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**.

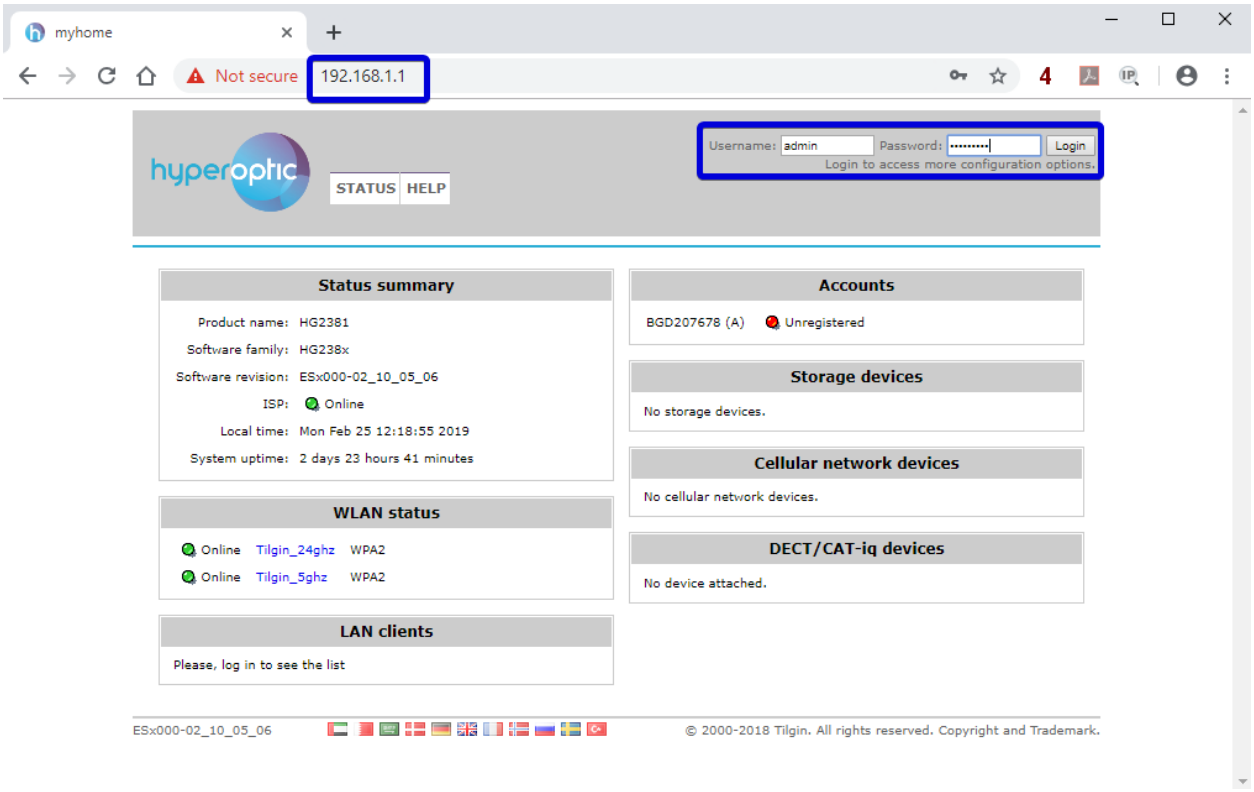

Image 1. Router HG2381 login screen

UPnP

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 **Advanced > Connection settings > UPnP**. See Image 2. If you're not using UPnP applications, UPnP should be set to Off (the default UPnP setting is Off).

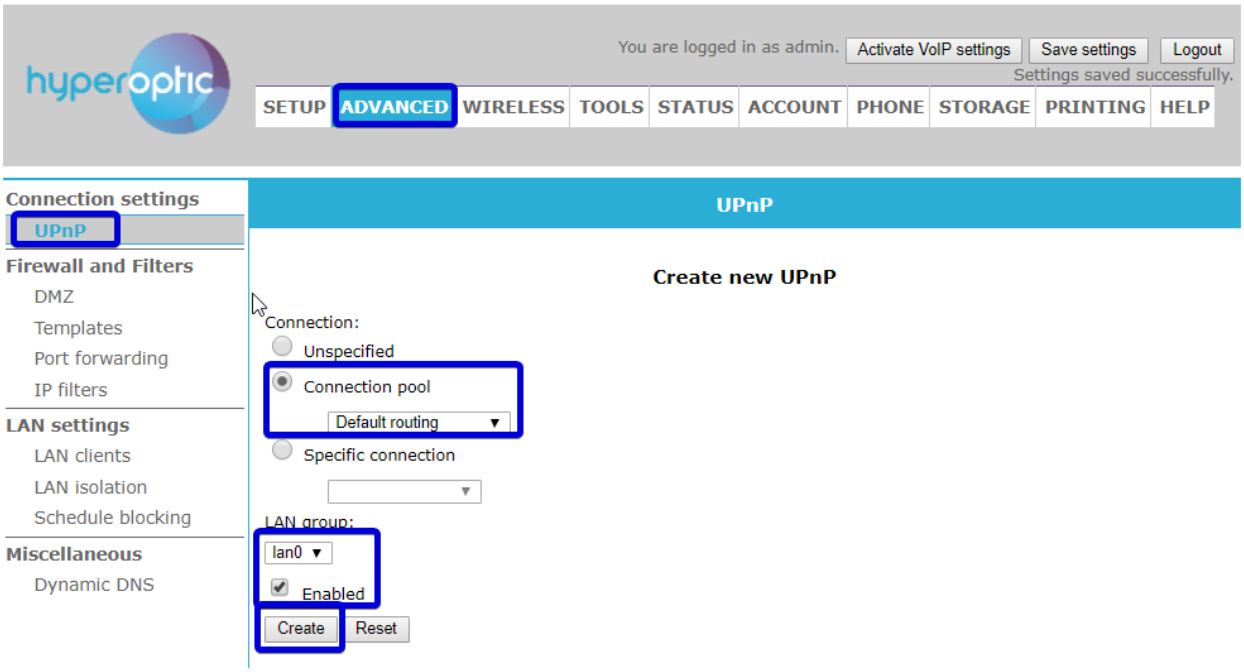

Image 2. Setting up UPnP service

Select options as in image 2, tick **Enabled** and click **Create**. Once this is done, click **Save settings** in the upper right side of the screen. You should see confirmation as per image 3.

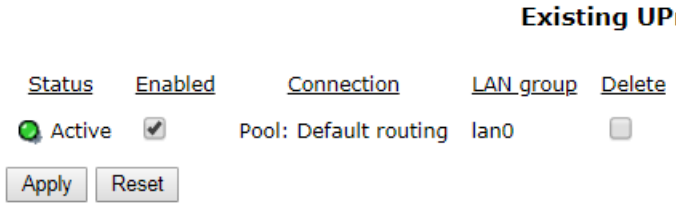

Image 3. Confirmation of UPnP settings

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 **Advanced > LAN settings > LAN clients**. Select the device which needs to be blocked and click **Apply**. This part of the process will create static DHCP binding for certain MAC address (LAN client). See Image 4.

If clicked on IPv6 button, IPv6 address of LAN client will be displayed.

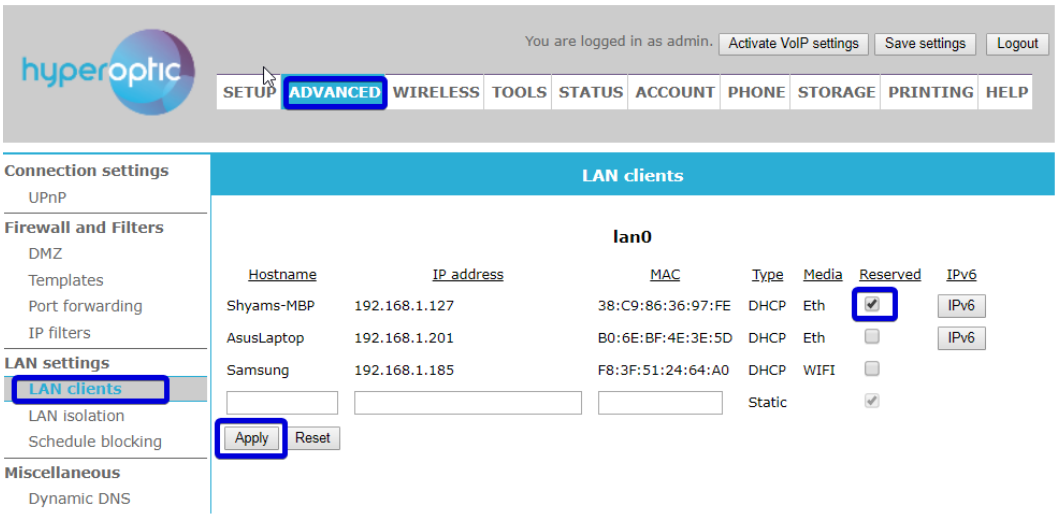

Image 4. Defining which LAN client will be blocked

Once completed, navigate to **Advanced > LAN settings > Schedule blocking**. Select the day and time you would like to restrict access and click **Apply**. Then click **Save settings**. See Image 5.

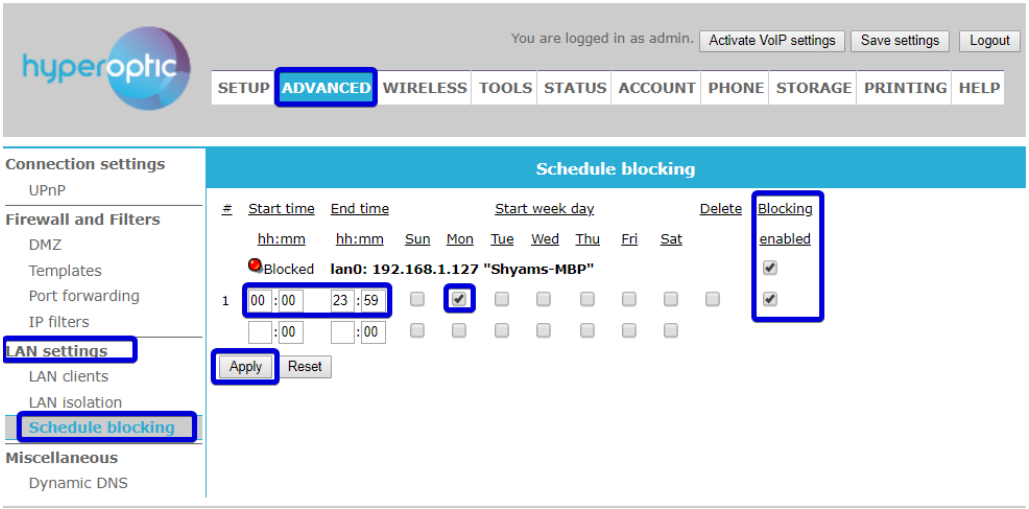

Image 5. Defining blocking time & day per week basis

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 **Advanced > LAN settings > LAN clients**. The connection type will be listed for every LAN client (see Image 6), and you'll be able to see all the devices that are using your router's LAN.

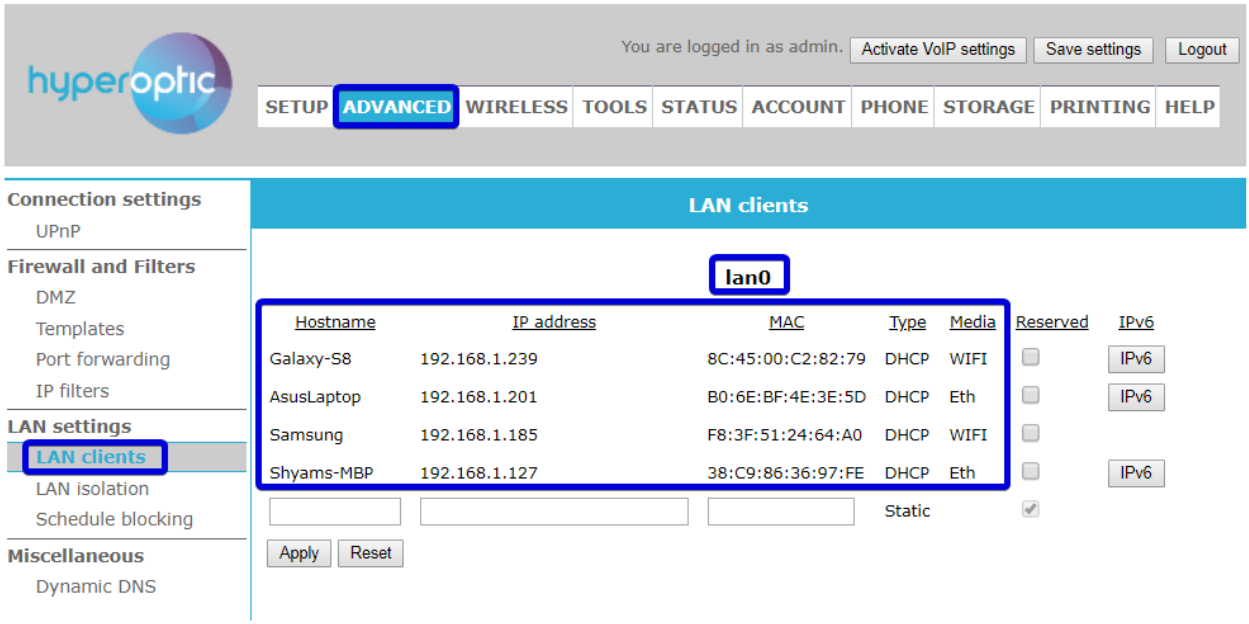

Image 6. Overview of LAN clients

Wi-Fi name (SSID) and password change

To change your wifi name or password for 2.4 GHz or 5 GHz bands, log into your router (see page 2) and navigate to **Wireless**. To change the parameters of your wifi connection, click on the **SSID** in the **Existing SSIDs** section. Configuration changes are the same for 2.4 GHz and for 5 GHz. See Image 7, where we've used 2.4 GHz for demonstration purposes.

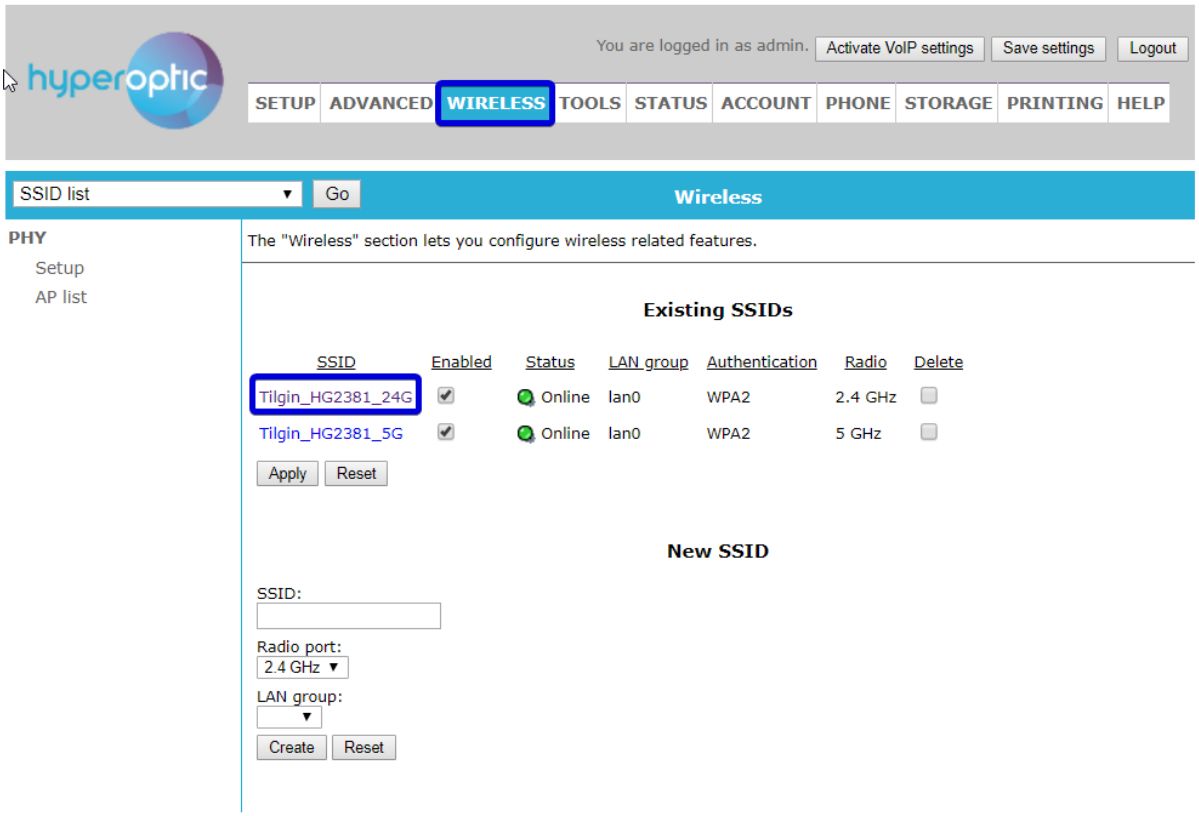

Image 7. Overview of existing Wi-Fi SSIDs

To change name of your wifi connection, navigate to **Wireless > SSID > Configuration**. Provide your desired connection name and then click **Apply** and **Save settings**. See Image 8.

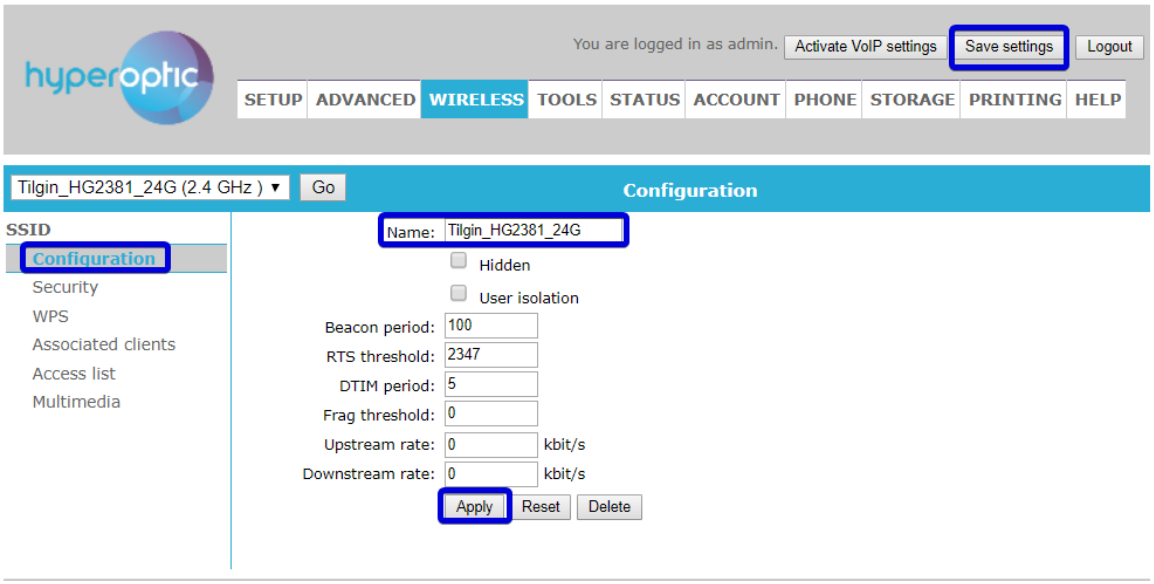

Image 8. Change of 2.4GHz connection name

To change your wifi password, navigate to **SSID > Security**. See Image 9. Please use passwords containing upper and lower-case letters and numbers, with a minimum of 12 characters in length. Once you've decided on a password, click **Apply** and **Save settings**.

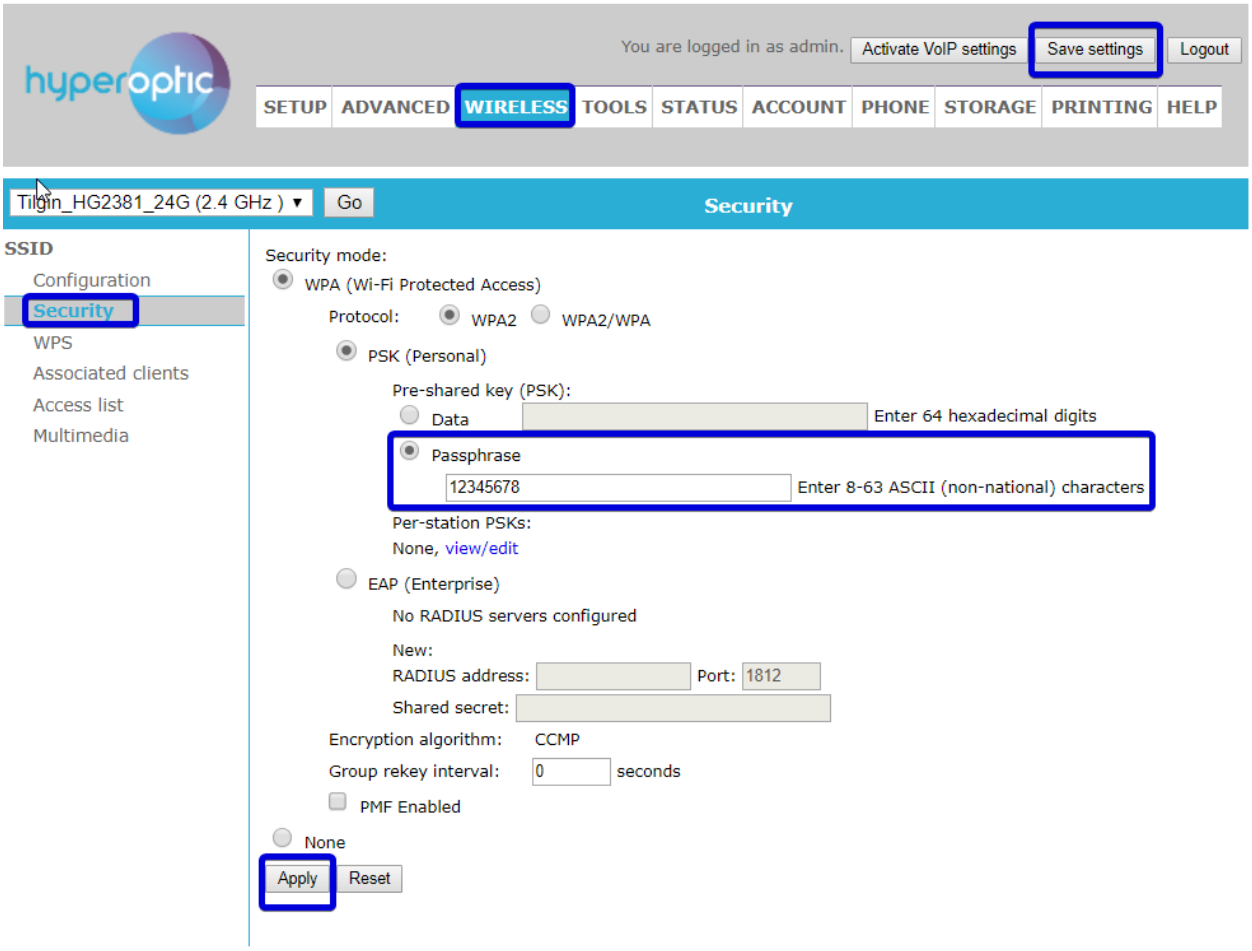

Image 9. Wi-Fi password change

Security modes of Wi-Fi

To change authentication setting for Wi-Fi, navigate to section **Wireless**. Click on either the **2.4GHz** or **5GHz** connection. Configuration is identical for both connections (see Image 10 for 2.4GHz example). Protocol **WPA2** or **WPA2/WPA** can be selected. After the protocol change, click **Apply** and **Save settings**. By default, advanced encryption algorithm is used.

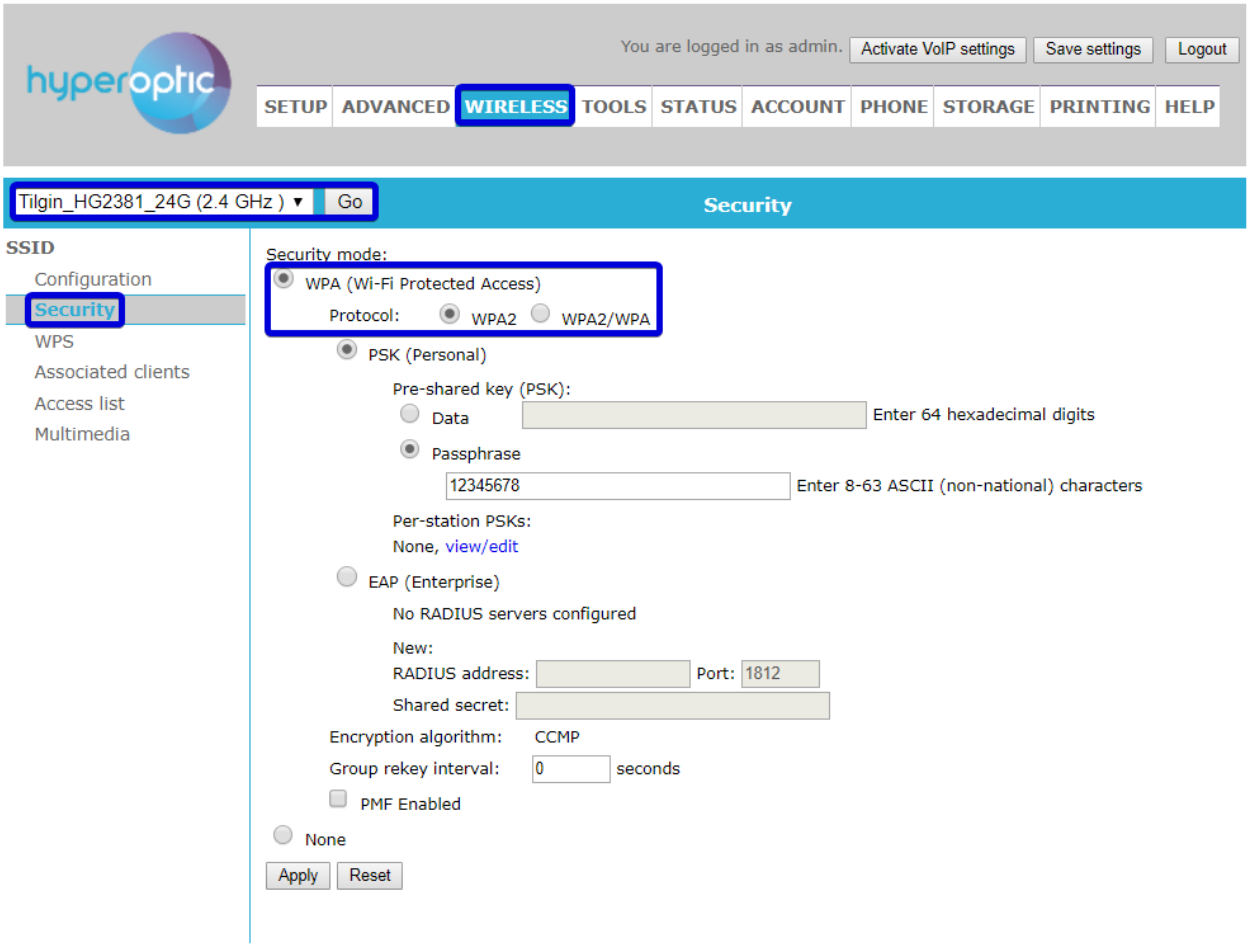

Image 10. Change of Wi-Fi security protocols

Creating new SSID

To create a new SSID, please log into your router (page 2) and navigate to **Wireless.** Under **New SSID**, use any name (e.g. New_2.4GHz), select **2.4 GHz** or **5GHz radio port** and select **lan0** LAN group. Click **Create**. See Image 11. If a new 5GHz network is needed, select 5 GHz radio port from the drop-down menu. The configuration steps for 2.4GHz SSID and 5GHz SSID are the same.

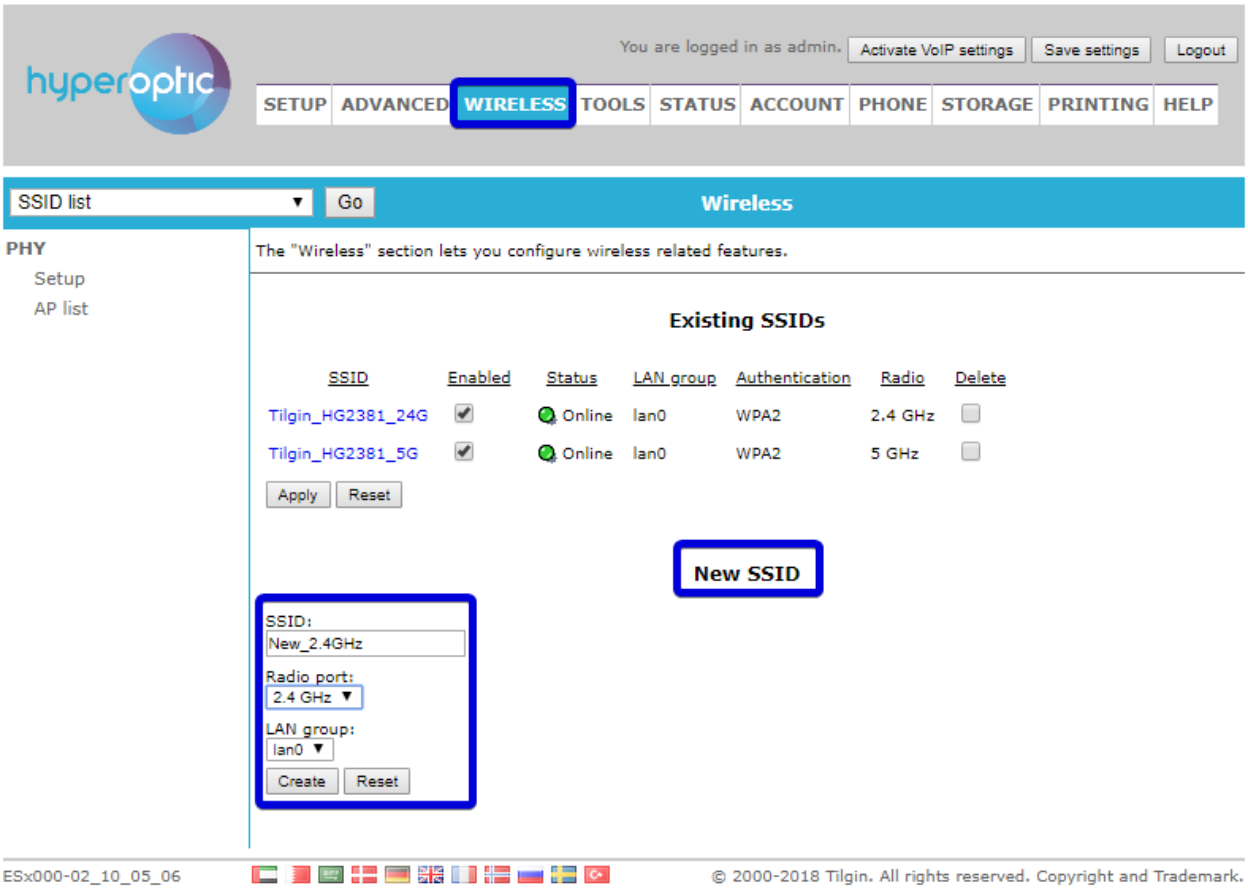

Image 11. Creating new SSID

Once your new SSID (in this case 2.4GHz) is created, you can change the passphrase of the SSID. Click **Apply** and **Save settings** in the upper right corner of the web page (see Image 12).

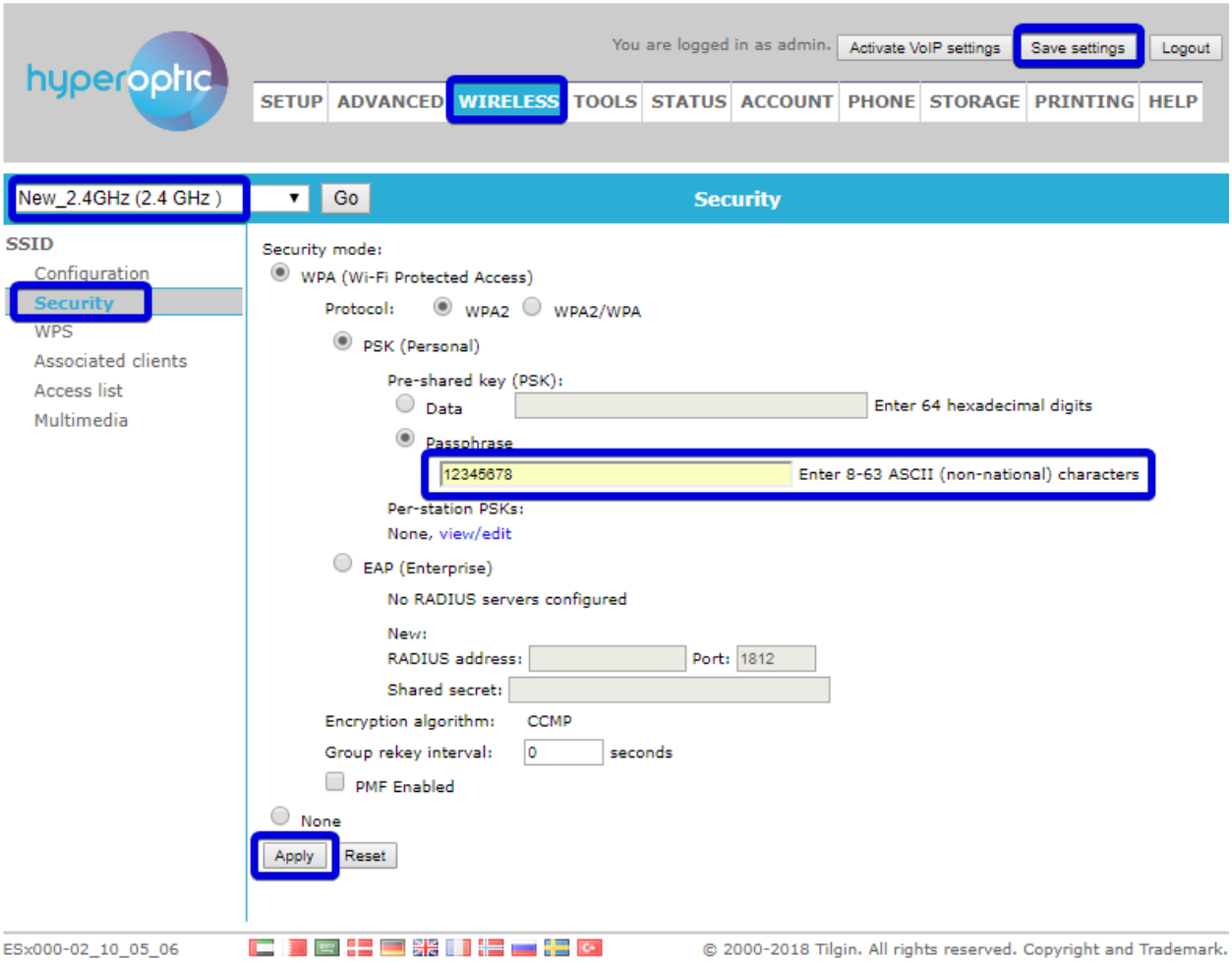

Image 12. Defining password for new SSID

Changing Wi-Fi channel

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 **Wireless > Setup**. Select either **2.4GHz** or **5GHz** frequency band. Once selected, refer to **Channel**. Select **Manual** configuration and choose one of the listed channels from the drop-down menu. Click **Apply** and **Save settings**. See Image 13 and Image 14.

Note: please avoid using channel 11 for 2.4GHz networks.

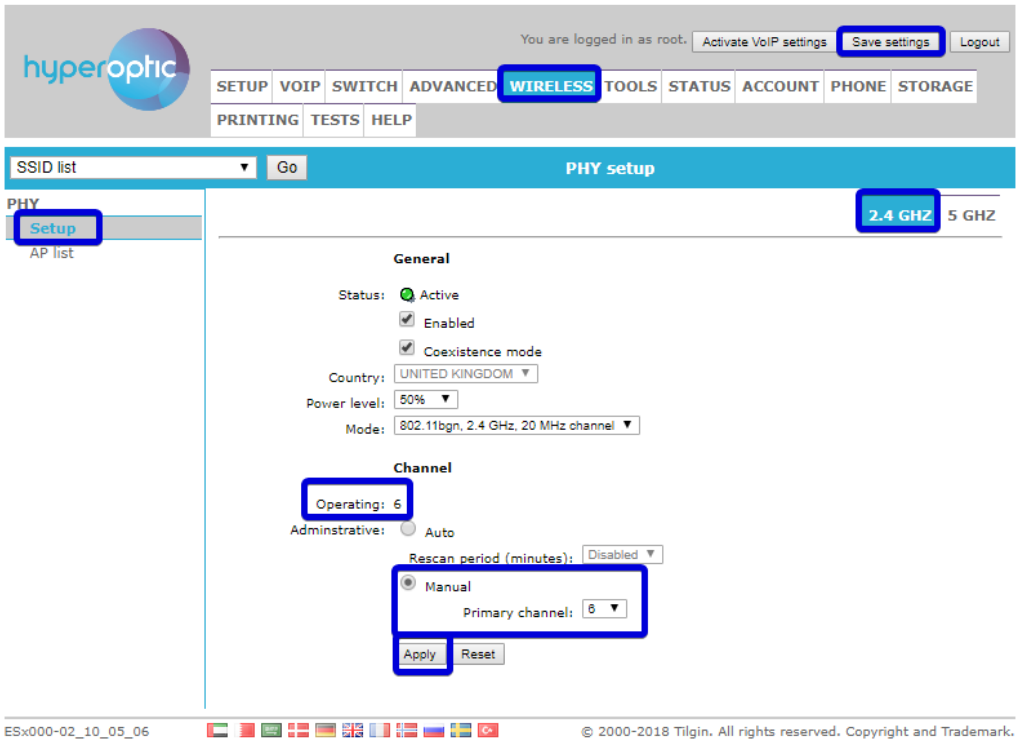

Image 13. Setting channel for 2.GHz network

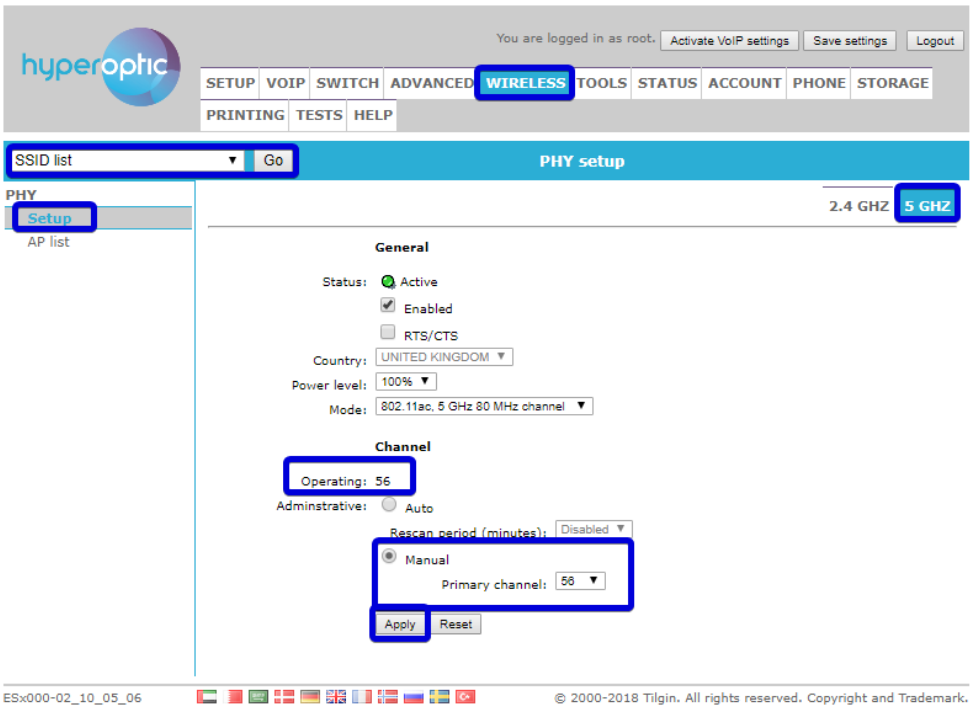

Image 14. Setting channel for 5GHz network

Deleting existing SSID

To delete an existing SSID, please log into your router (page 2) and navigate to **Wireless**. Tick **Delete** on the network you'd like to delete. Click **Apply** and **Save settings** (see Image 15).

Image 15. Deleting existing SSID

WPS

To connect to wifi without a password, please log in to your router (see page 2) and navigate to **Wireless.** Click on the desired SSID and go to **SSID > WPS**. See Image 16. Click **Add device**. Wait a few seconds and then click the WPS button on the desired LAN client. A wifi connection will then be made.

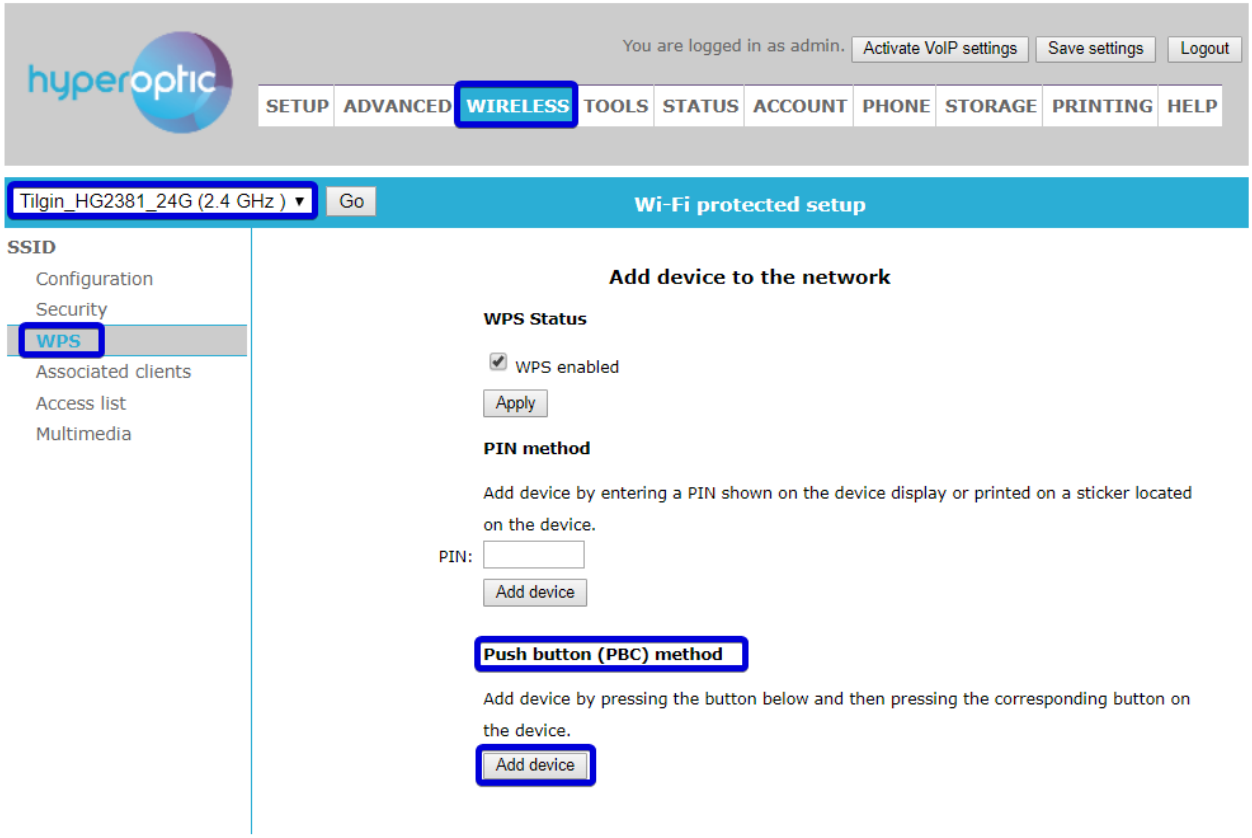

Image 16. WPS button and access method

Wi-Fi associated clients

For each SSID, the number of LAN clients can be checked. To check LAN Wi-Fi clients, navigate to **Wireless**. Click on the **2.4GHz** or **5GHz** connection. Under **SSID > Associated clients,** the MAC address of every LAN user is listed. See image 16.

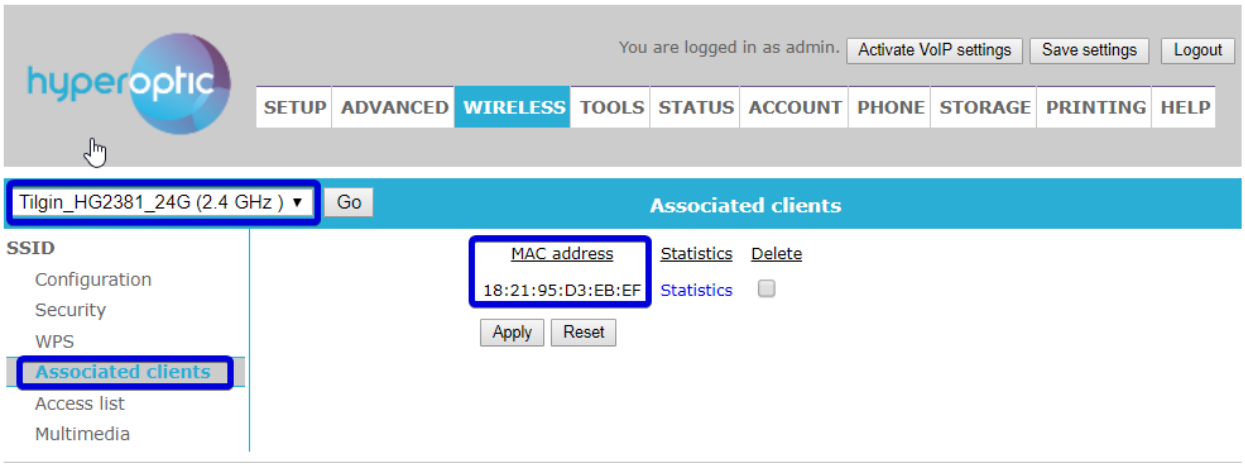

Image 16. Wi-Fi 2.4GHz LAN clients

Change of admin credentials

Your default admin credentials can be found on the router itself. If you'd like to make changes to these credentials, please contact Customer Support.

Factory reset and Restart of the router (admin account)

You can reboot your router via the web. Once you've logged in (see page 2), navigate to **Tools > Maintenance > Restart system**. Click on **Restart system**. See Image 17.

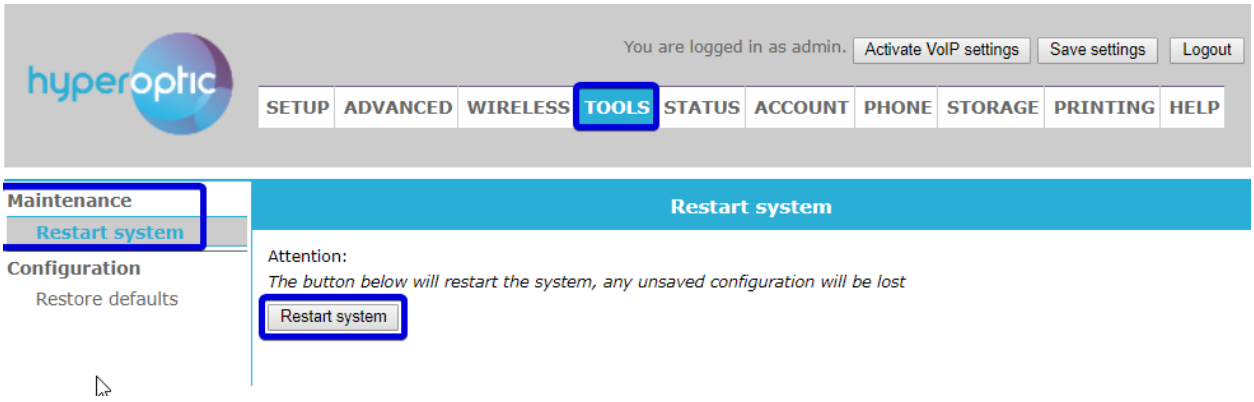

Image 17. Restart of router

To restore factory settings, navigate to **Tools > Configuration > Restore defaults**. Click on **Restore factory defaults**. See Image 18.

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.

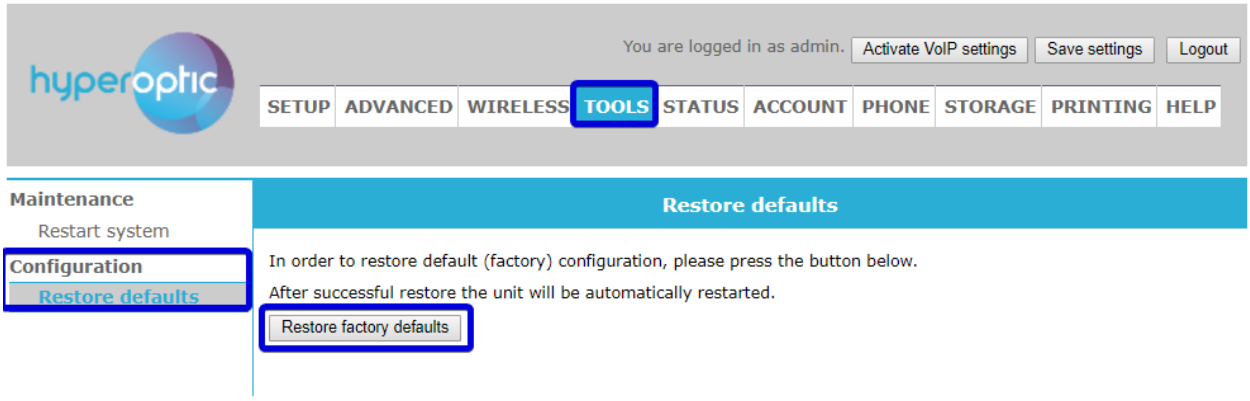

Image 18. Switching to factory router configuration

Access to USB flash drive attached to router

You can access the USB storage port on your router in a few ways. To access via HTTP protocol, please log into your router (page 2) and navigate to **Storage > General > Setup**. Click **Storage enabled** and **Enabled** under **Access via HTTP**. Click **Apply** and **Save settings**. To connect to flash drive type **http://ip_address/nas** into the browser. Router configuration is shown in Image 21. Router configuration is shown in image 19. Remote access is shown in image 20. Your router's USB port with attached flash drive can be used as additional storage, linked with LAN.

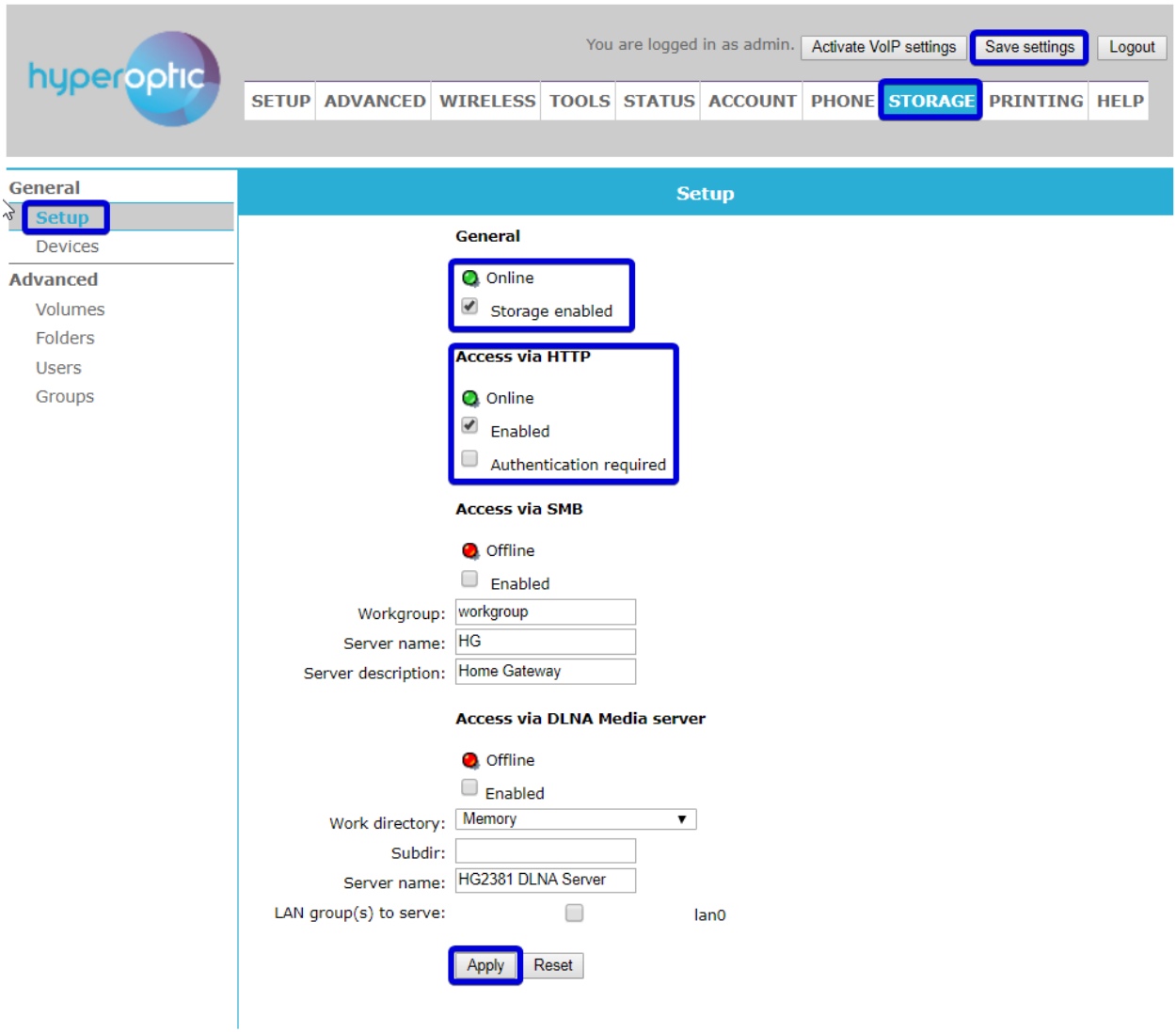

Image 19. Flash drive access via HTTP

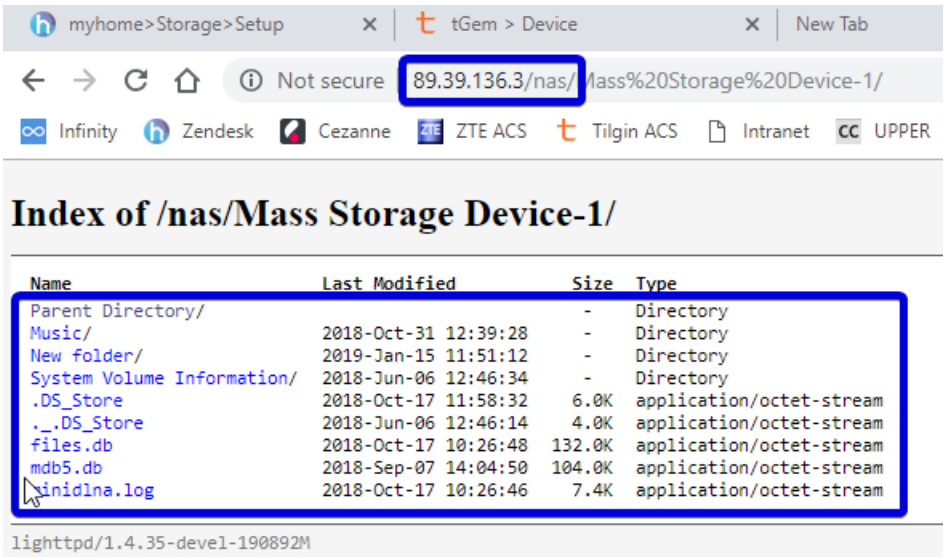

Image 20. Remote access to USB drive via http

To connect via SMB, click **Enabled** in the section **Access via SMB**. See Image 21. Once enabled, click **Apply** and **Save settings**. See Image 22 for SMB access.

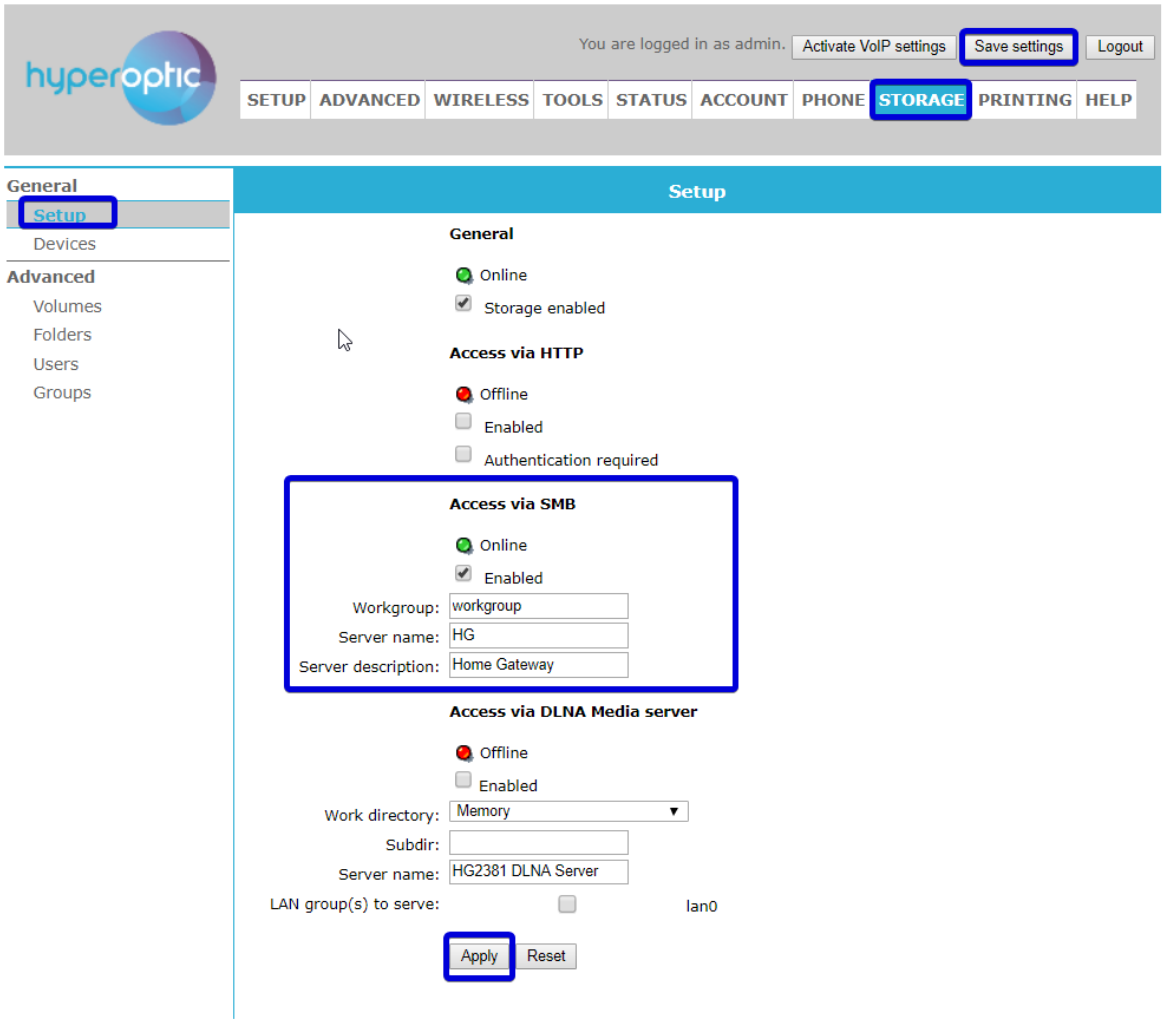

Image 21. Access to flash drive via SMB

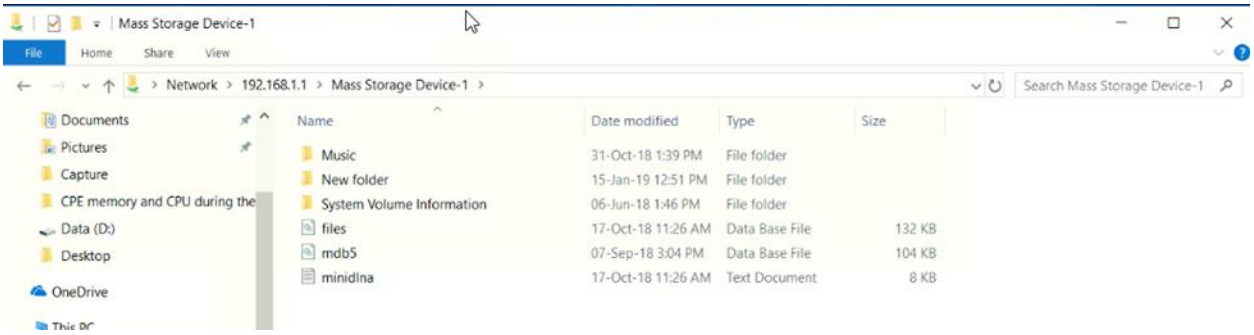

Image 22. LAN access via SMB (type ***192.168.1.1*** in browser search)

See Image 23 for access via DLNA Media server. Click to serve **lan0** group. Click **Enabled** and then **Apply**.

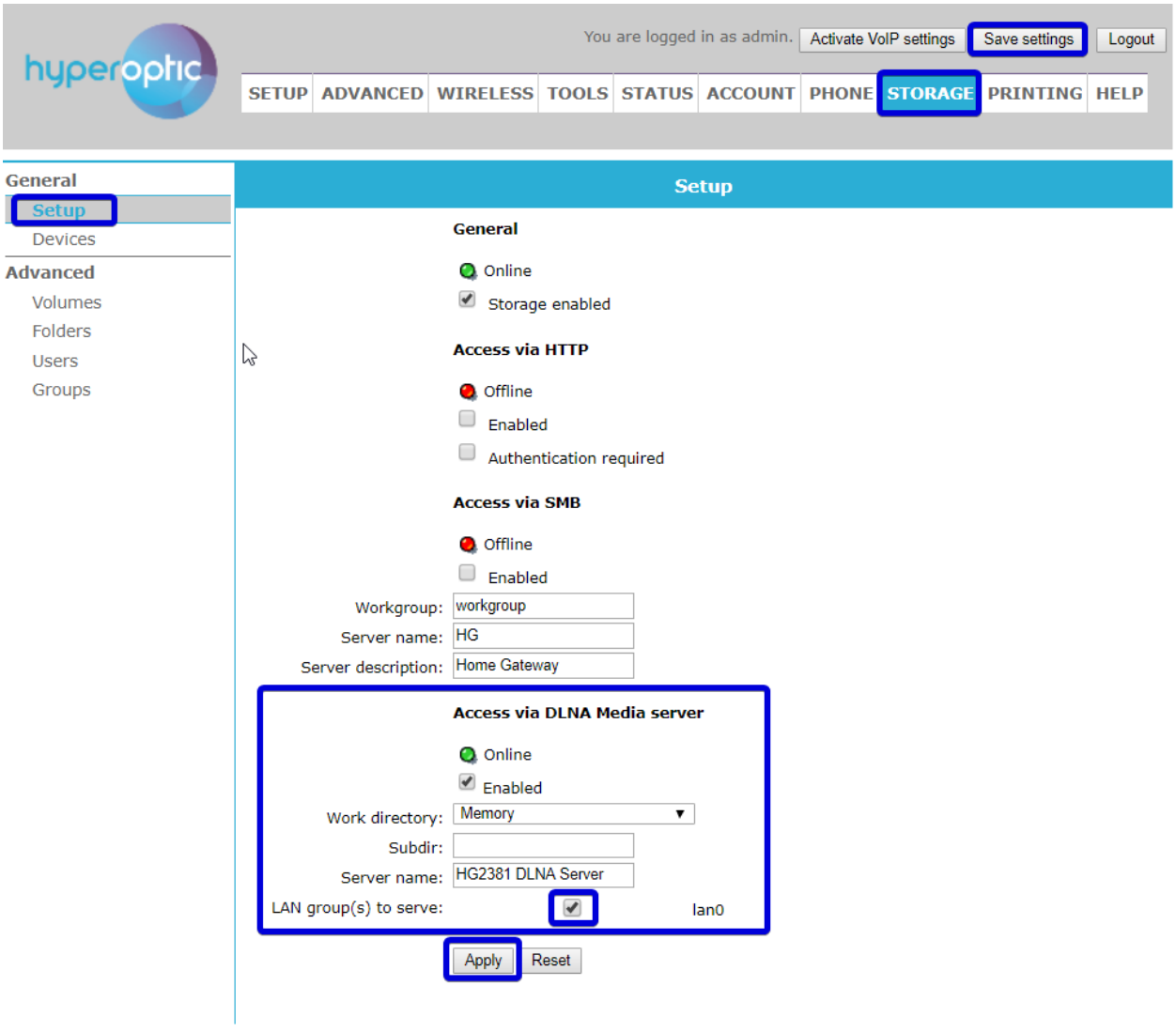

Image 23. Access to DLNA Media server

See Image 24 for access to flash drive via PC application e.g. VLC, Windows Media Player.

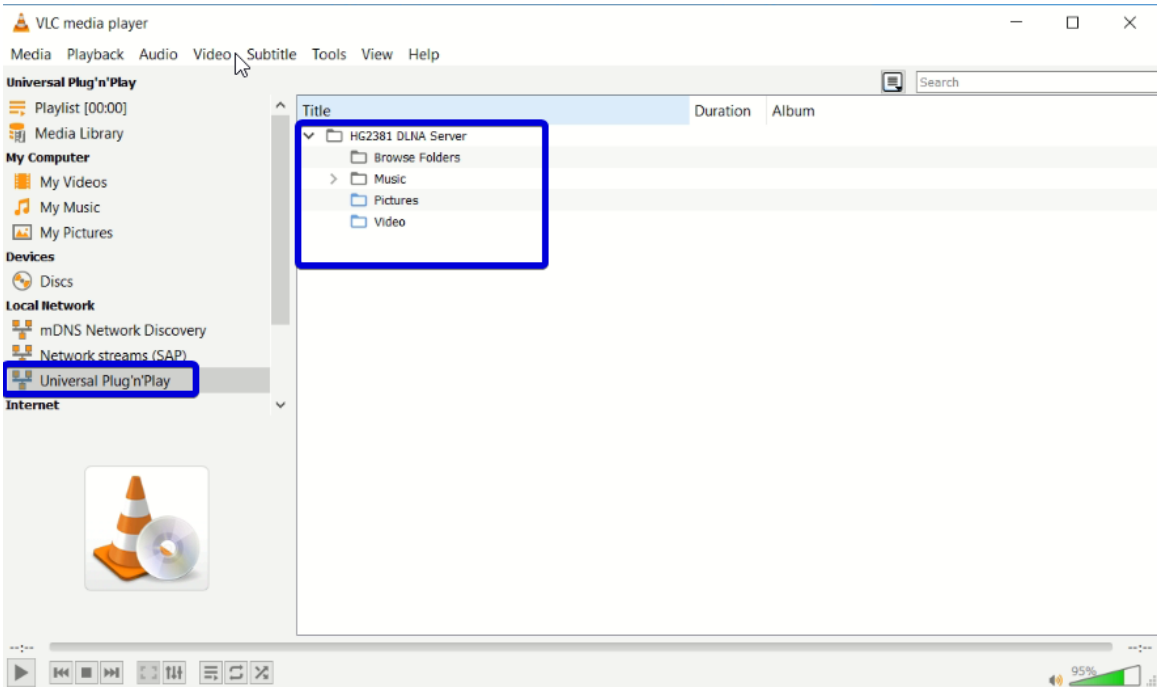

Photo 24. Access to USB flash drive DLNA Server

Change of DNS (admin account)

To change your DNS, please log into your router (page 2) and navigate to **Setup > LAN Setup > LAN configuration**. Click **View/edit all parameters** (see Image 25). 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.

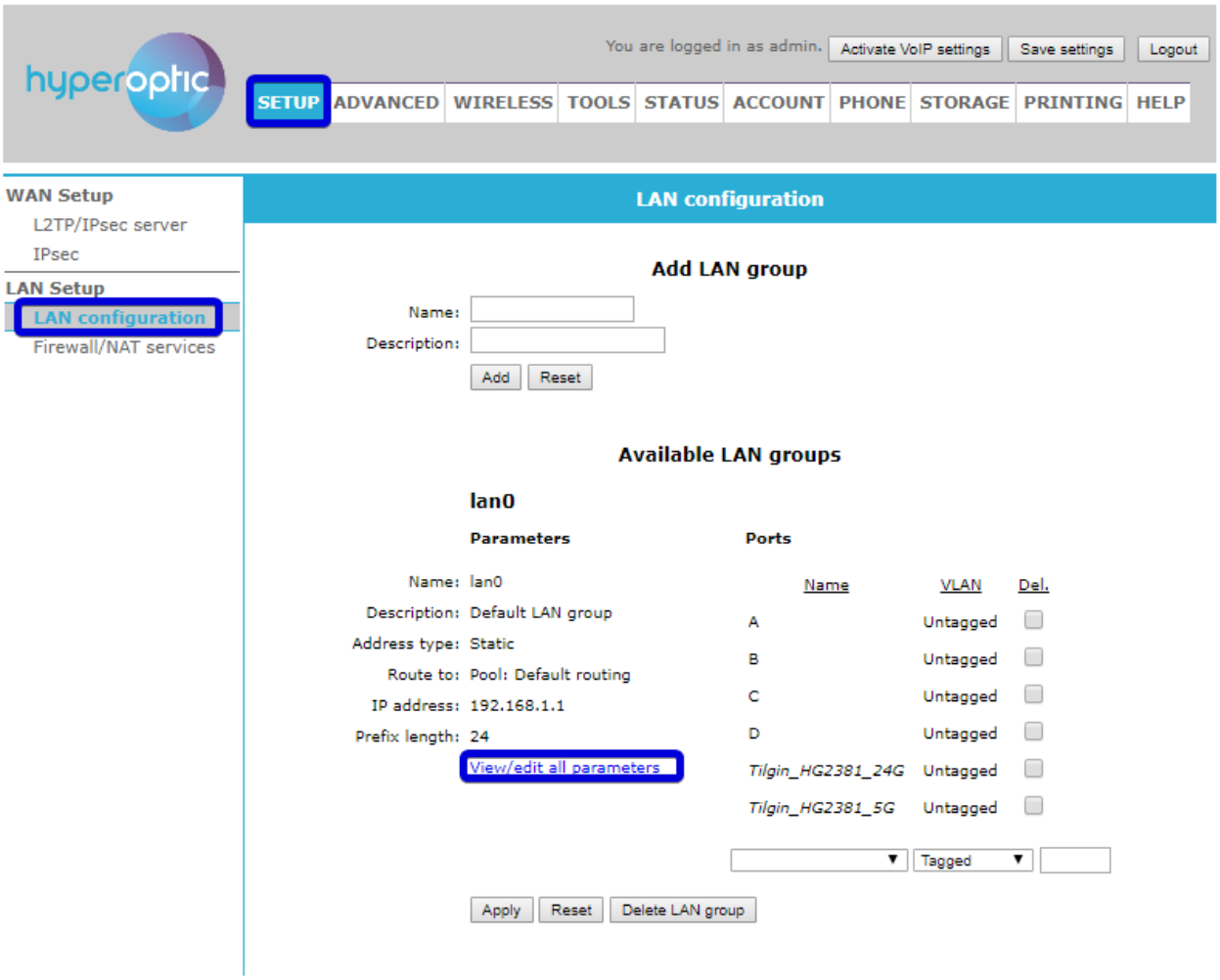

Image 25. Navigating to DHCP LAN settings

In the “Static Address” section, look for DHCP fields as shown in Image 16. Configure the public DNS as per your choice. To enable the use of an arbitrary DNS, please disable DHCPv6 server. See Image 26.

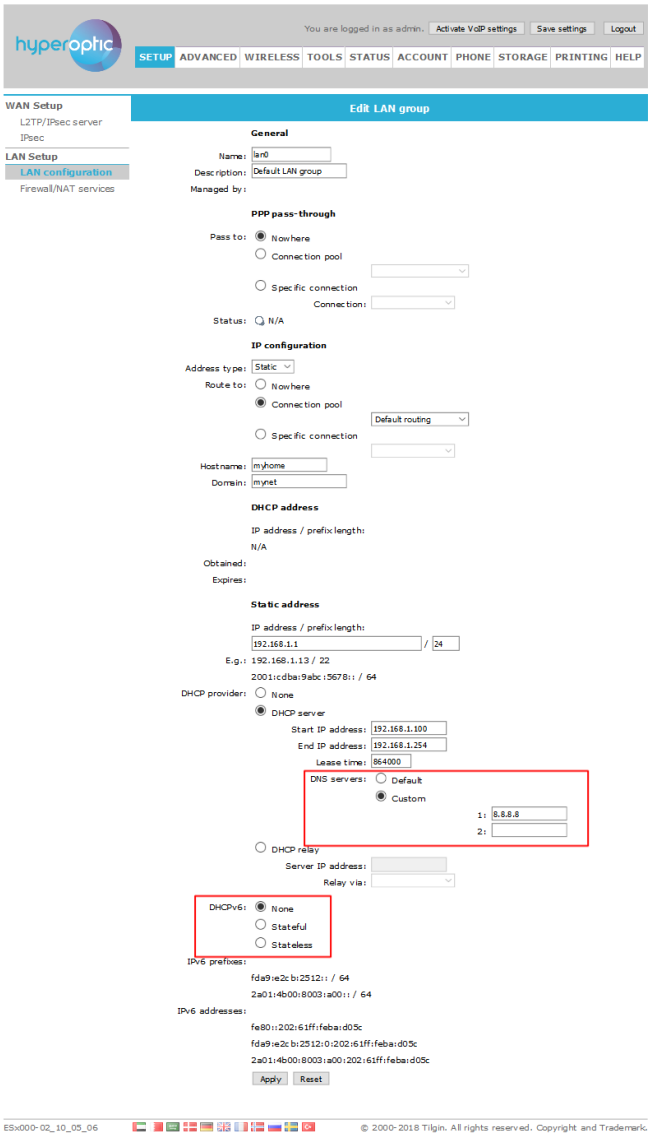

Image 26. DNS section of LAN configuration

Port forwarding (admin account)

Port forwarding is currently only being used for IPv4 addresses. Tilgin is developing firmware which will allow usage of IP Filtering for IPv6 addresses. Port forwarding can be used to establish home-based FTP server, web server or similar kind of a server.

To change your port forwarding parameters, connect your personal computer via ethernet cable or via wifi to the router. Open a web browser and type **192.168.1.1** in the search line of the browser. You should then see a login page, as below (Image 27).

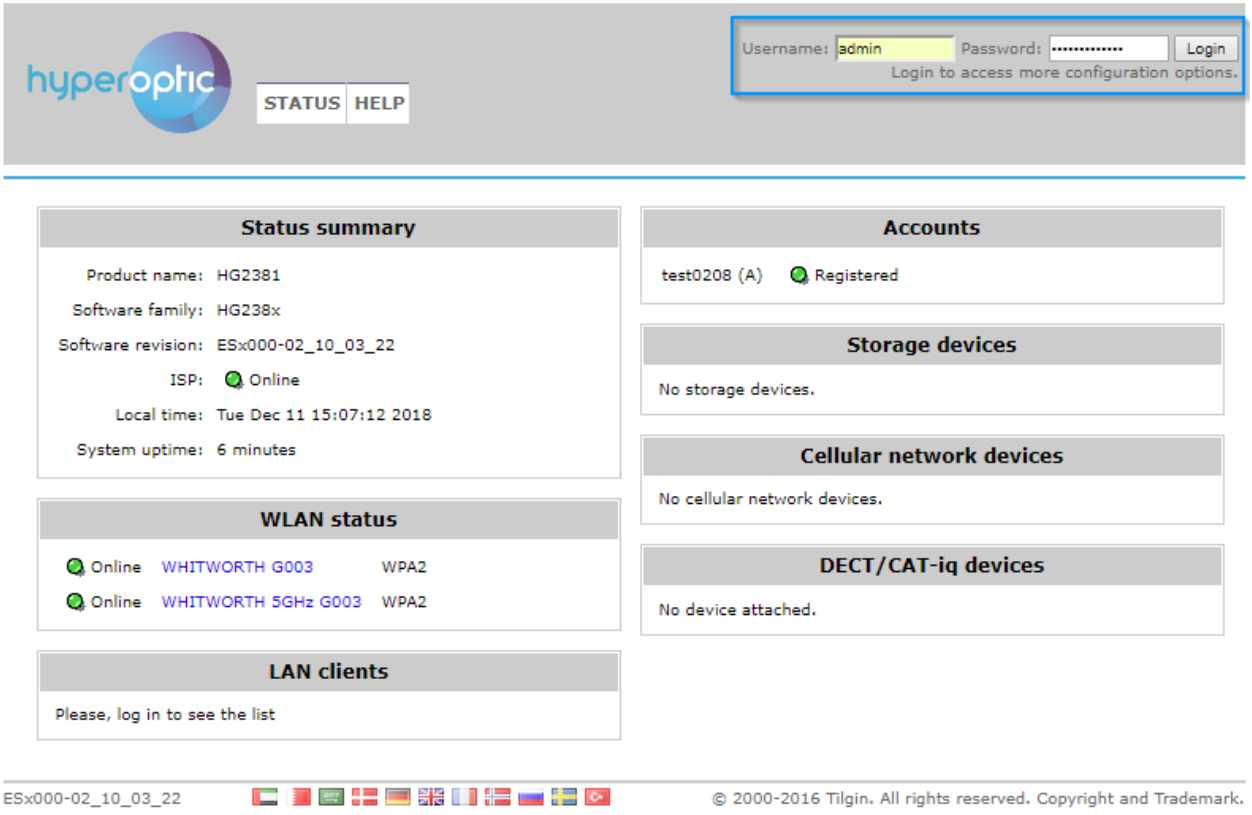

Image 27. Login page of the router

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 **Advanced > Port forwarding**, as illustrated in Image 28.

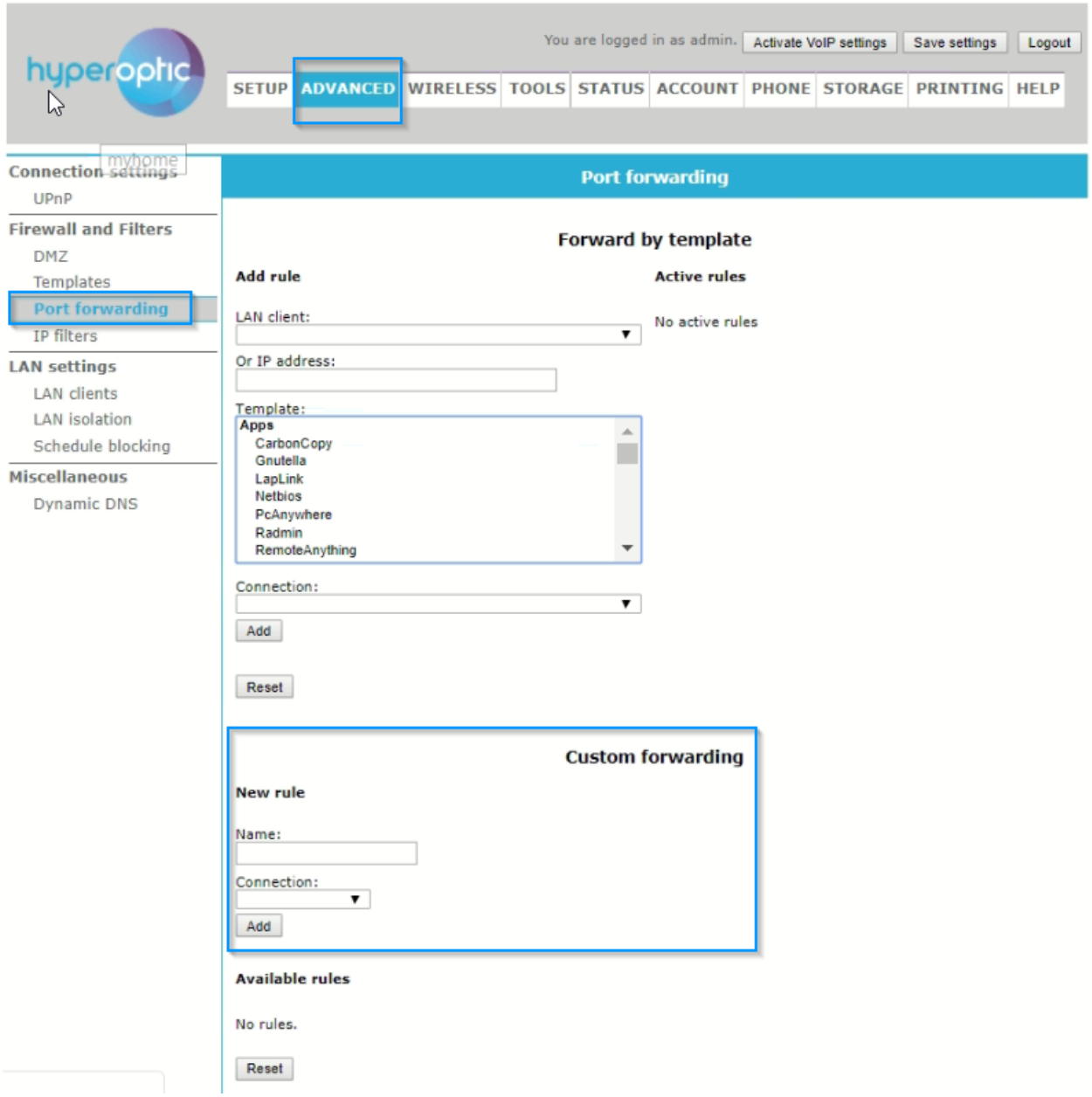

Image 28. Port forwarding section of the router web UI

At the bottom of this page, refer to the section **Custom forwarding**. Name the port forwarding rule and associate WAN connection to it. The connection type should be **dhcp-over-eth**. An example of the creation of a port forwarding rule for local web server is illustrated in Image 29. Once the **Name** and **Connection** type are set, click **Add**.

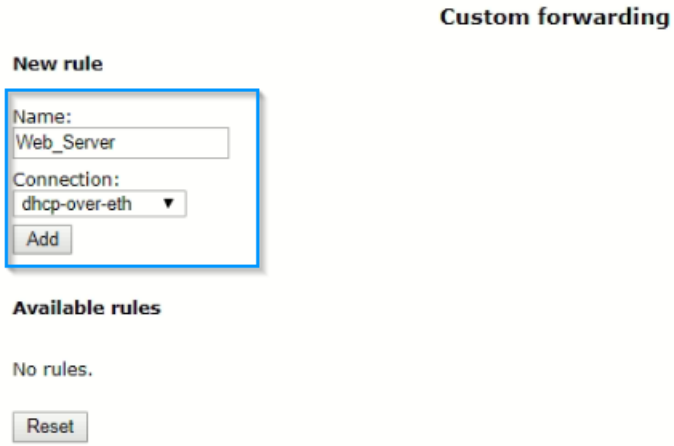

Image 29. Creating web server port forwarding rule

Image 30 illustrates the main parameter configuration of port forwarding rules.

First, click on **Enabled** field to make the port forwarding rule active.

Check your personal computer's private IPv4 address and type it in the **Destination IP address** field.

List which ports need to pass the router's firewall. In the example illustrated in Image 30, the **TCP** port **8080** which will serve local Web server placed in LAN.

If the web server needs to be seen from any public IPv4 address, type **0.0.0.0** in the **Source IP address** and list **0** as **prefix length**. Otherwise, if the web server needs to be accessed from just one IPv4 address, list that one address as illustrated in Image 30.

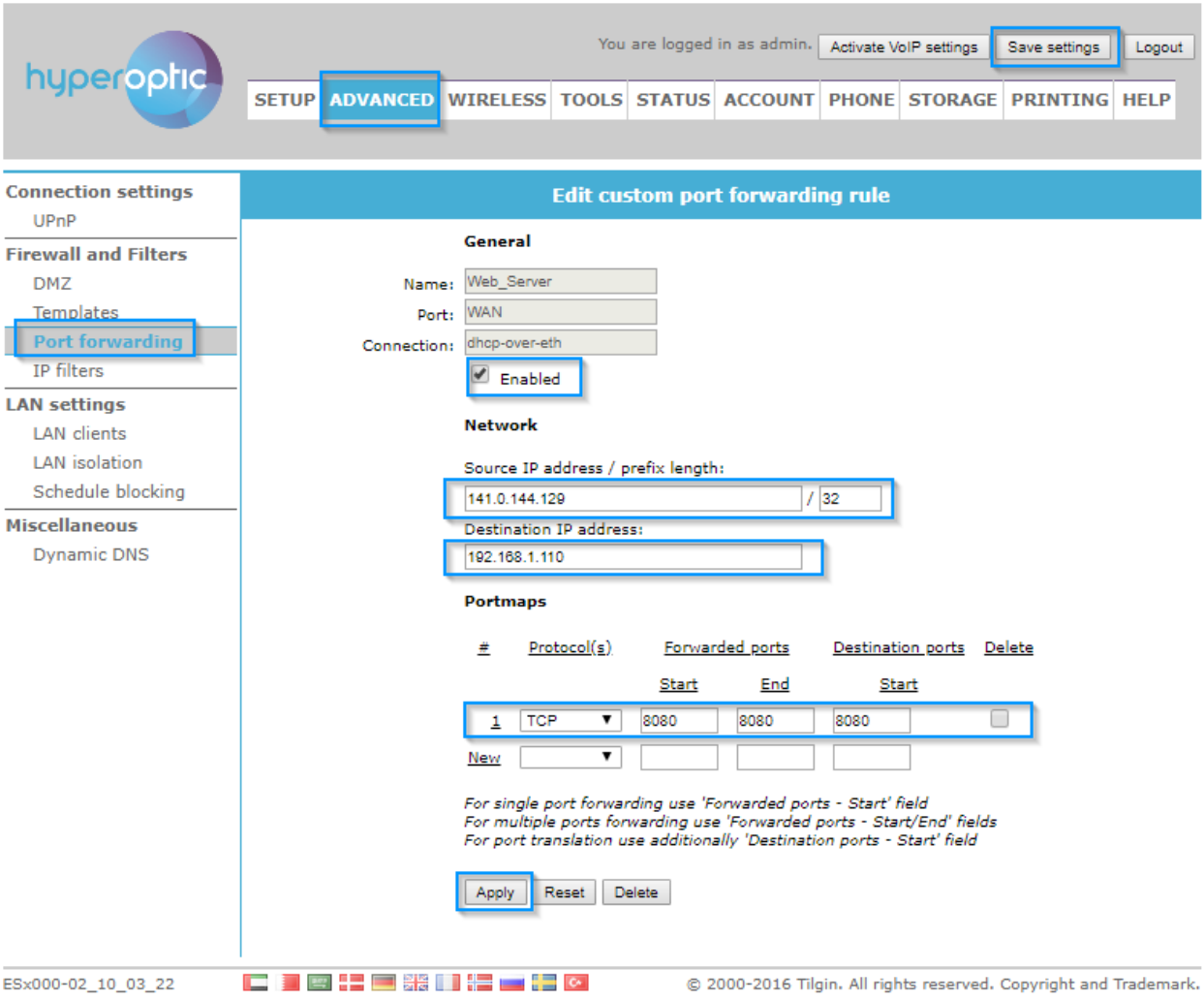

Image 30. Configuring port forwarding rules

Once all parameters are entered, click **Apply**. Save the router configuration by clicking **Save settings** in the upper right corner of the screen.

A list of commonly used ports is illustrated in Image 31.

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 as shown on Image 32 (e.g. you can use ports on WAN side 12000, 12001 and map them to LAN ports 80, 443 respectively). For additional help on port numbers and TCP/UDP, 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 31. List of commonly used ports

Alternatively, it's possible to allow a certain range of WAN ports that will all be translated into one LAN port. This kind of configuration is illustrated in Image 32. In this case, a local web server placed in LAN is listening for connections on port **8080**. The router will forward all connection requests that come to WAN router port **12001** to this local server.

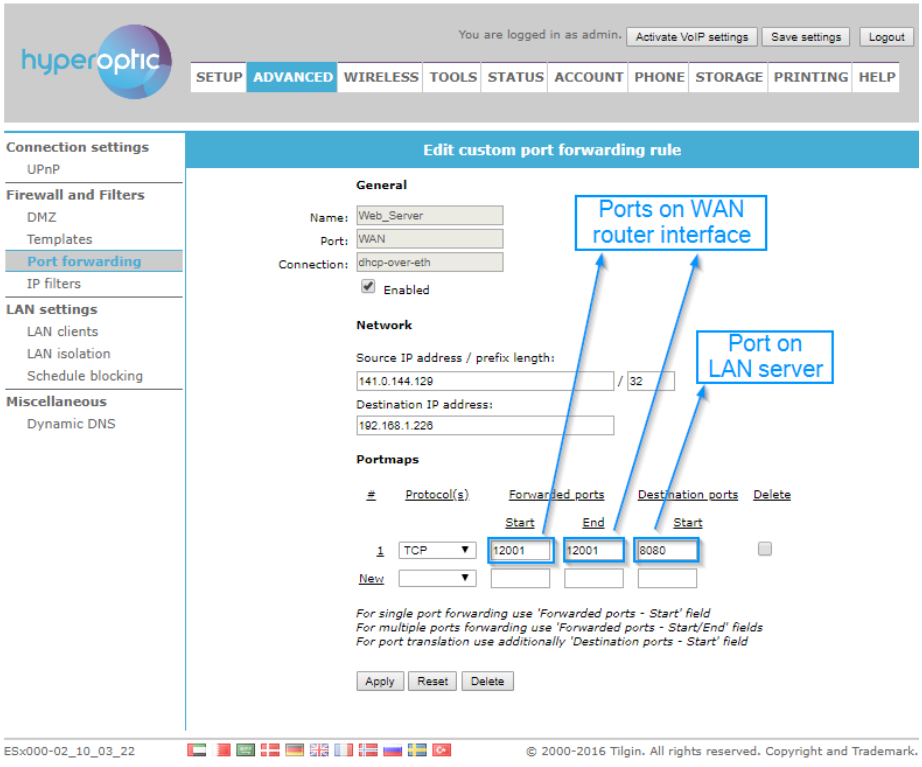

Image 32. Port forwarding with port mapping from WAN to LAN side

DMZ (admin account)

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 **Advanced > DMZ** (see image 33)

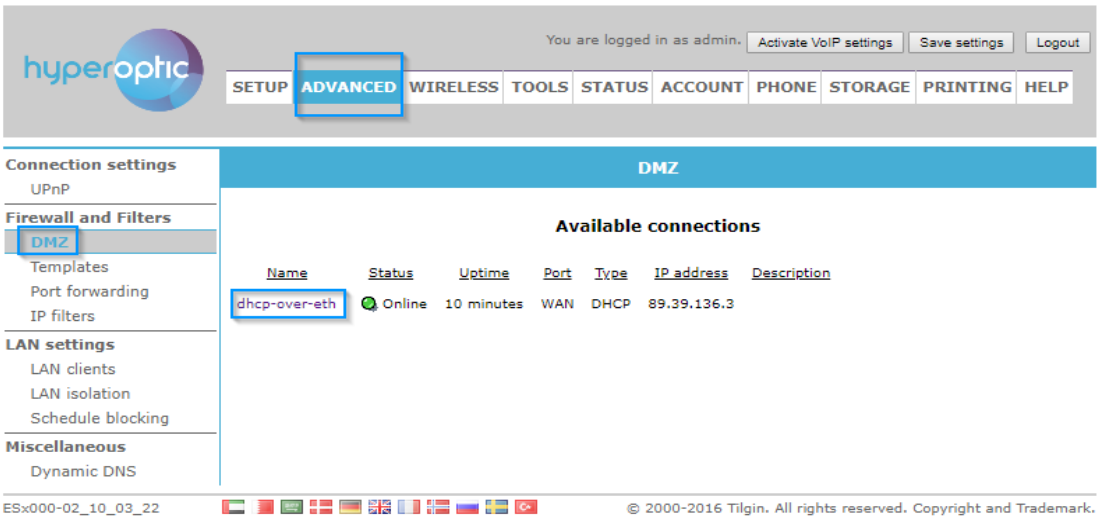

Image 33. DMZ section of router

Click on the Name of the connection – **dhcp-over-eth**. You should then be presented with Image 34.

List the IPv4 address of the LAN device and click **Apply**.

Save settings in the upper right corner of the screen.

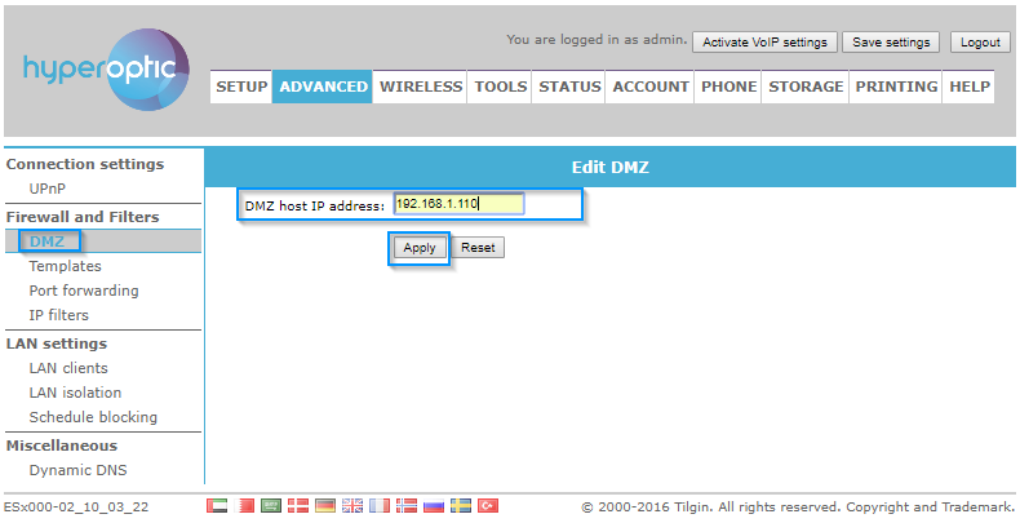

Image 34. List LAN device which needs to be placed in DMZ

DHCP binding (using User account)

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 photo 35. Navigate to section **Advanced > LAN settings > LAN clients**.

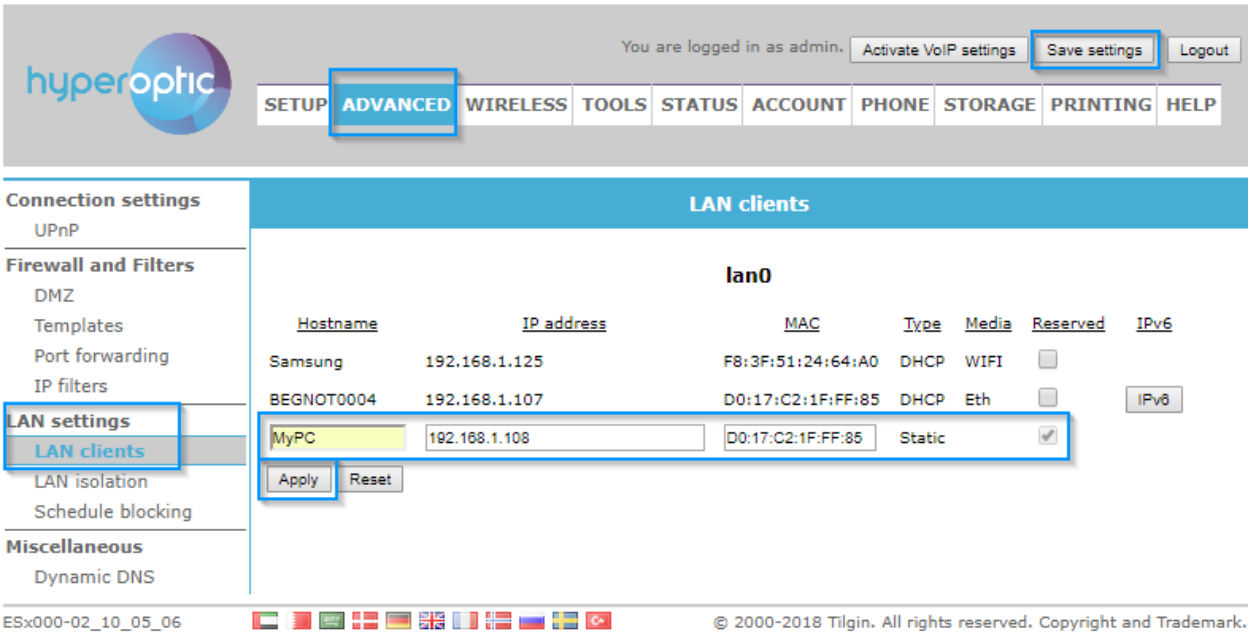

Photo 35. DHCP host binding

Use arbitrary **Hostname**, List wanted IPv4 address and list MAC address of LAN client. Valid range of IPv4 addresses is **192.168.1.100** to **192.168.1.254** . After the configuration is made click **Save settings**.

IPv6 port filtering (AKA Port forwarding)

Allowing some services (equivalent of ports TCP/UDP) to pass through router from WAN side to LAN side can be configured using port forwarding feature of a router. To set this up, please navigate to **Advanced > Port forwarding > Custom forwarding / New rule**. See image 36. **Name** of a rule can be arbitrary but for IPv6, connection must be **ipv6-over-eth**. Once this is selected, click **Add** button.

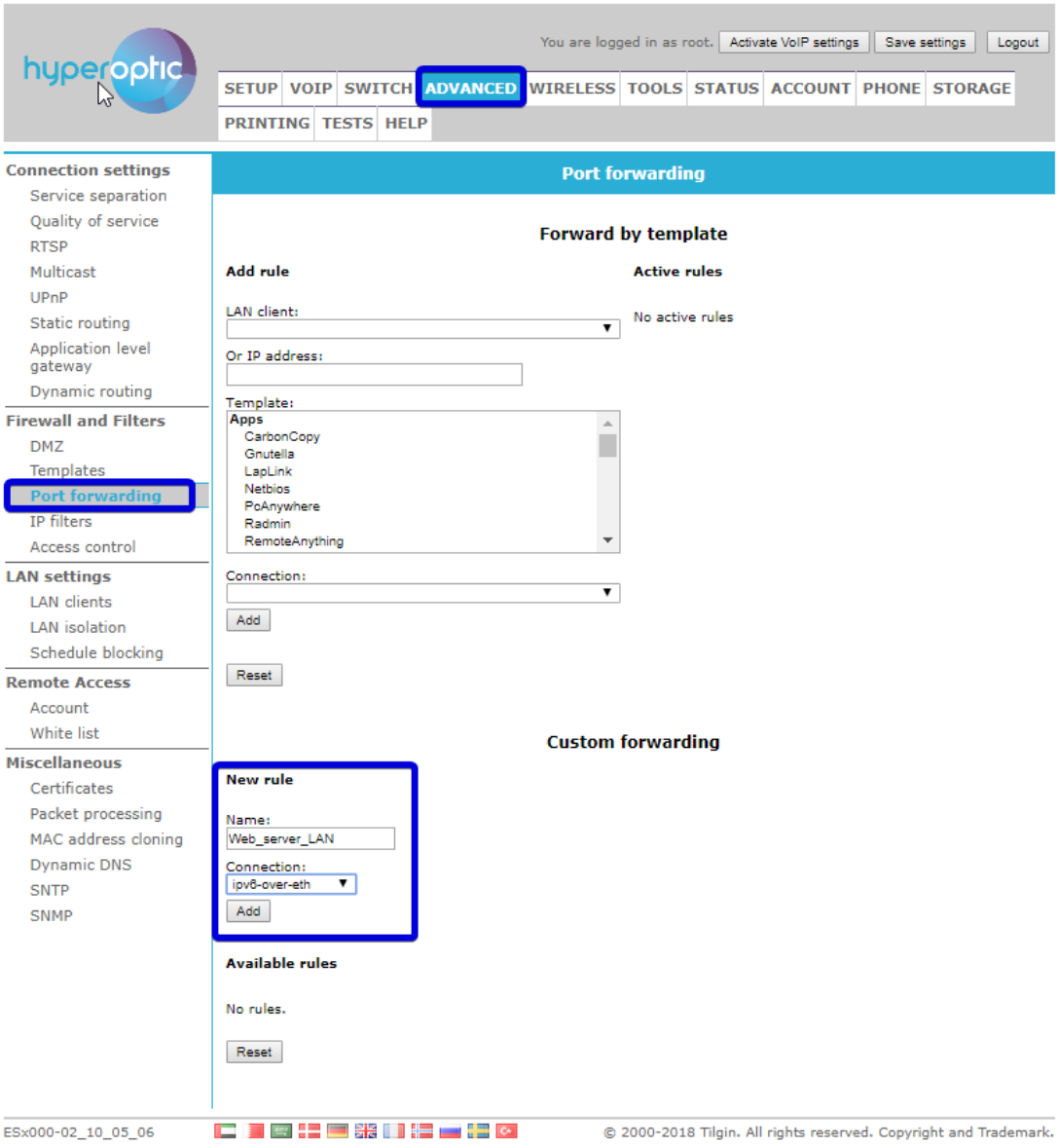

Image 36. Selecting IPv6 connection for Port forwarding router feature

In the new menu (see image 37), tick **Enabled** to allow this rule. **Source IP address** is the range or single address from which access to router is made. In case that from any location service must be available, state "**::**" as source address. **Destination address** is the public IPv6 address of LAN client machine. As last step, list ports that need to be allowed to pass through router (e.g. TCP port 80), then click **Apply** and **Save settings**.

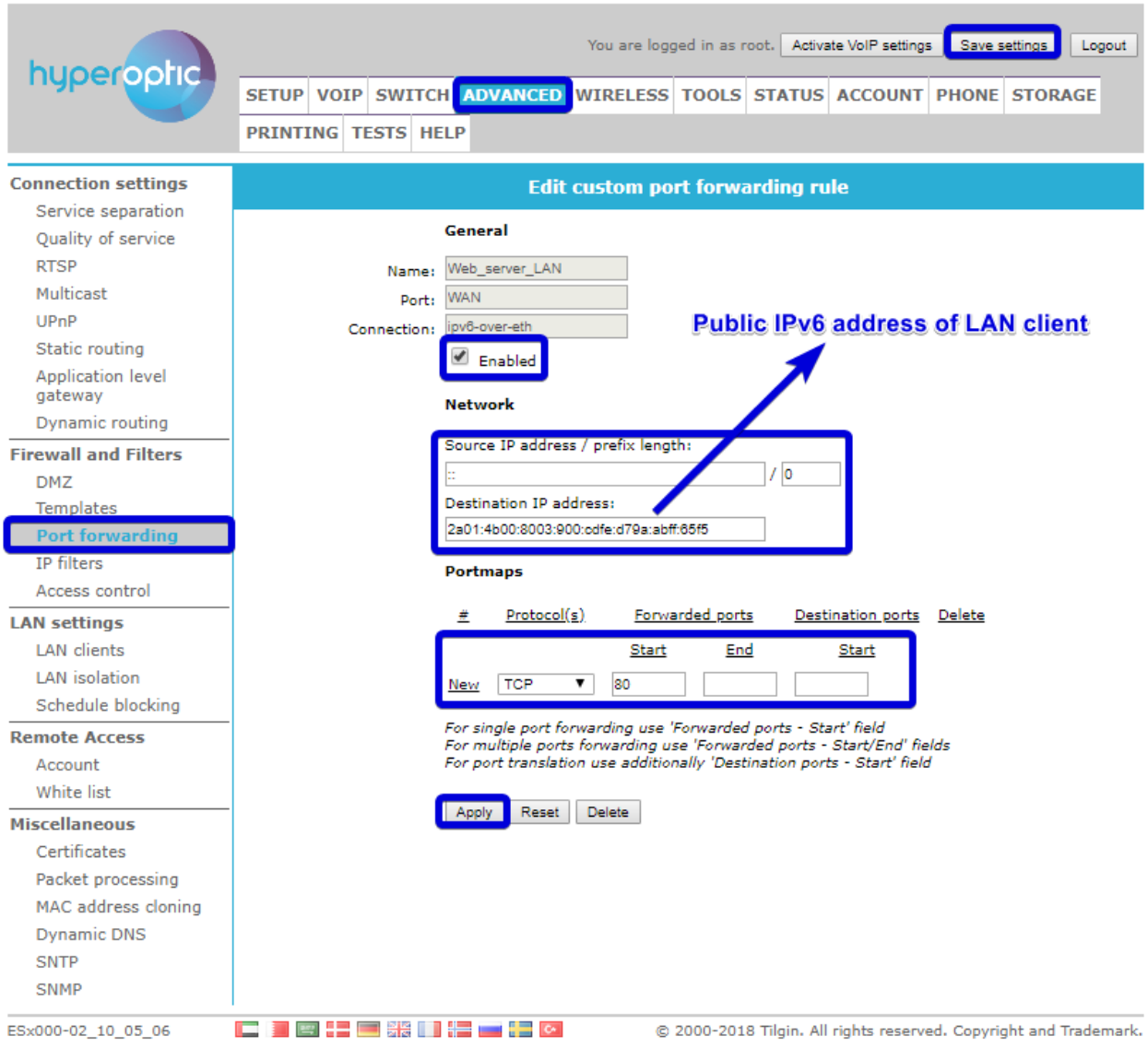

Image 37. Configuration of IPv6 port filtering

You'll see confirmation of setup in image 38.

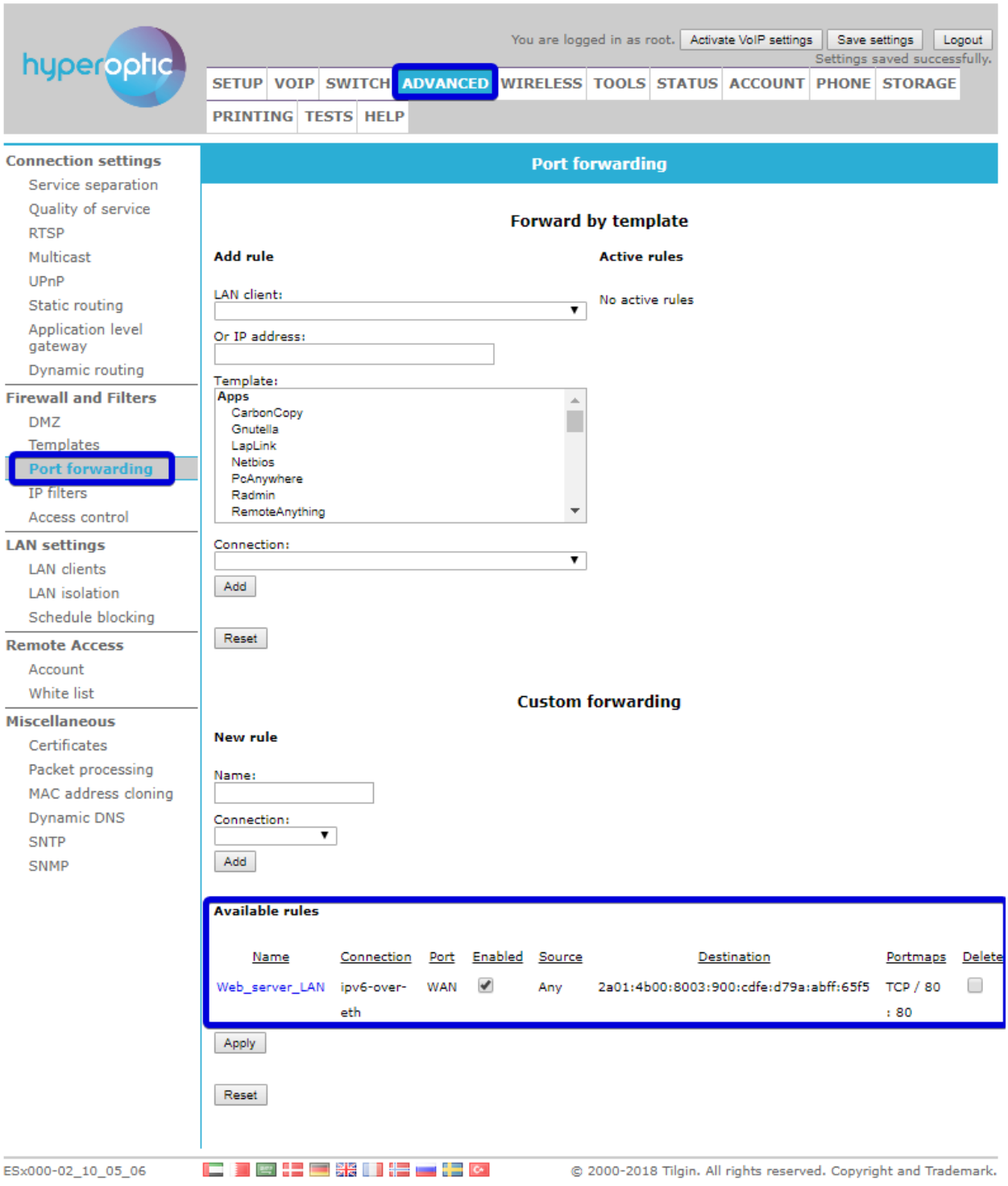

Image 38. Confirmation of IPv6 port filtering rule

Public IPv4 address block in LAN network

Navigate to section **Setup > LAN Setup > LAN configuration**. Click on the **View/edit all parameters**. See image 39.

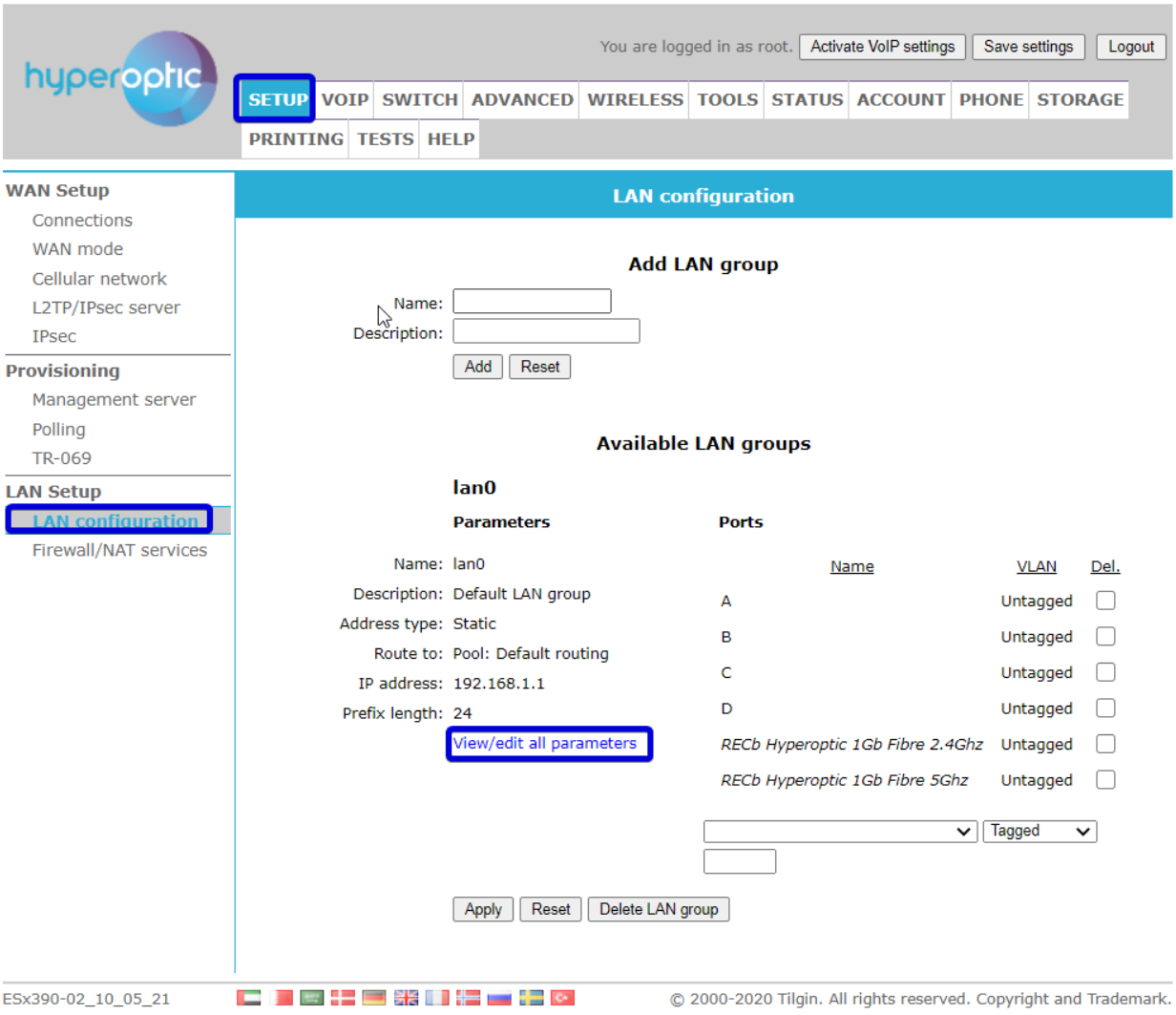

Image 39. LAN settings of HG2381

New screen opens as described in image 40. Focus on the part of **Static address**. Define **IP address / prefix length** field. Example is shown for public block 137.220.108.0/29. Enter valid **Start IP address** and **End IP address**. Click on **Save** button at the bottom of the page.

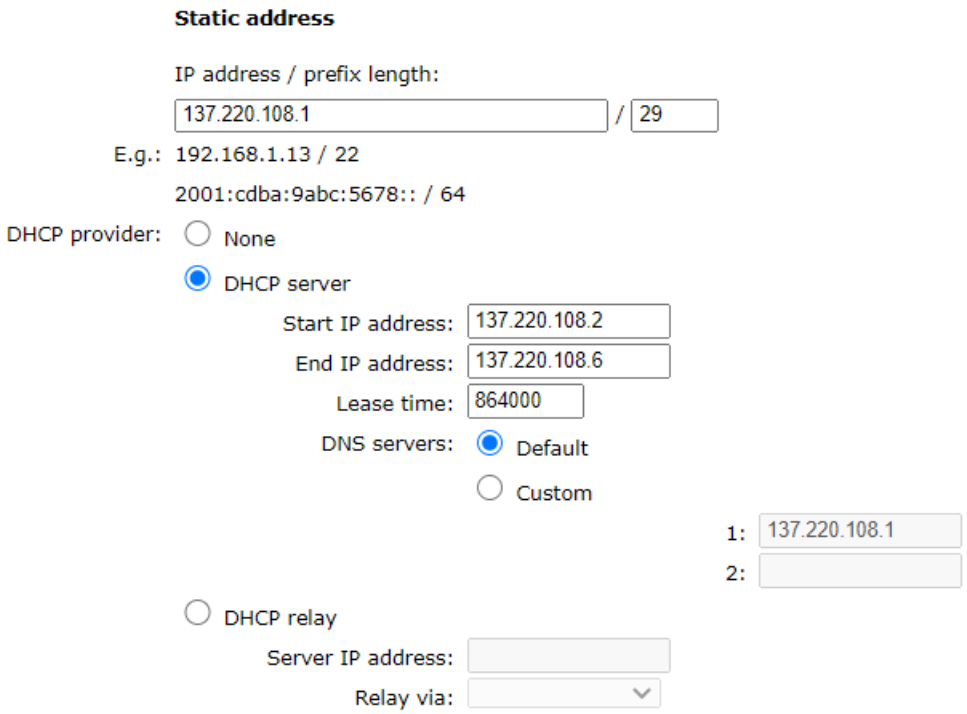

Image 40. DHCP setting of HG2381

Return to section **Setup > LAN Setup > Firewall/NAT services**. Untick option of **Enable NAT service**. Click **Apply** and **Save settings**. This is illustrated in image 41.

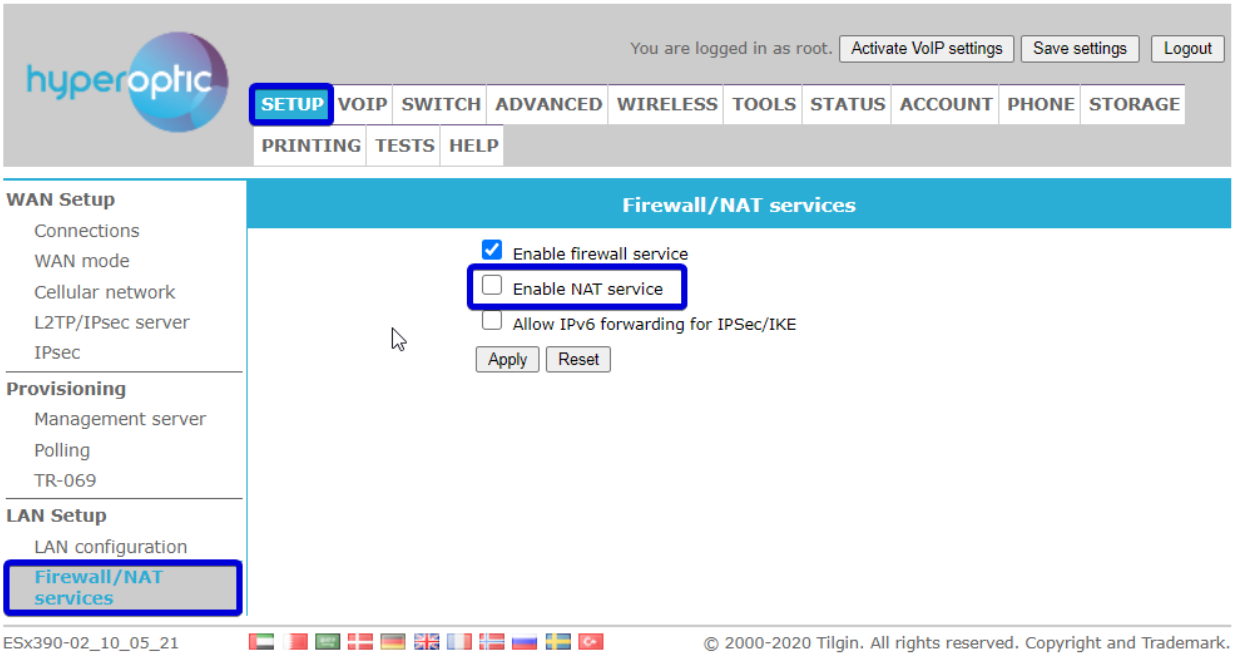

Image 41. Disabling NAT service