# 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**.

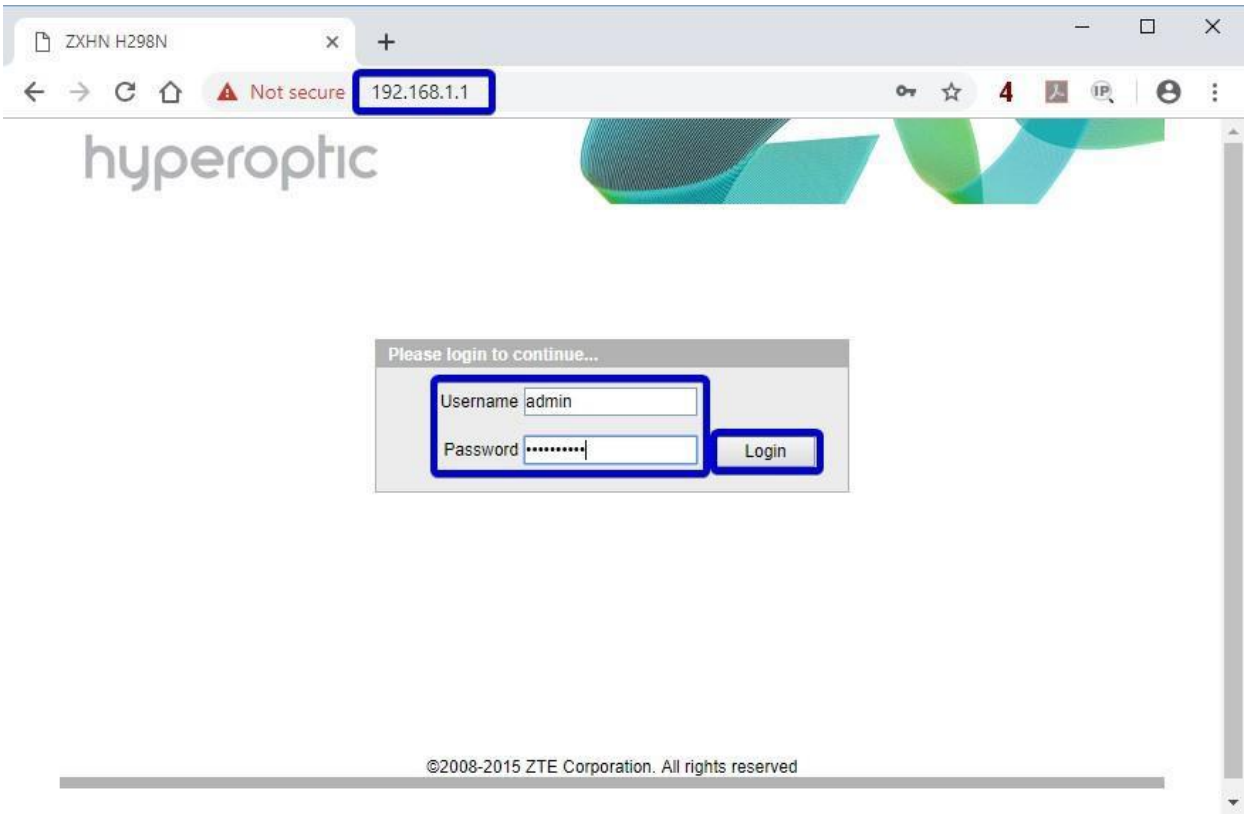


Image 1. Router H298N login screen

# DNS change

To change your DNS, please log into your router (page 2) and navigate to **Network > LAN > DHCP Server**. Change **DNS Server1/2/3 IP Address** fields with some of the public DNS servers and click **Submit**. 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.

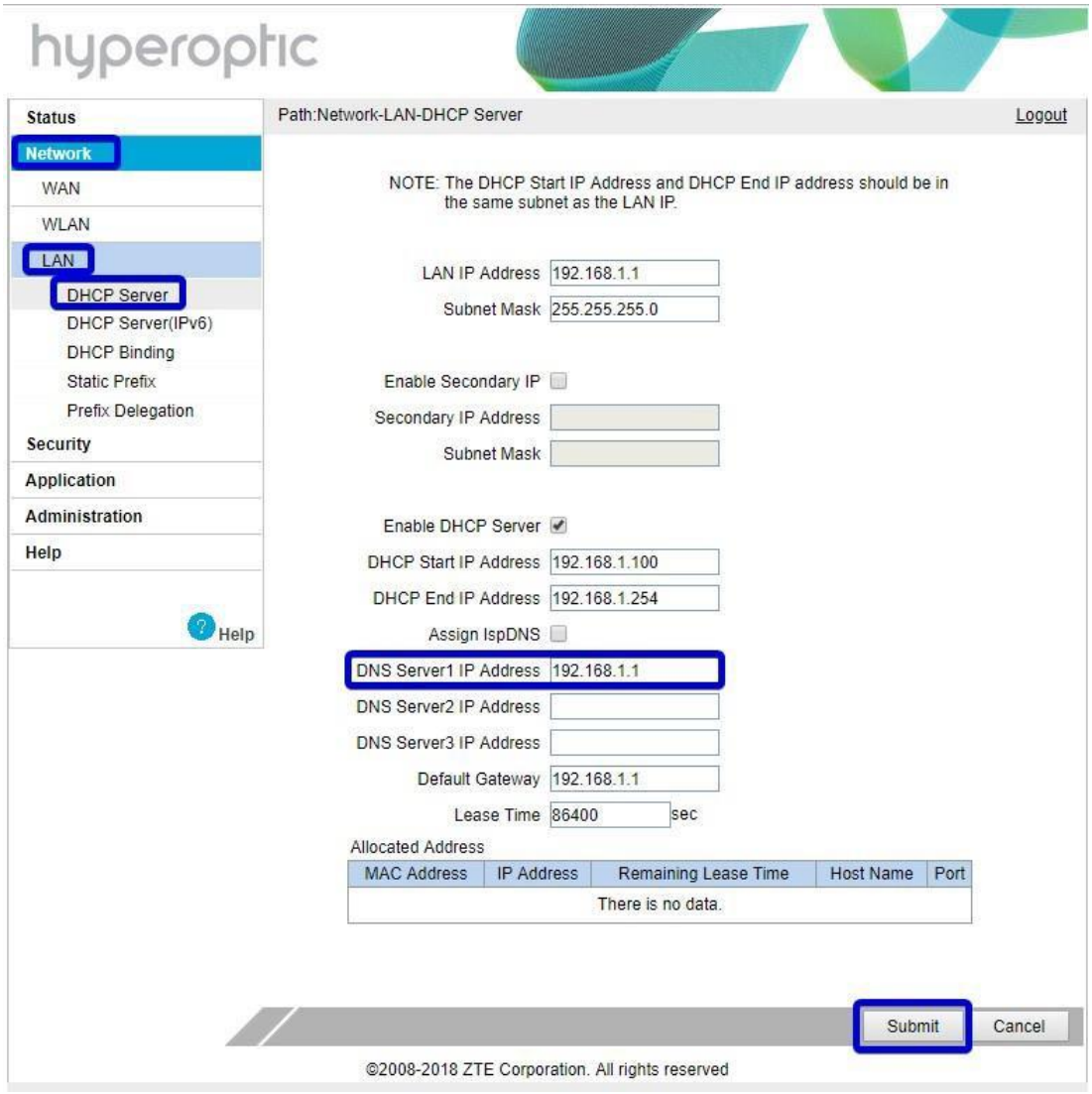


Image 2. Change od DNS server for LAN network

To enable the use of an arbitrary DNS, please disable DHCPv6 server by unticking the **Enable DHCP Server** box. See Image 3.

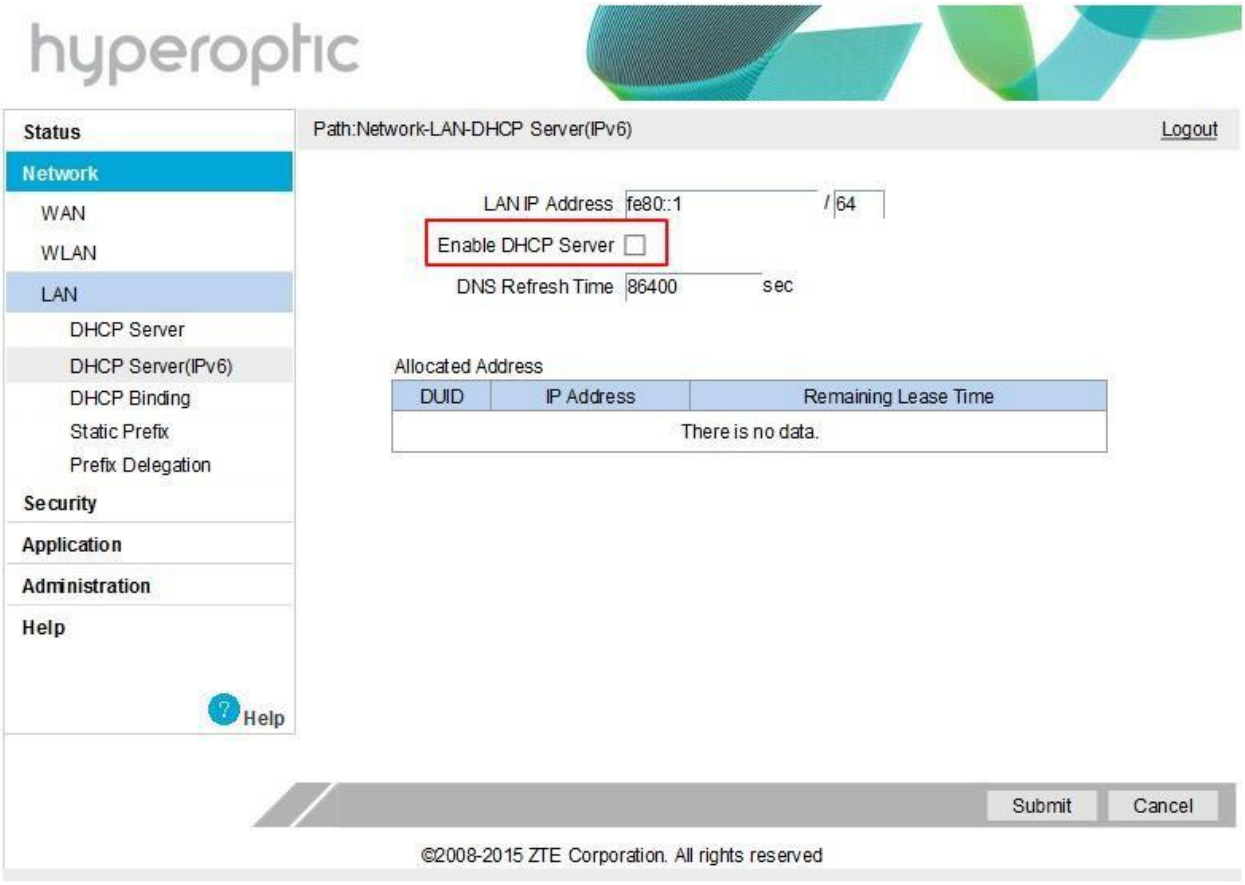


Image 3. Disabling DHCPv6 server on LAN

# UPnP service

UPnP service can be used for easier and more convenient router configuration. To configure your router using UPnP desktop applications (e.g. PortMapper Windows), please log into your router (page 2) and navigate to **Application > UPnP**. Click **Enable** and choose **WAN-DHCP-Connection**. Then click **Submit**. See Image 4.

If you're not using UPnP applications, UPnP should be set to **Off** (the default UPnP setting is Off).

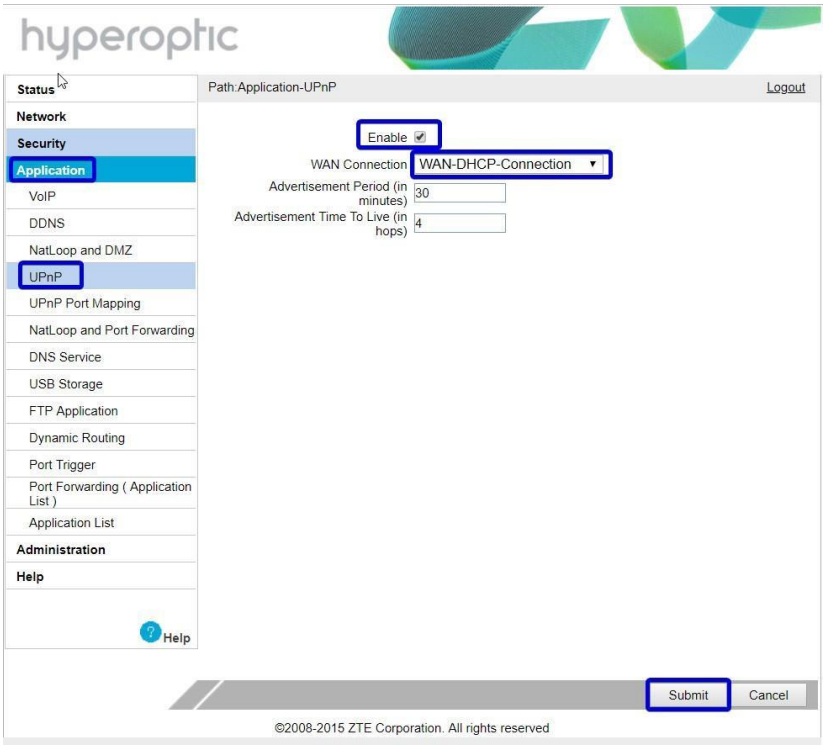


Image 4. Enabling UPnP service on a router

Please see Image 5 for the confirmation of UPnP router configuration. In this example, port mapping is configured.

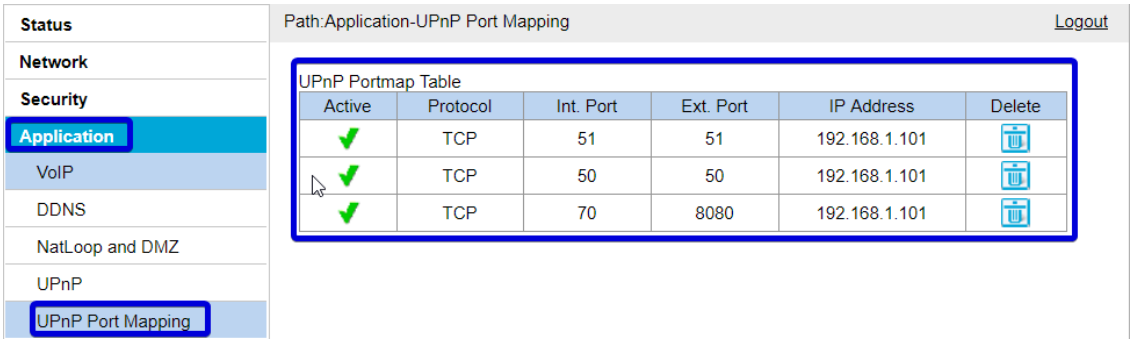


Image 5. Confirmation of UPnP router configuration

# Parental control

Parental control can be used to restrict access to sites. To enable parental control, please log into your router (page 2) and navigate to **Security > Parental Control > User Information**. Provide the MAC address of the LAN client (device) for which internet service should be blocked. Tick **Enable Parental Control**. Choose the day and time during which access should be restricted and click **Add**. See Image 6.

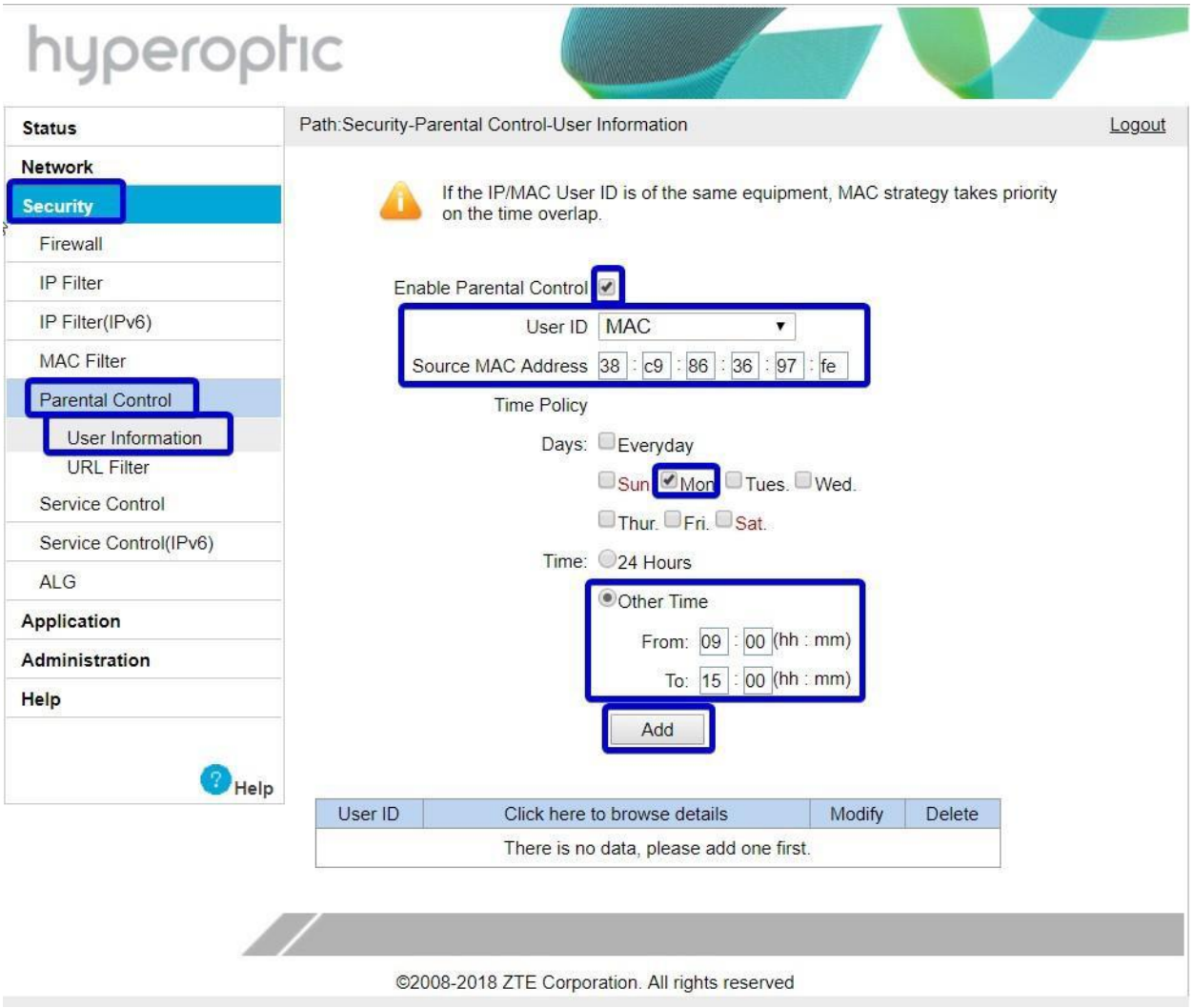


Image 6. Defining user for which internet access should be restricted

After defining LAN client, navigate to **Security > Parental Control > URL Filter**. Tick **Enable**, list the URL you would like to block and choose mode **Discard**. Then click **Add**. See Image 7. Please note that parental control will not filter IPv6 websites.

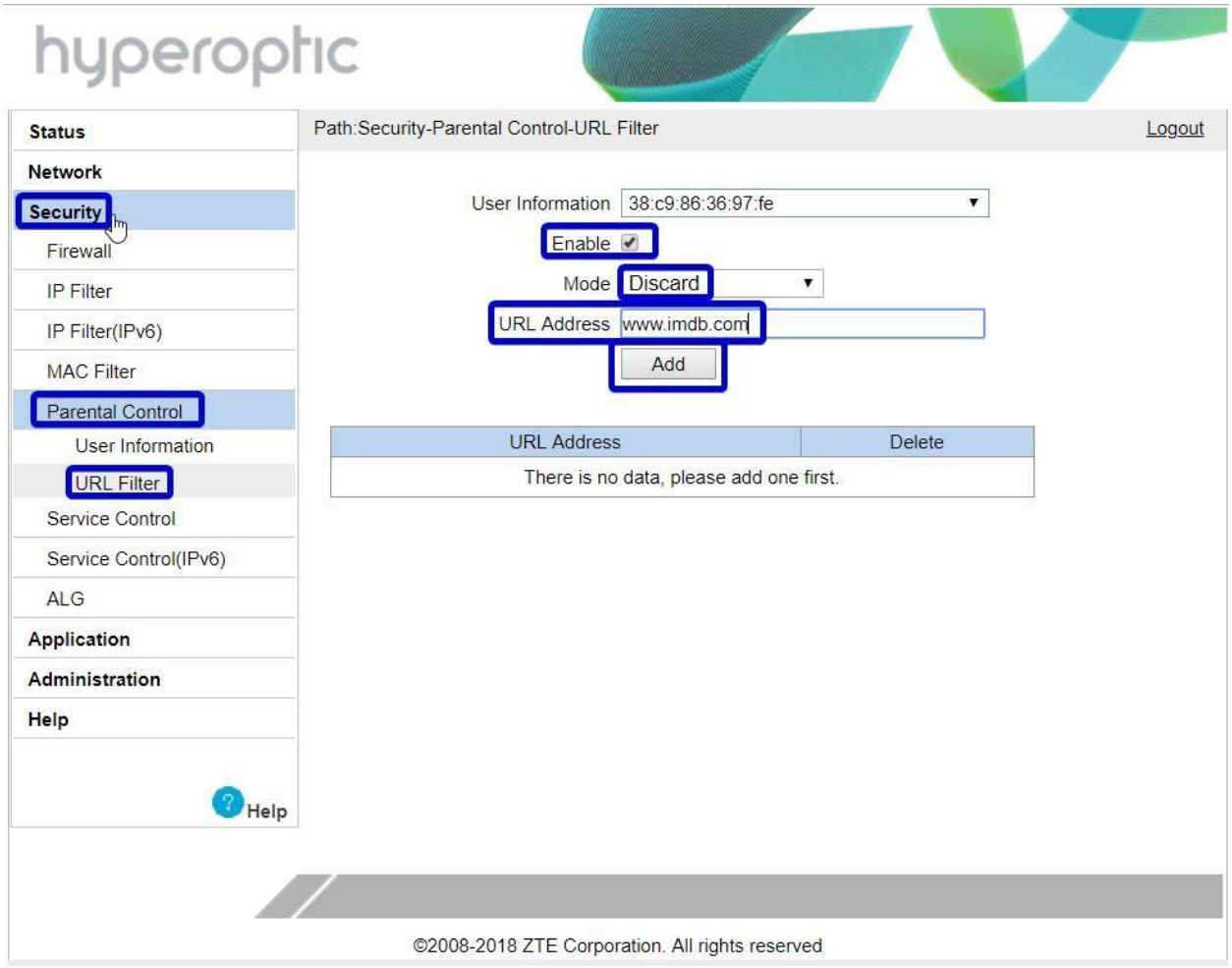


Image 7. Example of blocking access to one web site

# 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 **Network > LAN > DHCP Server**. See Image 8.

Here you'll be able to see all the devices that are connected to your router's LAN network.

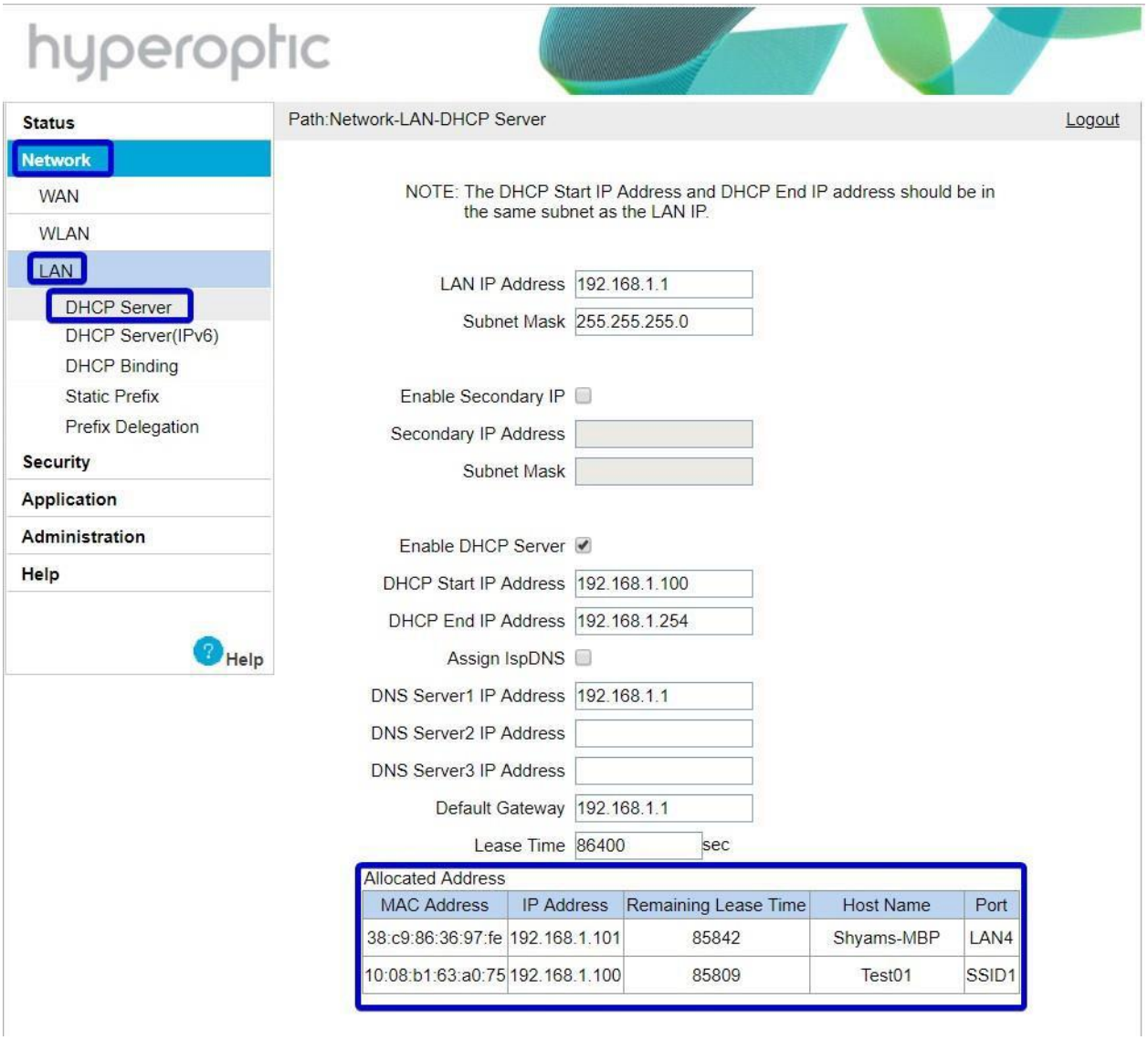


Image 8. List of LAN clients

Please note, if a LAN client is using a static IP and connects via cable, it won't be listed here.

# Wi-Fi password and SSID change

To change your wifi password or SSID name, log into your router (see page 2) and navigate to **Network > WLAN**. To change the name of your wifi connection, click on **SSID Settings** and change the **SSID Name** field. Once changed, click **Submit**. See Image 9.

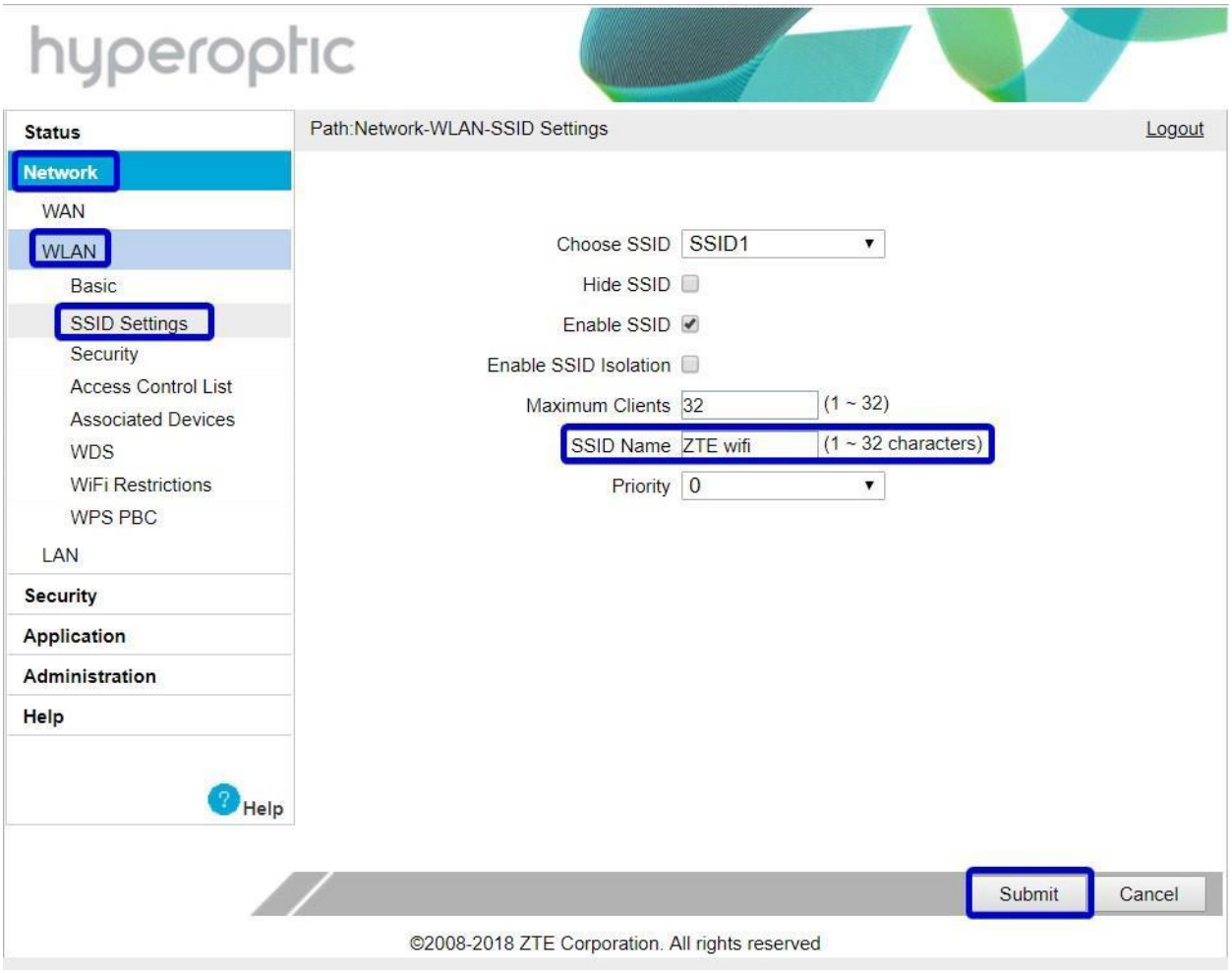


Image 9. Change od Wi-Fi network name (SSID)

To change your wifi password, navigate to **Network > WLAN > Security**. Change **WPA Passphrase** field and click **Submit**. See Image 10. Please use passwords containing upper and lower case letters and numbers, with a minimum of 12 characters in length.

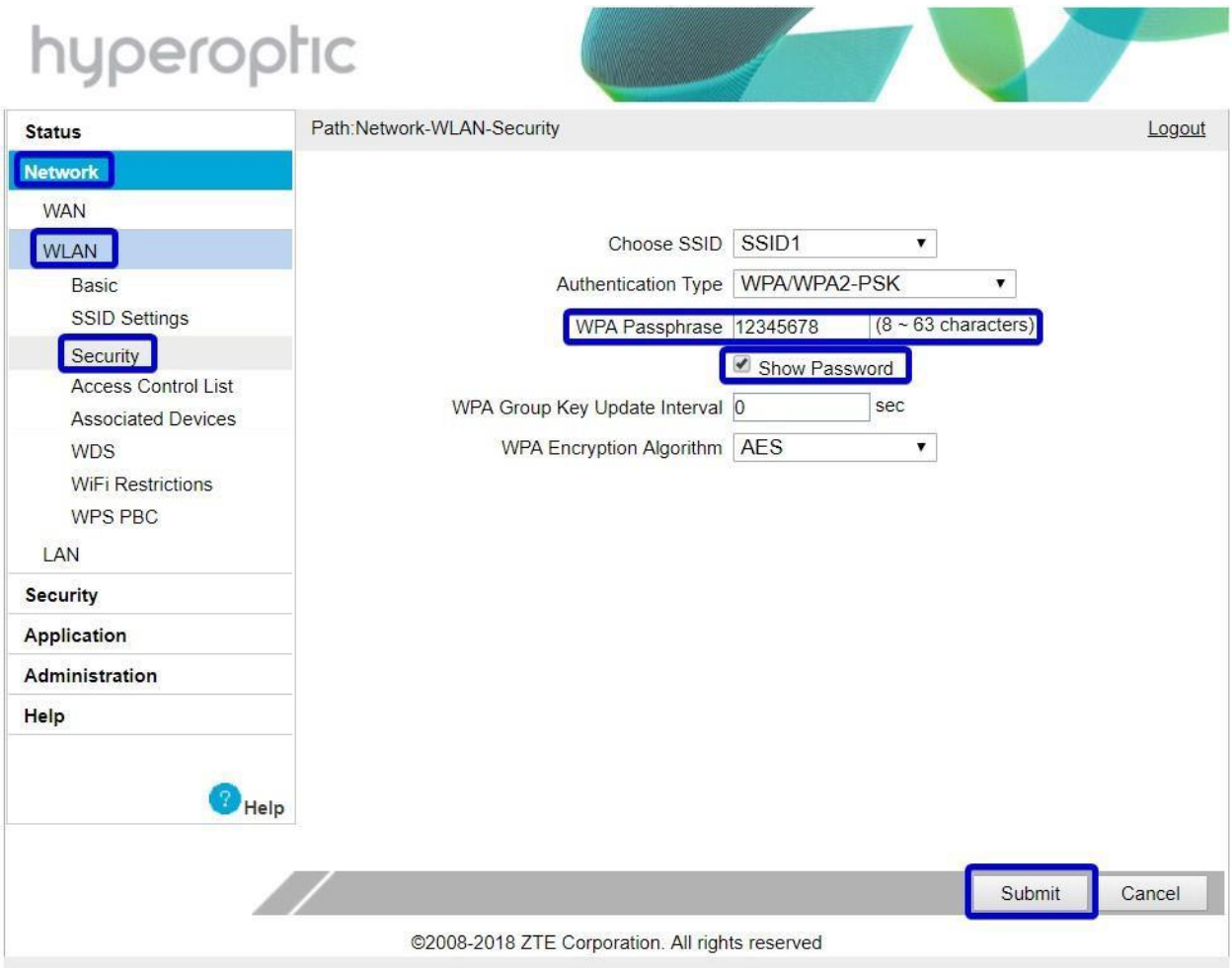


Image 10. Change of Wi-Fi password

# Wi-Fi authentication

To change your wifi authentication settings, please log into your router (page 2) and navigate **to Network > WLAN > Security**. Select **Authentication Type** from the drop-down menu and click **Submit**. See Image 11. By default, advanced encryption algorithm is used.

Please note, it's highly recommended to use only WPA2-PSK-AES.

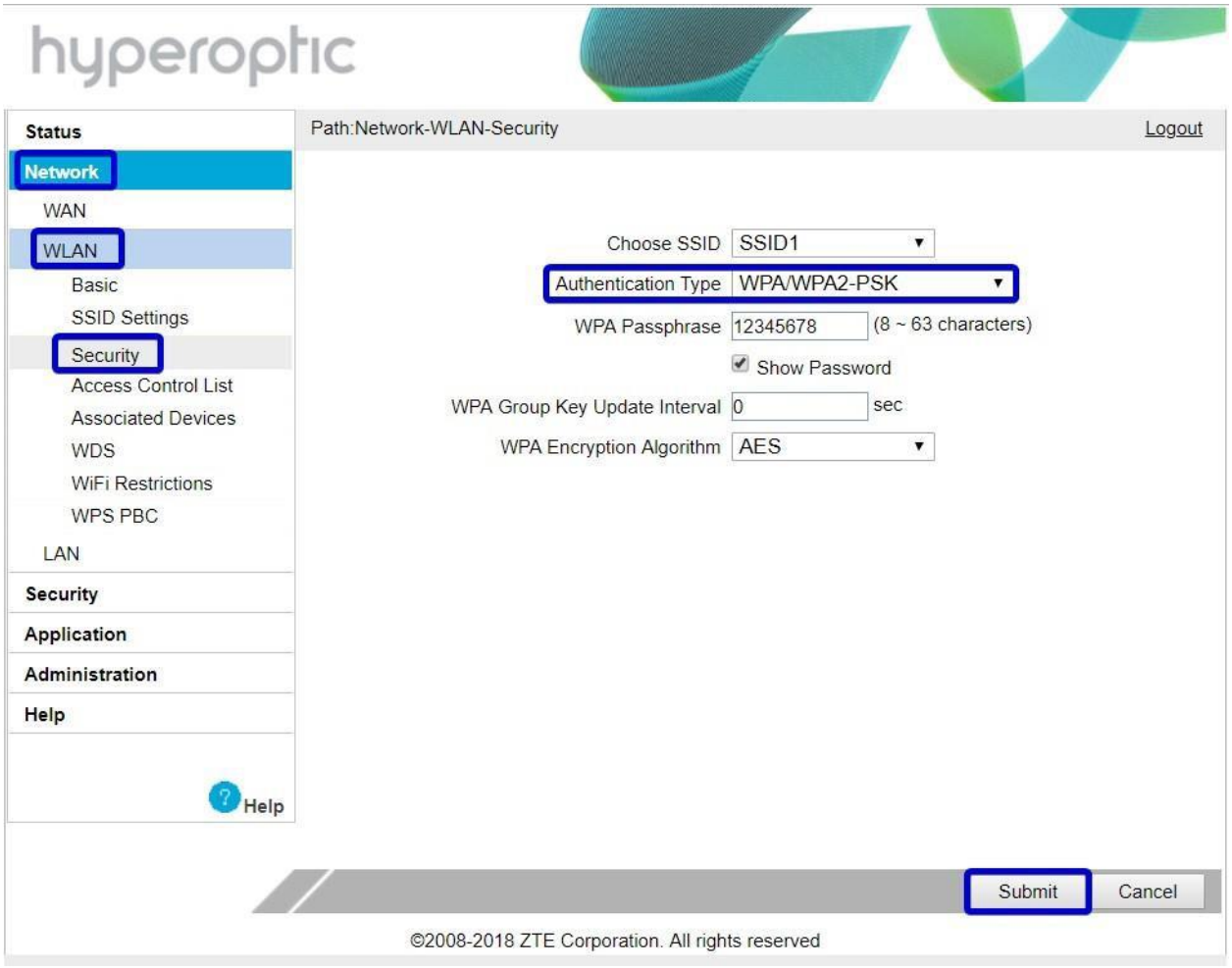


Image 11. Authentication types of Wi-Fi connection

# WPS

To connect to wifi without a password, please log into your router (see page 2) and navigate to **Network > WLAN > WPS PBC**. Press the **WPS** button on your router and on the LAN host. A connection will then be made. See Image 12.

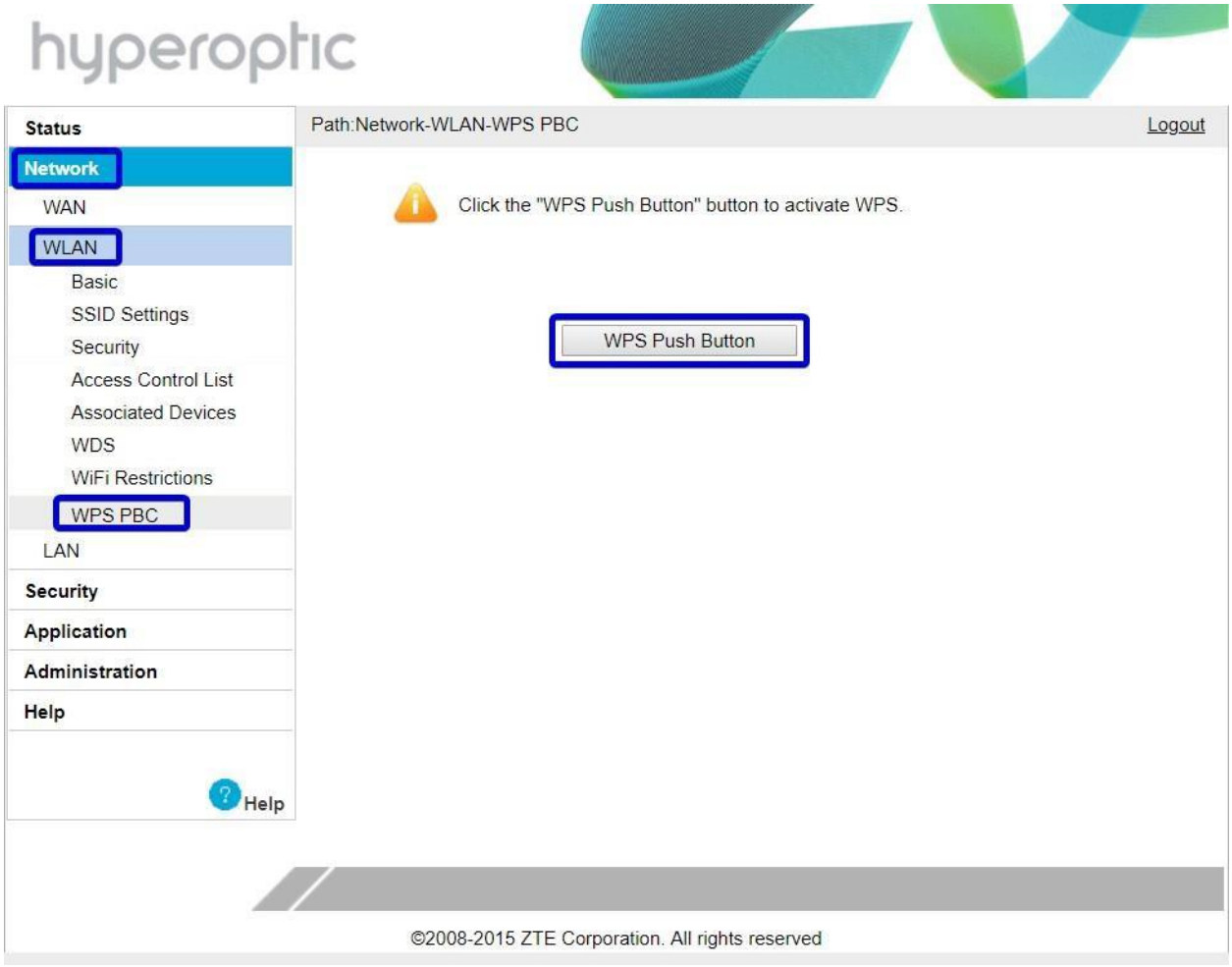


Image 12. WPS button on router

# Wi-Fi associated clients

The number of wifi clients (i.e. devices connected to the router wifi) can be checked once you're logged into your router (see page 2). Navigate to **WLAN > Associated Devices**. To refresh the page, click **Refresh**. See Image 13.

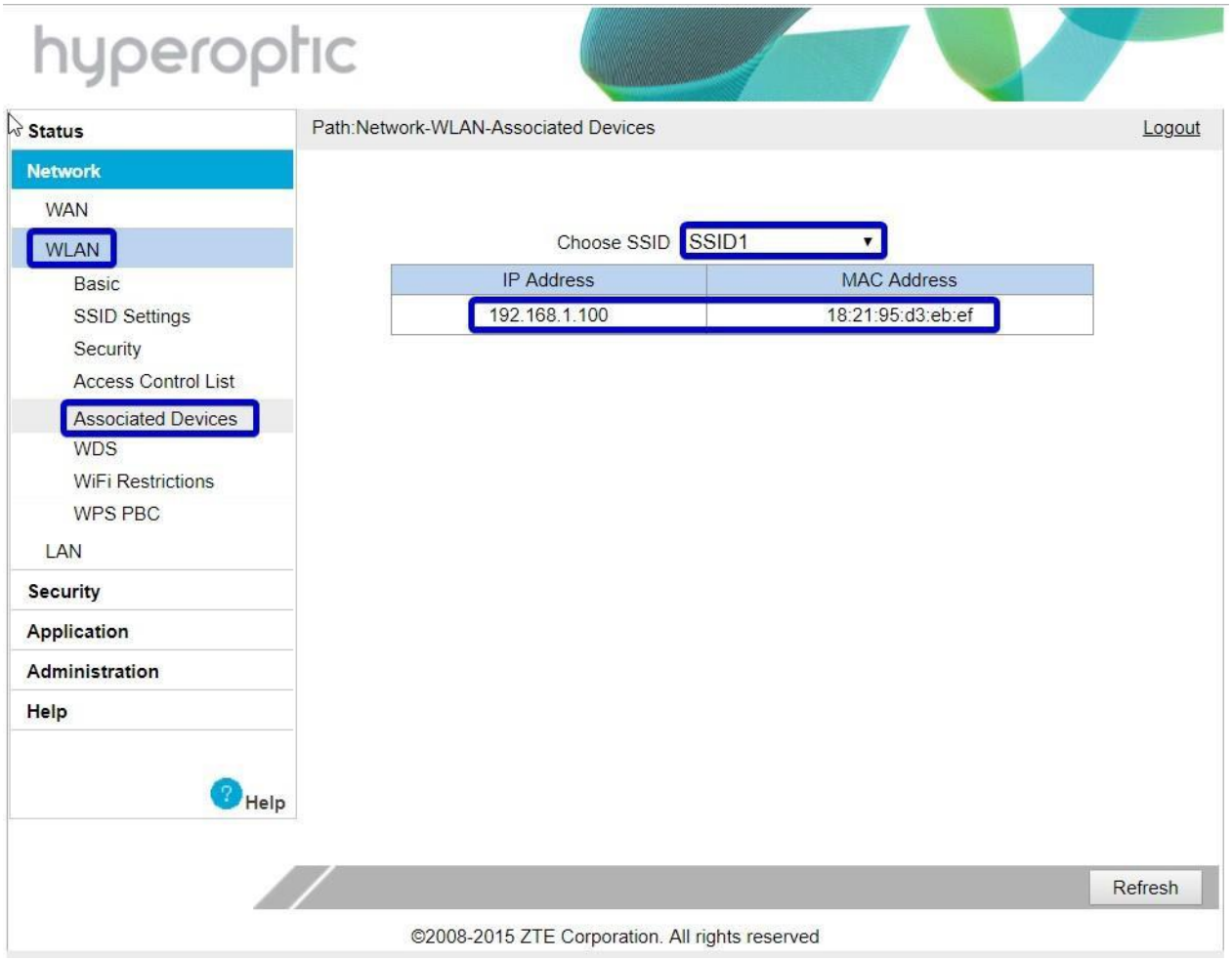


Image 13. List of WLAN clients

# Wi-Fi channel change

To minimise interference, we highly recommend leaving your wifi channel selection on its default settings. If you'd like to change your channel selection, however, you can do so by logging into your router (see page 2) and navigating to **Network > WLAN > Basic**. Select your desired channel from the drop-down menu and click **Submit**. See Image 14.

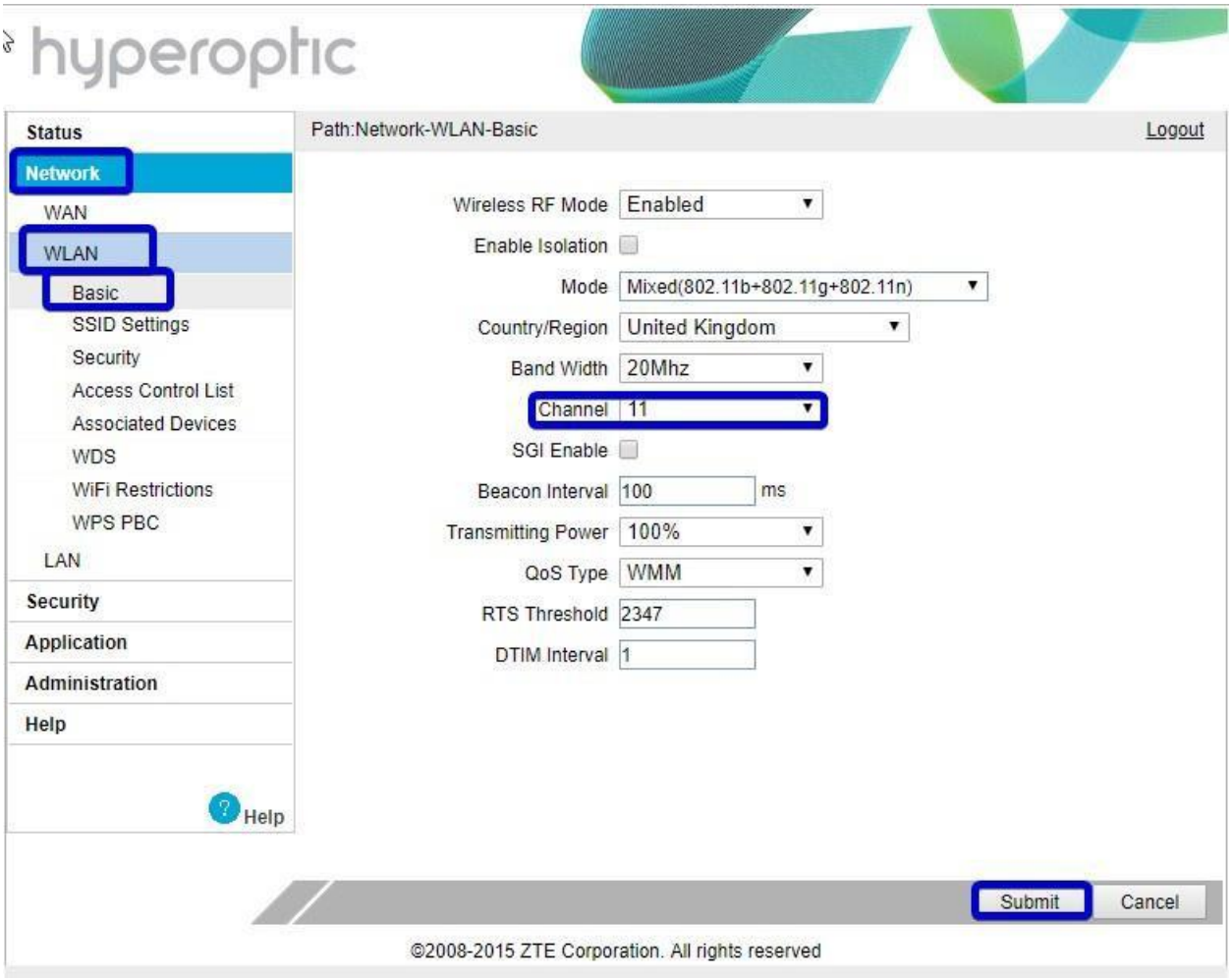


Image 14. Wi-Fi channel change

# Change of admin credentials

To change your admin login password, log into your router (see page 2) and navigate to **Administration > User Management**. Once the new details are entered, click **Submit**. See Image 15.

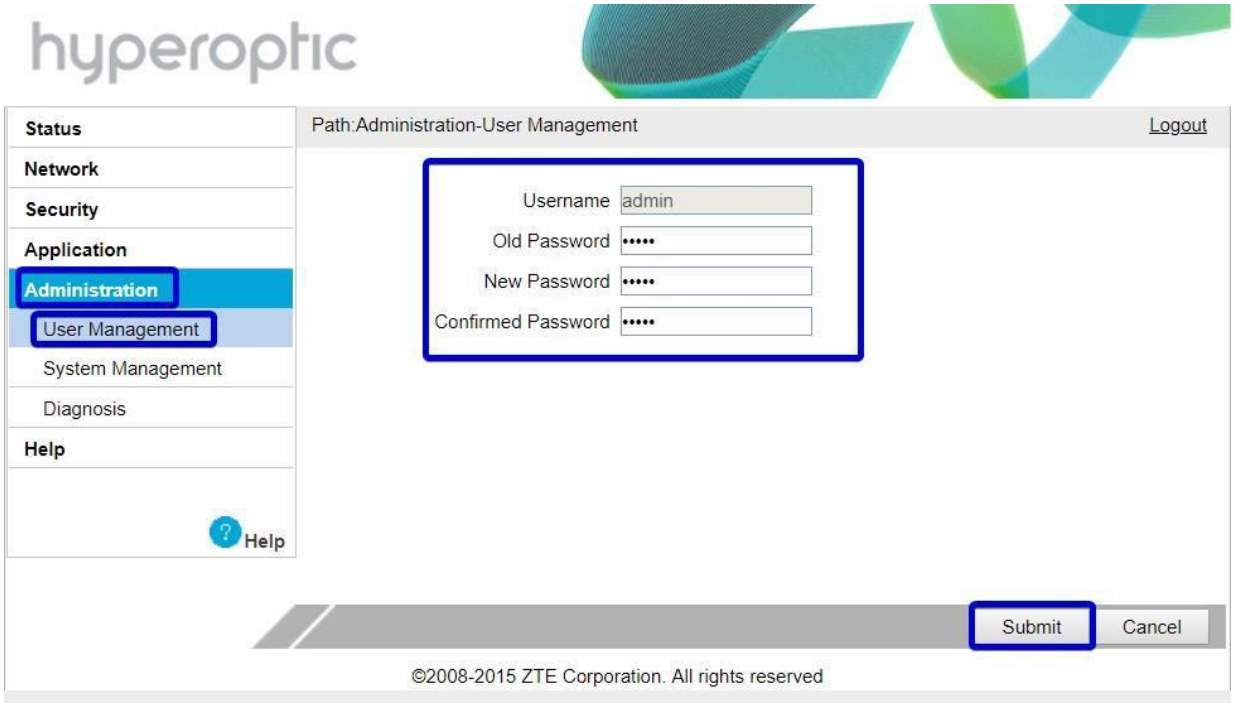


Image 15. Change old admin credentials

# Ping tests from router

To check your connection using ping command, log into your router (see page 2) and navigate to **Administration > Diagnosis > Ping Diagnosis**. See image 16. Once parameters are defined, press **Submit**.

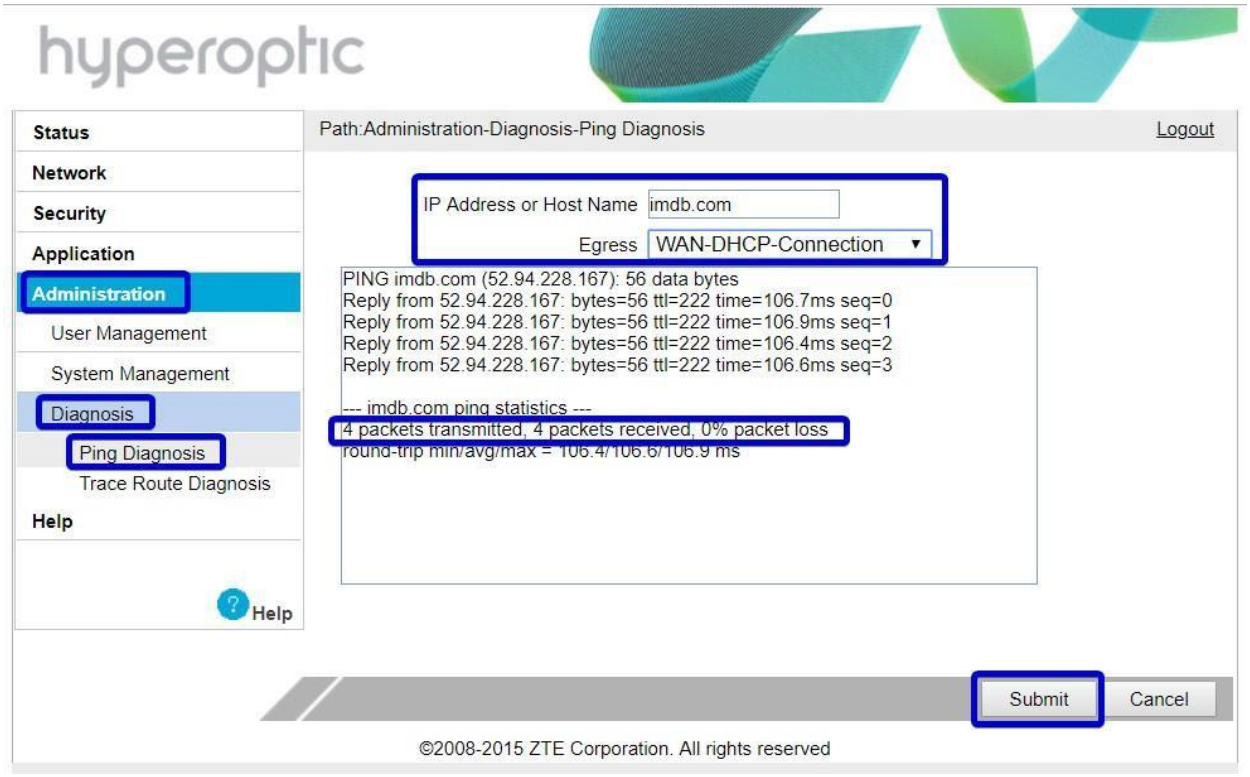


Image 16. Testing router status via ping command

# Factory reset and reboot of router

You can reboot your router or restore it to factory settings by logging in (see page 2) and navigating to **Administration > System Management > System Management**. Then select either **Reboot** or **Restore Default**. See Image 17.

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.

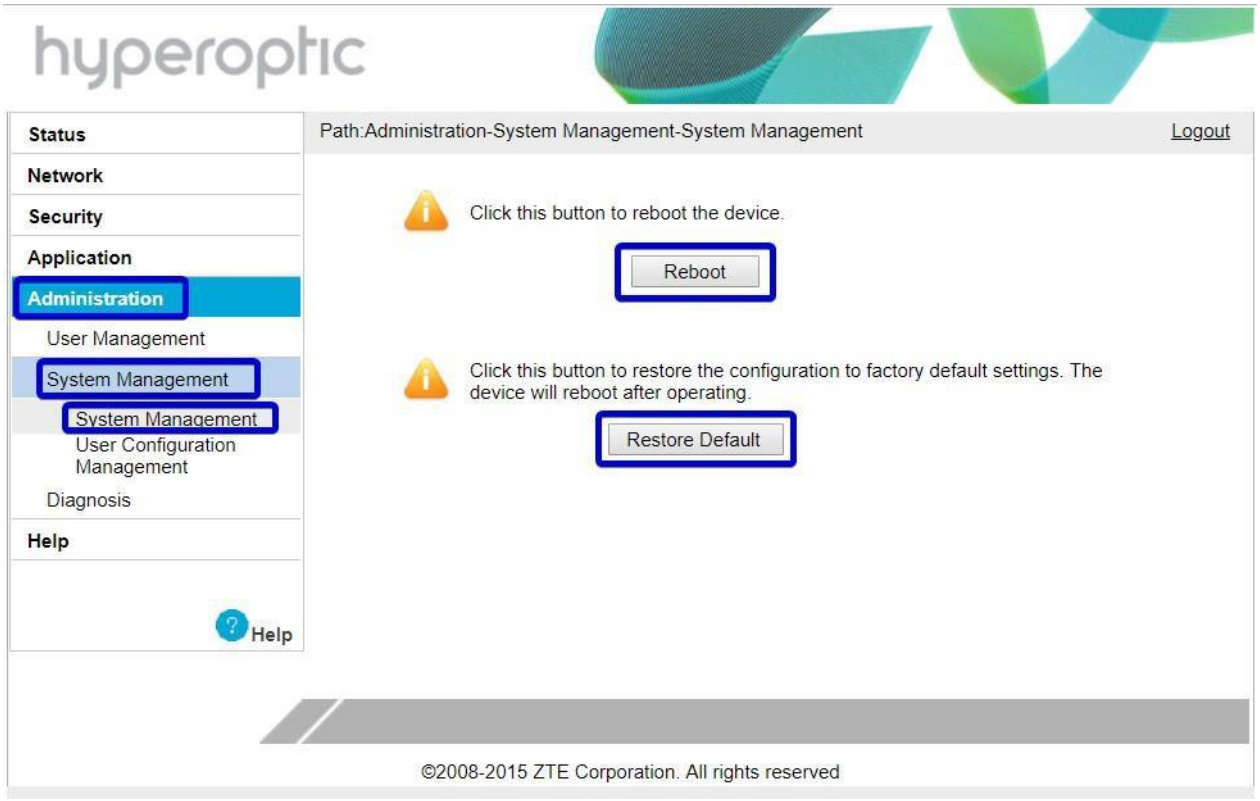


Photo 17. Reboot and factory reset buttons

# USB flash access

Once USB flash drive is attached to the router, you can access it using FTP protocol. To enable FTP server, navigate to **Application > FTP Application**. Tick **Enable FTP Server**, configure **username** and **password** and click **Submit**. See image 18. The router's USB port with attached flash drive can be used as additional storage area linked with LAN network.

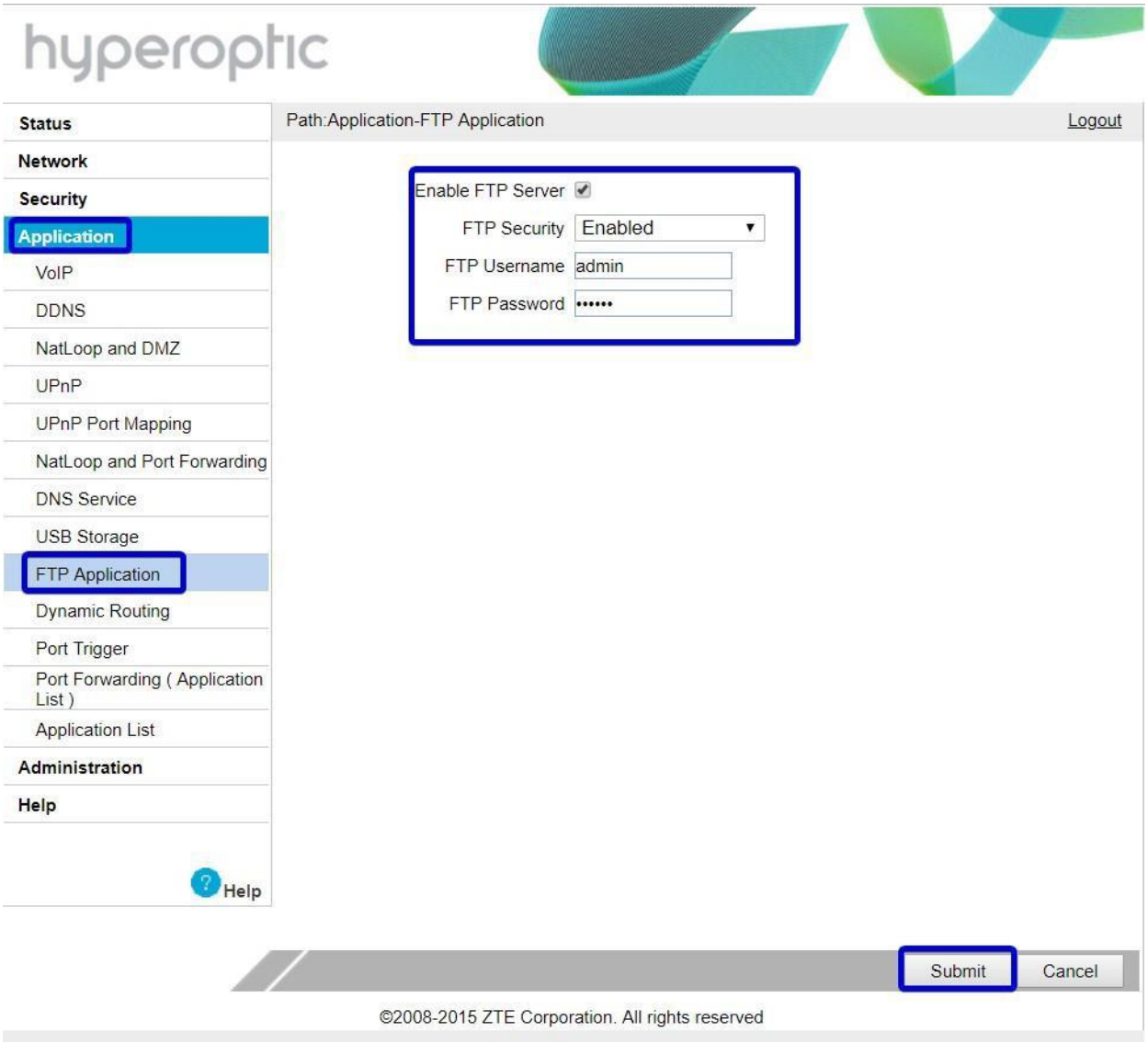


Image 18. FTP server enabling on router

To enable remote access to FTP flash drive, navigate to **Security > Service Control**. Tick **Enable**, select **Ingress** connection as per image 19. If remote address is known, this can be defined in source IP fields. **Permit FTP** access and click **Add**.

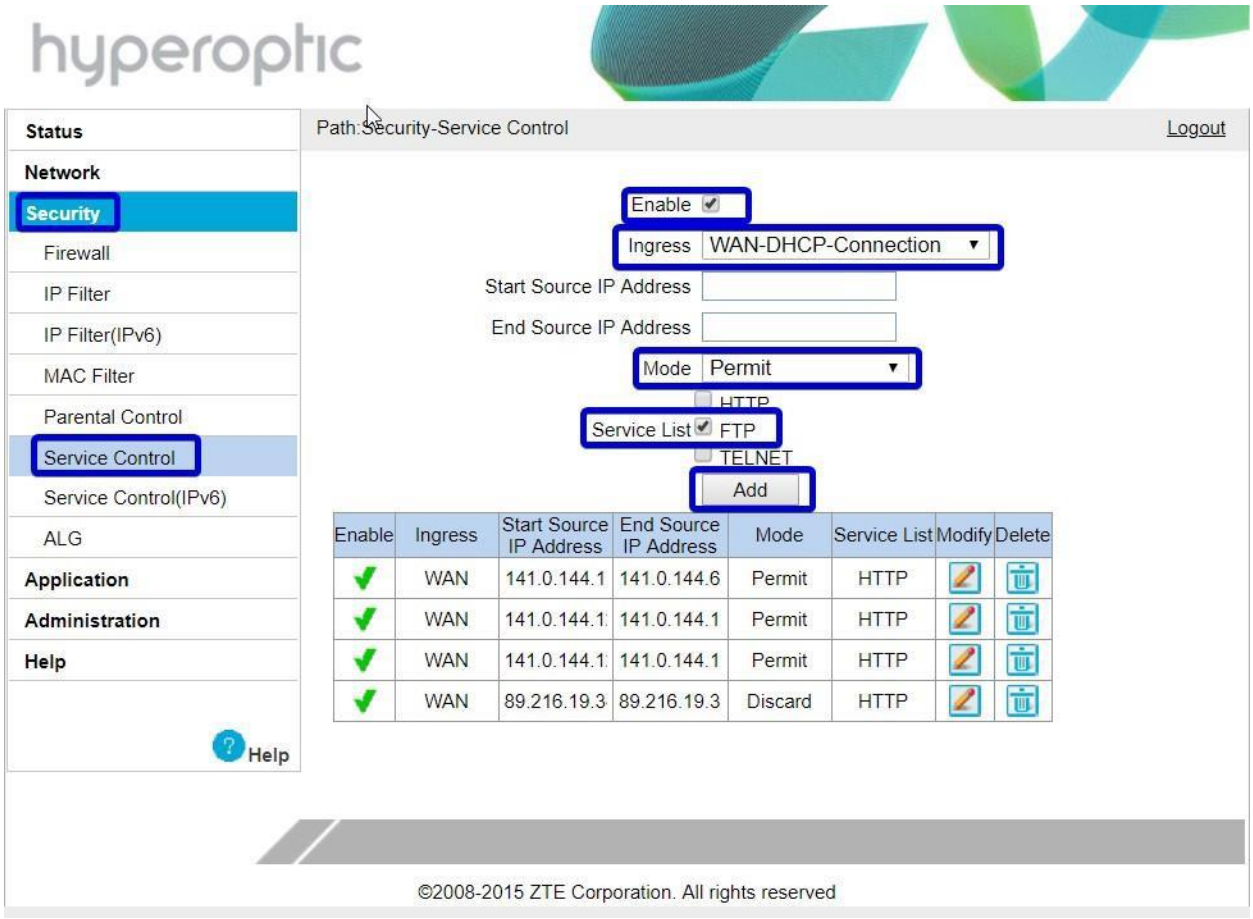


Image 19. Allowing remote FTP access to USB flash drive

From local LAN station, access can be performed by typing ftp://192.168.1.1 into the web browser. See image 19. Using web browser, it is possible only to download, but if FTP client is used (e.g. FileZilla, etc.), upload is also available. Remote access is described in image 20. Please note, **length of filename must be less than or equal to 8 characters and length of its suffix must be less than or equal to 3 characters**. So, the structure filename is like this, for example: 'xxxxxxxx.xxx'.


Image 19. LAN access to USB flash drive

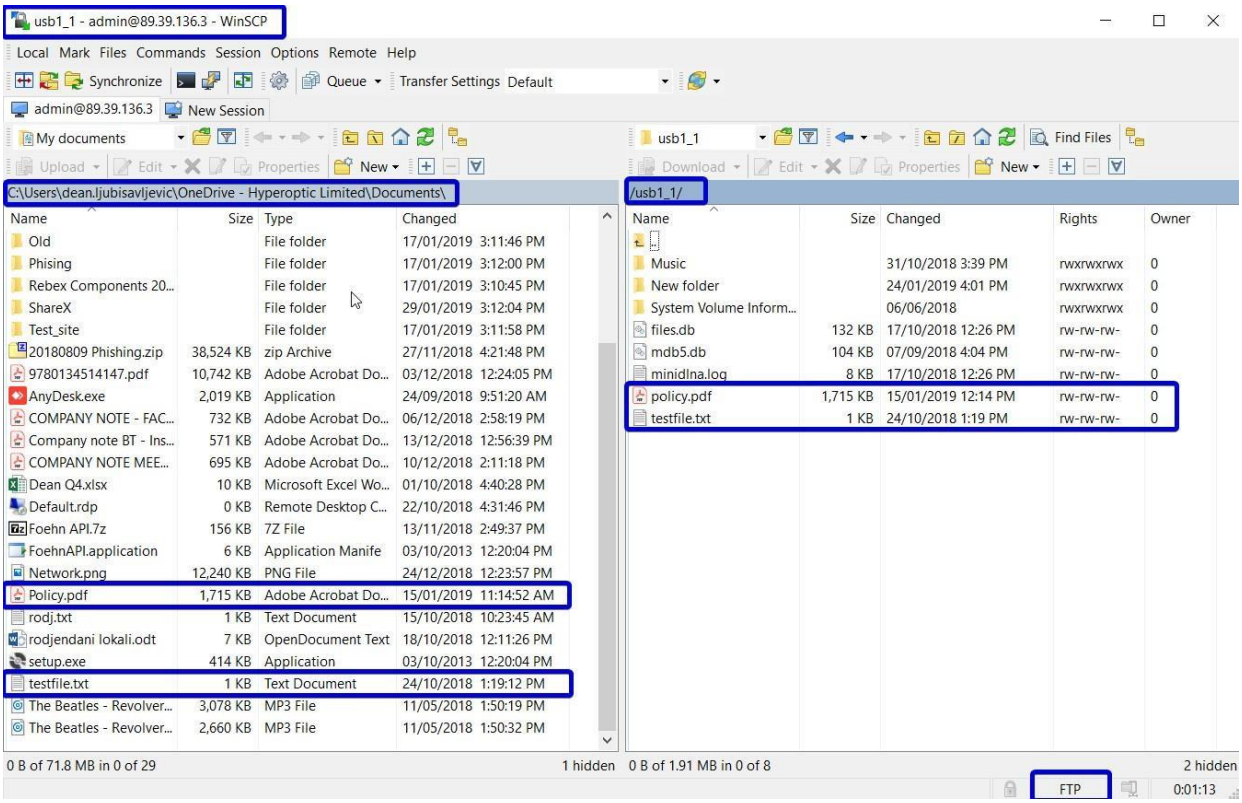


Image 20. WAN access and upload to USB flash drive

# 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 21). Port forwarding can be used to establish home-based FTP server, web server or similar kind of a server.

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.


Image 21. Login screen of ZTE H298N router

Once logged in, navigate to **Applications > Application List.** Select **Click here to add an application** to make new port mapping, as illustrated in Image 22.

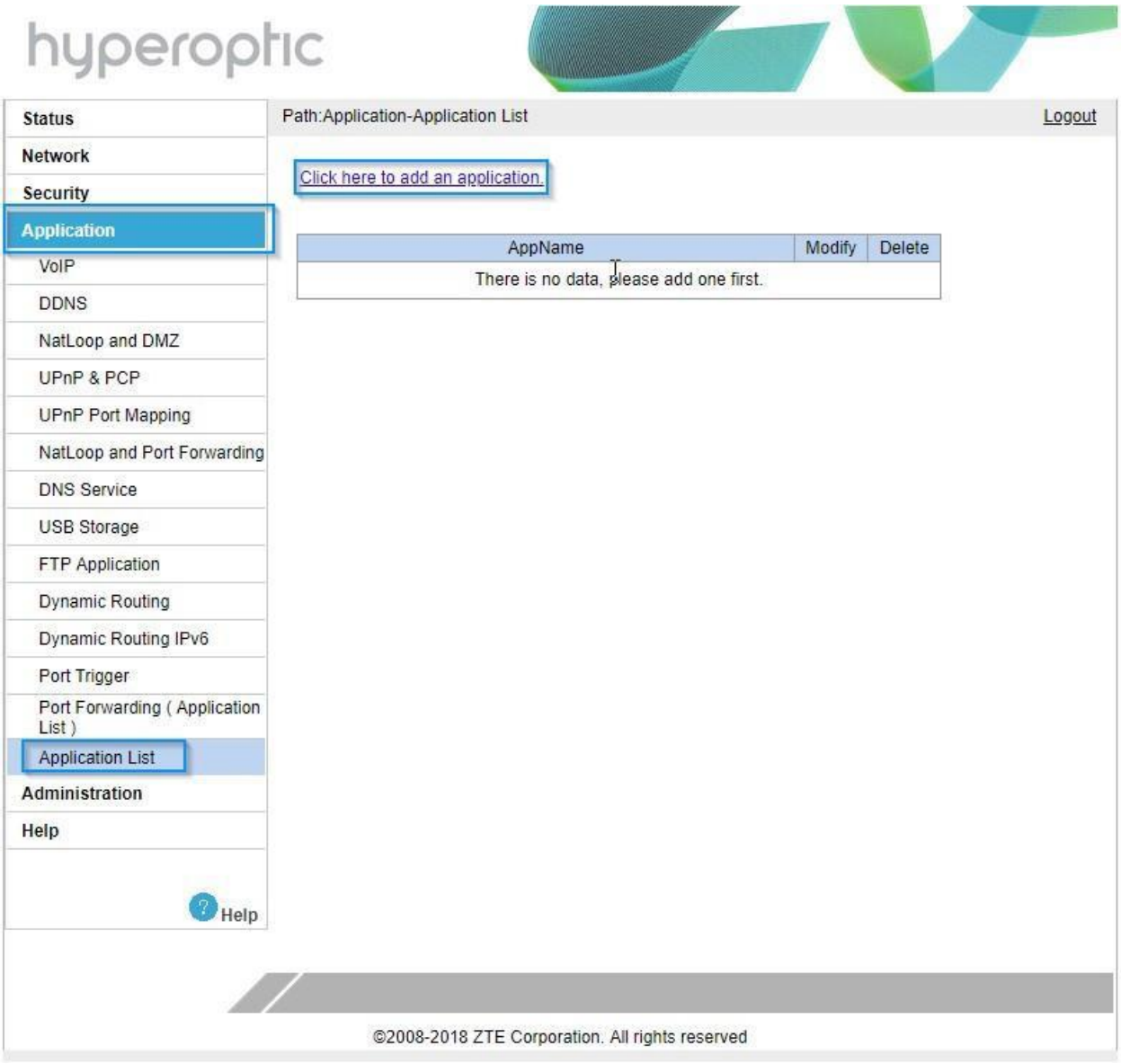


Image 22. Defining local application on router

You should then be presented with the webpage illustrated in Image 23. List any name in the **Application Name** field. In case of local web server, use **TCP Protocol**.

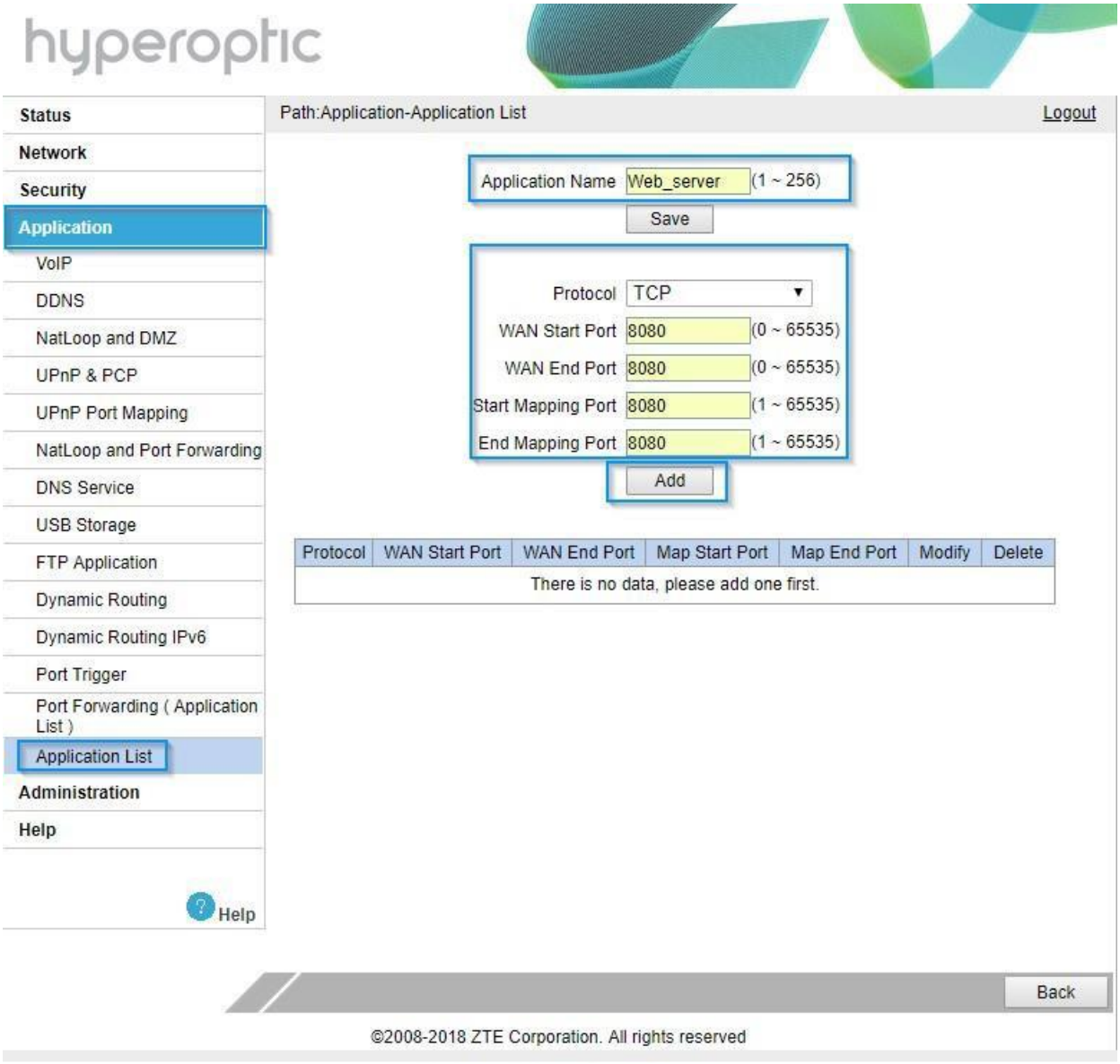


Image 23. Defining LAN application in router GUI

List the port that will be used for the local web server (in this case, the server will be listening for connections on TCP port 8080). Populate **WAN Start Port**, **WAN End Port**, **Start Mapping Port** and **End Mapping Port** with the value **8080**. Once completed, click **Add**. Confirmation should appear as illustrated in Image 24.

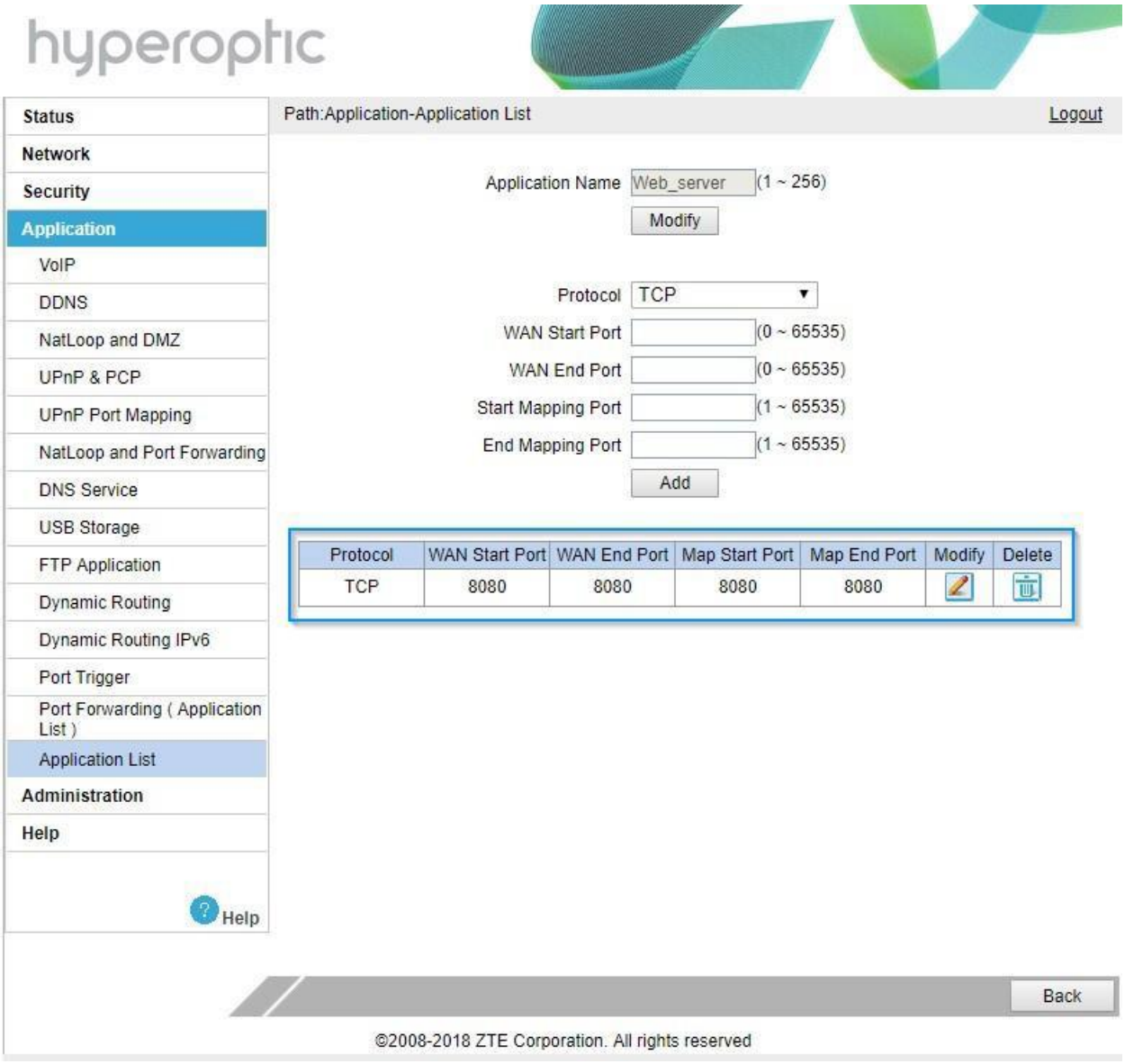


Image 24. Confirmation of application creation

After creating the application, navigate to **Application > Port Forwarding (Application List)**. This section will link the application with the relevant LAN device's IPv4 address. Enter **LAN Host IP Address** and click **Add**. This configuration is illustrated in Image 25.

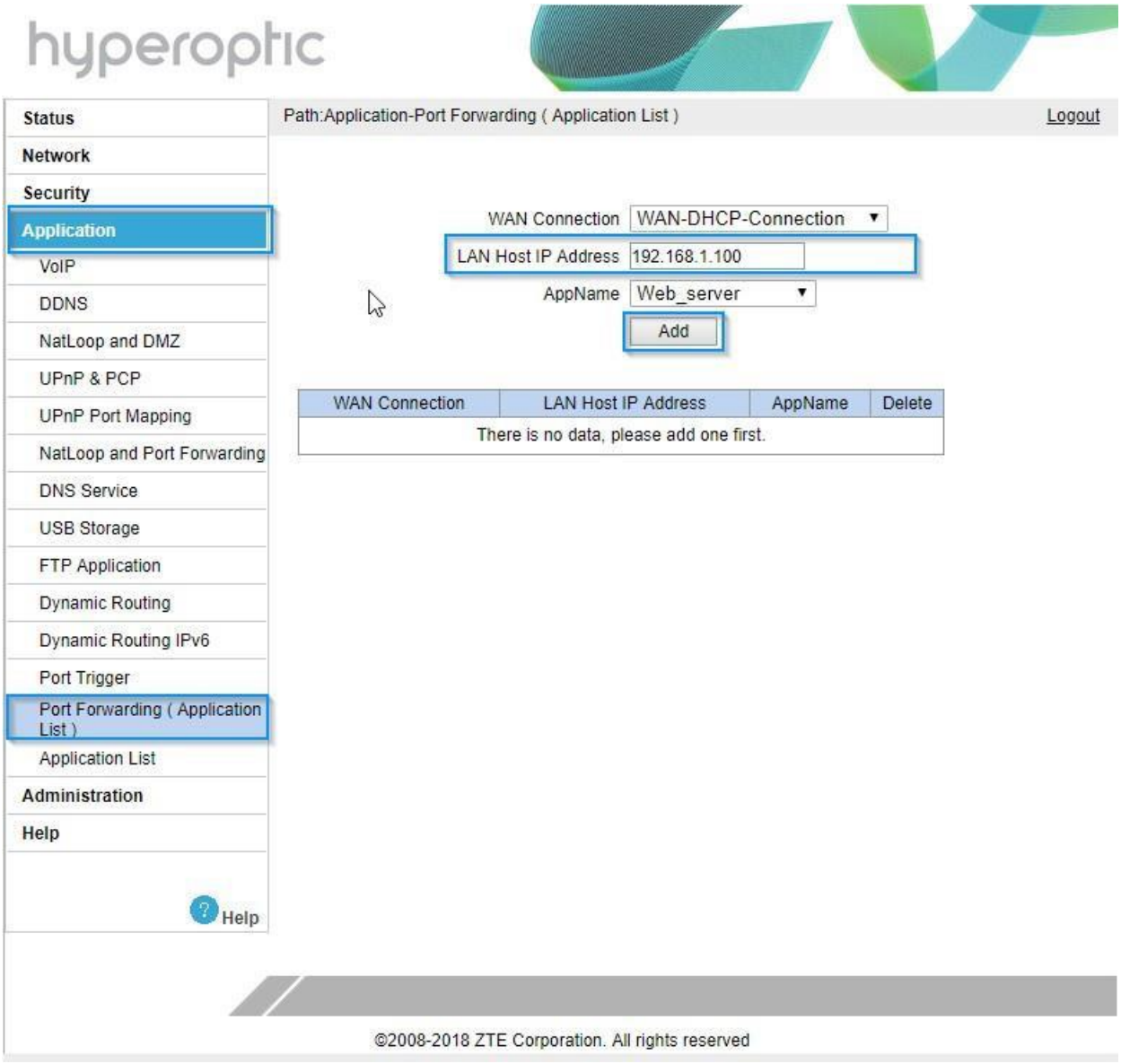


Image 25. Linking application with the LAN host

If the application is linked with the LAN device, you should see confirmation as illustrated in Image 26.

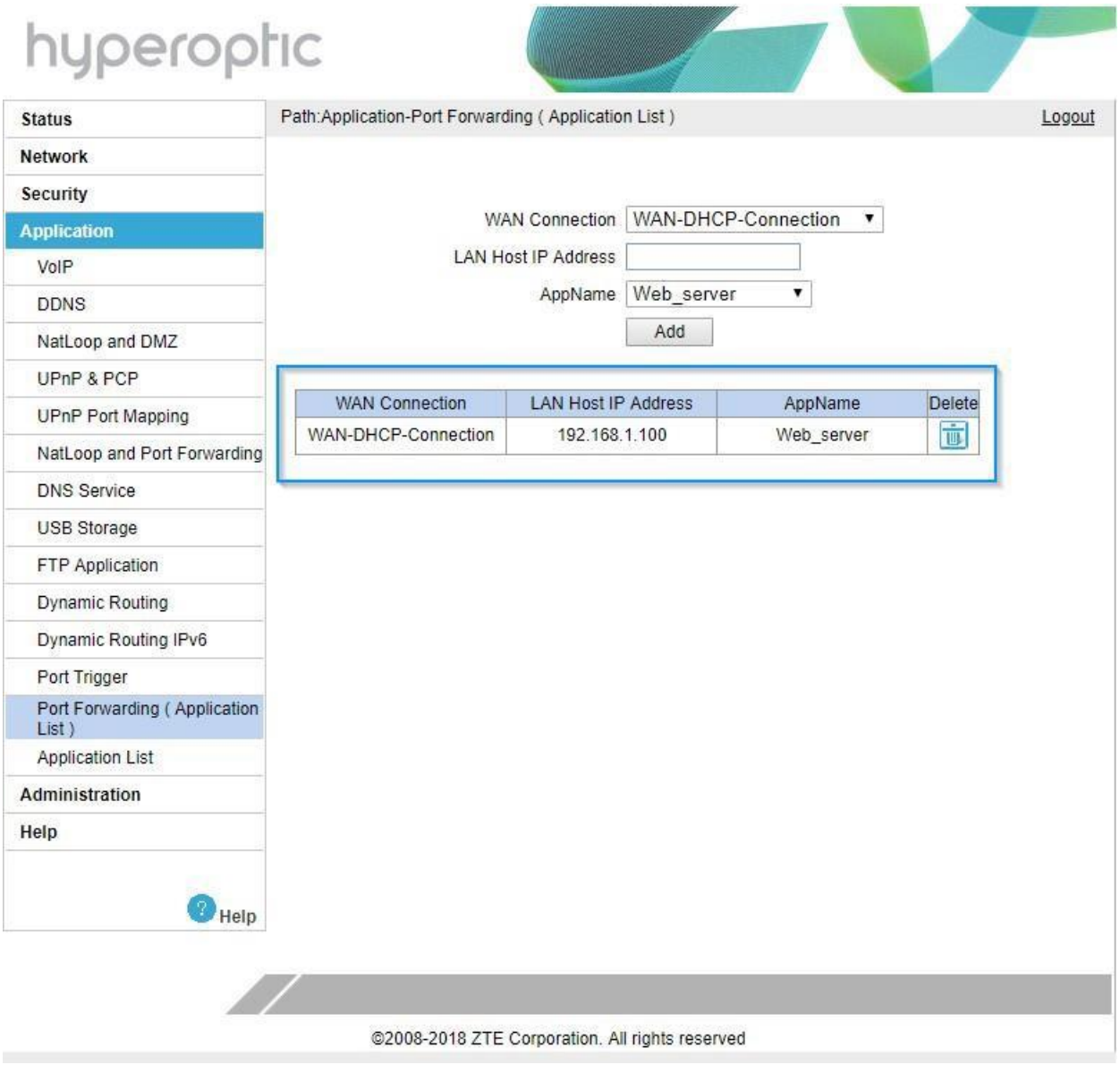


Image 26. Confirmation that port forwarding is configured

Alternatively, the router can be configured to perform port mapping (port translation) during port forwarding. To configure the router in this way, navigate to **Application > NatLoop and Port Forwarding** (see Image 27). In this example, the router will map traffic with destination port 12001 to port 8080. Inbound traffic on WAN ethernet port with destination port 21001 will be forwarded to LAN server. After all parameters are set, click **Add** to save router configuration.

Please also note that ports 80 and 443 **should never be used on WAN side**, as these ports are reserved for Hyperoptic Ltd. remote management. If you would like to use these ports on your server in a LAN, then you can use different ports on WAN side, e.g. you can use ports on WAN side 12000, 12001 and map them to LAN ports 80, 443 respectively). See image 27.

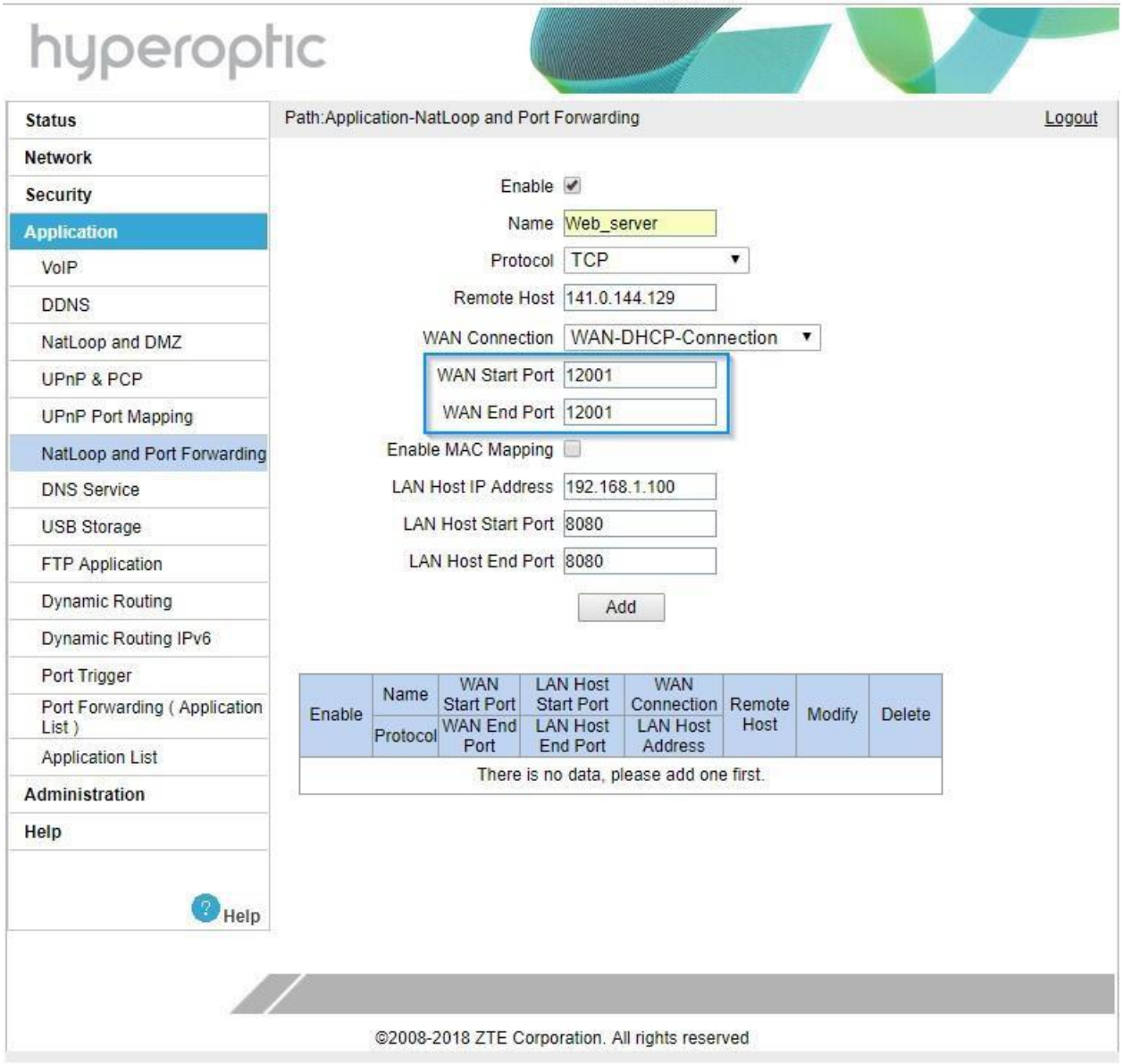


Image 27. Port forwarding with port mapping

A list of commonly used port is illustrated in Image 28. For additional information about TCP and 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 28. 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 **Application > NatLoop and DMZ** (see Image 29).

Click **Enable**. Select **WAN Connection** as **WAN-DHCP-Connection**. List the **LAN Server IP address**. Click **Submit**.

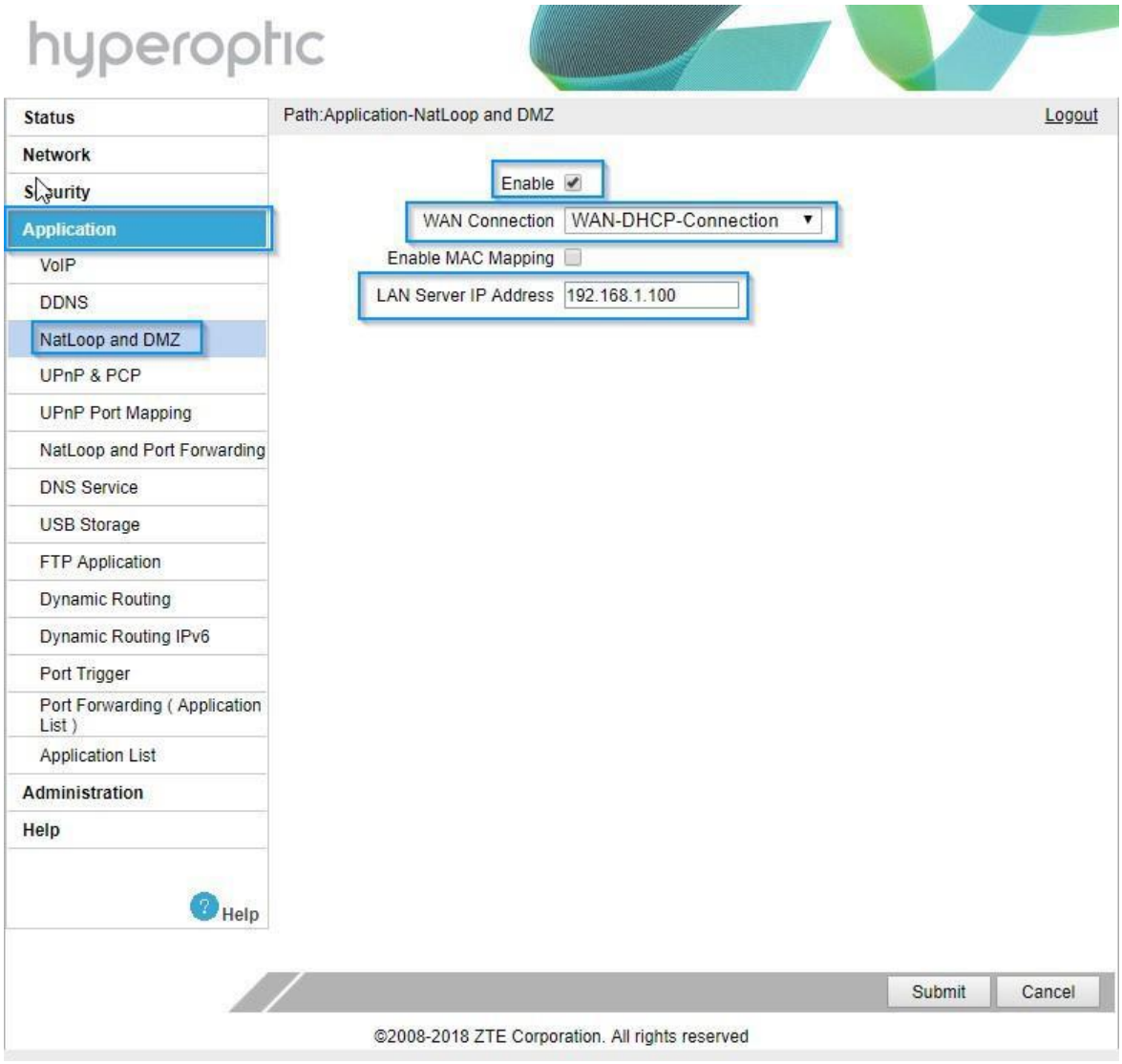


Image 29. DMZ configuration on router

# IPv6 Filter

IPv6 servers placed in LAN can be accessed from any remote IPv6 address. Access can be granted using the router's IPv6 filters. To configure a Hyperoptic router, navigate to **Security > IP Filters(IPv6)**. Image 30 illustrates an example of a local IPv6 web server.

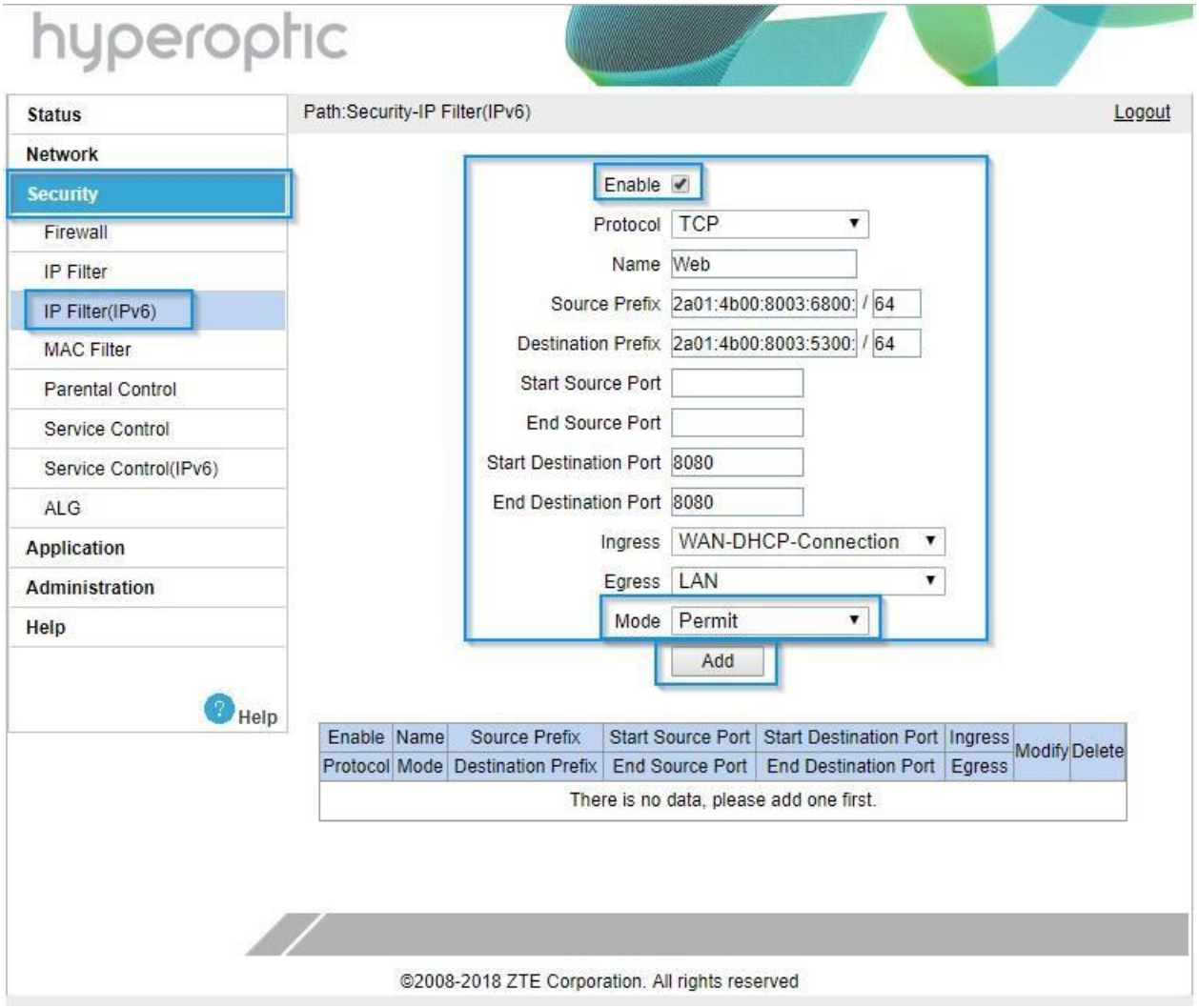


Image 30. IPv6 filter configuration

Click **Enable** to make the filter rule active.

For web servers, use **TCP** as **Protocol** type.

Use any **Name** for the filter.

List the **Source Prefix** (IPv6 address range of remote computers) - for example, **2a01:4b00:8003:6800::** with prefix length **64**.

For **Destination Prefix,** use the address range assigned to the router. In the example illustrated in Image 30, this range is **2a01:4b00:8003:5300::** with prefix length **64**.

**Start Destination port** and **End destination port** define the range of ports that will be allowed to pass through local router. In this case only one port is permitted – port **8080**.

Define **Ingress** and **Egress** ports as per Image 30.

Choose **Permit** mode and click **Add** to save router configuration. Once configured, confirmation should appear as illustrated in Image 31.

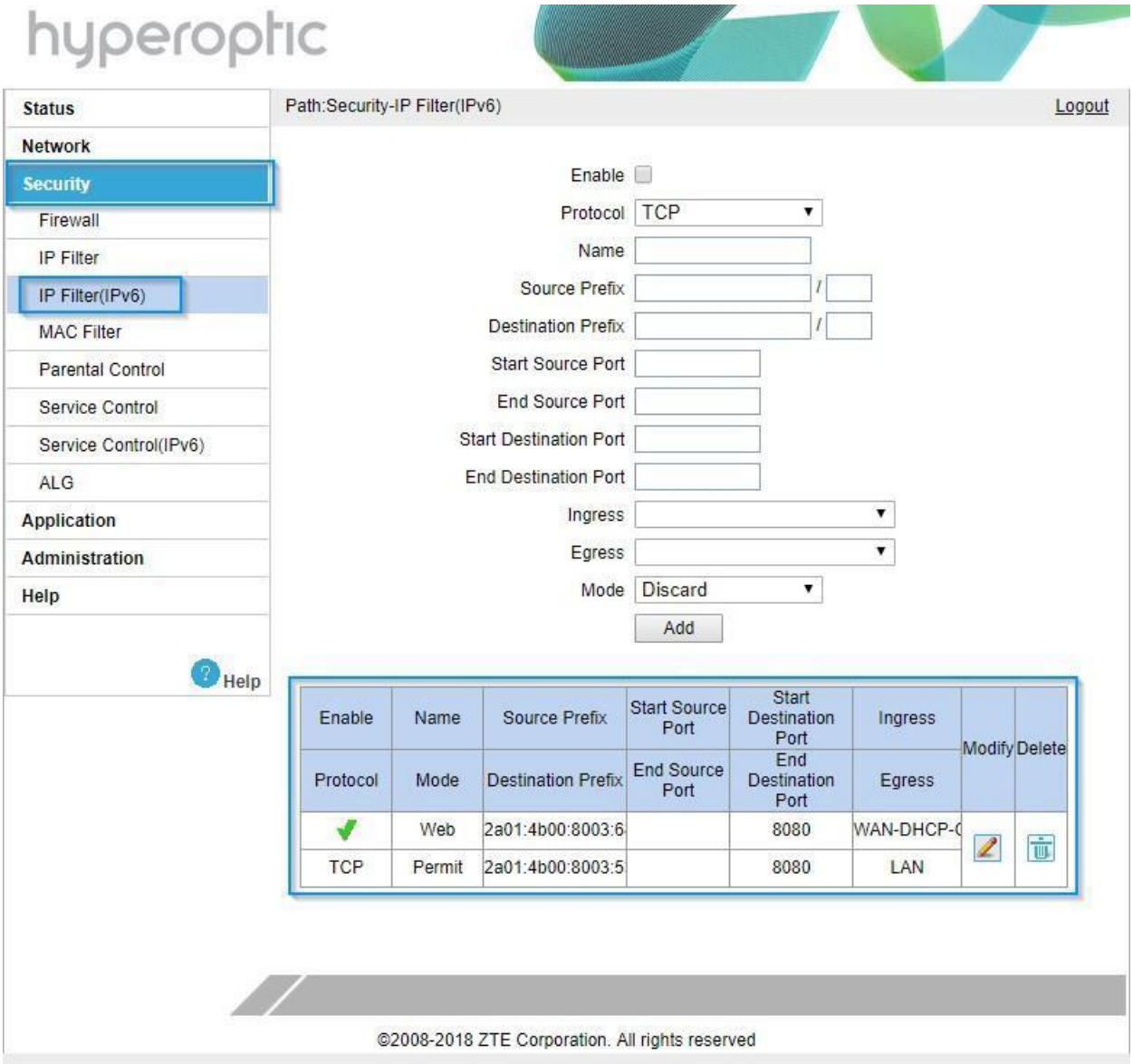


Image 31. Confirmation that IPv6 filter is made and Enabled

# DHCP Binding

Specific LAN client can have same IPv4 address all the time. To define which LAN client will have which IPv4 address, configuration of binding must be completed. This is described in image 32. Navigate to section **Network > LAN**.

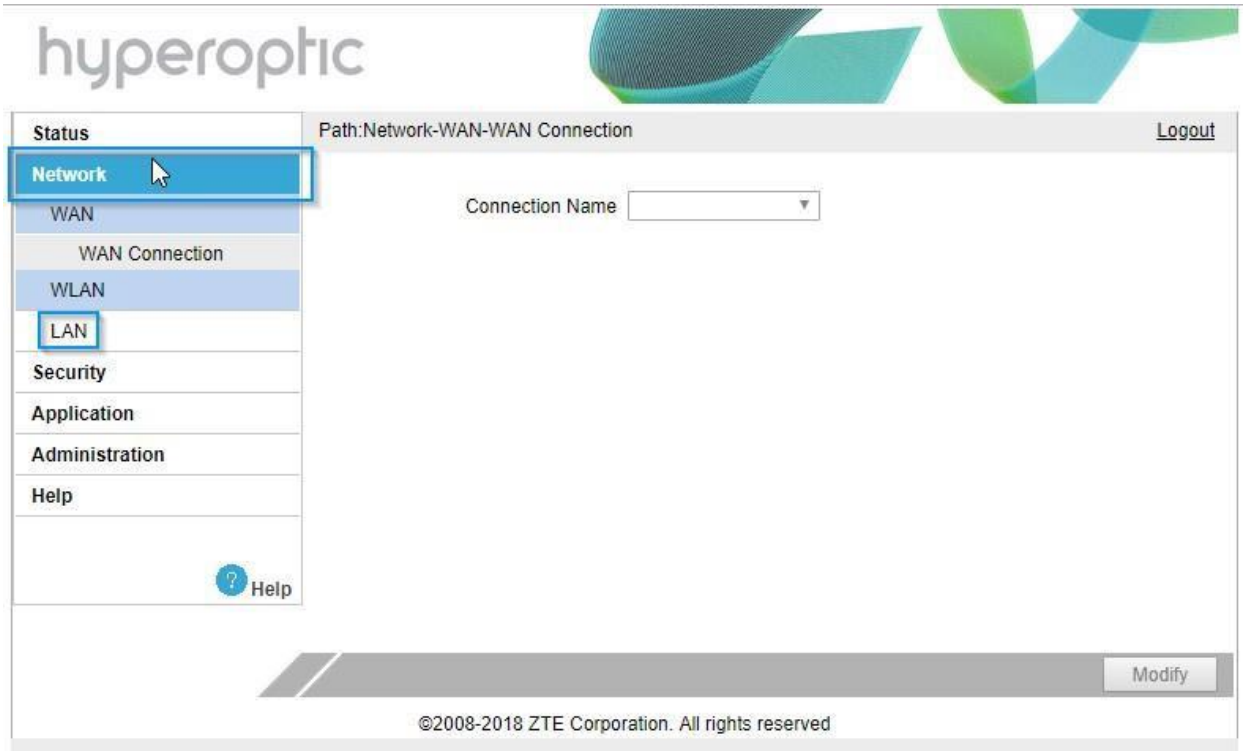


Image 32. LAN section of router configuration

Click on **LAN** segment and then click on **DHCP Binding**. This is described in image 33. List IPv4 wanted address and list MAC address of LAN client. After configuring these parameters click on **Add** to save settings.

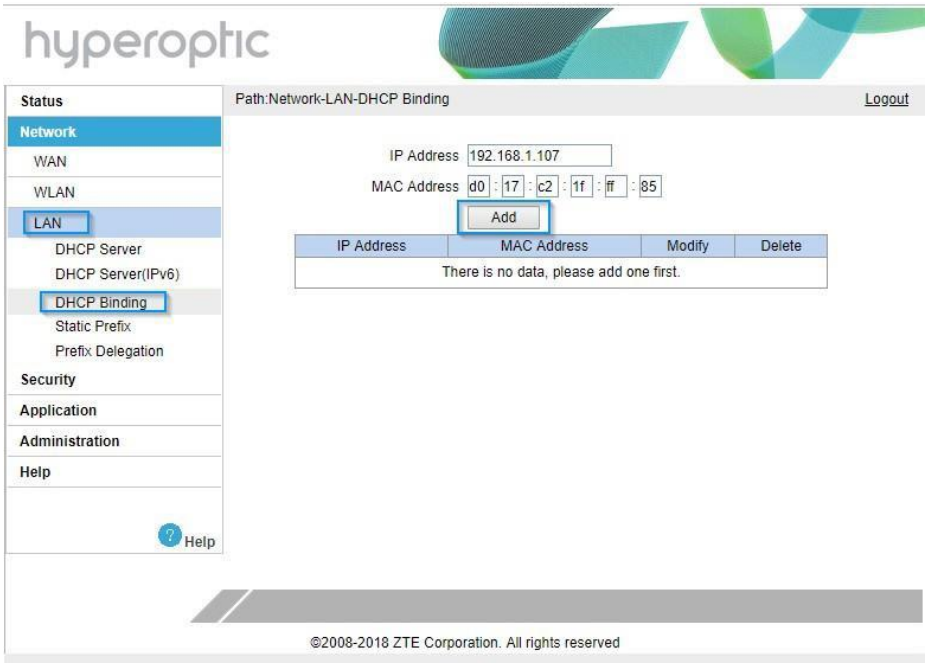


Image 33. Configuring DHCP binding

Confirmation of configuration looks like described in Image 34.

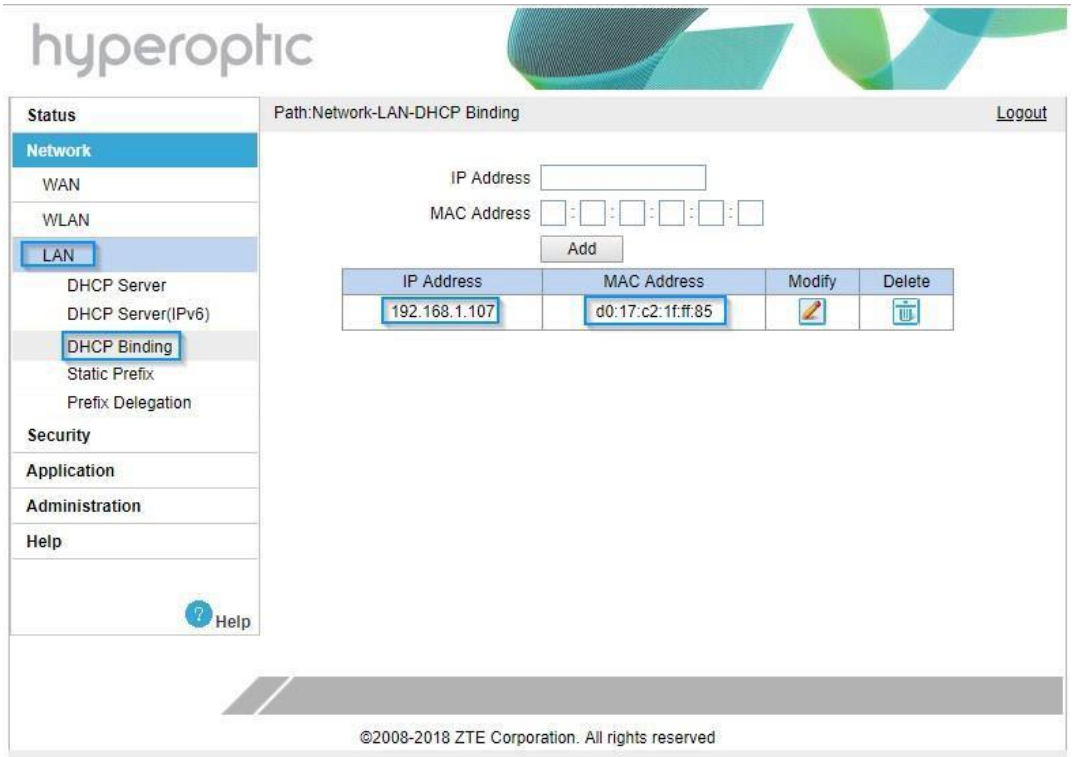


Image 34. Confirmation of DHCP binding

# Public IPv4 address block in LAN network

Navigate to **Network > LAN > DHCP Server**. Image 35 describes example of public block 137.220.108.0/29. Take first address from the IPv4 block and assign it to the router – **Secondary IP Address** field. Populate **Subnet mask** field as per table 1. Click **Submit** at the bottom of the page to save settings.

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** |

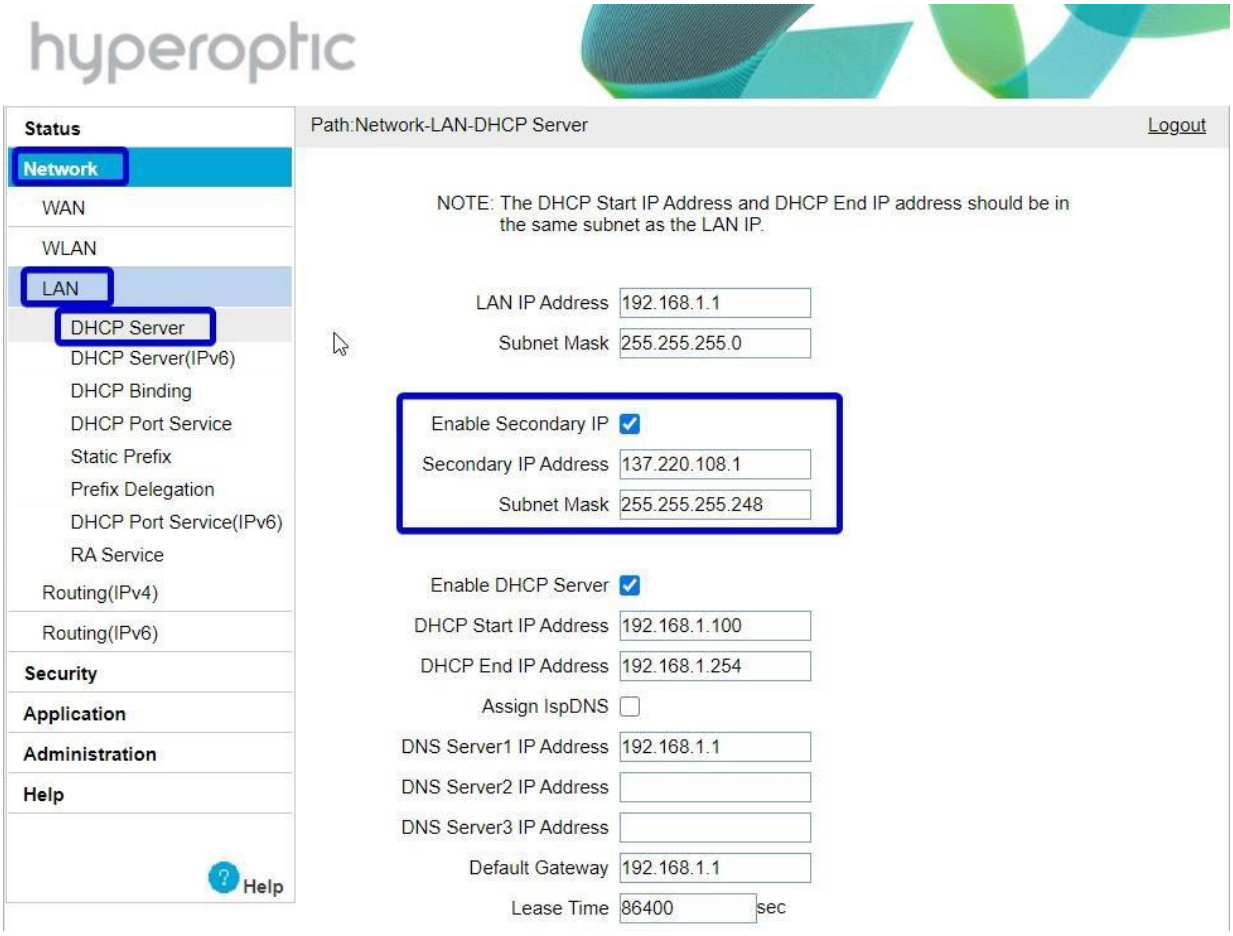


Image 35. Setting secondary IP block

Navigate to **Network > WAN > WAN Connection**. Select **WAN-DHCP-Connection** from first dropdown menu. Untick **Enable NAT** option and click **Modify** at the bottom of to save settings.

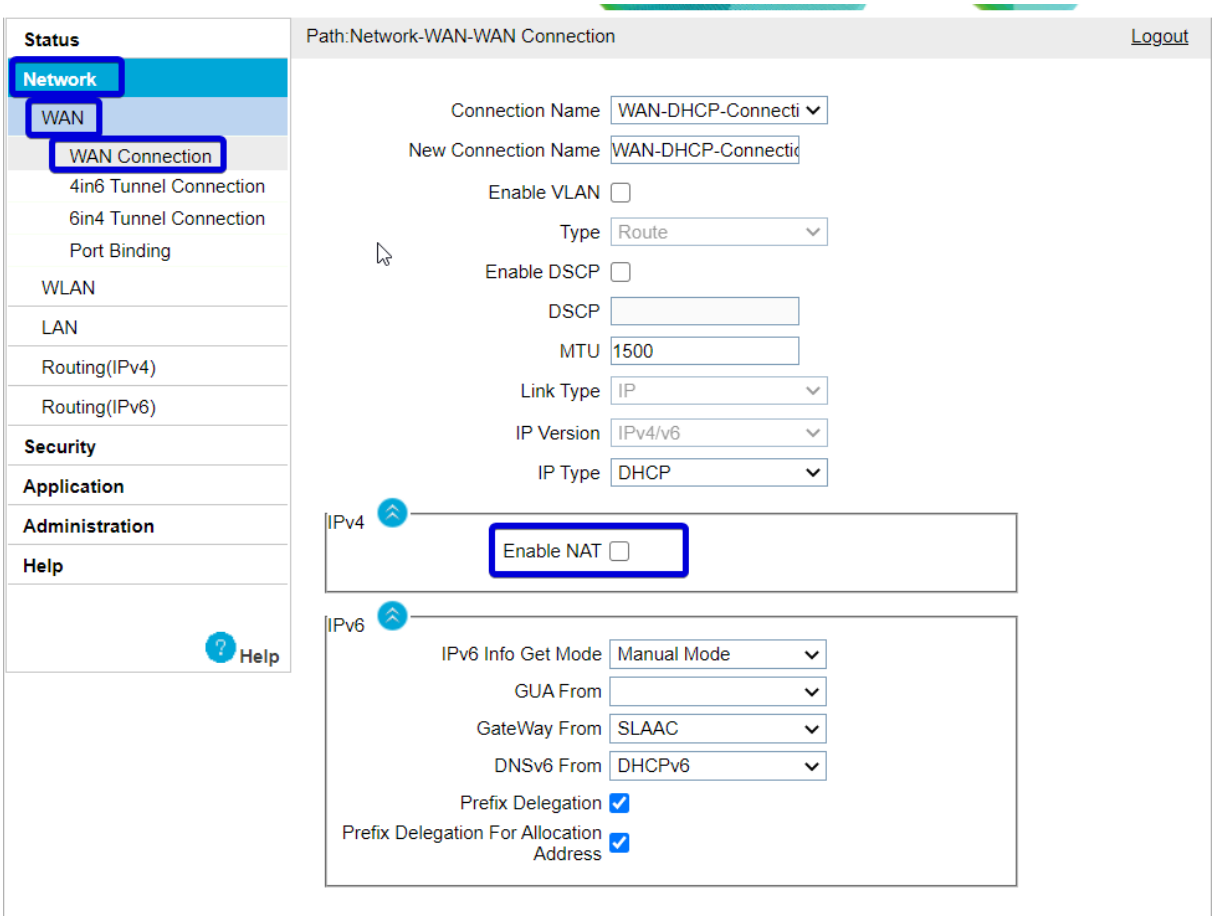


Image 36. Disabling NAT on the router

# DDNS – Dynamic DNS

You can use Dynamic DNS to associate a fully qualified domain name (FQDN) with a public IPv4 address, which is present on WAN router interface. With this feature, you can access your router via a "descriptive" name, rather than via its IPv4 address.

To access this feature, please navigate to **Application > DDNS**.

Before setting parameters on the router, please register the FQDN with a DNS provider (e.g. https://now-dns.com/). Tick **Enable**, select **Service Type** from the dropdown menu, enter **Server** location, and the **Username** and **Password** which were used in registration process. For **WAN Connection,** select **WAN-DHCP-Connection**. Click **Submit** (see image 37).

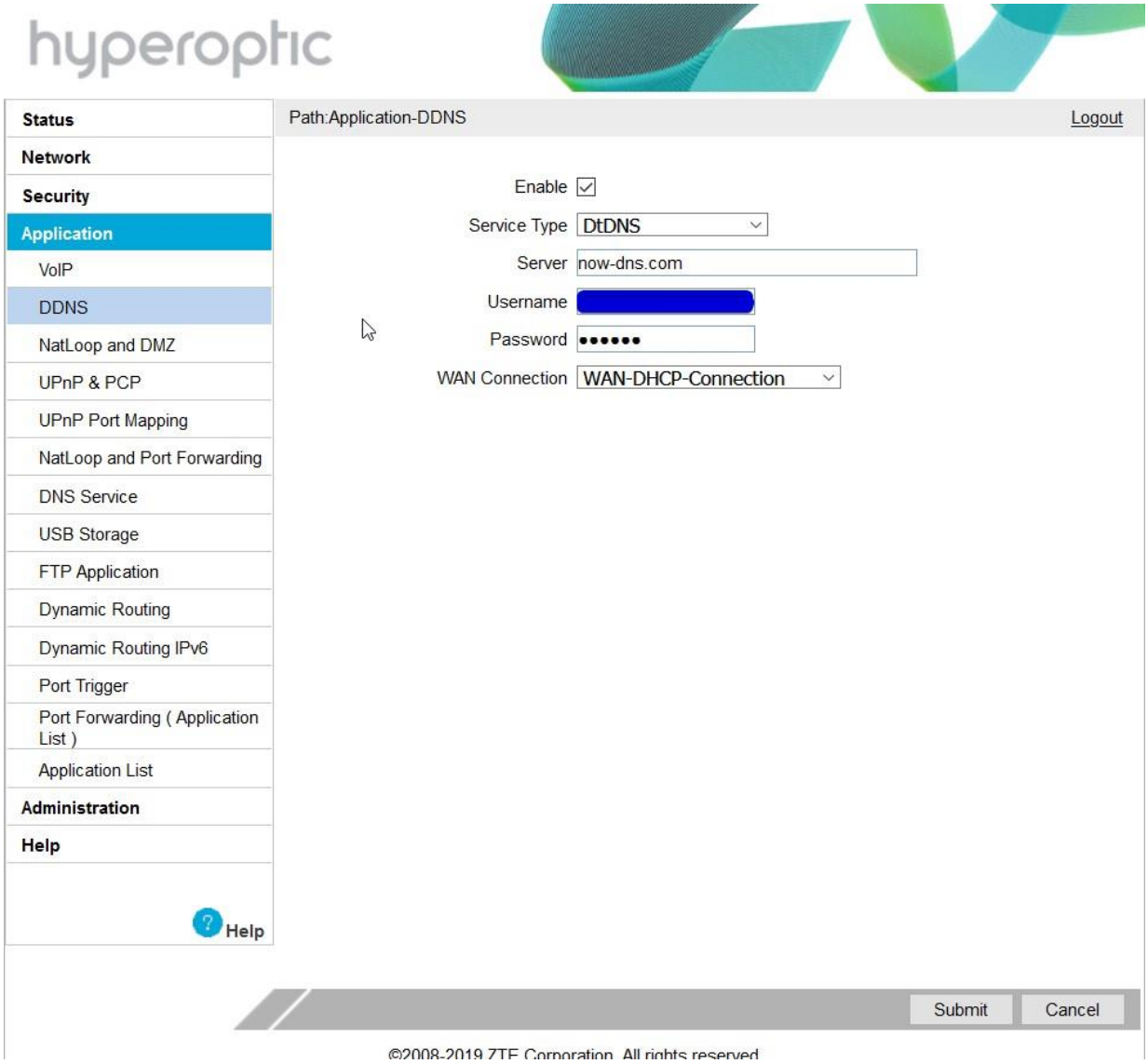


Image 37. Configuration section for DDNS

Confirmation can be seen in image 38. Router web GUI is seen after entering example FQDN of *mytest222.dtdns.org* in the web browser.

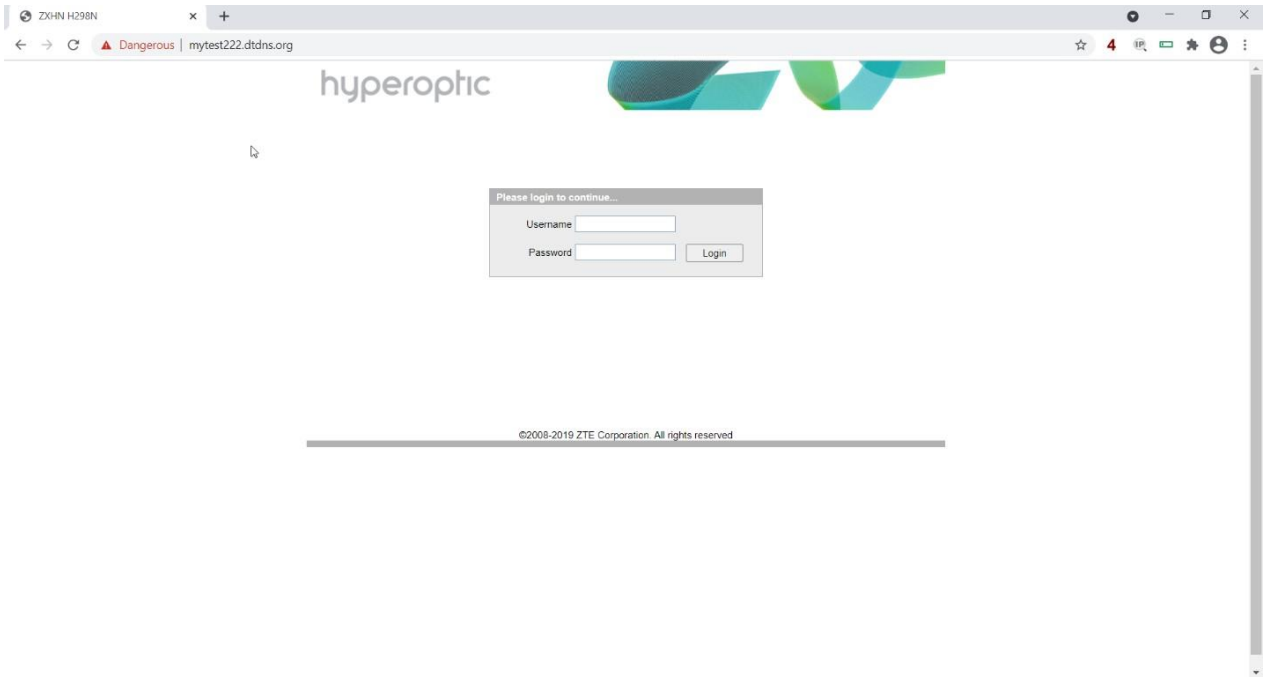


Image 38. Reaching ZTE H298N router via registered FQDN

Once this is done, please contact Customer Support to complete the process.