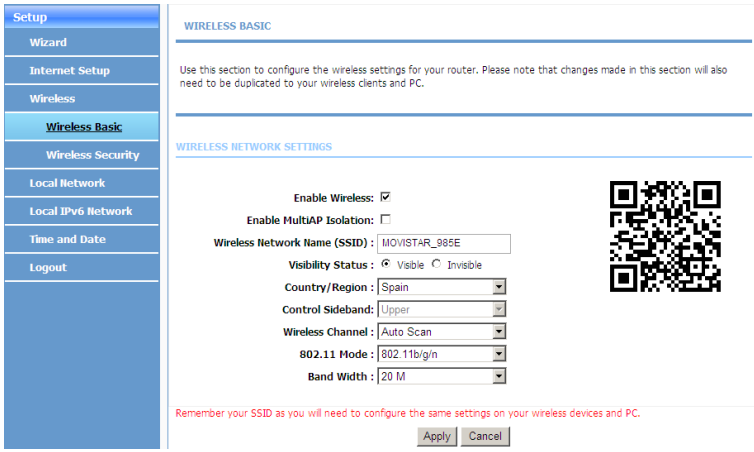
This section describes the wireless LAN and basic configuration. A wireless LAN can be as simple as two computers with wireless LAN cards communicating in a pear-to-pear network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic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

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



2.3.1 Wireless Basics

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



The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
Enable MultiAP Isolation	Select this to turn MultiAP isolation on. In this way, the computers in separate wireless networks will not be able to see each other.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

Field	Description
Visibility Status	Select **Visible** to allow your network to be detected by your computer or any other computer. Select **Invisible** and it will be harder to connect to your network because the SSID name is not broadcasted.
Country	Select the country from the drop-down list. This may change the number of wireless channels available for WiFI (Spanish law allows up to 13).
Control Sideband	This setting applies only for WiFI N of 40M. Choose the main channel location as **Upper** or **Lower**. For example main channel 6 “lower”, will be occupying also channel 10 as secondary (thus 20+20). Select this to avoid interference with neighbors’ WiFI.
Wireless Channel	Select the wireless channel from the pull-down menu. Automatic mode will try to avoid interference with neighbors’ WiFI. Otherwise to make a smart manual selection you can view the free available channels with scanning programs as inSSIDer.
802.11 Mode	Select the appropriate 802.11 mode based on the wireless clients in your network. It is recommended to keep it as default.
Band Width	Select the appropriate band of **20M**, **40M** or **20M/40M** according to your subscribed broadband service. If you are in a dense neighborhood, selecting 40M may not be appropriate because your network it will occupy 9 channels bandwidth (in 2.4G), thus you will experience mutual interference and reduced speed.

Click **Apply** to save the settings.

Note:

By default, there are only 16 allowed computers for each WiFI which are enough for home or small office. Refer to further section titled “advanced wireless” to increase this number.

There is a **QRcode** square on the right of the page. This QRcode can help your cell phone connect to the wireless network of **H108V** automatically. It can also help you to note down / recover your Wi-Fi's password if you forgot it.

Note:

Just taking photo of QRcode will not work. Instead you need to have a reading application, for example: QR barcode scanner (Android), Bidi (iPhone), BeeTagg (WP7), etc.

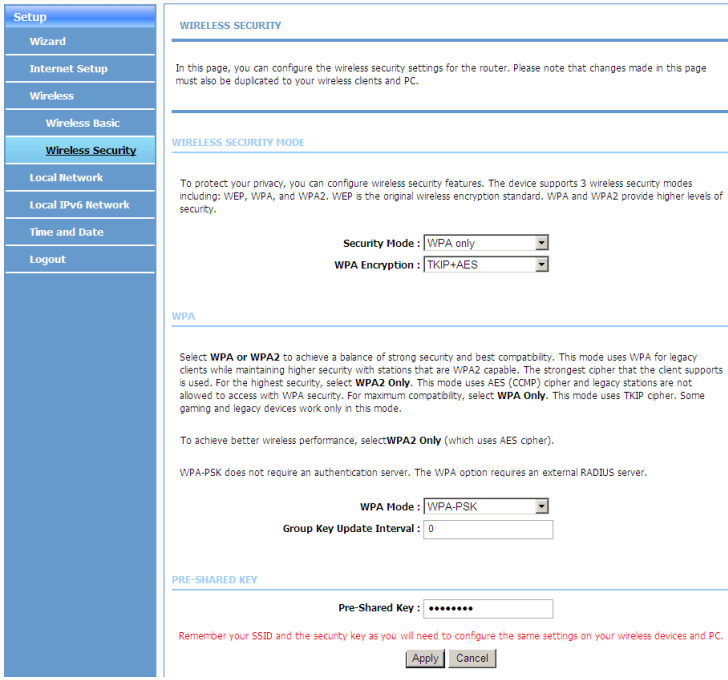
2.3.2 Wireless Security

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

Note:

Enable Wireless before configuring the wireless security settings in this page. Refer to **2.3.1** ¡Error! No se encuentra el origen de la referencia. to enable Wireless.

If the Security Mode is set to be **Auto (WPA or WPA2)**, **WPA2 only**, or **WPA only**, the following page appears.



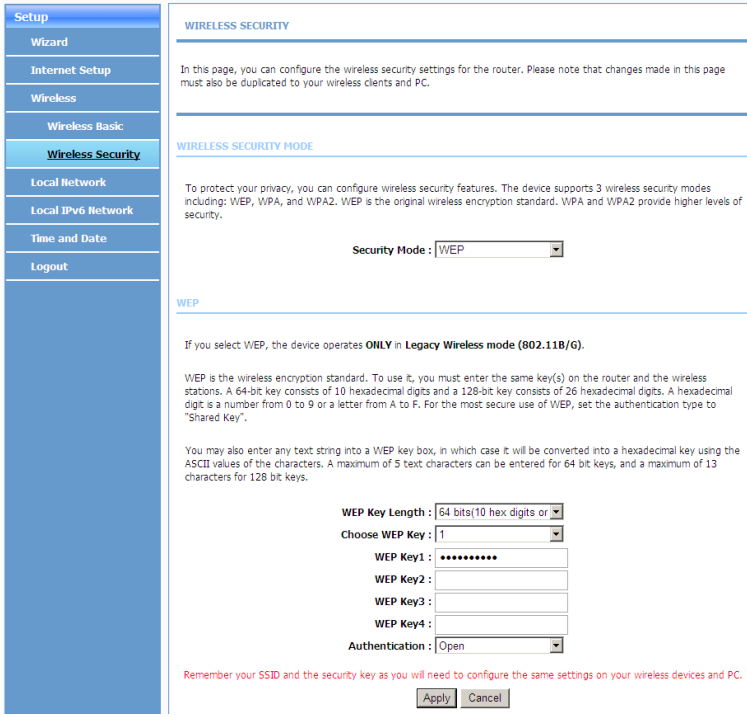
The following table describes the parameters in this page.

Field	Description
Security Mode	Configure the wireless encryption mode. You can choose **None**, **WEP**, **Auto (WPA or WPA2)**, **WPA 2 Only** or **WPA Only**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft.

Field	Description
	● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption. Currently WEP is considered easily vulnerable.
WPA Encryption	When WPA or WPA2 is selected, you can select WPA encryption as **AES** or **TKIP+AES**.
WPA Mode	● Select **PSK (Pre-Shared Key)**; enter the pre-shared key in the **Pre-Shared Key** field. ● Select **Enterprise (RADIUS)** if you have an external accounts' server. Enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem.
Group Key Update Interval	When WPA encryption is applied, messages sent are encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.

Click **Apply** to save the settings.

If the Security Mode is set to be **WEP**, the following page appears.



The following table describes the parameters of this page.

Field	Description
WEP Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Choose WEP Key	Choose the index of WEP Key. You can choose **Key 1**, **2**, **3** or **4**.
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is **1234567890**.

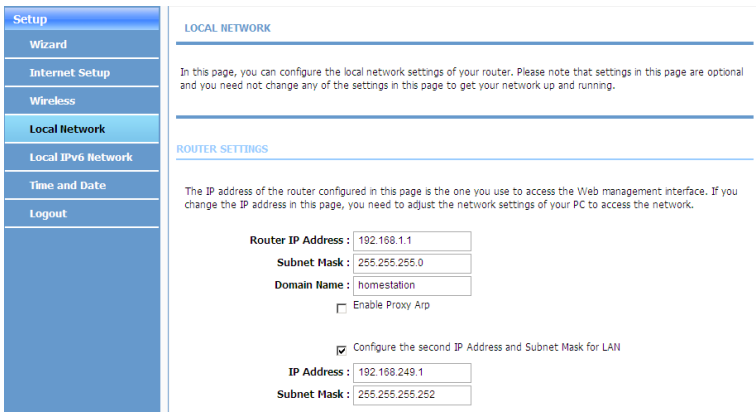
Field	Description
Authentication	There are 2 authentications in WEP encryption. **Open** and **Share key**. Both authentications support WEP encryption. But the message header is different in wireless broadcast.

2.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks. Usually the second network is used for STB devices providing IPTV service.

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

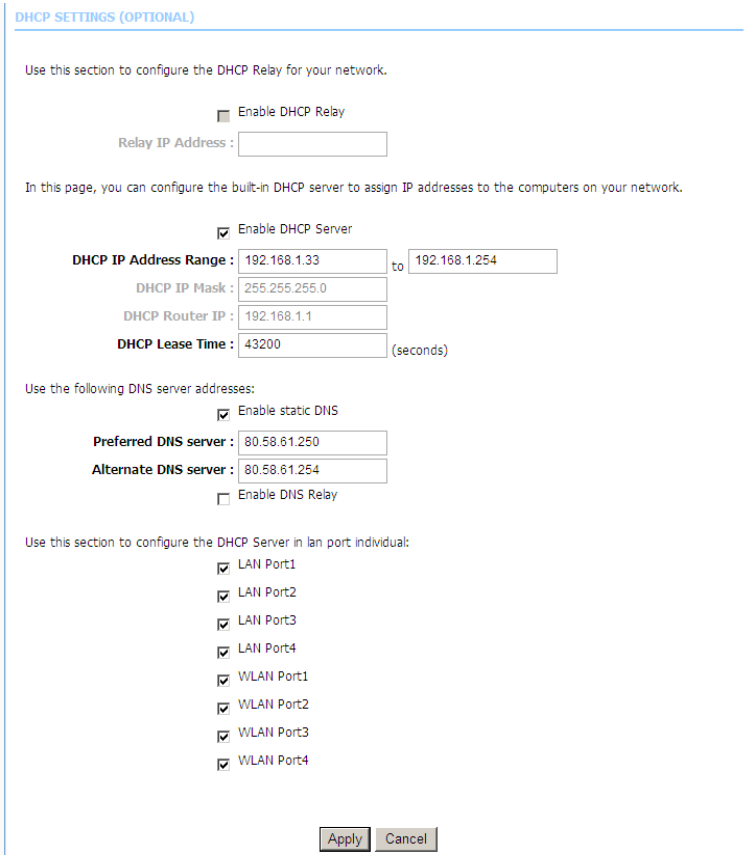


The following table describes the parameters in this page

Field	Description
Router IP Address	Enter the IP address of LAN interface. It is recommended to use an address from a block that is reserved for private use (192.168.1.1-192.168.255.254). The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254. The default mask 255.255.255.0 allow up to 253 computers in the private network.
Domain Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
Configure the second IP Address and Subnet Mask for LAN	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in the different network.

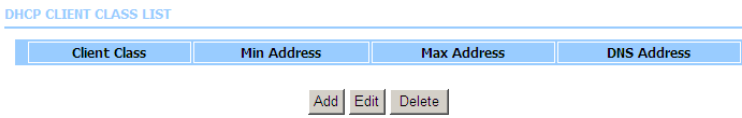
By default, **Enable DHCP Server** is selected for all the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it.

If you change the IP address of the home gateway, it will also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

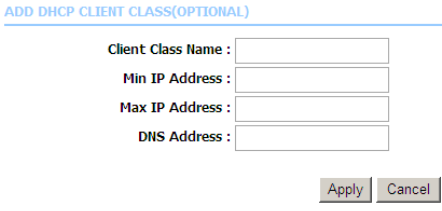


Click **Apply** to save the settings.

The **DHCP Client Class List** section shown in the following figure appears.



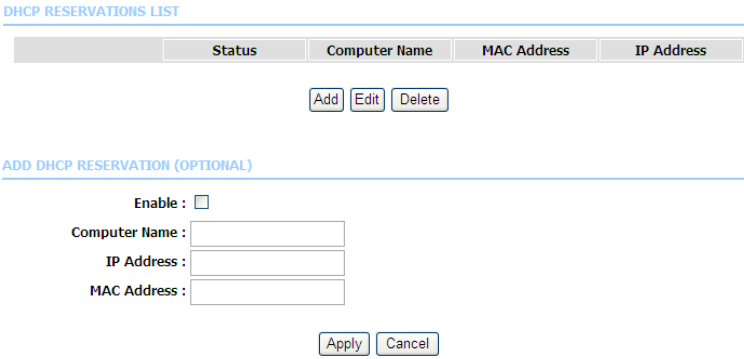
Click **Add** to add DHCP client class (optional). The page shown in the following figure appears.



You can assign IP addresses on the LAN to specific individual computers based on their MAC addresses. The following page shows the **DHCP RESERVATIONS LIST**.

This is commonly used to assign a “fixed permanent IP” to videogames (Xbox, PS, Nintendo, etc), or sometimes to computers, that need opening ports for playing network games or downloading files.

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



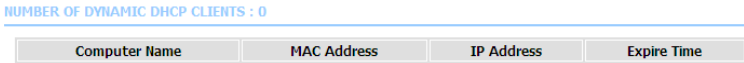
Select **Enable** to reserve the IP address for the designated PC with the configured MAC address. The **Computer Name** helps you to recognize the PC

with the MAC address, for example, Father's Laptop. Click **Apply** to save the settings.

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

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

You can query from here easily the MAC address of your videogame or computer, if you want to reserve it a "fixed IP" (DHCP Reservation) as explained before.



2.5 Local IPv6 Network

The IPv6 is the new standard for networking. It allows new functionality and much more addresses than the previous one which was running short - so many address that it can be considered unlimited. It had its premiere on 6th June 2012 by some important Internet companies like Google®, Facebook®, Microsoft®, Movistar®, etc.

For the above reason, the "Local IPv6 network" is normally used together with "Internet Setup" checking IPv6 too. This way you enable IPv6 on both sides and you are able to browse "pure-IPv6" web sites in a standard way. All these IPv6 options are enabled by default in the router ZTE H108N V2.1.

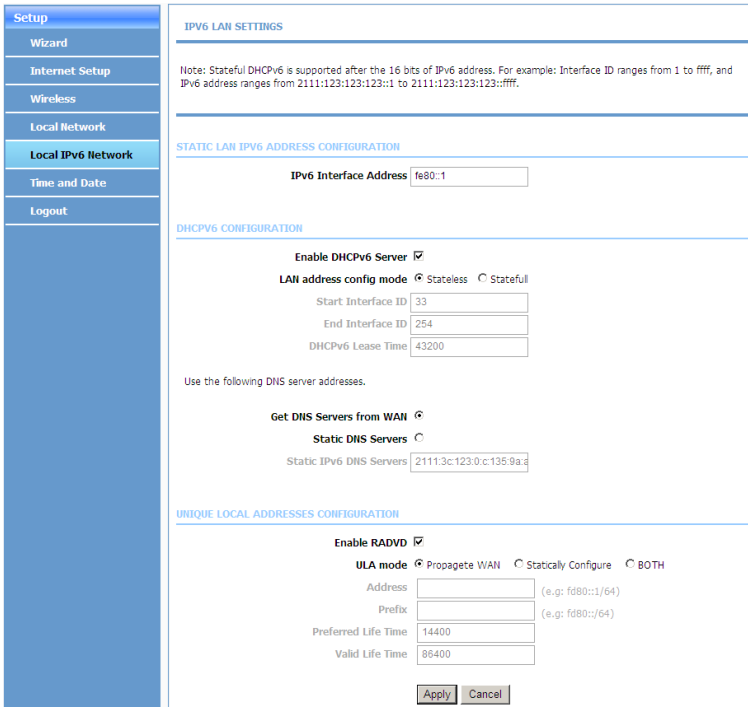
Note:

Windows has a built-in feature called "Teredo". To ensure compatibility it will always send the IPv6 through the "old network" (encapsulated). In this way even you are still using the old network, the new IPv6 web sites will work for you. This is okay while the older networks still exist.

Note:

Starting at Windows 8 the network is automatically tested so that if IPv6 works correctly then Windows will choose “pure-IPv6” network. Otherwise when it detects some problems, it will fall back to the old Teredo for your convenience.

Choose **Setup** > **LAN IPv6**. The page shown in the following figure appears. This page allows you to config IPv6 LAN.



The following table describes the parameters of this page.

Field	Description
IPv6 Interface Address	The address through which your PCs access the router (equivalent to 192.168.1.1). Here it's default fe80::1 which is standard local link gateway.
Enable DHCPv6 Server	Choose to enable or disable DHCPv6 service.
LAN address config mode	Set the mode for obtaining IP from LAN PCs. You may choose **Stateless** or **Statefull**. Stateless is default, where all hosts get always the same IP of type "fe80::MAC". This is more convenient for port redirection.
Start/End Interface ID	The address pool using DHCPv6 for address assignment under statefull mode.
DHCPv6 Lease Time	The address lease time using DHCPv6 for address assignment under statefull mode.
Enable RADVD	Choose to enable or disable router advertisement service (RADVD). Necessary for routing to work.
Propagate WAN	Use the site prefix obtained at the WAN side as the prefix to issue (from your Internet Provider). This is the default and recommended configuration. Your PCs will get a public IPv6.
Static	Manually add a site prefix. This will create an internal network.

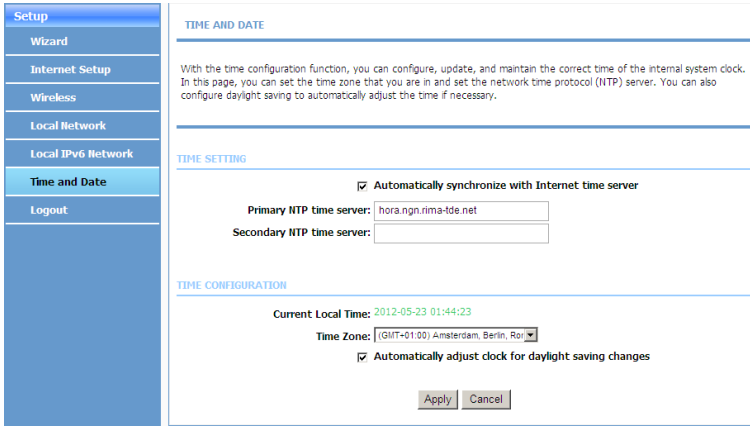
Note:

Even when your PCs get a public IPv6, they are still protected by the "port filtering" function. Please refer to the section regarding port opening.

2.6 Time and Date

The router will automatically sync with Movistar time server.

To change this choose **Setup** > **Time and Date**. The page shown in the following figure appears.



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

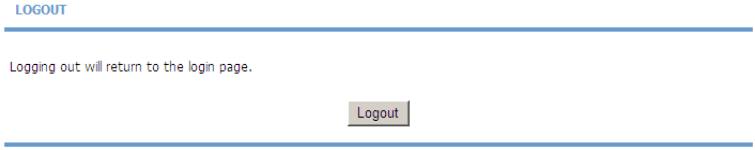
Select **Automatically synchronize with Internet time servers**. Enter the specific time server and select the time zone from the corresponding drop-down lists.

Select **Automatically adjust clock for daylight saving changes** if necessary. Set the daylight as you want.

Click **Apply** to save the settings.

2.7 Logout

Choose **Setup** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page. Please close your browser window or tab for increased security.



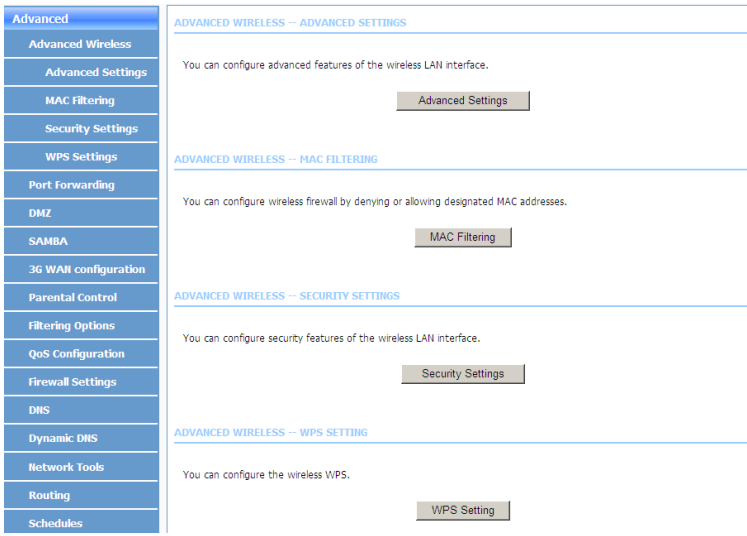
3 Advanced section

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

3.1 Advanced Wireless

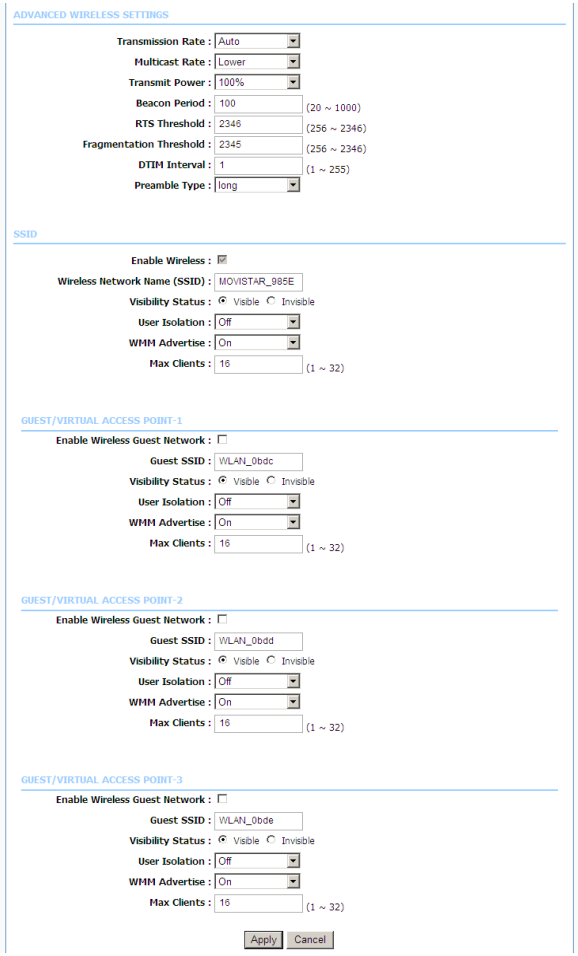
This function is used to modify the standard 802.11g wireless radio settings. It is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

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



3.1.1 Advanced Settings

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



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

Note:

By default, there are only 16 allowed computers for each WiFI which are enough for home or small office. You can change it in this screen, under your WiFI name, attribute “max clients”.

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

Here are some tips for troubleshooting advanced users:

- In a large environment, let’s say multi-roomed offices or hotel floors (>300m²), where you have many devices (>7) with traffic collision at the same time causing the performance speed is very low, you can avoid this problem by reducing “RTS threshold” down to 500.

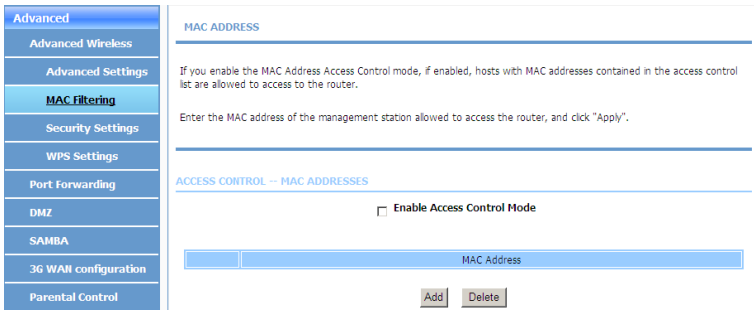
- In a high interference environment, let’s say near microwaves, electric motors, Bluetooth devices, wireless phones at home (DECT), etc, where many packets are lost due to errors and performance speed is low, you can avoid this problem by reducing “fragmentation threshold” down to 820 normally or even 500. Lower values can also be used, but it can start to affect the performance for the added overhead.

- In reduced home environment, without multicast voice-video or network gaming (none of these take place) you can increase the DTIM interval to 2 or even 4. This will save battery on your mobile equipment (phone, tablet and laptop) with a imperceptible delay at message reception.

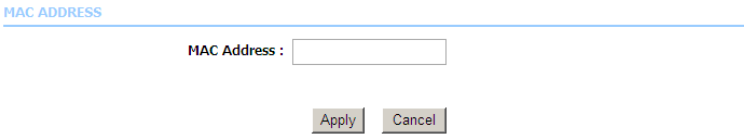
Click **Apply** to save the settings.

3.1.2 MAC Filtering

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



Choose **Enable Access Control Mode**, and then click **Add** to add a MAC Address as shown in the following figure. You can get the MAC address of your connected devices in the “local network” chapter former in this document.



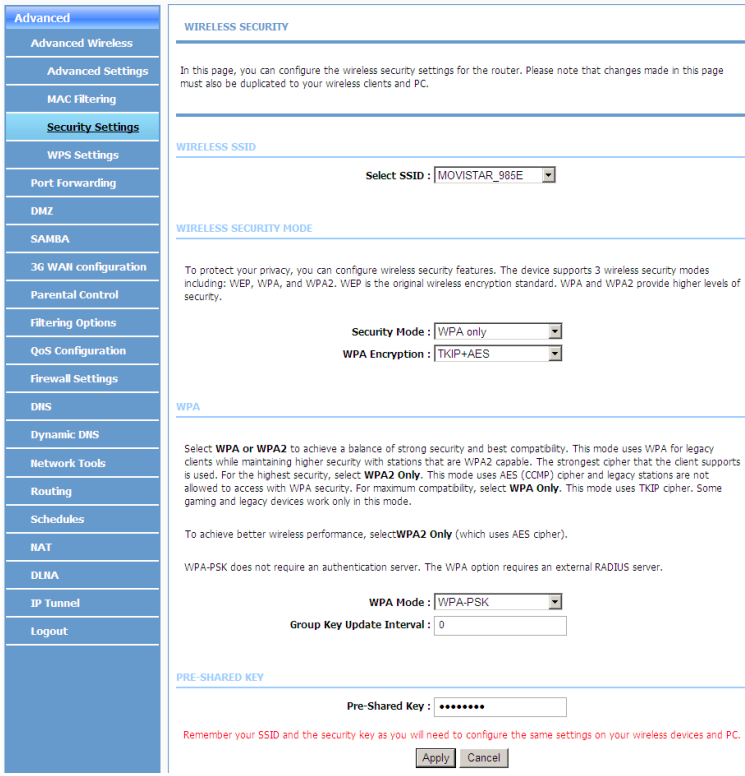
This will help you to restrict who can connect to your WiFI network. Click **Apply** to finish.

Note:

Before enabling this option please add your own address to the list first. Otherwise you won’t be allowed into your own WIFI. If this happens somehow you will need to connect to the router by cable to fix or disable this protection.

3.1.3 Security Settings

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



Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Security Mode** drop-down list. You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only** or **WPA2 Only**. The defaulted security mode is **WPA only**. For detailed configuration, you may refer to 2.3.2 Wireless Security.

3.1.4 WPS Settings

The WPS helps your computer PC to connect easily to the WIFI network using a small PIN number or without password at all with the push of a button.

By default, the router brings WPS in “enrollee mode” and the WPS led turned on. When your computer wants to connect to a WiFI network for the first time (Windows Vista or above), it will display a window to ask for a password or alternatively “push the button on the router”.

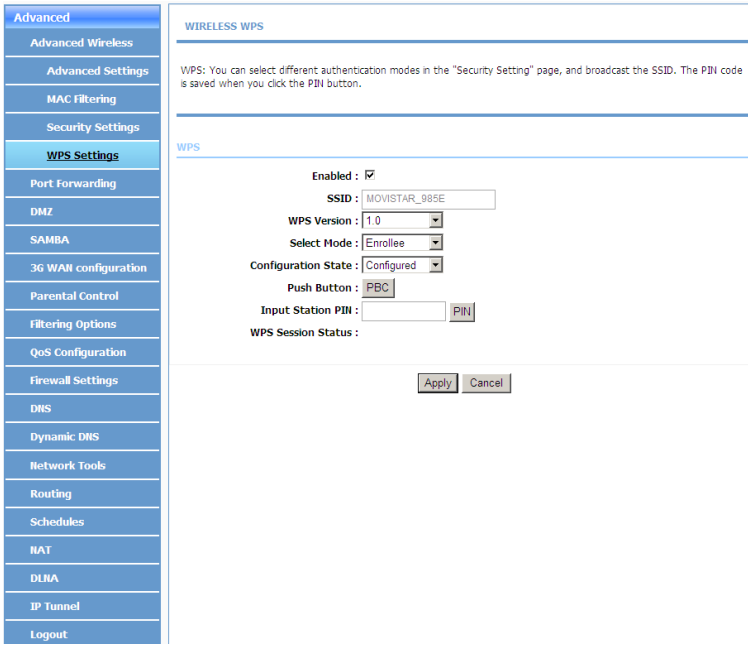
Note:

Press for 5 seconds the small black button labeled “Wifi/WPS” on the back of the router, and the WPS led will blink green. This will allow just ONE device (your PC) to register into the WiFI network without password during the next 150 seconds. Once done correctly your PC will remember and login automatically in the future.

Note:

Pressing less than 1 second the button “Wifi/WPS” will disable the WiFI network. Press again to enable it back. This functionality is used by many people that want to turn off the WiFI at night time for security reasons, or even to save electric power consumption.

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

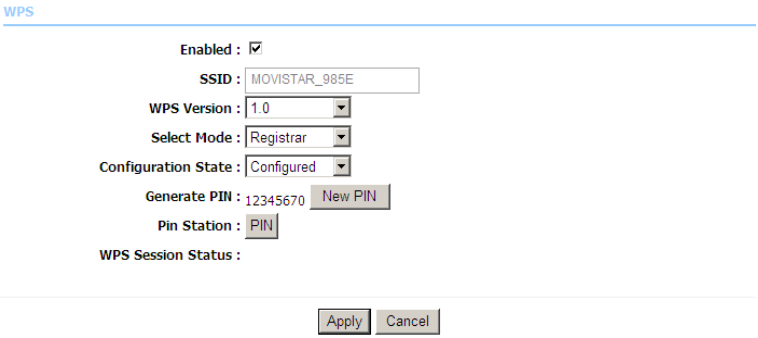


The following table describes the parameters of this page.

Field	Description
Enabled	To enable WPS function and be able to set the following settings.
SSID	The name of your wireless network.
Select Mode	Select the mode either **Registar** or **Enrollee**. – **Registrar**: the router will act as a credentials server and will permanently accept incoming connections with a PIN introduced at the client PC side. – **Enrollee (default)**: when PC tries to connect, you need to enter the PIN (or press button) on the router side. This avoids hacking attempts.

Field	Description
	When a router is in Registar mode, the client should be in Enrollee mode, and vice versa. Keep reading for more info on “Registrar” mode.
Configuration State	When **Configured** state is selected, wireless parameters (for example, the encryption password) are provided by the CPE in WPS negotiation. When **Unconfigured** state is selected, wireless parameters are provided by the connecting user end (for example, PC).
Push Button	Press the button, the CPE will connect the station automatically without password.
Input Station PIN	You need to enter the PIN of the enrollee. If the router is in “enrollee mode”, you can press the “PIN” button and the router will generate one valid PIN for you. Not all PIN numbers are valid.

When **Registrar** mode is chosen, the following page appears. In this condition, only PIN button can be used.



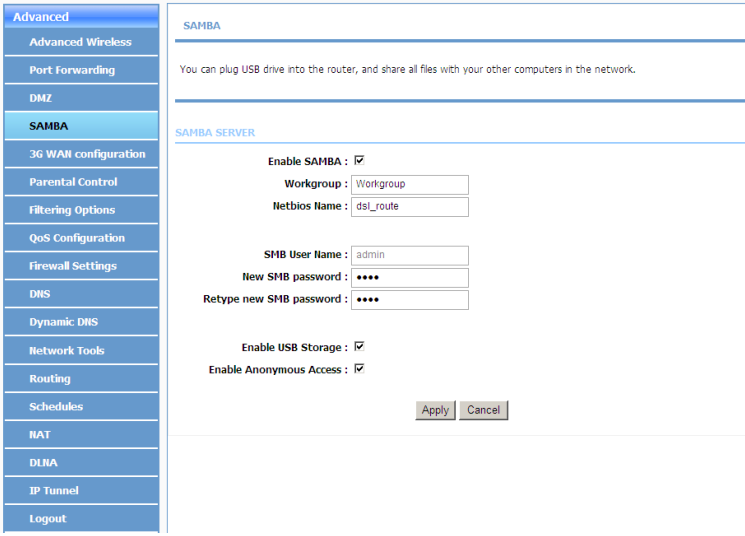
The following table describes the parameters of this page.

Field	Description
Generate PIN	Press the button to generate a PIN number that the client PC must know. Because PIN testing can be attacked, only 10 attempts are allowed.
PIN Station	Press the button to connect the station with the pin.
WPS Session Status	Display the session status.

3.2 SAMBA file share

SMB or SAMBA is a well known protocol for sharing files over your private network. You can plug one or more USB hard drives/pen drives into the router and share it with all your devices (Smart TV, computers, etc). If necessary you can use a USB hub.

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



The following table describes the parameters.

Field	Description
Enable SAMBA	Select the check box to enable this service
Workgroup	Enter the name of your home network (LAN). Default by windows is “Workgroup” and all computers are placed inside.
NetBIOS Name	Enter your NetBIOS name. The router will be listed in the above “workgroup” with this name.
New SMB password	Enter your password to access the files.
Retype new SMB password	Reconfirm your above password.
Enable USB Storage	Select the check box to enable USB storage.
Enable Anonymous Access	Select the check box to allow anonymous users access. The password will NOT be required. This is the default option.

Click **Apply** to save the settings.

Plug your USB memory drive firstly into the router, so that your computer can detect it after one minute.

Note:

There are three ways to access the shared files on the USB port:

1) Open the “start menu” and select “run”. Paste the following address and press OK: \\192.168.1.1\

2) On your keyboard, hold down the “Windows Logo Key” and press letter “R” (Win+R). Paste the address and press OK: \\192.168.1.1\

3) Find the network icon on your desktop. On the left click view workgroup computers, and find the “dsl_router”.

3.3 Port opening

The following section explains the difference between “uPnP”, port forwarding and port filtering. The first two are used mainly for a NAT scenario, while the latter is used normally when NO-NAT takes place.

3.3.1 Automatic uPnP

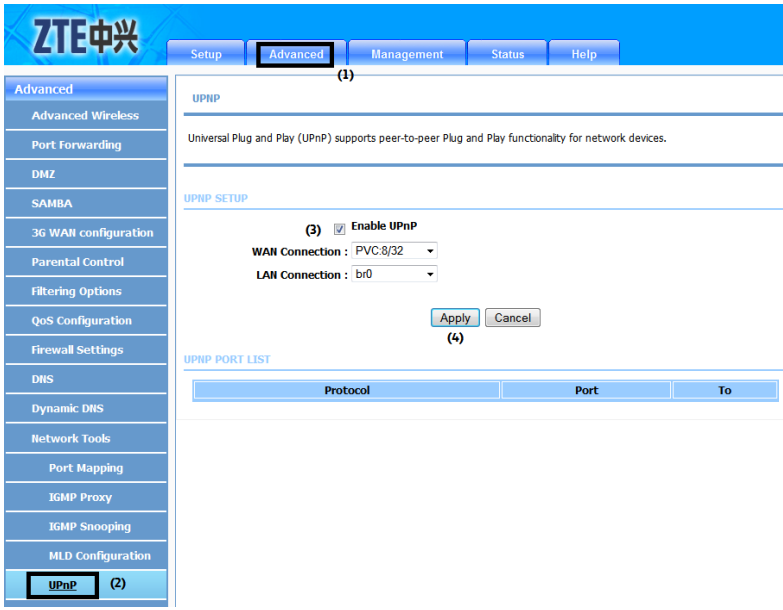
If you enable the *Universal Plug and Play* function in the router, any compatible application that requires opening any port will work automatically. With this option enabled, you don’t need to worry about port opening.

For example modern videogames (Xbox, PlayStation, Nintendo, etc) and downloading software (torrent, emule, etc) currently support from factory this way of working.

This option comes disabled in your router, and it is secure to enable it because it will only attend internal LAN queries.

When enabling the uPnP, please make sure you select the proper WAN connection that is active at home. If you have multiple items, you can check which one is working for you in the upper menu “**Setup > Internet Setup**”. The list will display status as “connected” (most probable it’s 8/32).

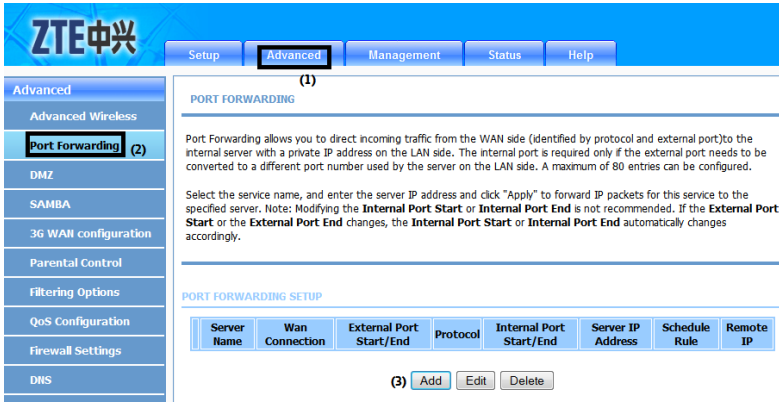
To enable the uPnP, refer to the menu **Advanced > Network Tools > UPnP**:



3.3.2 Port forwarding

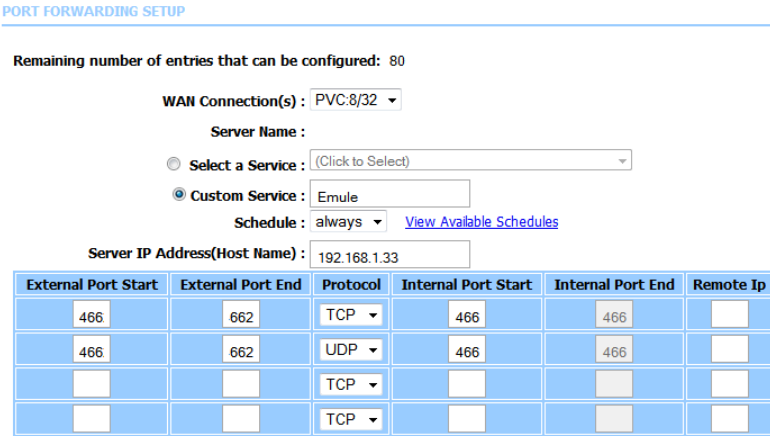
You can open manually the ports in the router. It is necessary that your device (computer, videogame, etc) has a static/fixed IP address.

Please note: the (possibly empty) list of forwarded ports that you will find is NOT synced with the “easy configuration user portal“. The ports that you open in one of the web portal cannot be seen on the other web portal.



There is a list of pre-selected services that you can select easily (Kazaa, Quake, MSN, Yahoo messenger, FTP, etc). Otherwise you can write your own service name and specify the desired ports.

Please make sure you select the proper WAN connection where the port will be open (probably 8/32). If you have multiple WAN connections, you can check which one is working for you in the upper menu "**Setup > Internet Setup**". The status will list as "connected" (8/32 or 8/36 or 8/35).



3.3.3 Port filtering

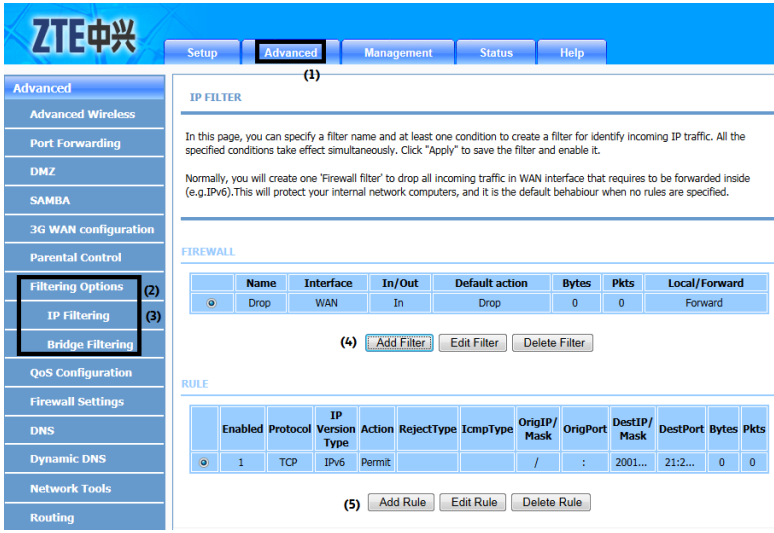
When there is no private NAT in your network because all your computers have public IP, like it may happen with IPv6, then there is no need to “port forwarding”.

Instead you should allow the incoming traffic passing through the router, by the “port filtering” function. By default no traffic is allowed to come into your network for security reasons, but if you start creating rules this behavior may change.

For this reason we recommend you create a firewall filter to “drop” everything, and then add any exception rule that you wish (like allow incoming traffic to some public IP or to port 21). Currently only some operating systems fully support IPv6, starting at Windows Vista.

Normally this scenario (“no-NAT / port filtering”) does not happen at home internet users yet, and you should not worry about this configuration.

If you cannot configure this function due to with an “invalid value!” error, please use Internet Explorer in its latest version and repeat the operation.



3.4 Other options

This guide describes the most used functions in a user-friendly way.

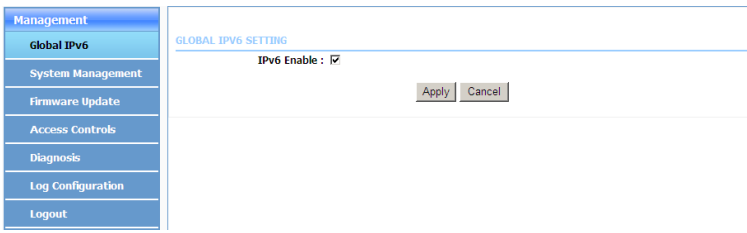
Please refer to the full guide for all available options.

4 Management section

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure.

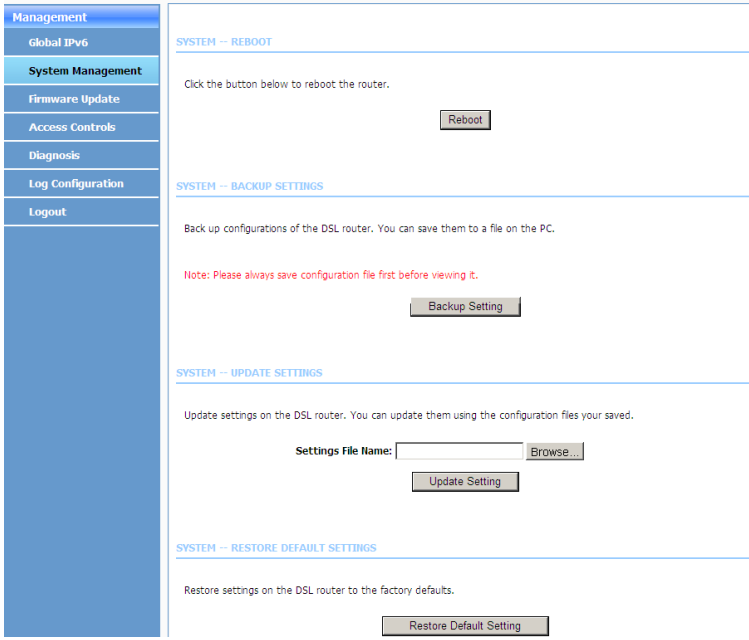
4.1 Global IPv6

Choose **MANAGEMENT** > **Global IPv6**. The page shown in the following figure appears. In this page you can enable or disable IPv6 function.



4.2 System Management

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



In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.
The buttons in this page are described as follows.

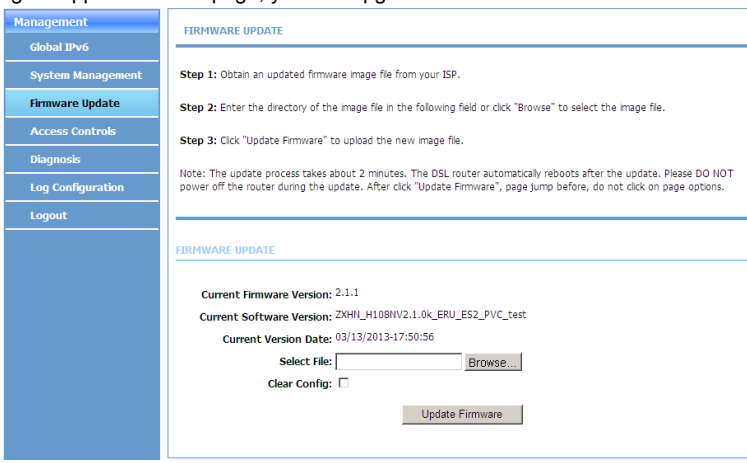
Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.

Update setting	Click **Browse** to select the configuration file of device and then click **Update Settings** to begin updating the device configuration.
Restore Default Setting	Click this button to reset the device to default settings.

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

4.3 Firmware Update

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



To update the firmware, take the following steps.

Step 1 Click **Browse…**to find the file.

Step 2 Select **Click Config**.

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

The device loads the file and reboots automatically. If you checked the “clear config” option, the router will revert to factory settings, which is the proper configuration for your Internet Provider (printed on the case of the router).

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

Note:
The H108N V.2.1 has built-in a dual bank memory. After the reboot the “Internet LED” will blink green/red for some minutes while it upgrades the secondary bank. It is recommended to wait until finished.
This secondary bank helps boot when the main memory is corrupted somehow or wrong upgrade (detected by wrong CRC).

5 Hardware notice

The H108N V2.1 supports multiple line modes. With four 10/100 base-T Ethernet interfaces at the user end, the device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users like net bars and office users. It provides high performance access to the Internet with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps. It supports 3G WAN, 3G backup, Samba for USB storage and IPV6.

The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security. The WLAN of the device supports 2T2R.

5.1 Safety Precautions

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

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.

- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

5.2 System Requirements

- A 10 baseT/100BaseT Ethernet card is installed on your PC.
- A hub or switch when several PCs attached through one of Ethernet interfaces on the device
- Internet Explorer 7 or higher, Chrome 1.0, Firefox 1.5 or higher.

5.3 Features

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade: Web, TFTP, FTP
- Reset to the factory defaults
- DNS relay
- Virtual server
- DMZ
- Two-level passwords and user names
- Web user interface

- Telnet CLI
- System status display
- PPP session PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management (telnet and HTTP)
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP
- IPV6
- 3G WAN and 3G Backup
- Samba sharing for USB storage