Contents

Router Login

To log into your router, open a web browser (for example, Google Chrome, Microsoft Edge, Mozilla Firefox etc.). Type **192.168.1.1** in the address bar of the browser. You should then see a login page (Image 1). In the Username field, type “admin”. In the Password field, type the password shown on the sticker on the back of your router. Once all fields are populated, press **Login**.

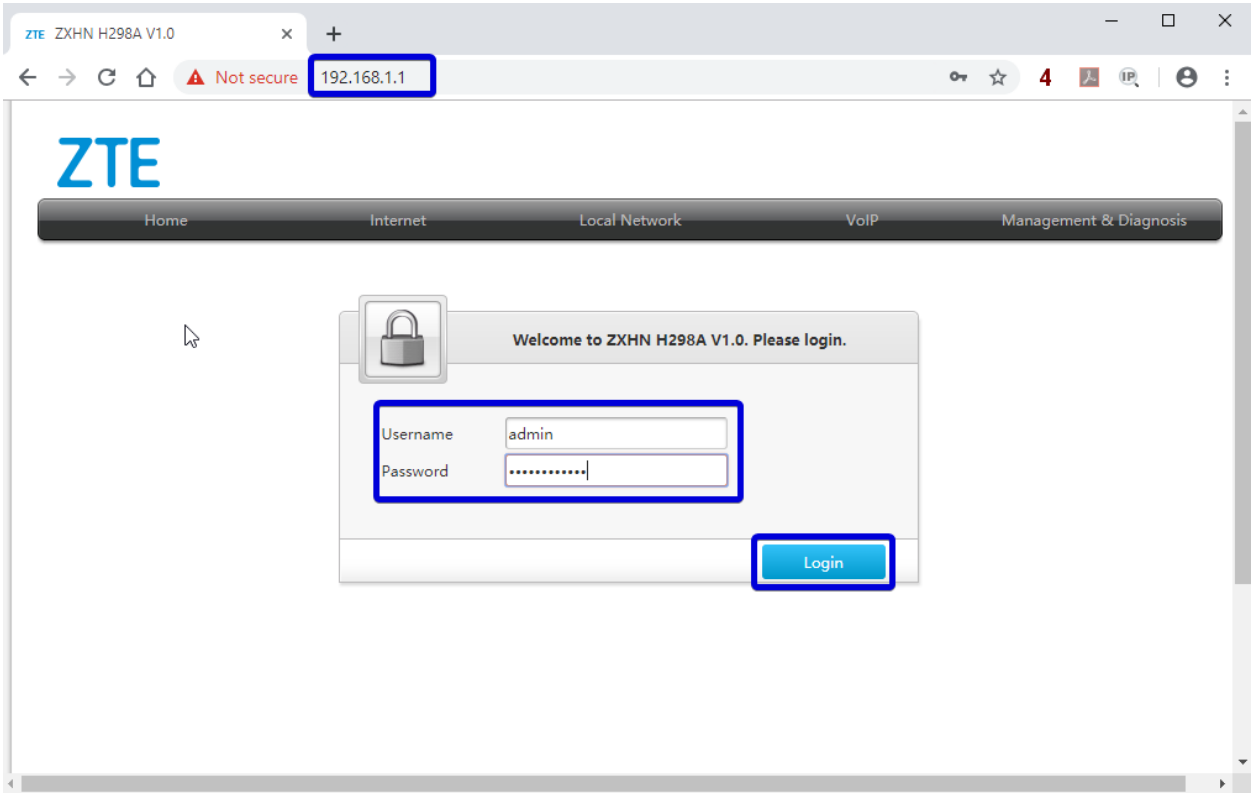


Image 1. Router H298A login screen

Change of DNS

Your DNS properties can be changed for local LAN clients. To change, you'll need to follow these steps, and then call Hyperoptic Customer Support to complete the final step.

To change your DNS, please log into your router (page 2) and navigate to **Home > LAN Devices**. Click on **LAN Settings**. See Image 2.

By default, the router uses two Hyperoptic DNS servers which provide redundancy and address resolution. These servers communicate directly with the WAN ethernet router port and provide means for swift browsing.

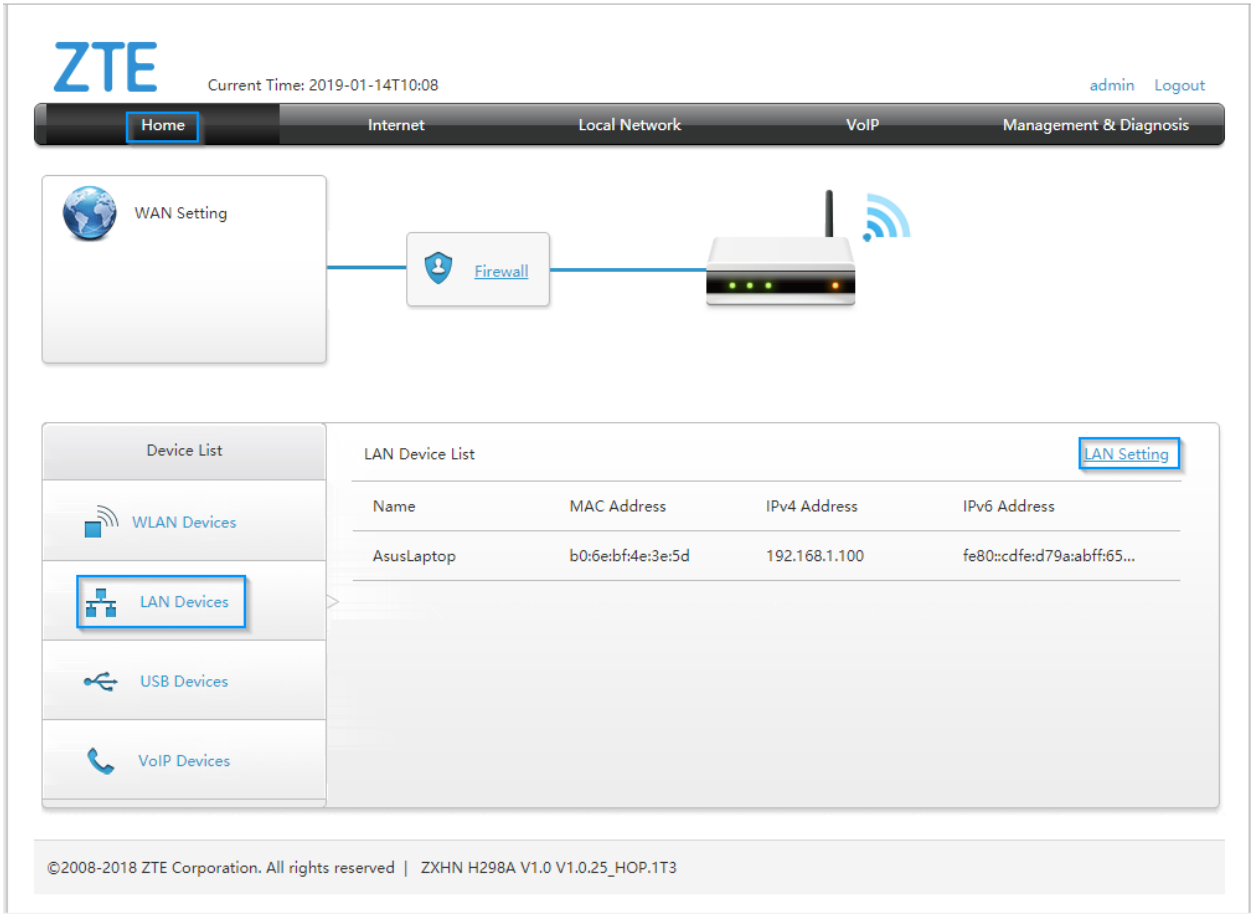


Image 2. Section of LAN Settings

Click on **DHCP Server** and edit **Primary DNS** and/or **Secondary DNS**. See Image 3, where DNS server with IPv4 address 8.8.8.8 is used. Click **Apply**.

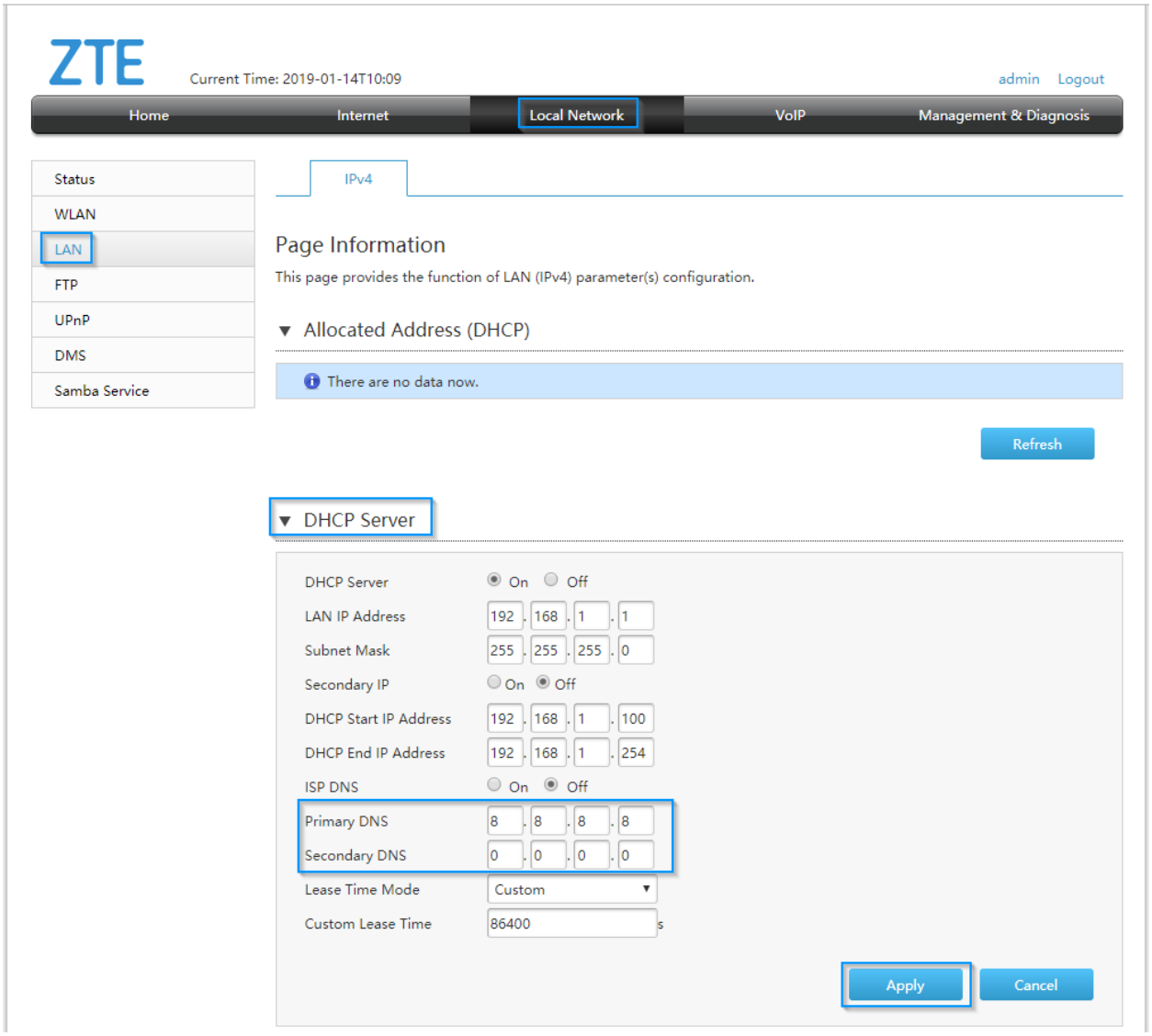
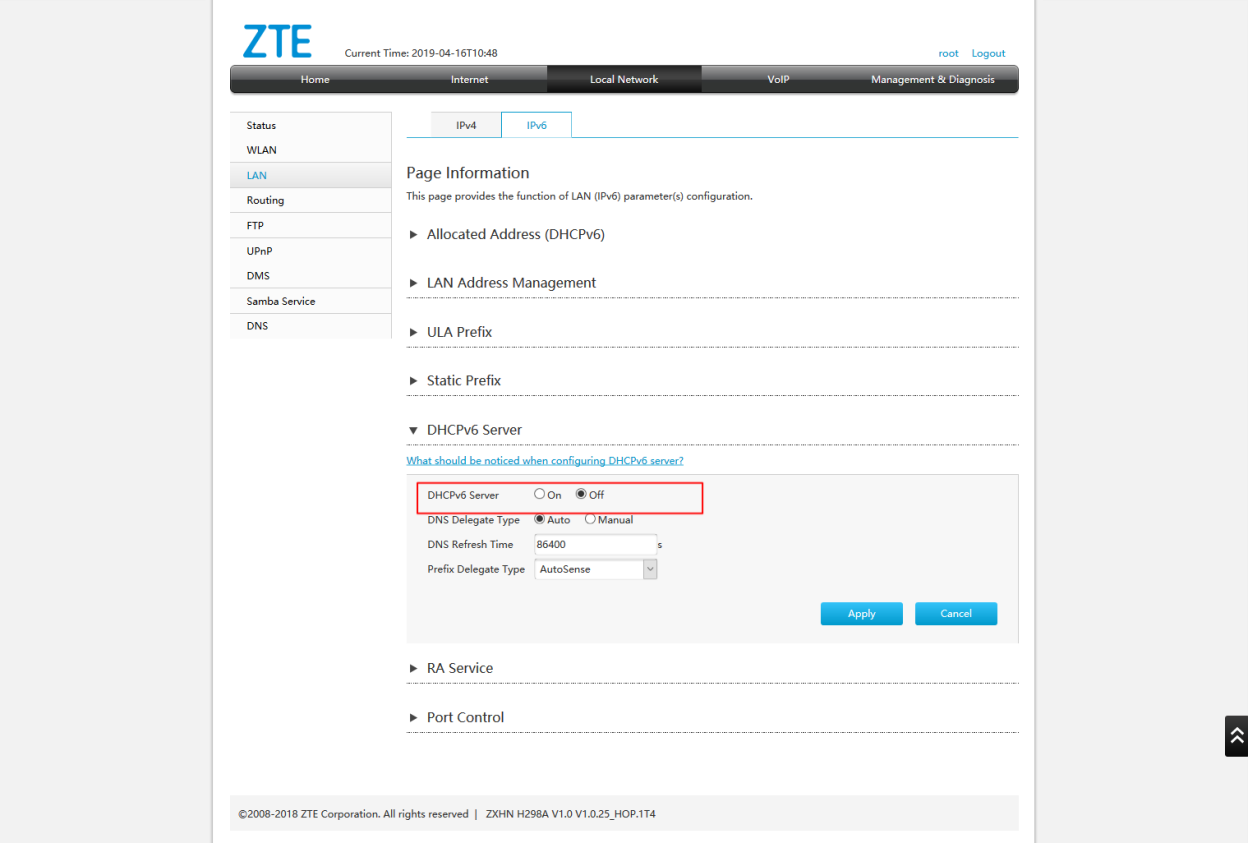


Image 3. DNS change section of router configuration

To complete the DNS change, please **call Customer Support** who will perform the final step for you.



3.a Disabling DHCPv6 server on LAN

UPnP router configuration

To configure your router using LAN UPnP applications, please log into your router (page 2) and navigate to **Local Network > UPnP**. Click **On** to activate UPnP service. Click **Apply.**

See Image 4, where UPnP is used to configure port forwarding. If you're not using UPnP applications, UPnP should be set to **Off** (the default UPnP setting is Off).

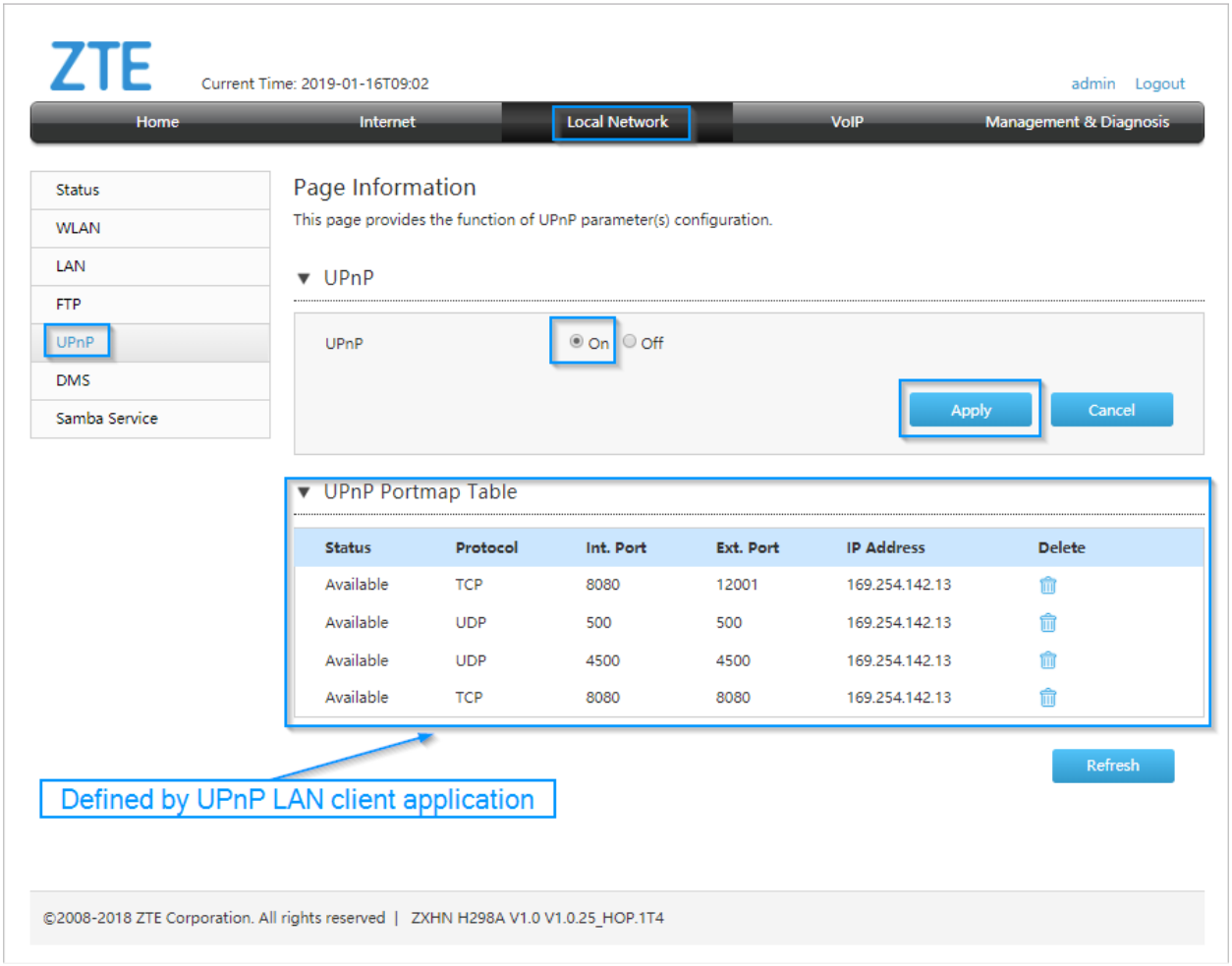


Image 4. Enabling UPnP

Parental control

Parental control can be used to restrict access to sites. To enable parental control, please login to your router (page 2) and navigate to **Internet > Parental Controls**. Click on **Parental Controls**. Name your parental control rule and, under **User Identity**, provide the **MAC address** of the LAN client for which internet service should be blocked.

Choose the day and time during which access should be restricted and provide any keyword or URLs

you would like to block and click **Apply**. See Image 5.

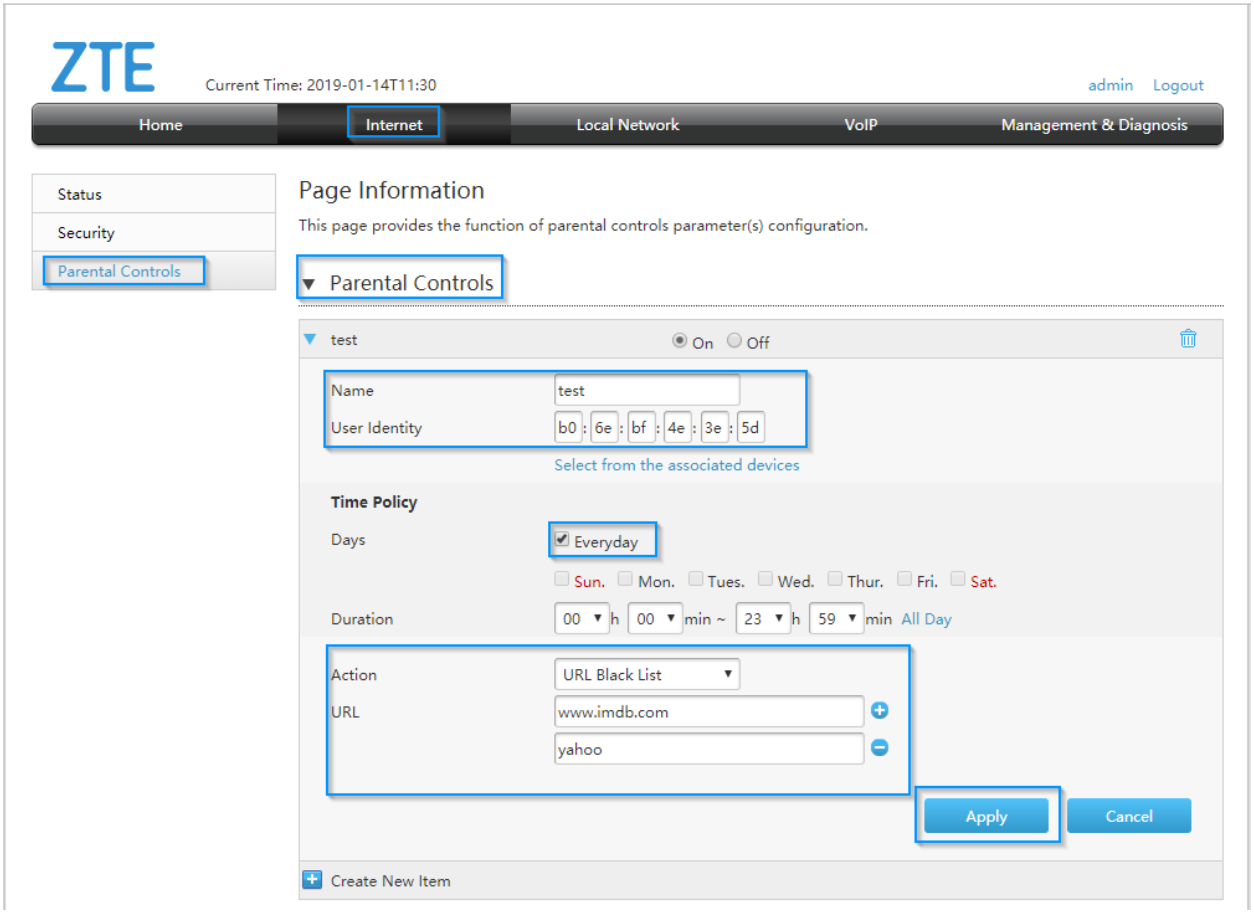


Image 5. Example of traffic blocking to Yahoo and imdb

Please note that parental control won't filter any website which contains https in the address bar (e.g. https://www.youtube.com). This means it will only filter websites with http (e.g. http://www.yahoo.com)

LAN clients

The number of LAN (Local Area Network) clients, their MAC addresses and associated IPv4 addresses can be checked once you're logged into your router (see page 2). Navigate to **Local Network > Status > WLAN Client Status** and **LAN Client Status**. See Image 6.

Here you'll be able to see all the devices connected to your Wi-Fi and Ethernet network.

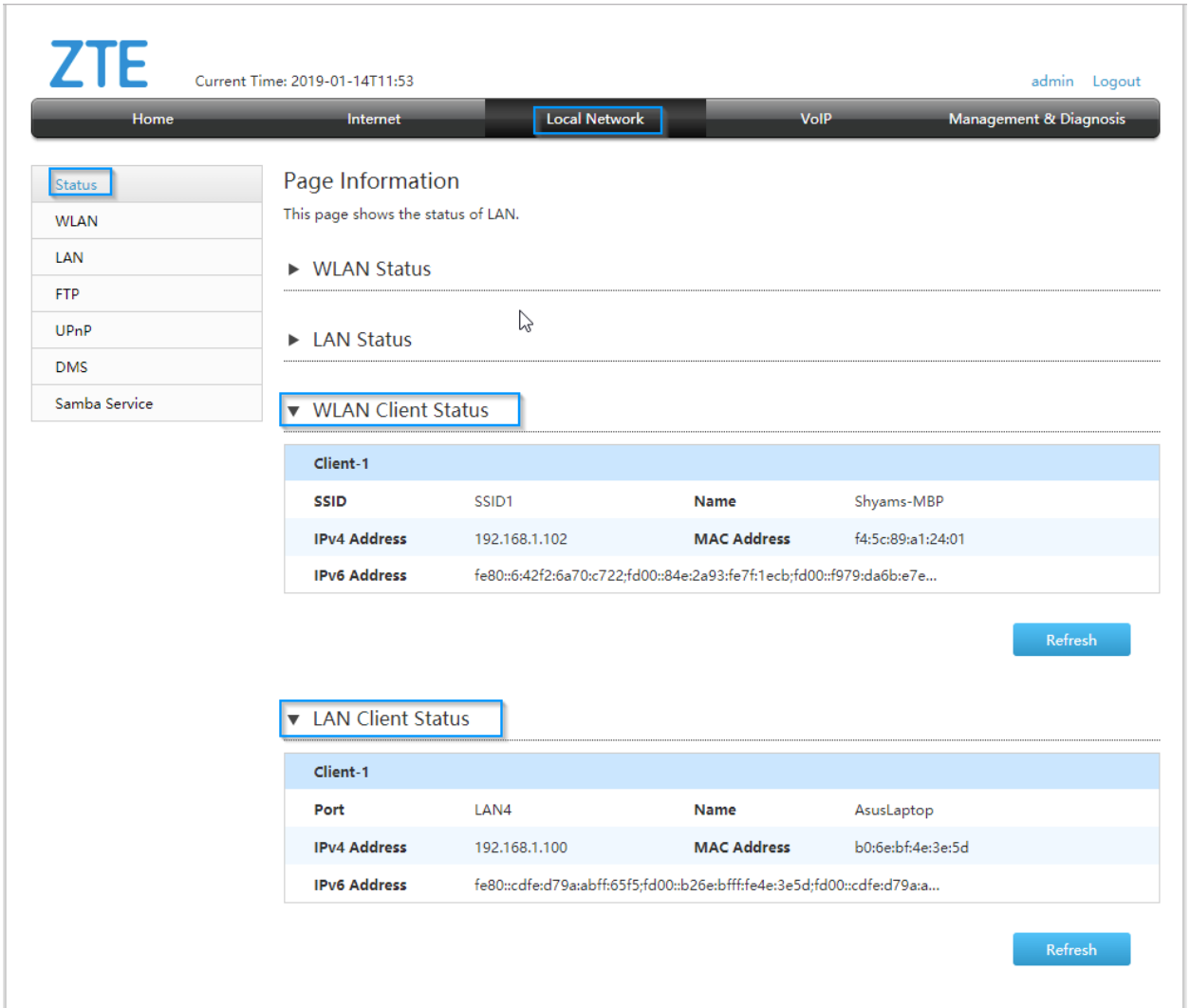


Image 6. List of WLAN and Ethernet LAN clients

When moving your mouse over IPv6 addresses, all IPv6 addresses will be shown inside a yellow/white comment box.

Wi-Fi password and SSID change

To change your wifi password or SSID name, log into your router (see page 2) and navigate to **Local Network > WLAN > WLAN Basic > WLAN SSID Configuration**. See Image 7.

You can then choose the SSID name and WPA Passphrase. Please use passwords containing upper and lower-case letters and numbers, with a minimum of 12 characters in length. Once changed, click

Apply.

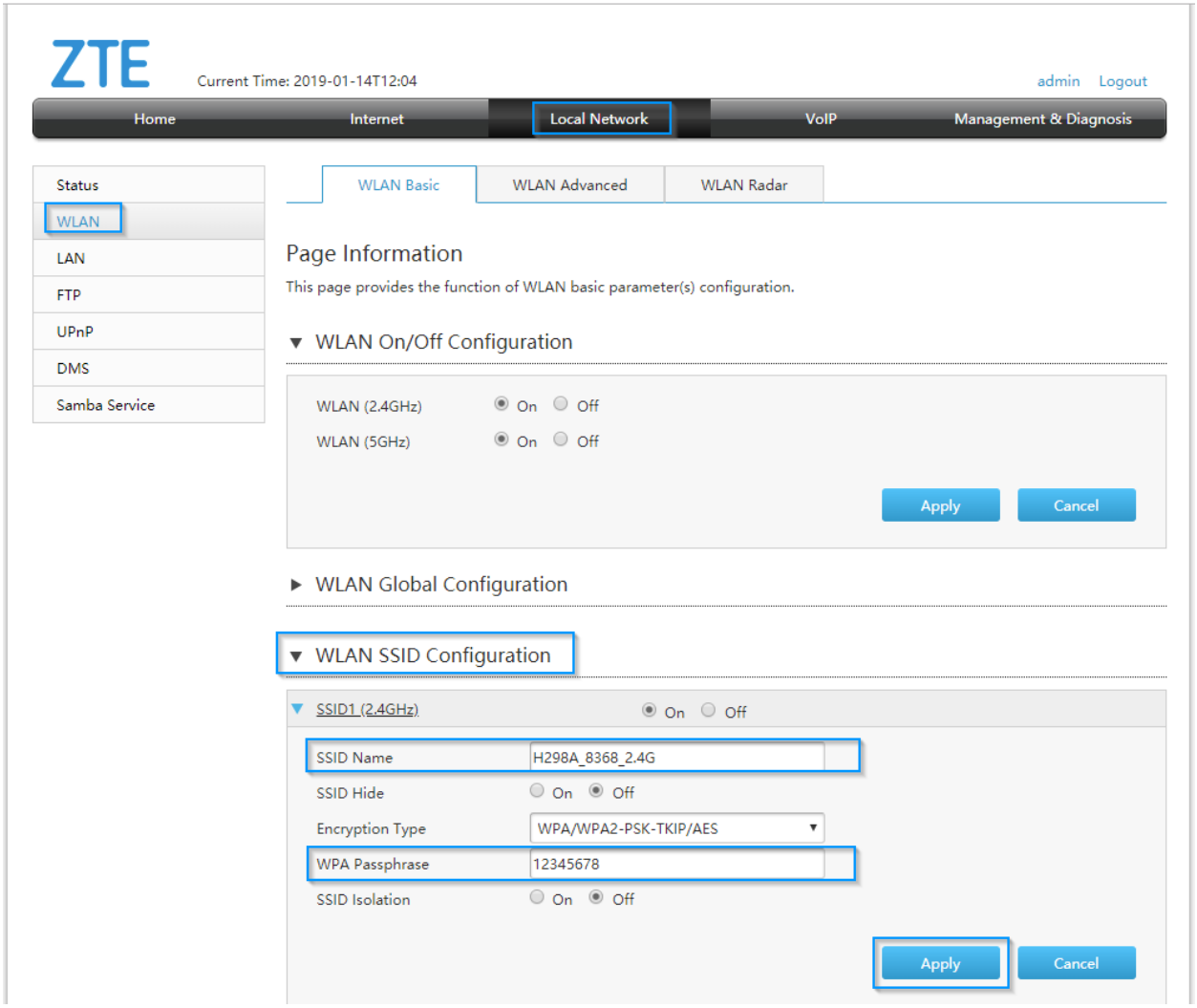


Image 7. Configuration of 2.4GHz Wi-Fi parameters

Please note, it's highly recommended to use only WPA2-PSK-AES for 2.4GHz and 5GHz.

Configuration of 5GHz wifi parameters is described in Image 8. Again, SSID Name and WPA Passphrase can be chosen by you. Once changed, click **Apply**.

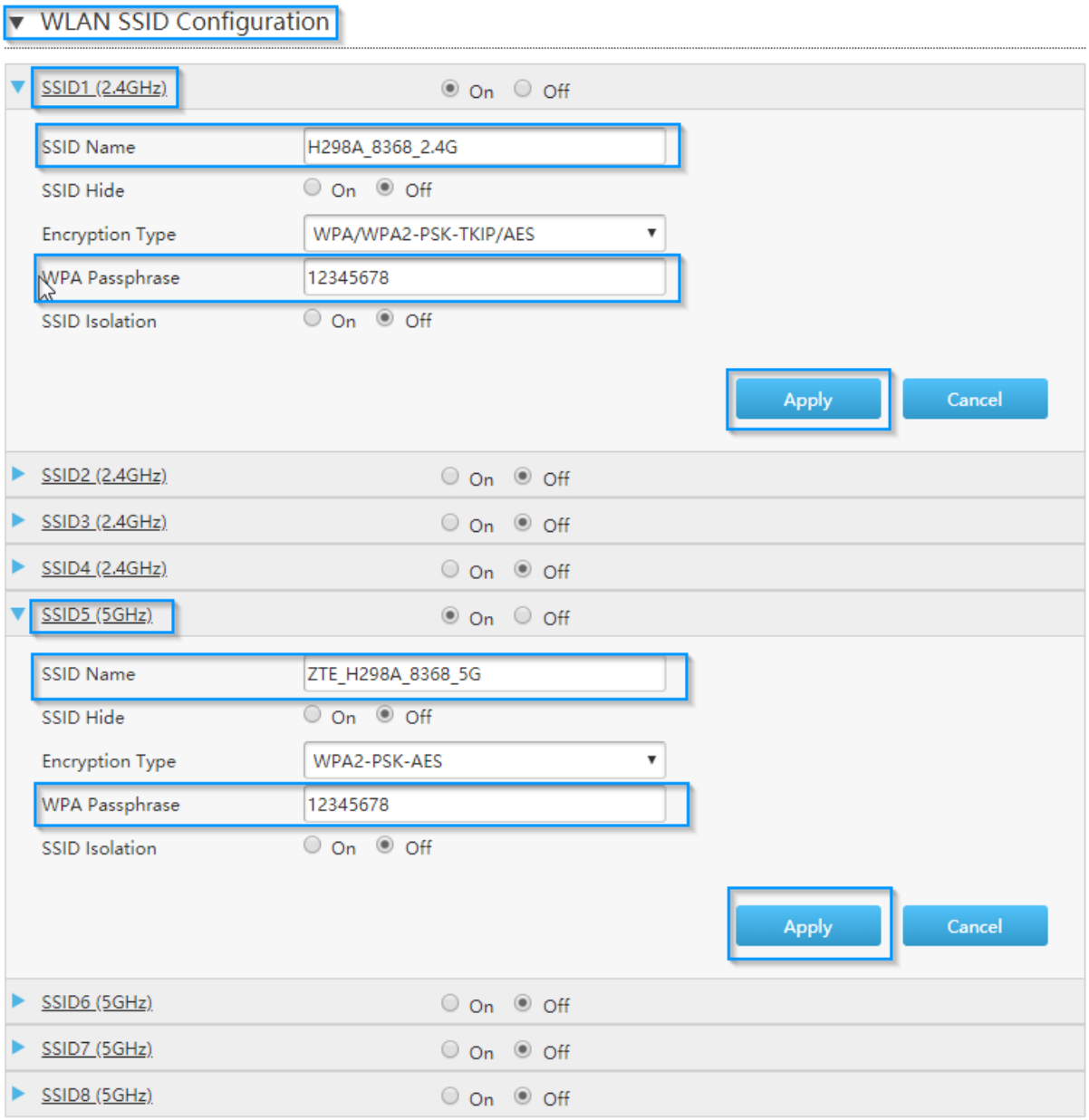


Image 8. Configuration of 5GHz Wi-Fi parameters

Creating, disabling and changing settings for SSIDs

To create a new SSID, log into your router (see page 2) and navigate to **Local Network > WLAN > WLAN SSID Configuration**. Enable an SSID by clicking **On**. See Image 9.

If a newly created SSID is enabled, it'll be visible on the Home page.

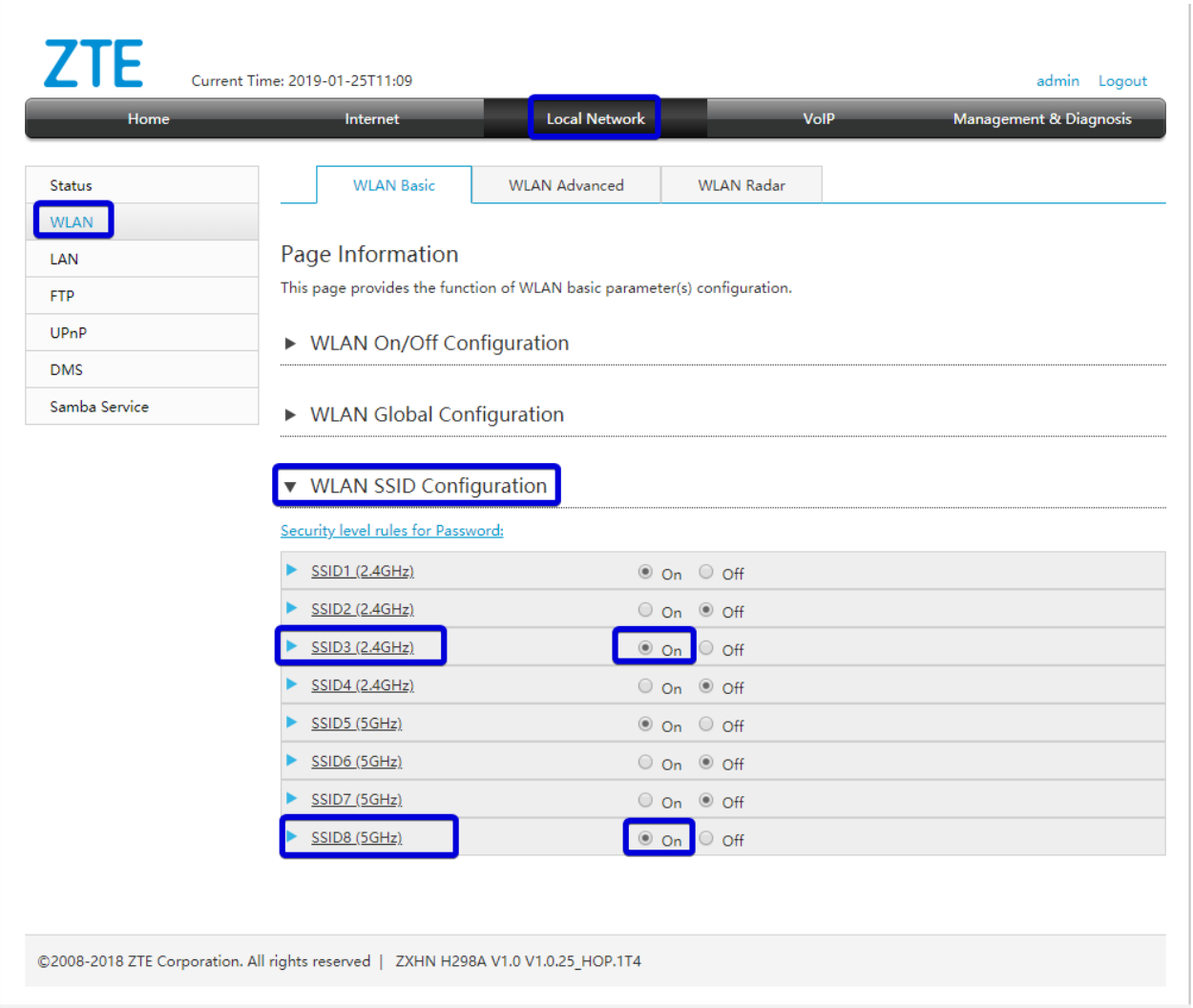


Image 9. Creating new SSID

Once new or existing SSIDs are enabled, you can expand their properties by clicking on the blue triangle. See Image 10. Type your chosen **SSID Name** and supply the **WPA Passphrase** that would be needed for access. Click **Apply**.

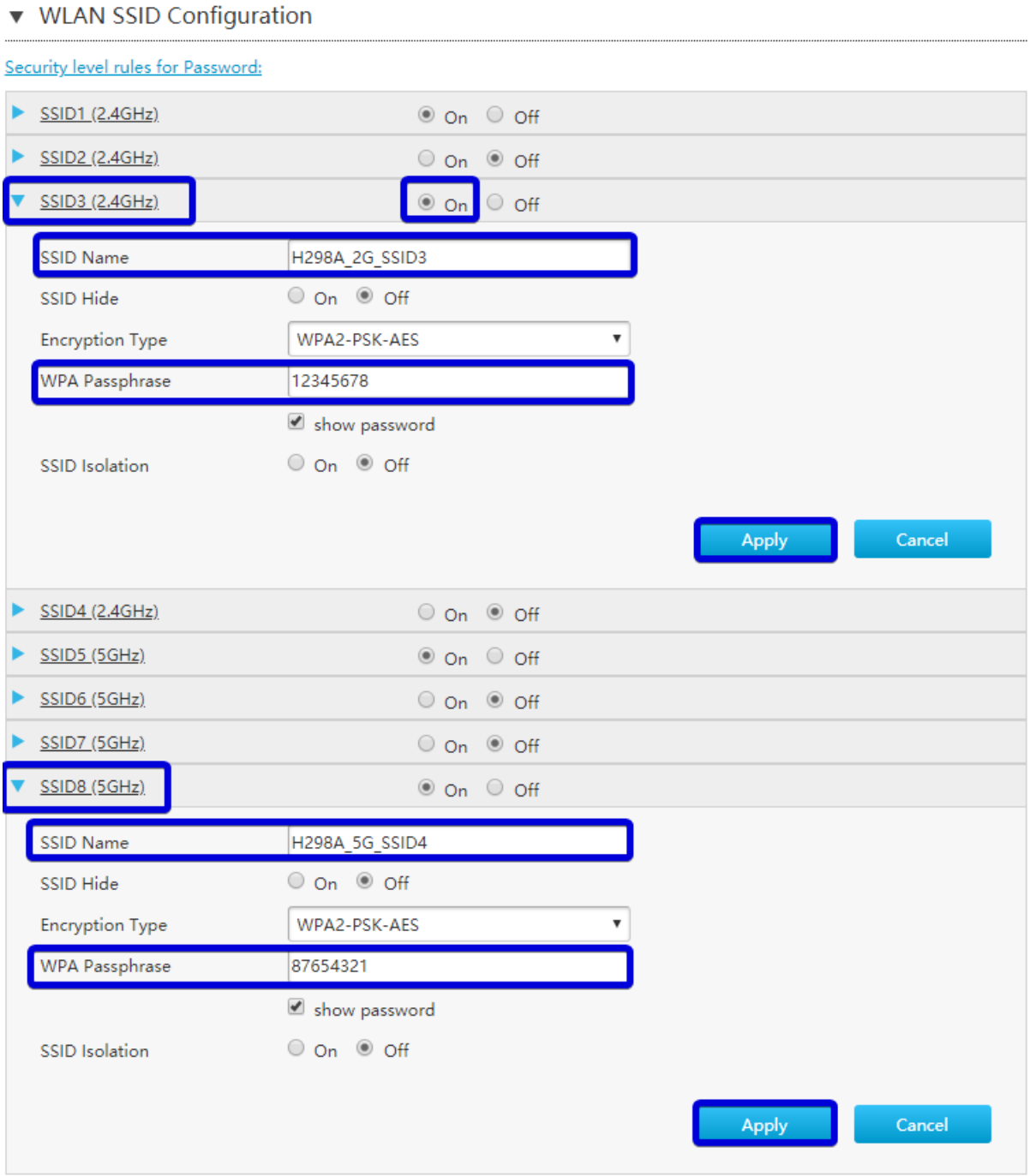


Image 10. Changing SSID Name and WPA Passphrase for new SSIDs

To disable an existing SSID, click the **Off** button associated with that SSID.

Wi-Fi channel change

To minimise interference, we highly recommend leaving your wifi channel selection on its default settings. If you would like to change your channel selection, however, you can do so by logging into your router (see page 2) and navigating to Local **Network > WLAN > WLAN Basic > WLAN Global Configuration**.

Expand properties by clicking on the blue rectangle near the 2.4GHz and 5GHz frequency bands. For 2.4GHz, select **Channel Range of United Kingdom(CH1-11),** select your desired channel and click **Apply**. See Image 11.

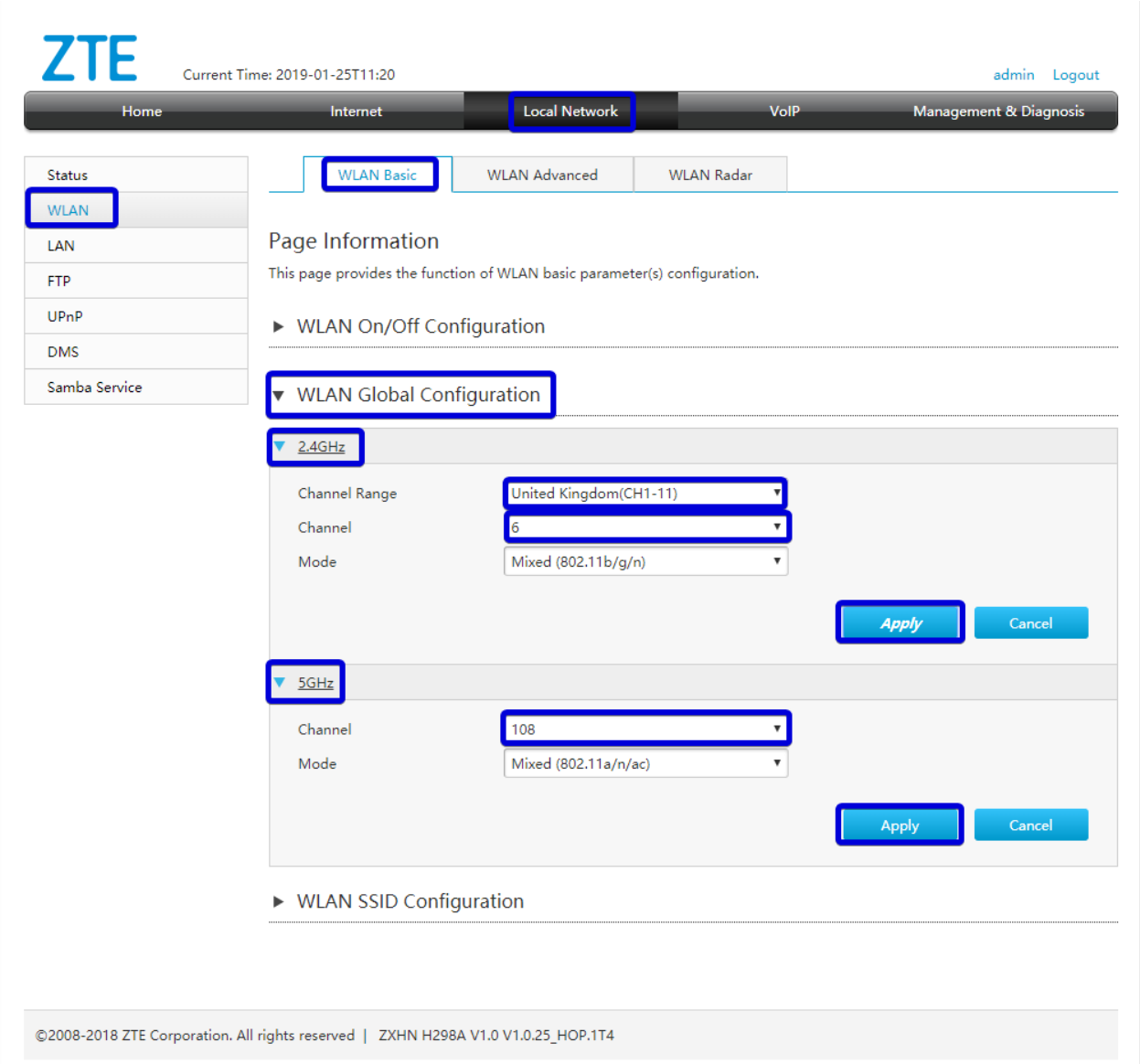


Image 11. Selecting channel for Wi-Fi

Wi-Fi authentication

To change your wifi authentication settings, please log into your router (page 2) and navigate **to Local Network > WLAN > WLAN Basic > WLAN SSID Configuration**. Select **Encryption Type** from the drop-down menu and click **Apply**. See Image 12. By default, advanced encryption algorithm is used. Please note, it's highly recommended to use only WPA2-PSK-AES for 2.4GHz and 5GHz.

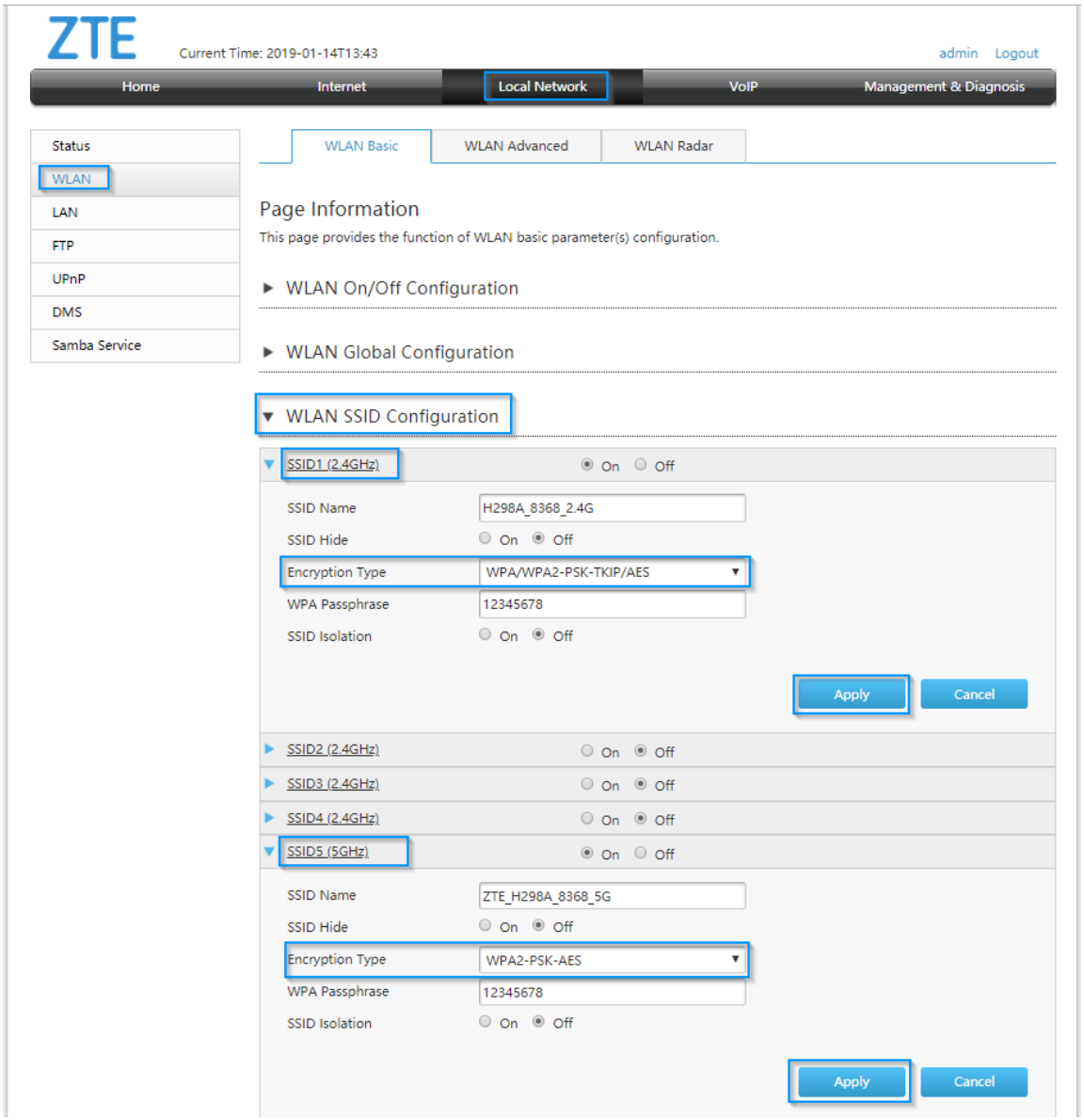


Image 12. Encryption types per SSID

WPS connection

To connect to wifi without a password, press the **WPS** button on the router until the LED light indicates that WPS is active. Once the LED lights green, press the **WPS** button on your LAN device. After a few seconds, the connection will be made.

Change of admin credentials

To change your admin login password, log into your router (see page 2) and navigate to **Management & Diagnostics > Account Management > User Account Management**. See Image 13. You can find the old password on the router itself. Once the new details are entered, click **Apply**.

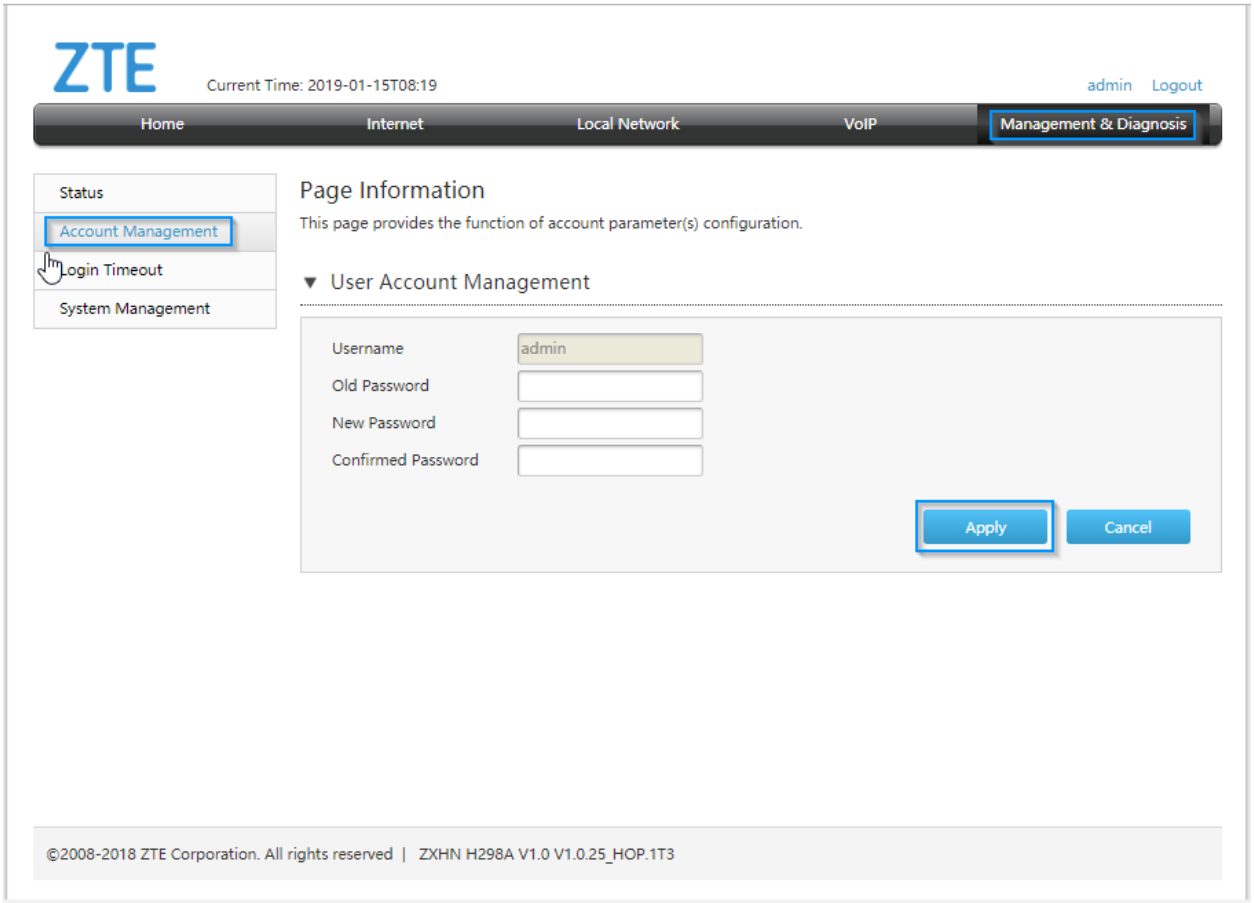


Image 13. Changing old admin password

Reboot and Factory Reset

You can reboot your router or restore it to factory settings by logging in (see page 2) and navigating to **Management & Diagnostic > System Management > Device Management**. See Image 14.

Please note, factory reset isn't recommended as it can shorten the life of a router if used often. Also, factory reset will delete any user-made configuration, such as wifi SSID, wifi password, port forwarding rules, etc.

If you're experiencing significant issues with your connection, we recommend trying a reboot first.

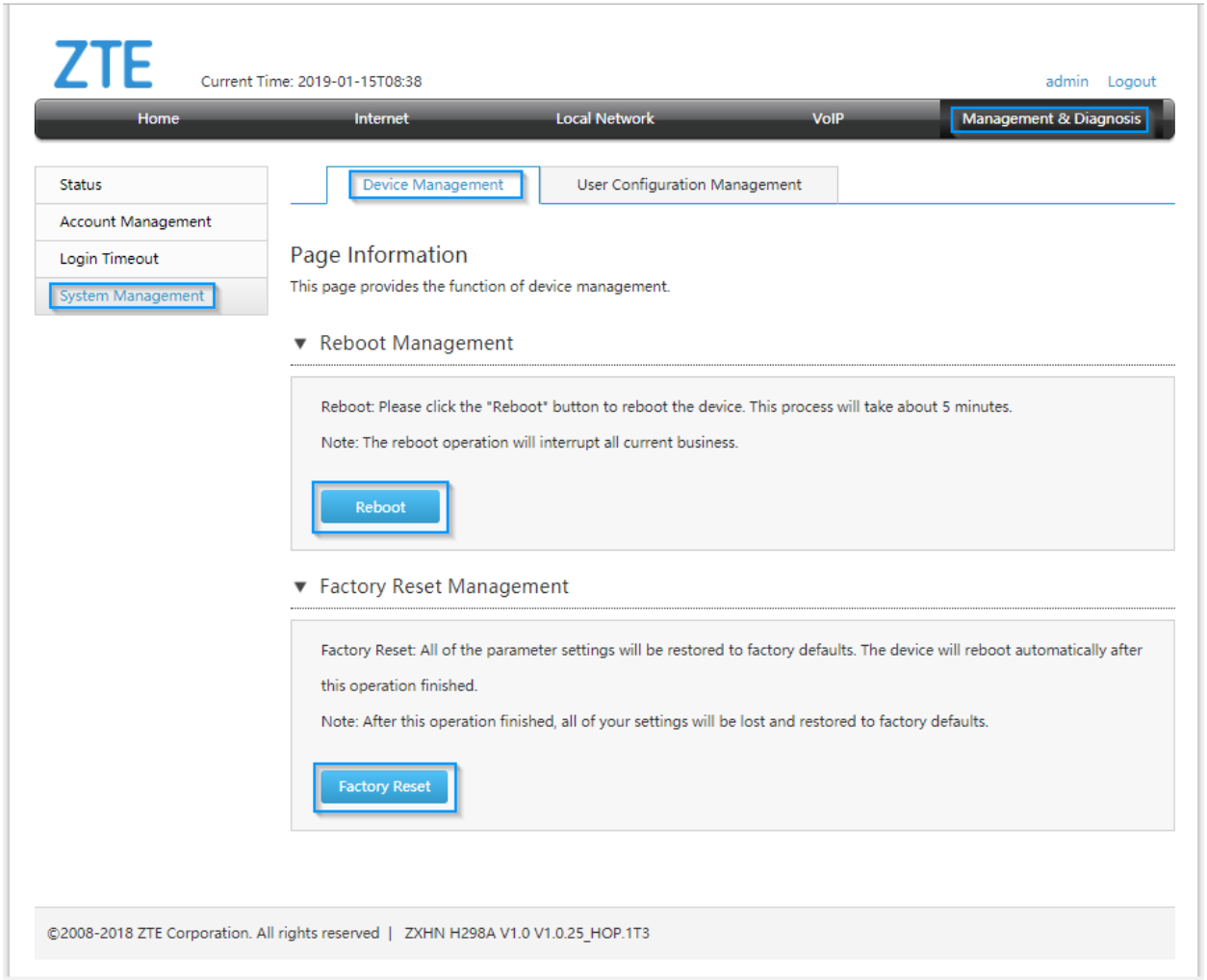


Image 14. Reboot and Factory reset buttons

USB storage

You can access the USB storage port on your router from a LAN client. To grant access to USB flash, please log into your router (page 2) and navigate to **Local Network > FTP**. Enable FTP server and enable security (click **On** buttons). Once enabled, configure **FTP username** and **FTP password** and click **Apply**. See Image 15. Your router's USB port with attached flash drive can be used as additional storage, linked to LAN network.

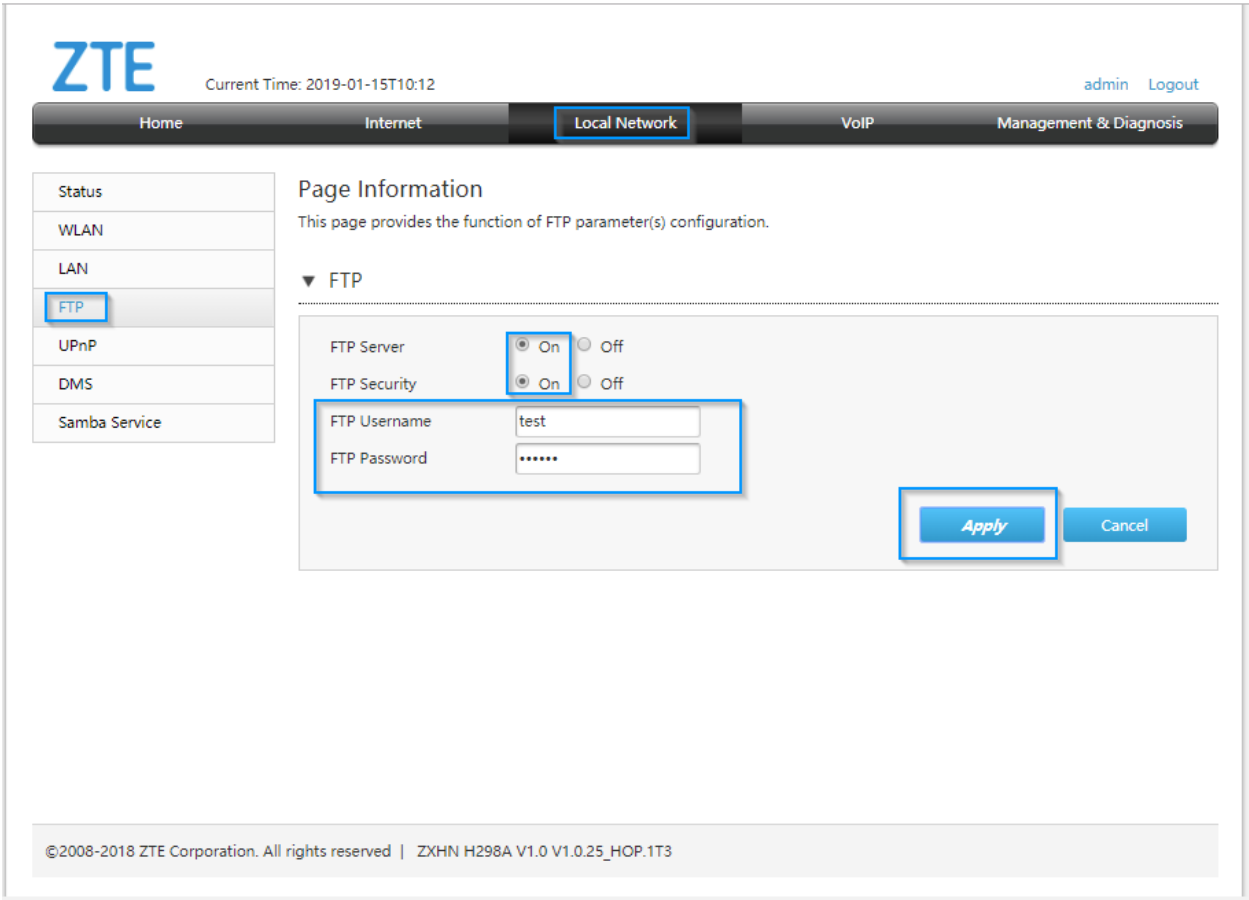


Image 15. Enabling FTP access to USB flash

From local LAN station, access can be performed by typing **ftp://192.168.1.1** in web browser. See Image 16. Using your web browser, it's only possible to download - but if FTP client is used (e.g. FileZilla), upload is also possible.

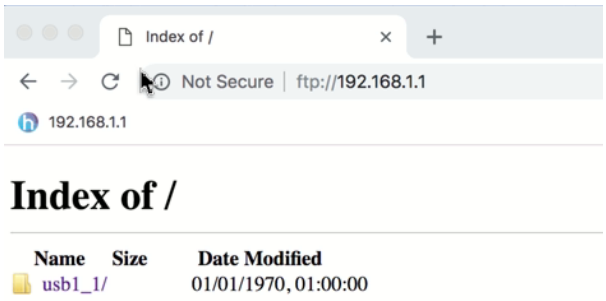


Image 16. LAN access to USB flash drive

Remote FTP access to USB flash drive requires advanced router configuration, and can be done on request.

Access to USB flash drive from LAN can be achieved via Digital Media Server feature. See Image 17. Navigate to **Local Network > DMS**. Click **On** and **Apply**. LAN applications that support DMS will enable access to USB drive (e.g. VLC player, Windows Media Player).

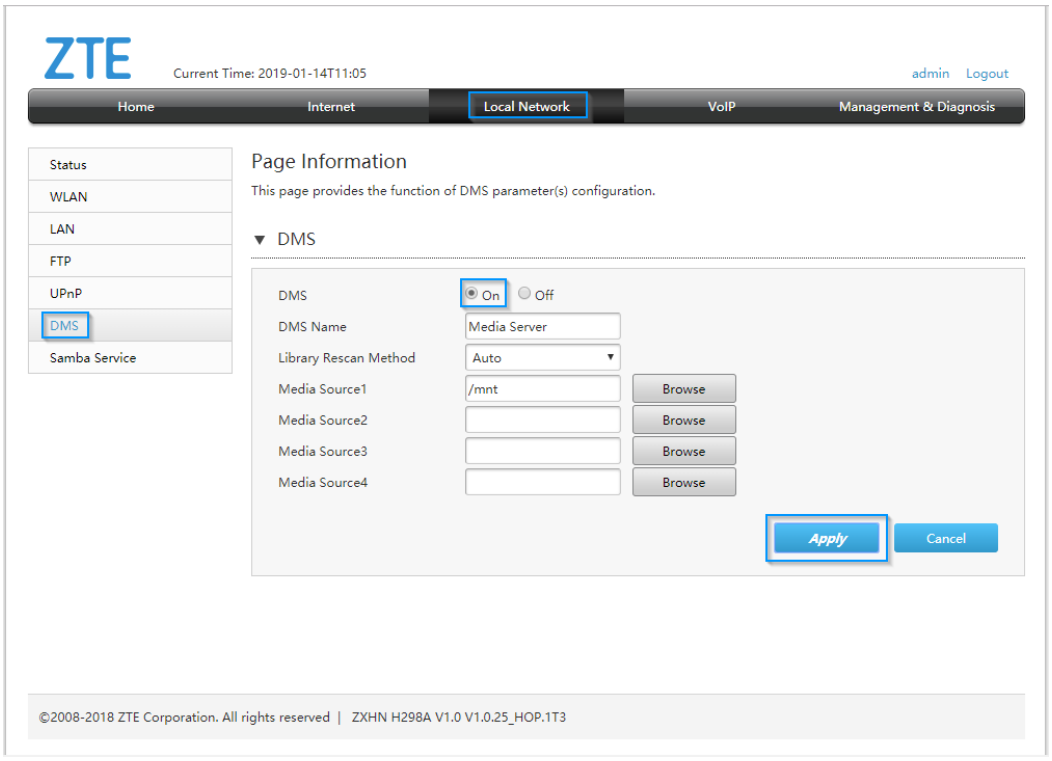


Image 17. Enabling Digital Media Server feature

You can also access USB flash drive from PC application. See Image 18.

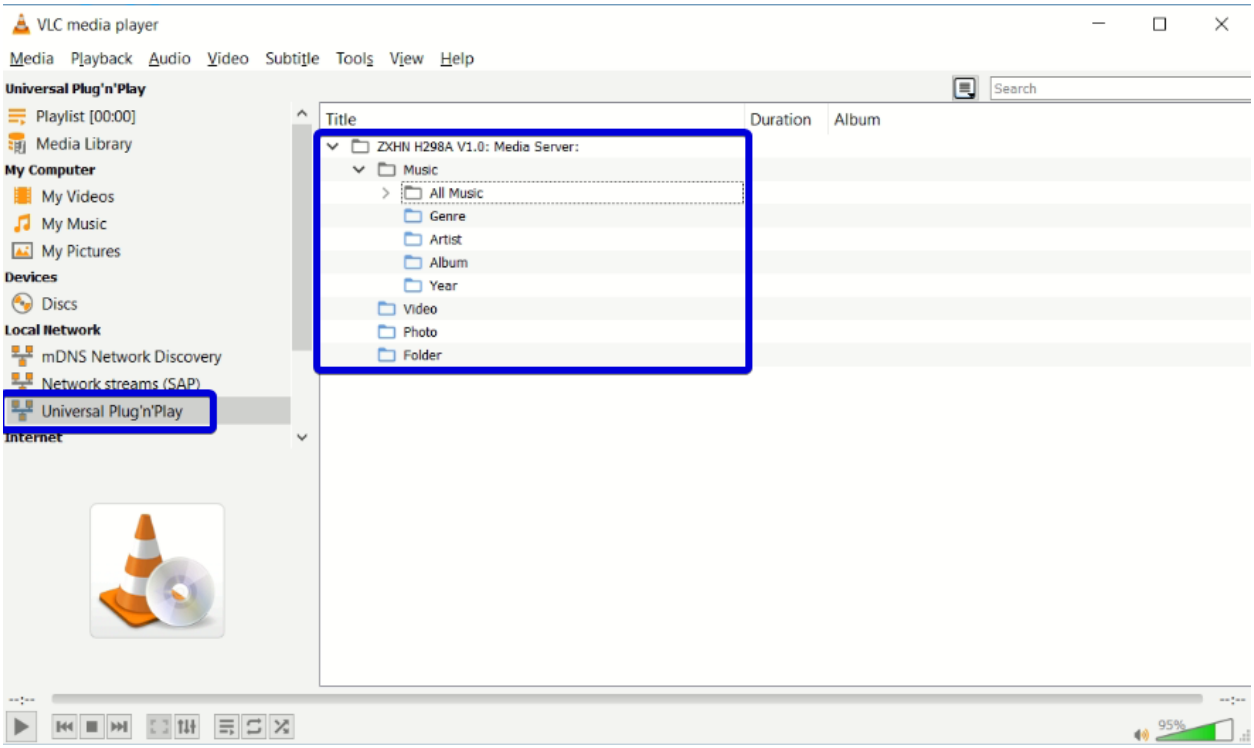


Image 18. Access to USB flash drive from PC application

Port forwarding

Connect your personal computer to the router via an ethernet cable or Wi-Fi. Open a web browser and type **192.168.1.1** in the search line. You should then see a login page, as below (Image 19). Port forwarding can be used to establish home-based FTP server, web server or similar kind of a server.

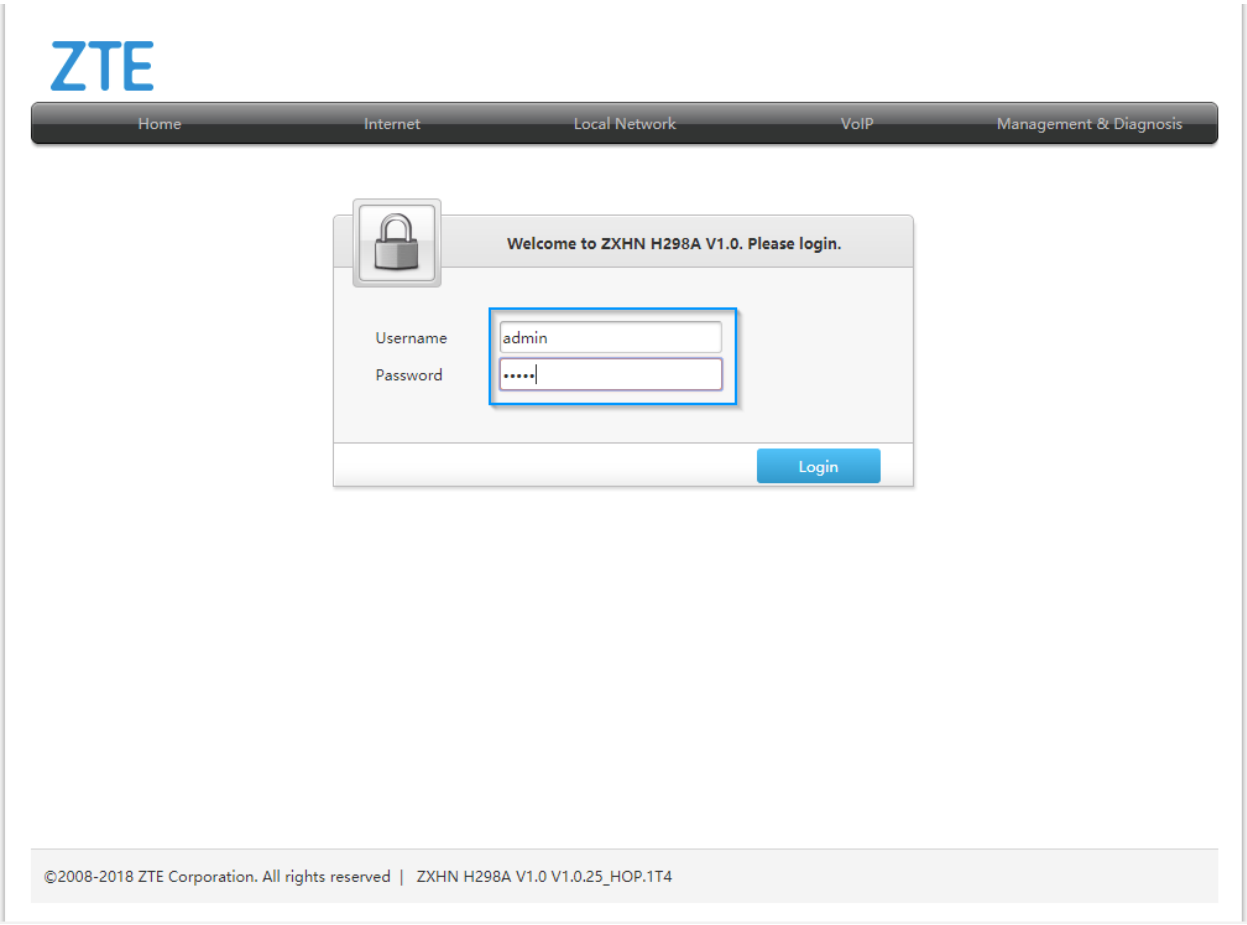


Image 19. Login page of a ZTE H298A router

In the Username field, type "**admin**". You'll be able to find the password associated with your router written on the back of the router itself. Once identified, type this into the Password field.

Once logged in, navigate to **Internet > Security > Port Forwarding**. See Image 20.

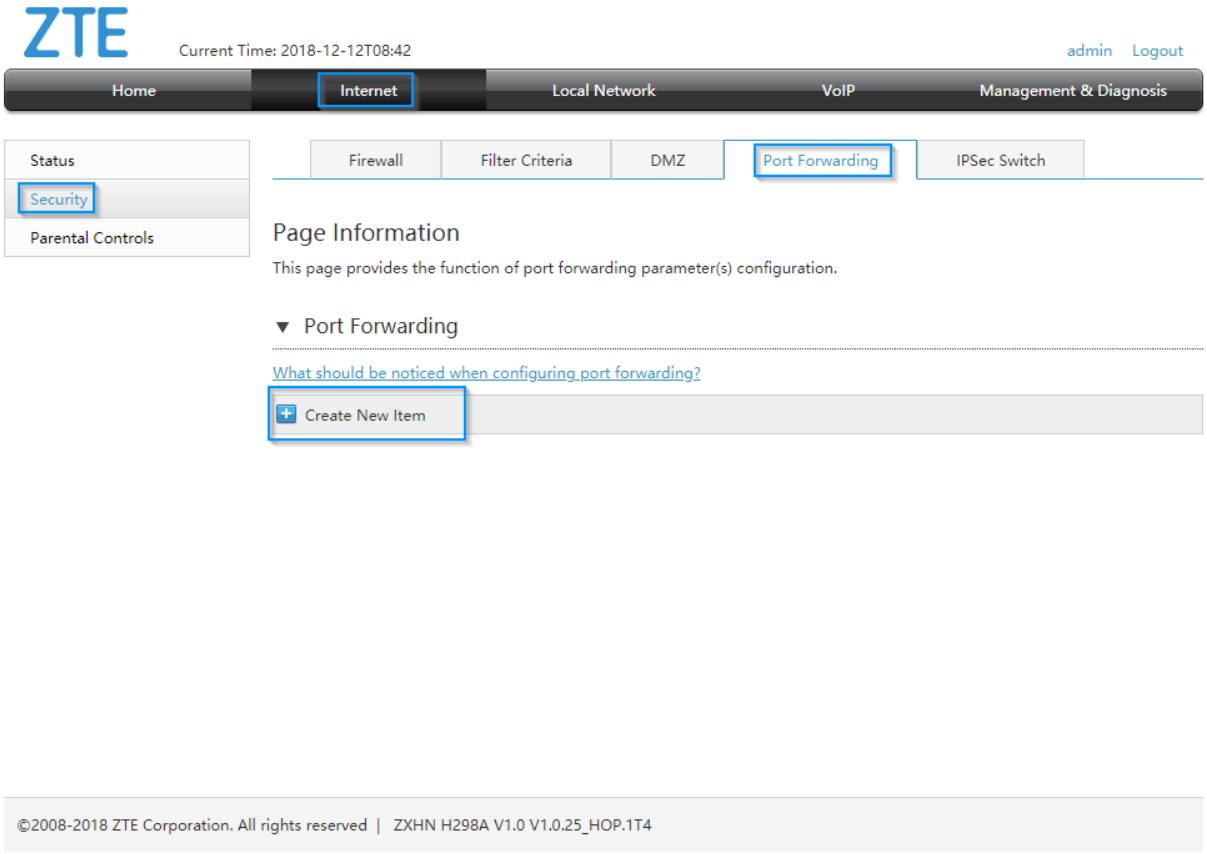


Image 20. Port forwarding section of the router configuration

Click on **Create New Item** to create a new port forwarding rule. This rule will use IPv4 addresses. The new section should appear with all relevant fields that need to be configured (see Image 21).

The **Name field** can be filled in with any name, which will be used to indicate which service is being served.

Select the **Protocol** type (**TCP** or **UDP**).

The **WAN Host IP address** fields can be left unpopulated if local service needs to be accessible from any location on internet (any IPv4 address). In this case, the values in all fields will be **0**.

If access is needed from a specific IPv4 address or from a range of IPv4 addresses, this section needs to be configured (e.g. 141.0.144.129 ~ 141.0.144.130). In the example illustrated in Image 21, the SFTP server is running in LAN. The SFTP server is located on the LAN client with IPv4 address **192.168.1.100**. The server will be listening for connections on TCP port 22, so TCP 22 must be listed. The list port ranges in sections **WAN port** and **LAN Host port**.

Once all the parameters are listed, click **Apply**. This will save your new router configuration.

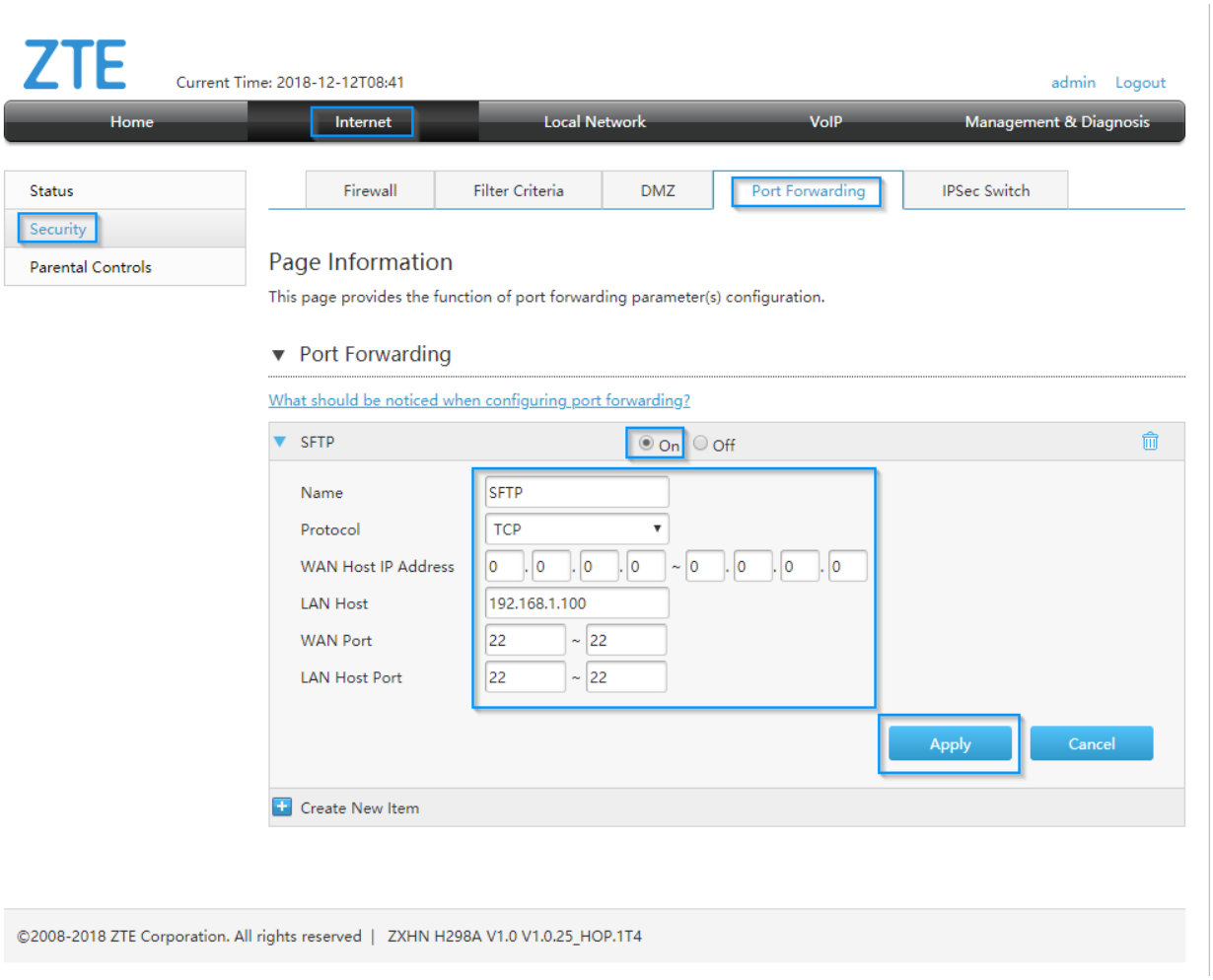


Image 21. Defining port forwarding rule

Alternatively, port forwarding can be configured in a way that port mapping is performed. An example of this is illustrated in Image 22. In this case, WAN port 12001 traffic has been forwarded to the local web server which is listening for connections on port 8080. The router does a port translation.

Please also note that ports 80 and 443 **should never be used on WAN**, as these ports are reserved for Hyperoptic Ltd. remote management. If you'd like to use these ports on your server in a LAN, then you can use different ports on WAN as shown on Image 22 (e.g. you can use ports on WAN 12000, 12001 and map them to LAN ports 80, 443 respectively).

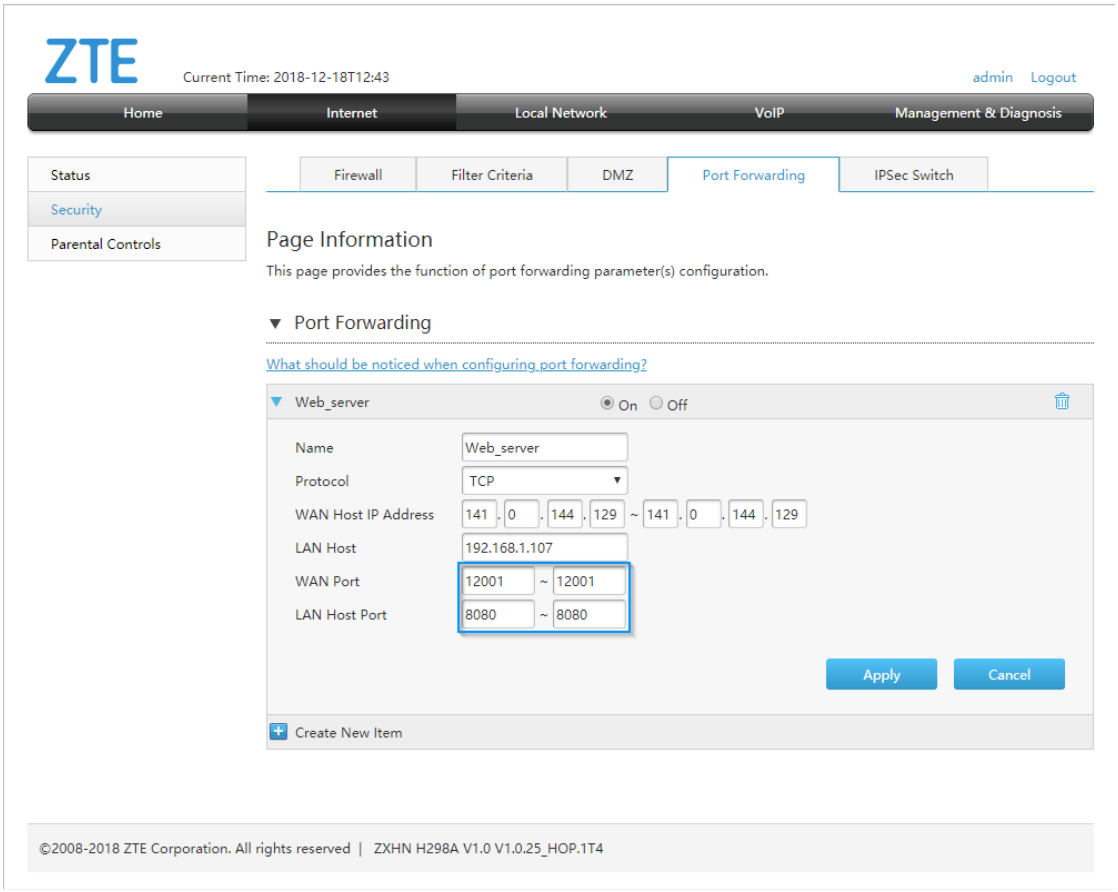


Image 22. Example when different WAN port is serving different LAN port

A list of commonly used ports is illustrated in image 23. For additional information on TCP/UDP port numbers, please refer to https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers .

Port Number(s)	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
514	UDP	Syslog
16,384 – 32,767	UDP	RTP (voice, video)

Image 23. List of commonly used ports

DMZ

Please be aware that devices placed in DMZ will not be affected by a router's firewall. Placing LAN devices in DMZ can therefore pose an IT security risk and this action should be taken with caution. If a LAN device needs to be placed in a demilitarized zone, log into your router (page 2) and go to **Internet > Security > DMZ** as seen in image 24.

Select **On** and list the IPv4 address of LAN device in the **LAN Host** field. Click **Apply**.

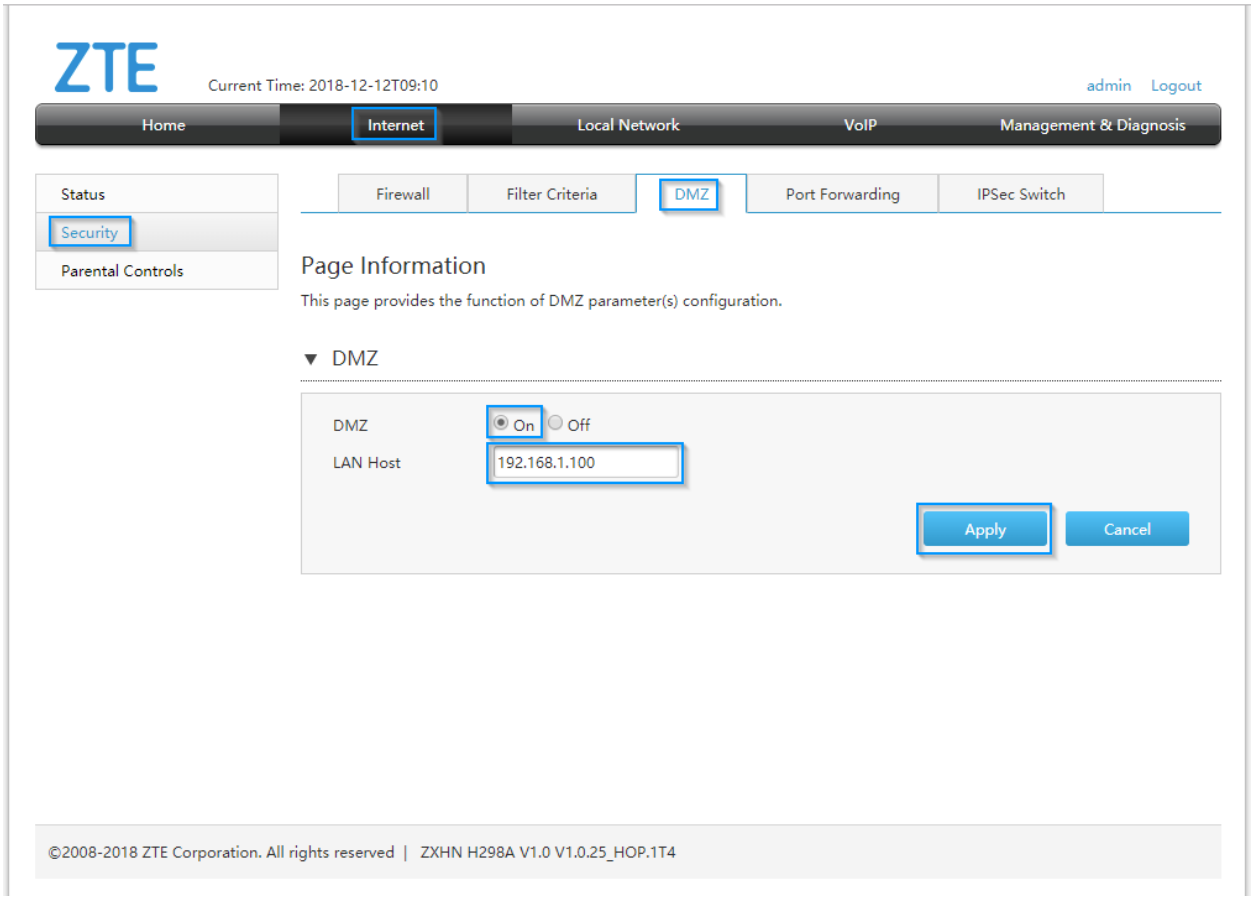


Image 24. DMZ configuration on router

IPv6 filters (equivalent to IPv4 port forwarding)

If IPv6 servers are available for the LAN device, access can be granted via IPv6 filters. To configure IPv6 filters, navigate to **Internet > Security > Filter Criteria > IP Filter – IPv6**. This is illustrated in Image 25.

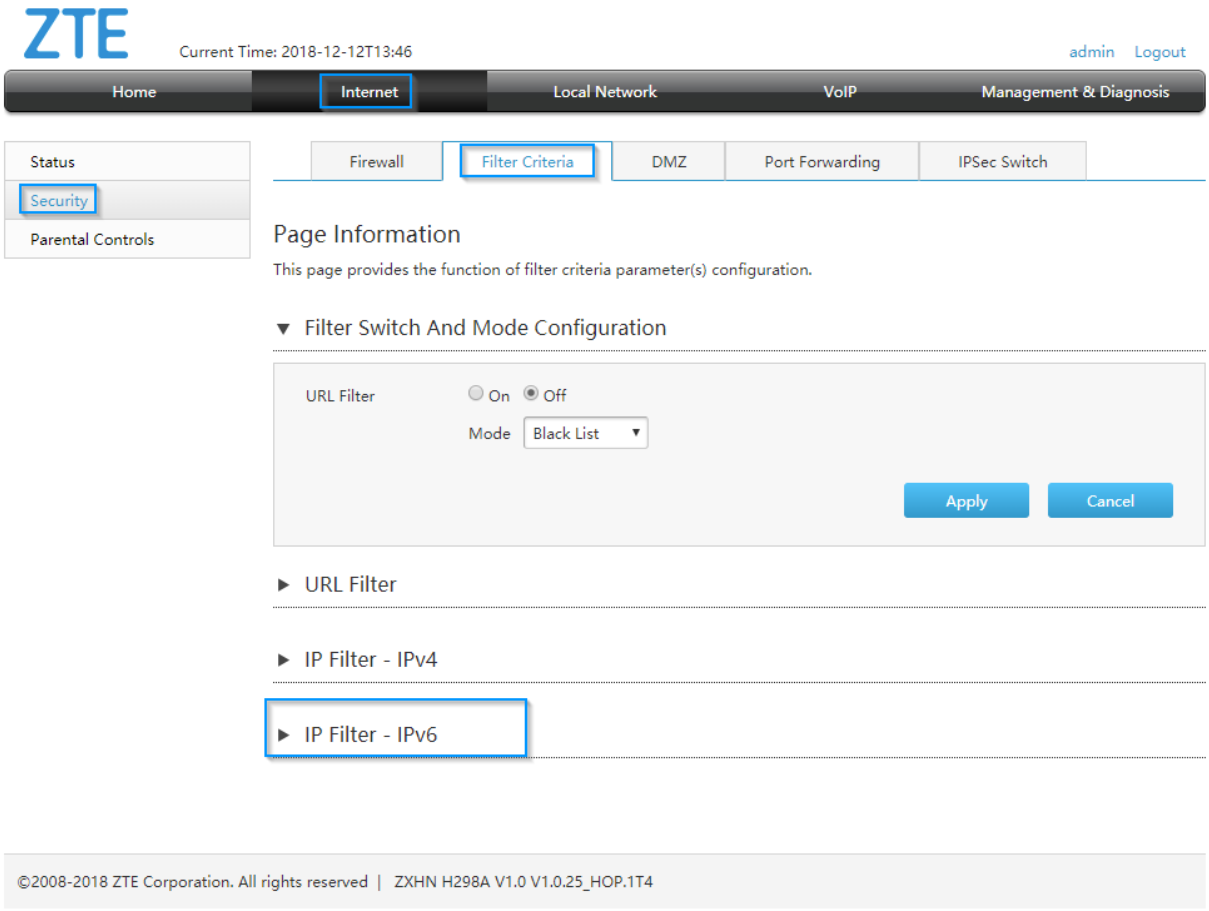


Image 25. IPv6 filters section of router configuration

Click on **IP Filter – IPv6**. You should then be presented with a page like in Image 26.

Click **On** in order to activate the IPv6 filter.

Use any **Name** for the IPv6 filter.

Click **Allow** to permit connections to the web server.

Select transport protocol – **TCP** in case of web server.

List the **Destination Port Range** which will be used for the local sever (port **8080**). Define the **Destination IPv6 Address** prefix which will be used in LAN (e.g. **2a01:4b00:8003:5300::/64**).

The **Ingress** port should be **WAN-DHCP-CONNECTION**.

The **Egress** port should be **LAN**.

If the remote address (internet side) is known, this can be configured in the **Source IPv6 Address** field.

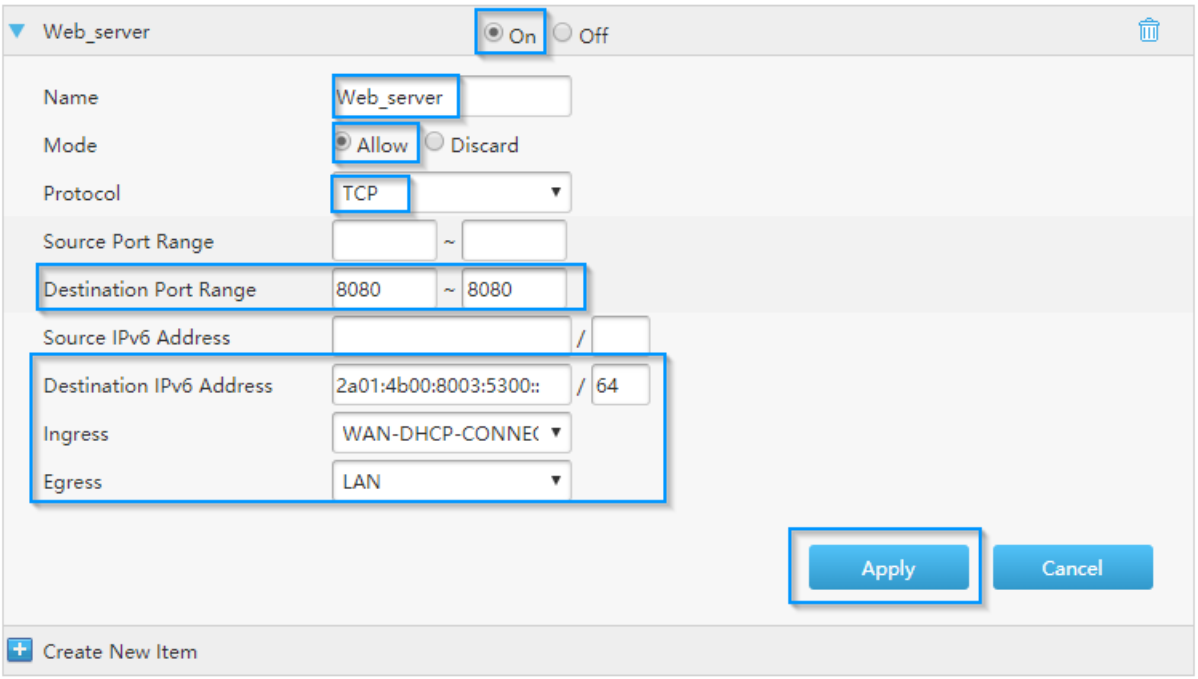


Image 26. Defining IPv6 filter parameters

DHCP Binding

Specific LAN clients can have the same IPv4 address all the time. To define which LAN client will have which IPv4 address, DHCP binding must be completed. To do this, log into your router (page 2) and go to **LAN Devices**. See Image 27.

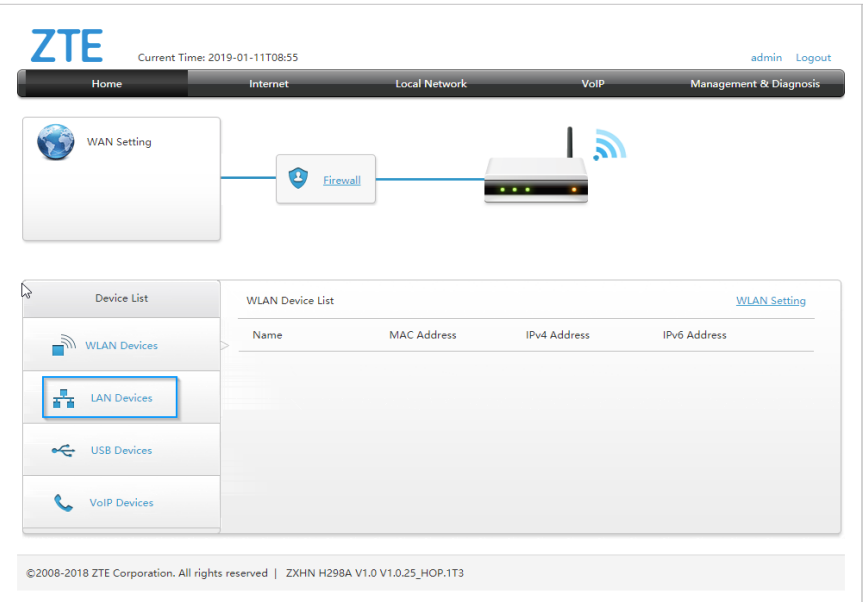


Image 27. Navigate to LAN Devices

Click on **LAN Settings** as described in photo 28. This will open another screen with **DHCP Binding** options.

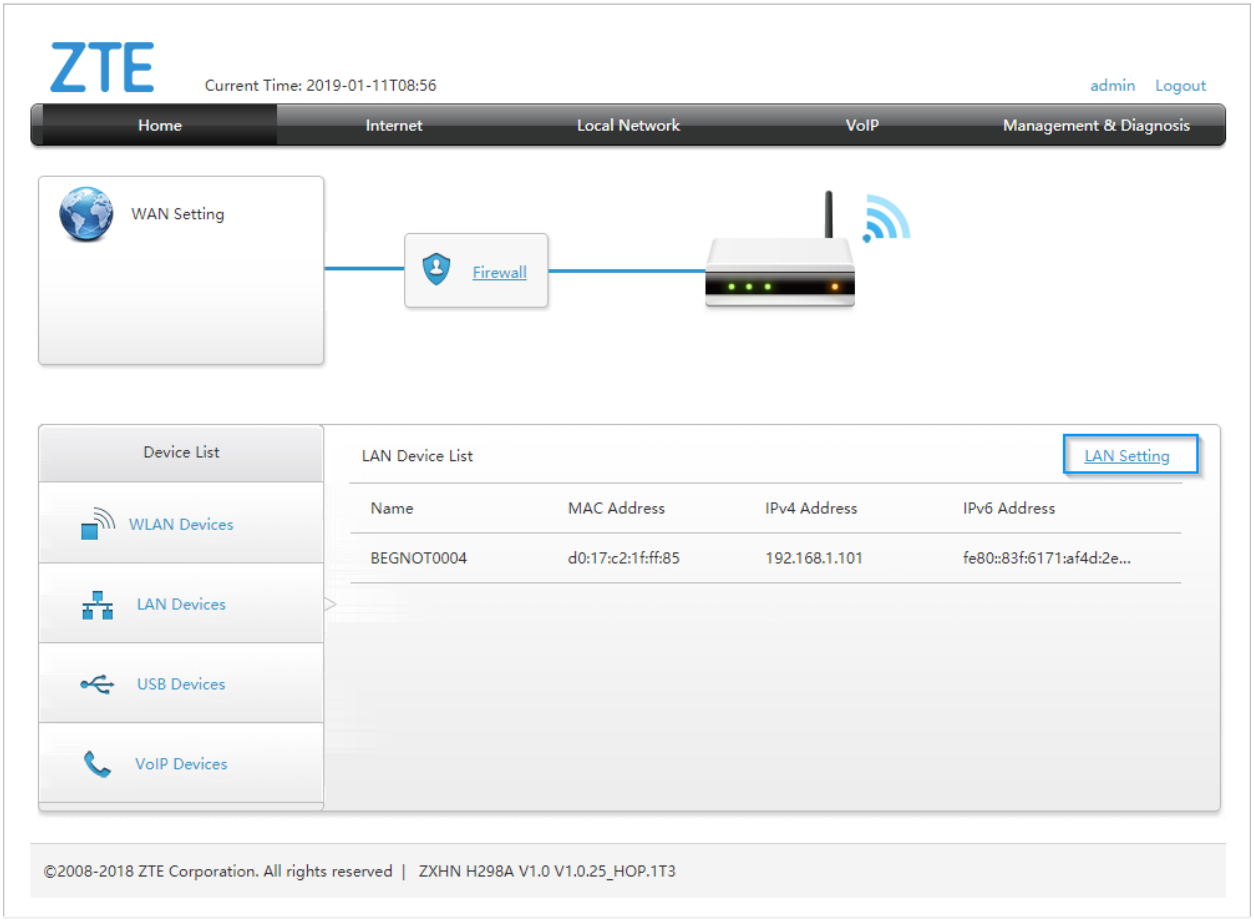


Photo 28. Navigate to section LAN Settings

After clicking on **LAN Settings,** a screen as in Image 29 should appear.

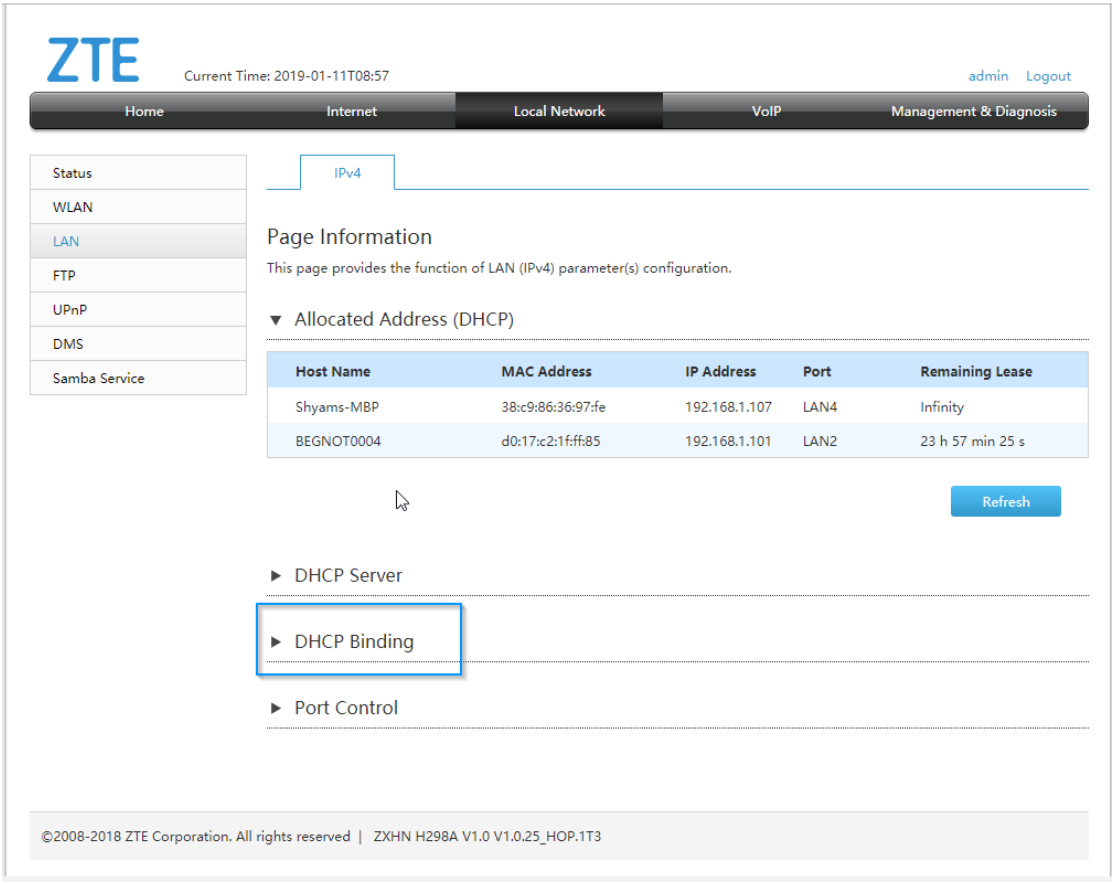


Photo 29. DHCP Binding section of router user interface

After clicking on **DHCP Binding**, define relevant parameters. **Name** can be whatever you choose. Check MAC address of the attached LAN client. Input **MAC address**. List wanted IPv4 for the LAN client. IPv4 addresses can be in range from **192.168.1.100** to **192.168.1.254**. An example can be seen in image 30.

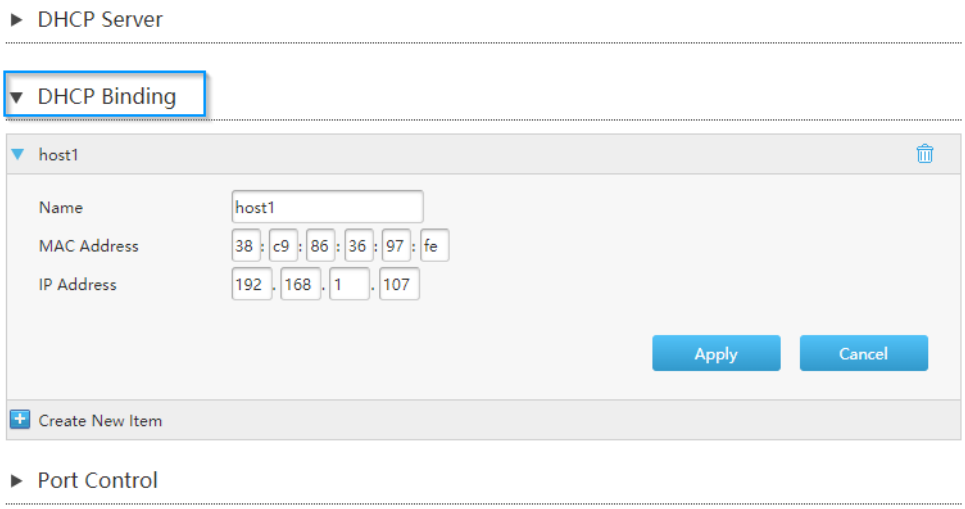


Photo 30. Linking MAC address to IPv4 LAN address

Public IPv4 address block in LAN network

Navigate to **Local Network > LAN**. Image 31 describes an example of public block 137.220.108.0/29. Check option **On** for **Secondary IP**. Populate address that will be present on router and input subnet mask as per table 1. At the end click **Apply** to save settings. To disable NAT on the router, please get in touch with our Customer Support team.

Table 1. Subnet mask values to be used in router config

Public IPv4 address block format	Subnet mask
x.x.x.x/**32**	255.255.255.**255**
x.x.x.x/**31**	255.255.255.**254**
x.x.x.x/**30**	255.255.255.**252**
x.x.x.x/**29**	255.255.255.**248**
x.x.x.x/**28**	255.255.255.**240**

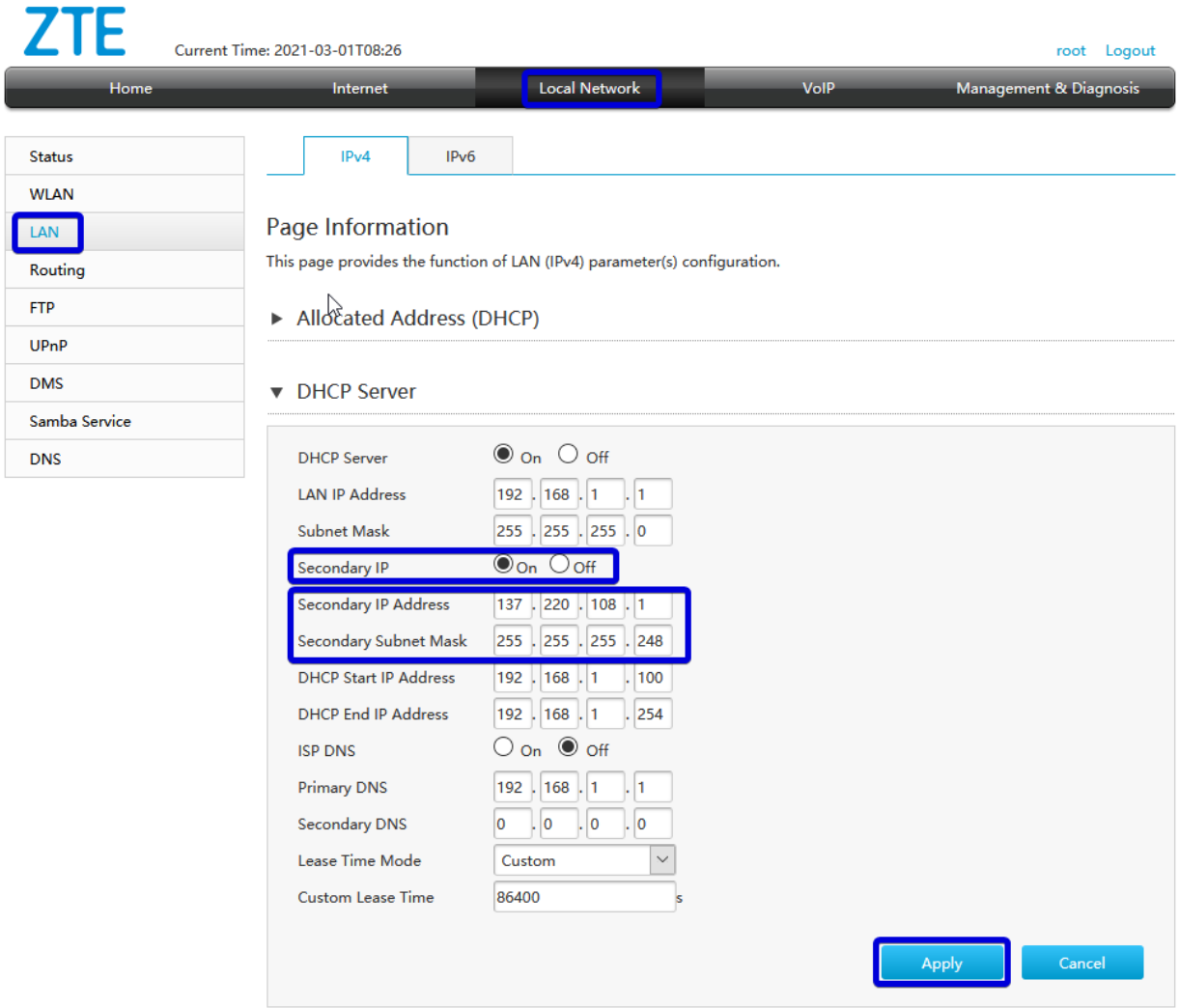


Image 31. Setting public IPv4 addresses for the LAN network