PYXIS LTE PRODUCT MANUAL

Issue 1 –2024

Ubiik Inc.

Issue 1 –2024
Pyxis LTE Product Manual

Disclaimer

While precaution has been taken in the preparation of this literature and it is believed to be correct at the time of issue, Ubiik Inc. assumes no liability for errors or omissions or for any damages resulting from the use of this information. Due to a policy of continuous technical improvement, the contents of this document and any specifications contained therein are subject to revision and may change without notice.

WARRANTY

Ubiik warrants for a period of 15 months from the date of delivery that its hardware items ("**Equipment**") will be free from defects due to defective design, workmanship or materials subject the conditions below ("**Warranty**").

CONDITIONS OF WARRANTY

This Warranty is strictly subject to the following conditions:

a. Ubiik will not be liable for breach of Warranty unless the customer (i) notifies Ubiik of the alleged defects within 30 days after the defect would have become reasonably apparent, and (ii) promptly returns the Equipment carriage paid with a full written report on the alleged defects.

b. The Warranty is not transferable.

c. Ubiik liability under this Warranty is dependent on an assessment by Ubiik to determine and validate the defect in design, workmanship or materials.

d. The customer shall refund to Ubiik the cost to Ubiik of any replacement, repair or redelivery of any Equipment effected by Ubiik where the failure is not within the terms of this Warranty.

e. Ubiik does not guarantee that any service performed under this Warranty will be carried out within any particular timeframe.

f. To the fullest extent permitted by law, Ubiik's liability under this Warranty is limited to (at Ubiik's option) replacing or repairing the Equipment or the relevant part thereof without charge provided that its liability shall in no event exceed the purchase price of the Equipment or the relevant part thereof. Where Ubiik authorises the customer to undertake Warranty repairs, no reimbursement will be made in respect of labour.

g. If the product has been discontinued and there are no replacement parts in stock, Ubiik has the right to replace it with a different model of product with the same function or superior specifications (or a new version of the hardware of the same model product).

h. The repaired or replacement Products will be warranted for the remaining time of the original Warranty Period or three (3) months, whichever is longer.

GENERAL EXCLUSIONS

Ubiik shall not be liable under this Warranty:

a. where the Equipment has not been stored, installed, maintained and used properly having regard in particular to Ubiik's and (if any) other agreed applicable specifications and instructions including (without limitation) in relation to the installation of engineering changes or enhancements;

b. where the Equipment has not been used in accordance with interference-free power, suitable environment (including but not limited to free from electronic or radio interference and pests) and correct maintenance of the Equipment;

c. for third party interference, fair wear and tear, abuse, damage or misuse, correction or repairs or modifications made other than by Ubiik or any repairs required due to events beyond the control of Ubiik;

d. for abnormal conditions (electrical, thermal, chemical or otherwise), including (without limitation) factors outside the operational parameters for the Equipment;

e. for any defect caused by or arising from use of any software not licensed or supplied by Ubiik, or otherwise caused by or arising from the customer's acts or omissions.

LIMITATION OF LIABILITY

Except as set out in this Warranty and to the maximum extent permitted by law:

a. all warranties, conditions, liabilities and obligations with respect to any Ubiik product, software or services (including as to merchantability, description quality, or fitness for a specific purpose) are expressly excluded; and

b. Ubiik shall not be liable for any losses or damages (whether direct or indirect) including property damage or personal injury, consequential loss, economic loss or loss of profits or other economic advantage, however caused which may be suffered or incurred by the customer or any third person, or which may arise directly or indirectly out of or in respect of any Ubiik product, software or services or by reason of any act or omission on the part of Ubiik.

CUSTOMER ACKNOWLEDGEMENT

The customer acknowledges that:

a. if the Consumer Guarantees Act 1993 ("**CGA**") applies, this Warranty shall be read subject to customer's rights under the CGA. Where the customer uses the Equipment for business purposes, the provisions of CGA, or any other relevant consumer protection legislation, shall not apply;

b. the Equipment is not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; intrinsically safe environments or in the design, construction, operation or maintenance of any nuclear facility. Ubiik disclaims any express or implied warranty of fitness for such uses. The customer will not use or resell Equipment for such purposes;

c. any software supplied by Ubiik cannot be tested in every possible permutation and accordingly Ubiik does not warrant that software supplied will be free of all defects or that its use will be uninterrupted.

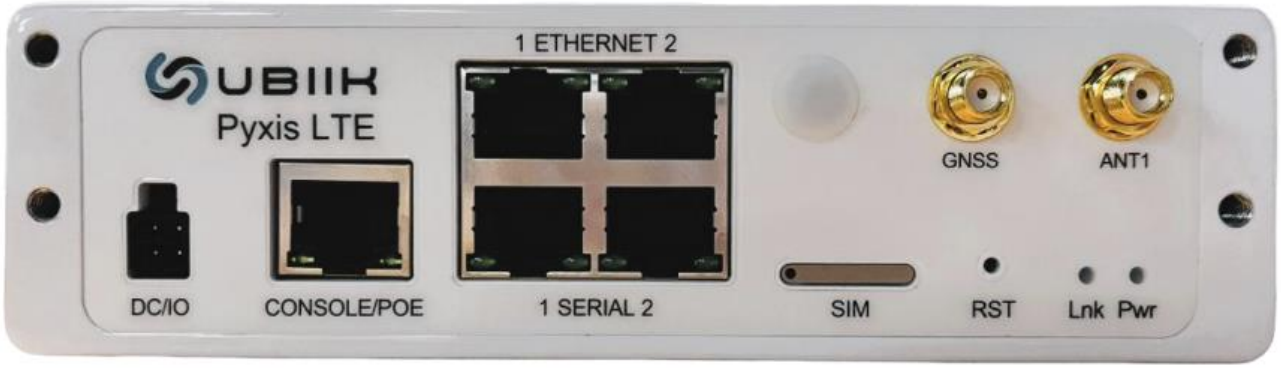
Table of Contents

1. PYXIS LTE SYSTEM OVERVIEW

Pyxis LTE is a small form factor, ruggedized LTE endpoint designed to either be mounted outdoors or within a cabinet.

The unit operates as a UE within a private LTE network and is compatible with Ubiik's goRAN™ LTE base station(Band 106) and freeRAN™ LTE base station(ISM Band).

As a 3GPP standardized device, the Pyxis LTE also has the capability to connect to public cellular networks (with advance approval required for each public network to which the unit would connect).



Pyxis LTE Radio

2 COMPLIANCE AND SAFETY STATEMENTS

2.1 OVERVIEW

2.1.1 FCC OVERVIEW

Pyxis LTE Router complies with Part 15 and Part 27 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 and Part 27 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial or industrial installation. This device generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one of the following measures:

Method	Action
1	Reorient or relocate the receiving antenna
2	Increase the separation between the device and receiver
3	Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
4	Consult the dealer or an experienced RF technician for help

Table 1.1: Approaches to correcting interference

CAUTION!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this device.

2.1.2 CANADA, INDUSTRY CANADA (IC) NOTICES

This device contains license-exempt transmitter(s) that comply with innovation, Science and Economic Development Canada's Licence-exempt RSS(s). Operation is subject to the following two conditions:

v.1.0 FCC ISED

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

3. Radio Frequency (RF) Exposure Information

The radiated output power of the Wireless Device is below the Innovation, Science and Economic Development Canada (ISED) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions. (Antennas are greater than 29cm from a person's body).

4.Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie rayonnée de l'appareil sans fil est inférieure aux limites d'exposition aux radiofréquences d'Innovation, Sciences et Développement économique Canada (ISDE). L'Appareil sans fil doit être utilisé de telle manière que le potentiel de contact humain pendant le fonctionnement normal soit minimisé.

Cet appareil a également été évalué et démontré conforme aux limites d'exposition RF IC dans des conditions d'exposition mobile. (Les antennes sont à plus de 29 cm du corps d'une personne).

Canada, Avis d'Industrie Canada (IC)

Cet appareil contient un ou des émetteurs exemptés de licence conformes aux normes RSS exemptes de licence d'Innovation, Sciences et Développement économique Canada. Son fonctionnement est soumis aux deux conditions suivantes : 1. Cet appareil ne doit pas causer d'interférences.

2. Cet appareil doit accepter toute interférence, y compris celles pouvant entraîner un fonctionnement non désiré de l'appareil.

2.2 RADIATION EXPOSURE STATEMENT:

The antenna(s) used for this transmitter must not be co-located of operating in conjunction with any other antenna or transmitter. This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 11.41 inches (29 cm) during normal operation.

2.3 PROFESSIONAL INSTALLATION STATEMENT:

1. **Installation personnel:** This device is designed for specific applications and needs to be installed by qualified personnel who have RF and related regulations knowledge. The general user should not attempt to install or change the settings.
2. **Installation location**: The device should be installed at a location where the radiating antenna can be kept 11.41 inches (29 cm) from any nearby person in normal operating conditions to meet regulatory RF exposure requirements.
3. **Installation procedure**: Please refer to procedure for mounting the device to a wall or pole.
4. **Warning**: Please carefully select the installation position and make sure that the final output power does not exceed the limits set in relevant rules. Violation of rules could lead to serious federal penalties.

2.4 SAFETY STATEMENT:

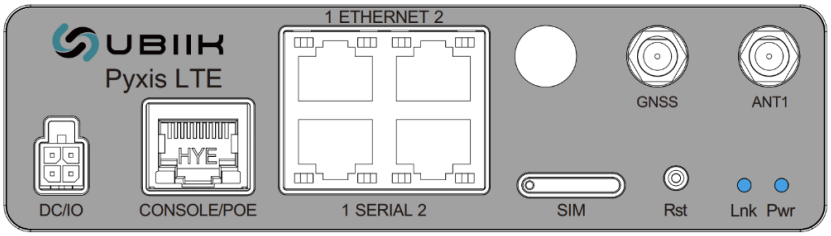
All instructions, warning and caution statements that accompany this device must be strictly followed at all times to ensure its safe use. Observe all warning and caution symbols that are fixed to this device. This device has been designed with the utmost care for the safety of installers and users. However, when using this device, basic safety precautions should always be followed to reduce the risk of injury and electric shock. Do not cover the device or block the airflow to the device with any other objects. This device was qualified under test conditions that included the use of the supplied cables between system components.

To comply with regulations, the user must use the cables supplied with the unit (including power adapter) and follow the installation guide. Place the unit to allow for easy access when disconnecting the power adapter from the main wall outlet. Operate this device only with the type of power source indicated on the marking label. If you are not sure of the type of power supplied to your facility, consult your dealer or local electricity provider.

Do not use this product near water, for example a swimming pool or a bathroom. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust. Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

3 PYXIS LTE RADIO UNIT OVERVIEW

The diagram below labels each of the different connectors.



3.1 POWER REQUIREMENTS

3.1.1 VOLTAGE RANGE

The operating input voltage range of the power supply is 9 to 15 VDC. This means that the voltage must not rise above 15 VDC under idle conditions or fall below 9 VDC at full load.

3.1.2 STATIC POWER PER INPUT

The DC feed should be designed for 1.5A maximum current draw when using a 12V source or 0.75A when using a 24V source.

Input Source Voltage (S)	Maximum Current in Amperes	Circuit Breaker Current in Amperes
12 Volts	1.5A	2A

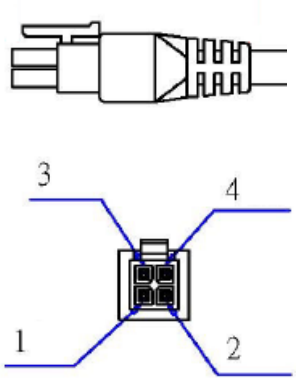
Current draw

3.1.3 STARTING CURRENT (CONFIRM)

There is no significant inrush current, as long as the power supply can supply the static power it should be able to provide sufficient current during start-up.

3.1.4 SUPPLY POLARITY

The power cable is wired to pin 1 (Ground) and Pin 2 (Positive). The required connector for the Power supply cable is E.C.I 3016H-04 (2*2) housing and 3016 crimp terminals.



Power supply connector

A 2metre long DC cable is available from Ubiik.

3.1.5 GROUNDING

The radio unit case must be grounded through an external earth strap. Any of the unused mounting screw points can be used with an appropriate star washed. Generally, this is done to the local rack frame, which in turn should be part of a well-designed station grounding system. This internal grounding is designed for EMC and transient protection currents.

3.1.6 SUPPLY NOISE

Regardless of the EMC provisions in the equipment, power wiring from the DC source should not be shared with other equipment that may introduce excessive noise. Nor should the power cables to the unit be run alongside cables that connect to other equipment that may produce high current noise or transients, e.g. power relays.

3.1.7 OPERATING FROM AC MAINS

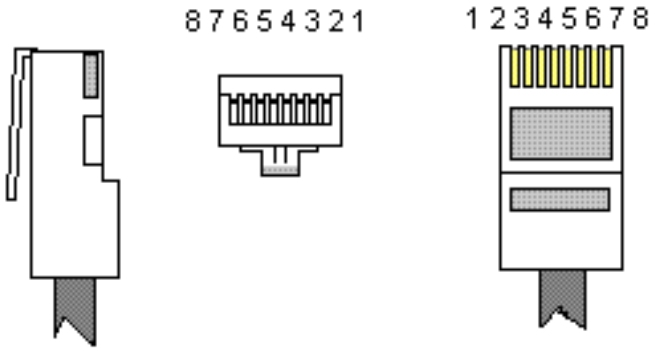
AC-DC 'plug pack' power supplies are available from Ubiik Mimomax with the required power.

3.2 ETHERNET 1, 2 AND CONSOLE

Three shielded RJ45 sockets provide the Ethernet connections to ethernet 1 and 2 and Console. The Console Ethernet port has POE (Power Over Ethernet) support and is compatible with IEEE802.3 AF or AT. Shielded cable is not normally required. The Ethernet ports are both 10/100/1000 BASE-T ports.

3.3 SERIAL 1 AND 2

Two shielded RJ45 sockets provide serial port connection. These ports can be connected to remotely via a TCP server and can be configured via the web UI.



3.3.1 RS232 PIN OUT

Signal Name	Pin number	Direction
Tx Data	6	Out of radio
Rx Data	5	In to radio
Ground	4	n/a

3.3.2 RS485 HALF DUPLEX PIN OUT

Signal Name	Pin number	Direction
Data n	6	In/Out of radio

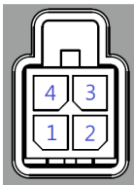
Data p	8	In/Out of Radio
Ground	4	n/a

3.4 GPIO

2 GPIO pins are available on the DC connector. The GPIO modes supported are:

1) Digital Push-pull output 5V
2) Digital Open Collector output, up to 24V pull up, requires 10k external resister
3) 5V Digital input

The GPIO connector is shared with the DC input, the pinout is below.



Pin Number	Name	Description
1	Ground	Ground for DC input
2	Positive	Positive for DC input, 9-15 VDC 1.5A DC input
3	Digital GPIO 1	Push-pull output / Open Collector output / Digital input
4	Digital GPIO 2	Push-pull output / Open Collector output / Digital input

DIGITAL I/O, ;T = -20℃ to + 65℃						
Push-pull output mode : 5V						
Symbol	Parameter	Conditions	Min	Typ	Max	Unit
IOL	LOW-level output current	VOL=0.4V			40	mA
VOH	HIGH-level output voltage	IOH=5mA			4.9	V
		IOH=10mA			4.6	V
		IOH=20mA			4.1	V
		IOH=30mA			3.5	V
		IOH=40mA			2.9	V
Open Collector output mode :						
Symbol	Parameter	Conditions	Min	Typ	Max	Unit
RE	Open Collector output Externa Resistor	Pull Voltage = 5V / 12V /24V		10K		ohm
Digital input mode						
VIL	LOW-level input voltage		-0.5	0	1	V
VIH	HIGH-level input voltage		4.7	5	24	V

3.5 ANTENNA

One antenna is for LTE. The other one antenna is for GPS.

- RF Antenna for Band-106
  The EUT supports the 1Tx/1Rx function.

	Brand Name	Model No.	Type	Antenna Gain(dBi)
Antenna SRD1	M.gear	C1991-510073-A	Dipole	0.2
Antenna SRD2	Grand-Tek	OA-L71-05-03A-C5-5G	Dipole	1.40
Antenna SRD3	JOYMAX	ZWX-715Bcc5B	Dipole	1.9
Antenna SRD4	Dawn	DB-896-960V-13-75-NV2	Panel	13
Antenna SRD5	Invax	DS0915-0726WN	Dipole	5.73

- RF Antenna for ISM-FDD
  The EUT supports the 1Tx/1Rx function.

	Brand Name	Model No.	Type	Antenna Gain(dBi)
Antenna SRD1	M.gear	C1991-510073-A	Dipole	0.2
Antenna SRD2	Grand-Tek	OA-L71-05-03A-C5-5G	Dipole	1.40
Antenna SRD3	JOYMAX	ZWX-715Bcc5B	Dipole	1.9
Antenna SRD5	Invax	DS0915-0726WN	Dipole	5.73

- GPS Antenna
  A GNSS receiver is built in, an external antenna is required and is connected via a SMA connector on the front of the Pyxis LTE. A passive GNSS antenna with SMA connection is required if GNSS is being used and should be fitted in a location with a view of the sky.
  Note: The GPS Antenna only have the Rx function.

	Brand Name	Model No.	Type	Antenna Gain(dBi)
Antenna-GNSS	Grand-Tek	OA-L71-05-03A-C5-5G	DIPOLE	0.7
Antenna-GNSS	INPAQ	ENS000041280	RHCP	4.87
Antenna-GNSS	Jinchang	JCA211Magnet	RHCP	2

3.6 LED BEHAVIOUR

The LEDs indicate

- Pwr – Indicates that unit has DC power connected and is powered on
- Lnk – The Link LED indicates the status of the LTE radio link.

4 RADIO INSTALLATION AND CONFIGURATION

4.1 BASIC INSTALLATION AND CONFIGURATION

Note: It is recommended that you configure the wireless router from a wired computer.

1. If you are using the provided antennas (as opposed to an external antenna), attach the antennas to the front of the router and position them to achieve the best coverage. It is recommended that you position all antennas vertically (as shown) for an initial installation and adjust as required.

2. Connect a network cable from one of the LAN ports of your router to your computer.

3. Connect the provided power adapter from a power outlet to your router power port.

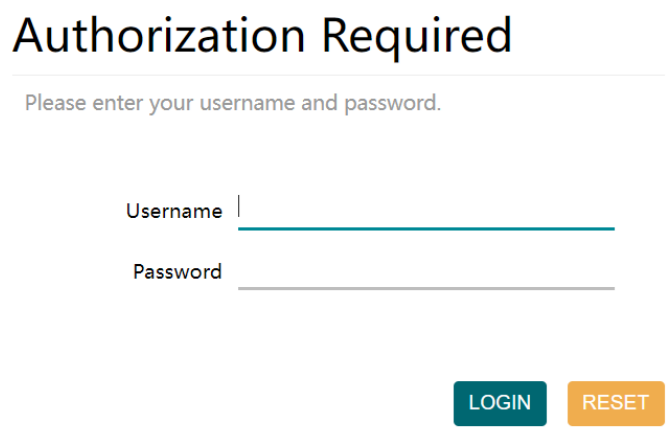
4. The Power LED will light up with a solid light, indicating that the router is ready.

5. Open your web browser on the connected computer and in the address bar, enter http://192.168.10.1 and press **Enter** to access the router web configuration page.

6. Enter the default **Username** and **Password**, then click **Login**. By default, the pre-configured username and password are located on the included preset wireless settings sticker or device label located on the bottom of the router.

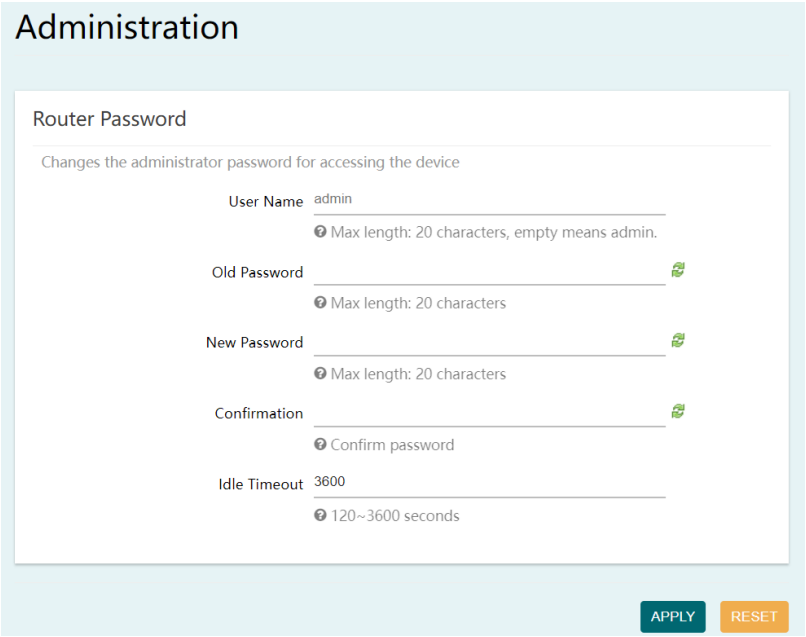
Default username: admin

Password: admin



7. To change the administrator password for the router configuration, click **Administrator** and click **Administration.**

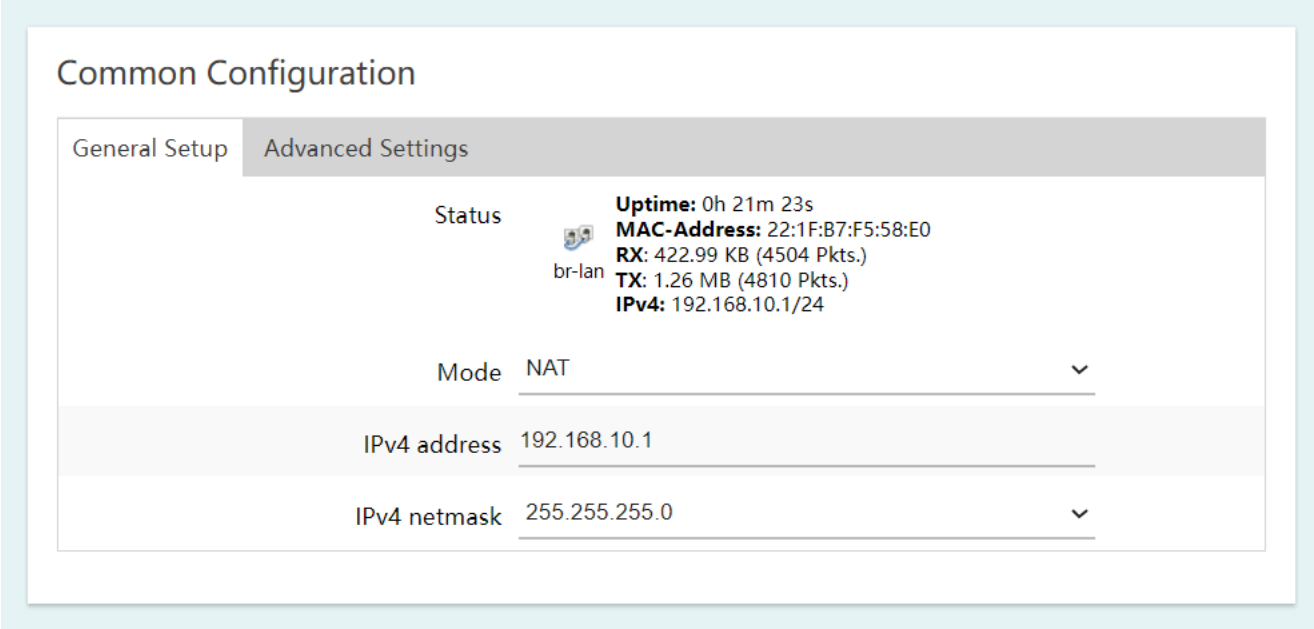
8. Enter the new administrator username/password in the **Username, Old Password, New Password** field and re-type the new password in the **Confirmation** field. Click **Apply** to save and commit the changes.



9. To change your router's LAN IPv4 address settings, click on **Network** and click **LAN**.

10. Under Common Configuration and General Setup, enter the new LAN IPv4 address and subnet maps in the **IPv4 address** and **IPv4 netmask** fields. Click **Apply** to save and commit the changes. Please wait for the new address settings to be applied and log back into the router web configuration page using the new LAN IPv4 address.

Note: *If your computer IP address settings are not automatically updated to the new settings, you may need to manually renew your computer IP address settings in order for you to log back into the router web configuration with the new LAN IPv4 address settings.*



11. The mode can be configured to NAT if the IoT router needs to hide the private subnet via NAT and perform address translation along with traffic routing. Alternatively, it can be configured to Route-only (NAT-less) if it just needs to route the traffic between air and ethernet subnet.

4.2 Basic Router Settings

4.2.1 Access your Router Management Page

Note: Your router management page IP address http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User Guide.

1. Open your web browser and go to IP address http://192.168.10.1. Your router will prompt you for a username and password.

2. For added security, the router is pre-configured with a unique administrator password. You can find the **Password** on the sticker included in the router package contents or on the device label located on the bottom of the router. Enter your **Username** and **Password**, then click **LOGIN**.

Note: Username and Password are case sensitive.

4.2.2 Saving and applying router configuration changes

In the router management page, pages may include all, some, or one of the options below. Some configuration changes may require a device reboot.

• **Reset** – Clicking this option will reset all settings to their previous configuration on a specific page.

• **Apply –** Clicking this option will save and apply the configuration changes on a specific page which will take effect immediately.

• **Save –** Clicking this option will temporarily save the changes and allow you to temporarily save multiple configuration changes and apply all configuration changes at the same time. When you are ready to save and apply the configuration changes permanently, click on the notification in the top right corner.

4.2.3 Change your administrator password

Administrator > Administration

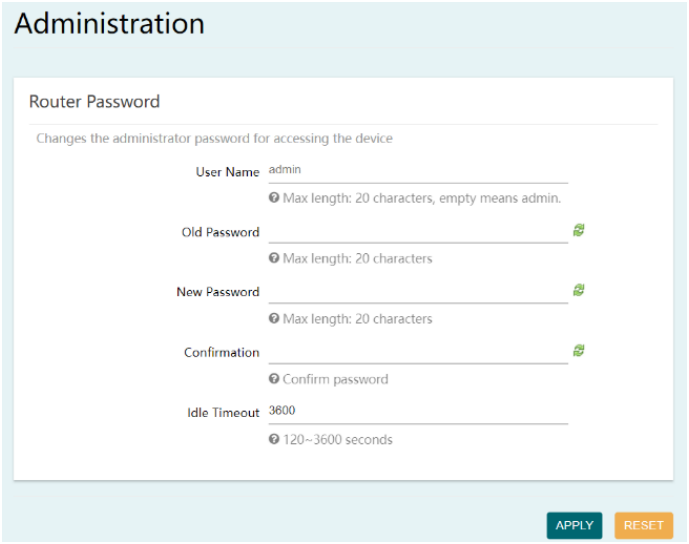
By default, the administrator password has been pre-configured with a unique password. You can find the pre-configured administrator password on the wireless sticker included in your router package contents or also located on the router device label located on the bottom of the device. This section will allow you to change the default administrator password used to log into your router management page.

1. Log into your router management page

2. Click on **Administrator** and click on **Administration**.

3. Enter the new administrator username/password in the **Username, Old Password, New Password** field and re-type the new password in the **Confirmation** field. Click **Apply** to save and commit the changes.

Note: The idle timeout setting is used to define the period of inactivity in the router management page before automatically logging out.



Note: If you change the administrator password, you will need to access the router management page using the Username “admin” and the new password instead of the pre-configured default password. If you reset the device to factory defaults, you will need to access the router management page using the pre-configured settings on the included wireless sticker in the router package contents or on device label located on the bottom of the router.

4.2.4 Set your router date and time

Administrator > System

It is recommended to set the router date and time for scheduling functions and logging functions for monitoring and troubleshooting.

1. Log into your router Administrator page

2. Click on **System.**

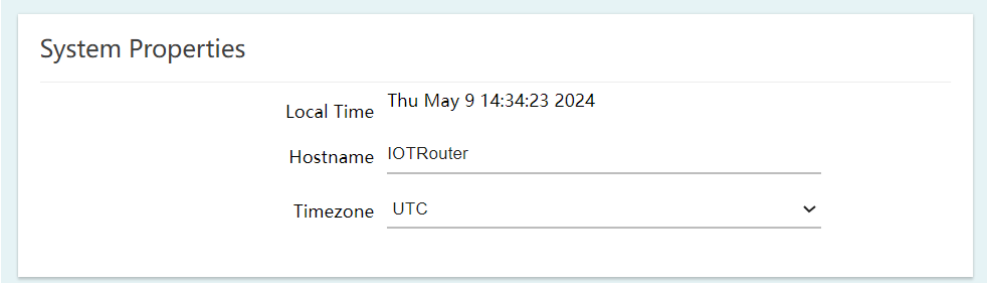
3. Review the settings below. Click **Apply** to save and commit the changes.

System Properties

• **Local Time –** Displays the current day, date, and time.

• **Hostname –** Modifies the router host name. The host name identifies is the name used to identify the router to other computer or devices on the network. Modifying this setting will modify the hostname used when accessing the router management page using the hostname or when using the Samba USB share feature.

• **Timezone –** Click the drop-down list to select the appropriate time zone.



Logging

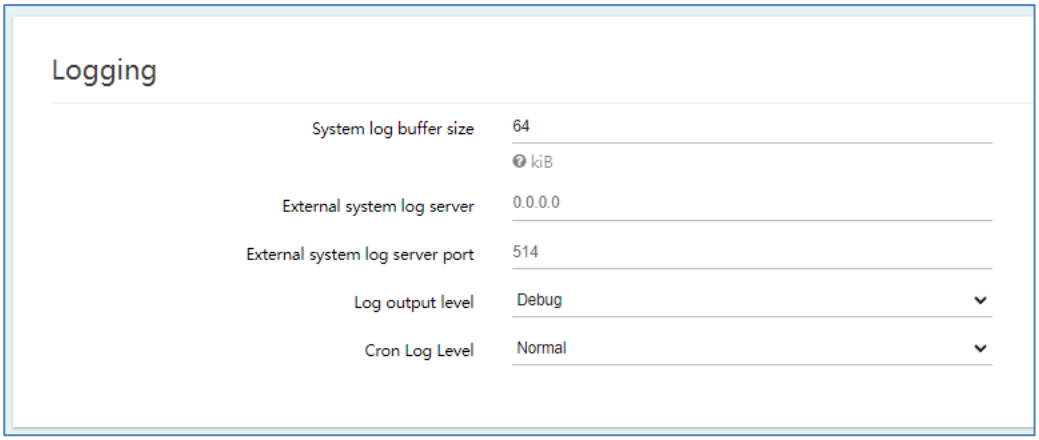
• **System log buffer size –** The system log buffer size in KB can be configured.

• **External system log server –** The logs can be redirected to an external syslog server which requires the server IP address configuration.

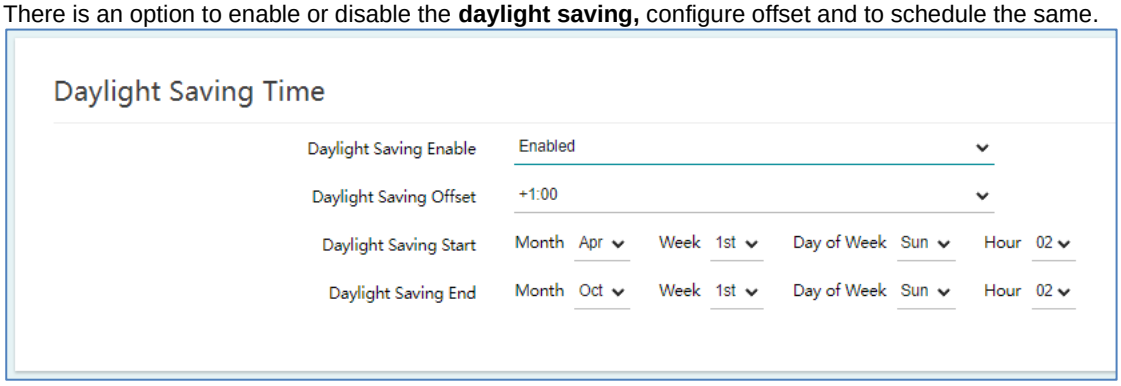
• **External system log port –** The port number for communication with log server.

• **Log output level –** The log level for system logs.

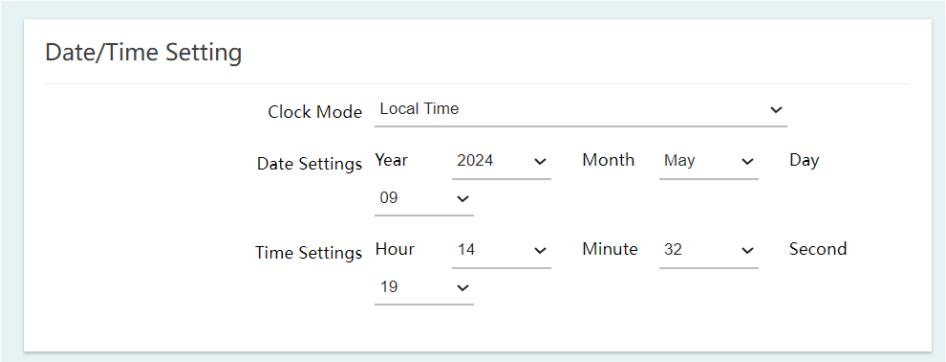
• **Cron log Level –** The log level for cron logs.



There is an option to enable or disable the **daylight saving,** configure offset and to schedule the same.



Time Synchronization



Clock Mode – Select the method of clock mode

- **Local Time:** Manually input the time
- **NTP:** Time is grabbed by a designated NTP server
- **NTP server candidates –** Enter the domain name of the network time server to obtain time and settings. (e.g. pool.ntp.org)
- An optional license is available for Cloud Sync Time which enables the time to be synched with the Ubiik cloud server

Note: *You can add multiple time servers by clicking the* icon *next to the NTP Server candidate domain name. If one server is not available, your router will try the next available server in the list.*

4.2.5 Create time schedules

Administrator > Schedule

Your router allows you to create schedules to specify a time period when a feature should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time and date settings are configured correctly.

1. Log into your router management page

2. Click on **Administrator** and click **Schedule**.

3. Review the settings below. Click **Add** to add the new schedule to the list and **Apply** to save and commit the changes.

• **Name –** Enter a name for the new schedule rule.

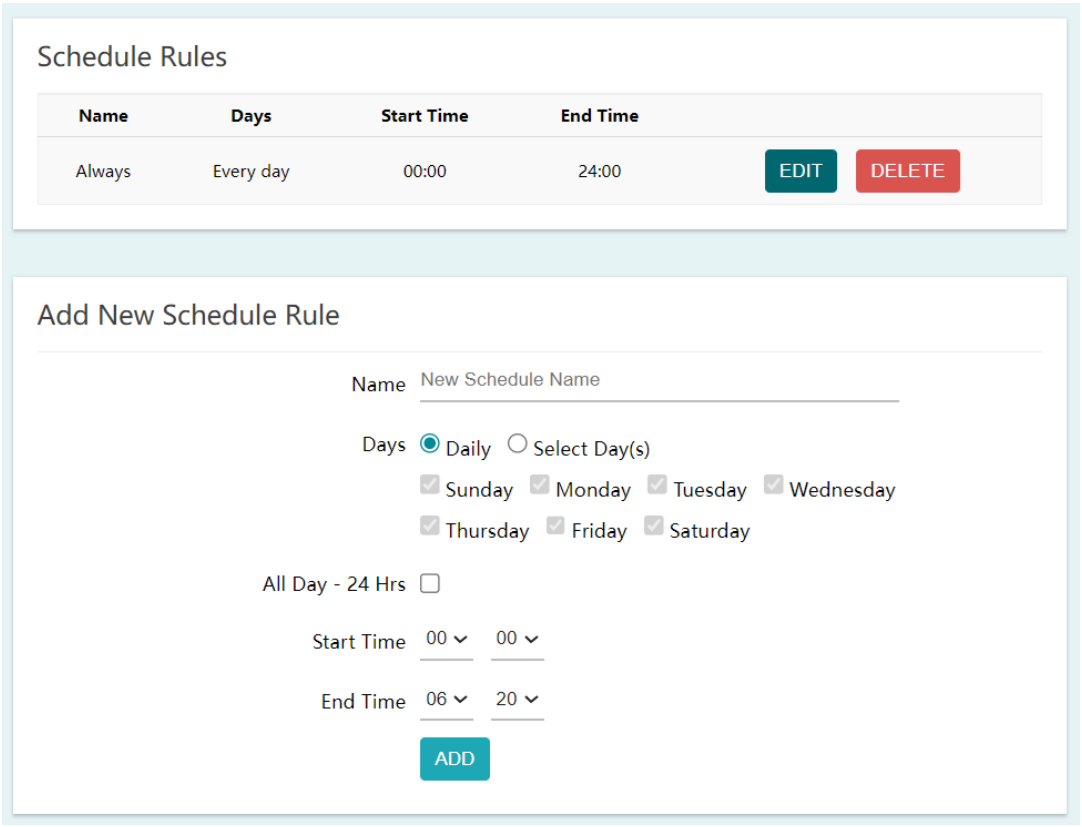
• **Days –** Choosing **Daily** will set the set the schedule rule to occur at the specified time every day. Choosing **Select Day(s)** will allow the user to manually select specific days for the schedule.

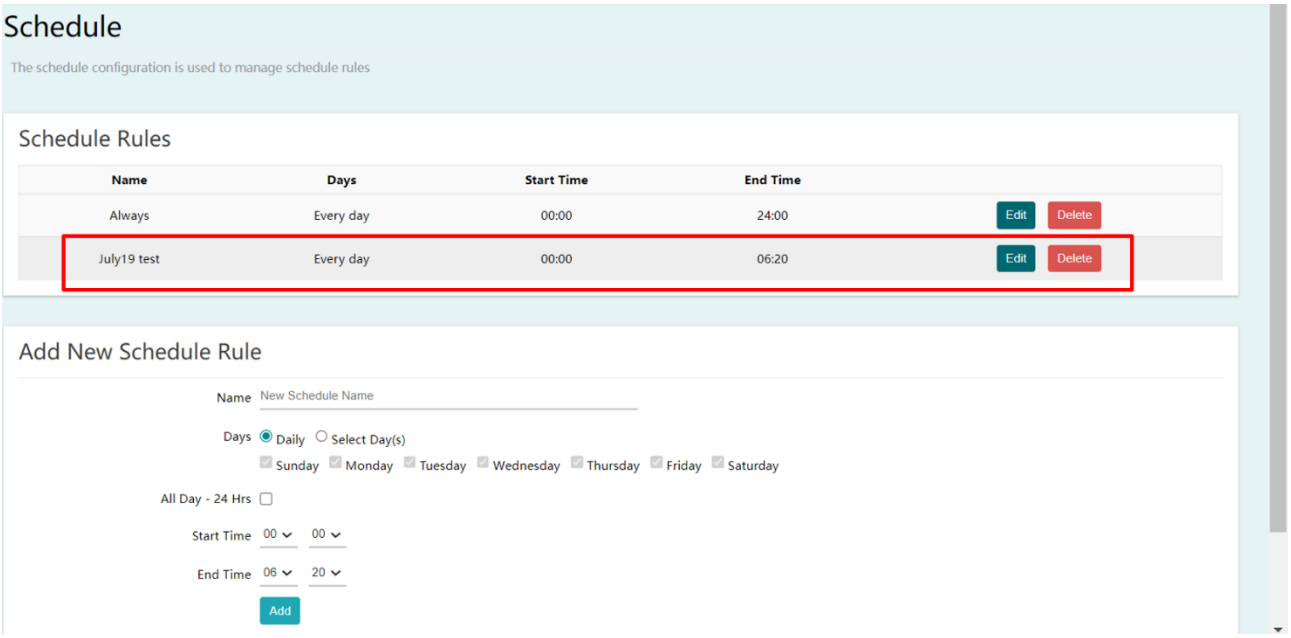
• **All Day – 24 Hrs –** Checking this option will set the schedule to run all 24 hours instead of a manually configured specified time period.

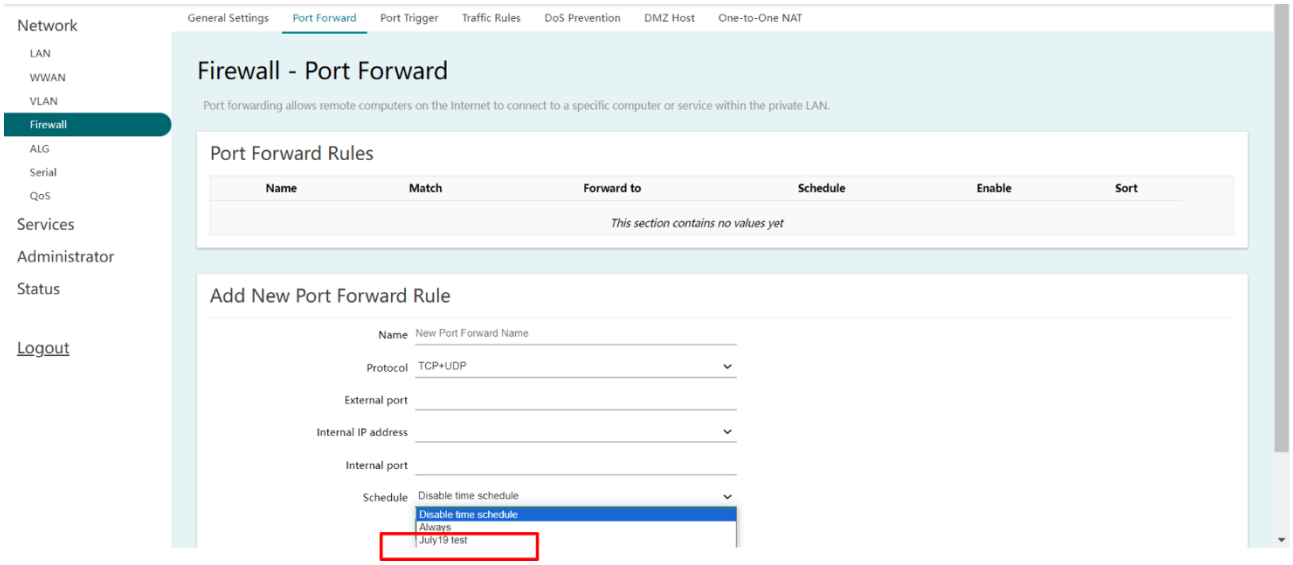
• **Start Time / End Time –** Manually define a time period for the schedule.

Notes:

- The time period is specified in 24-hour format.
- After adding a new schedule on this page, a corresponding selection shows in the dropdown list on the *Network>Firewall>Port Forward* page.


Schedule Rules
Name
Days
Start Time
End Time
Always
Every day
00:00
24:00
EDIT
DELETE
Add New Schedule Rule
Name
New Schedule Name
Days
Daily
Select Day(s)
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
All Day - 24 Hrs
Start Time
End Time
ADD


Schedule
The schedule configuration is used to manage schedule rules
Schedule Rules
Name
Days
Start Time
End Time
Always
Every day
00:00
24:00
Edit
Delete
July19 test
Every day
00:00
06:20
Edit
Delete
Add New Schedule Rule
Name
New Schedule Name
Days
Daily
Select Day(s)
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
All Day - 24 Hrs
Start Time
End Time
Add



4.2.6 Change LAN IPv4 address settings

Network > LAN

Note: The default LAN interface IPv4 address settings is 192.168.10.1 / 255.255.255.0. If the LAN IPv4 address settings are modified, you will need to log into the router management page with the new IPv4 address settings.

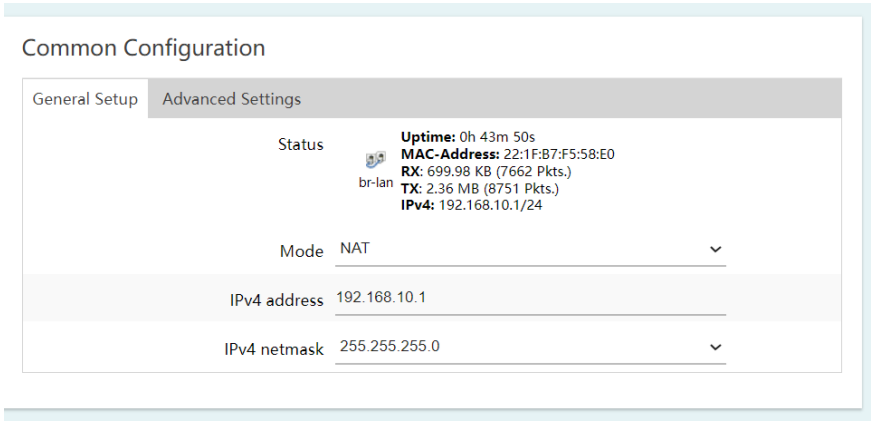
1. Log into your router management page

2. Click on **Network** and click **LAN**.

3. Under the Common Configuration section, you can enter the new LAN interface IP address settings.

• **IPv4 address** – Enter the new LAN IPv4 address. (e.g. 192.168.50.1)

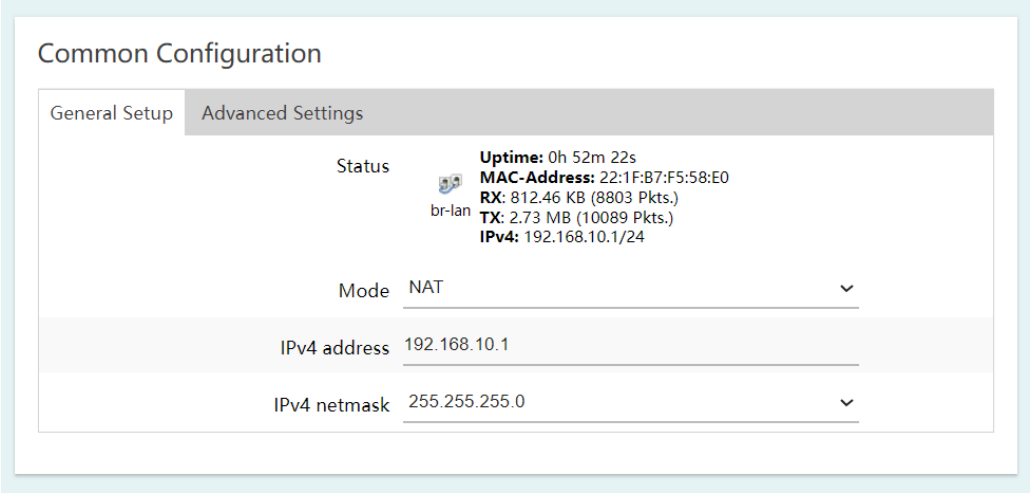
• **IPv4 netmask** – Select or Enter the new LAN IPv4 subnet mask. The drop-down menu will list class A, B, C, or custom which will allow you to manually enter a custom subnet mask. (e.g. 255.255.255.0)



4. Click **Apply**

Below is a reference of the additional LAN settings if you choose to make other configuration changes to these sections.

General Setup



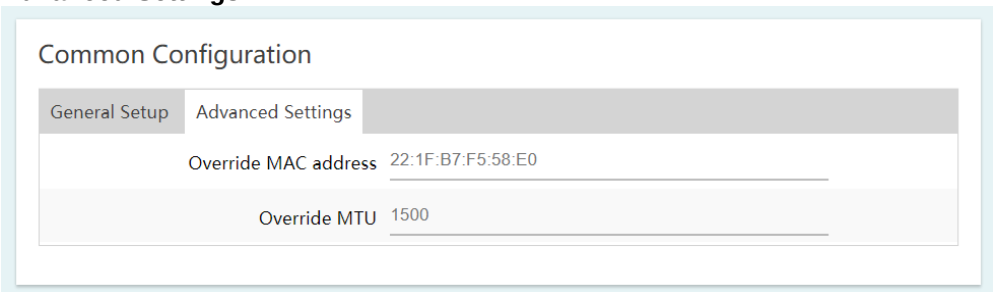
• **Status** – LAN Interface (br-lan)

- Uptime – Displays the amount time the LAN interface has been up and continuously running. This time will reset if the router is powered off or if the router is rebooted.
- MAC-Address – Displays the current MAC address assigned to the LAN interface.
- Rx – Displays the total amount of data received by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
- Tx – Displays the total amount of data transmitted by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
- IPv4: Displays the current IPv4 address settings assigned to the LAN interface.

• **Mode** – Allows you to change the function between NAT mode or Route Only (NAT-less).

- NAT – The default router mode which uses network address translation between the local internal (LAN/VLAN) interfaces and external (WAN1/WAN2) interfaces translating public and private IP addressing.
- Route Only (NAT-less) – This mode disables the NAT function between internal and external interfaces and may also be known as classical routing mode. This mode should only be used when the router is using for local internal IP routing only

Advanced Settings



• **Override MAC Address –** This parameter allows you to assign a new LAN interface (br-lan) MAC address. Typically, this parameter does not need to be modified. *(e.g. AA:BB:CC:DD:EE:FF)*

• **Override MTU –** The default MTU (maximum transfer unit) or frame size is set to 1500 bytes. This parameter allows you to assign a new MTU size. Typically, this parameter does not need to be modified.

4.2.7 Configure LAN IPv4 DHCP server settings

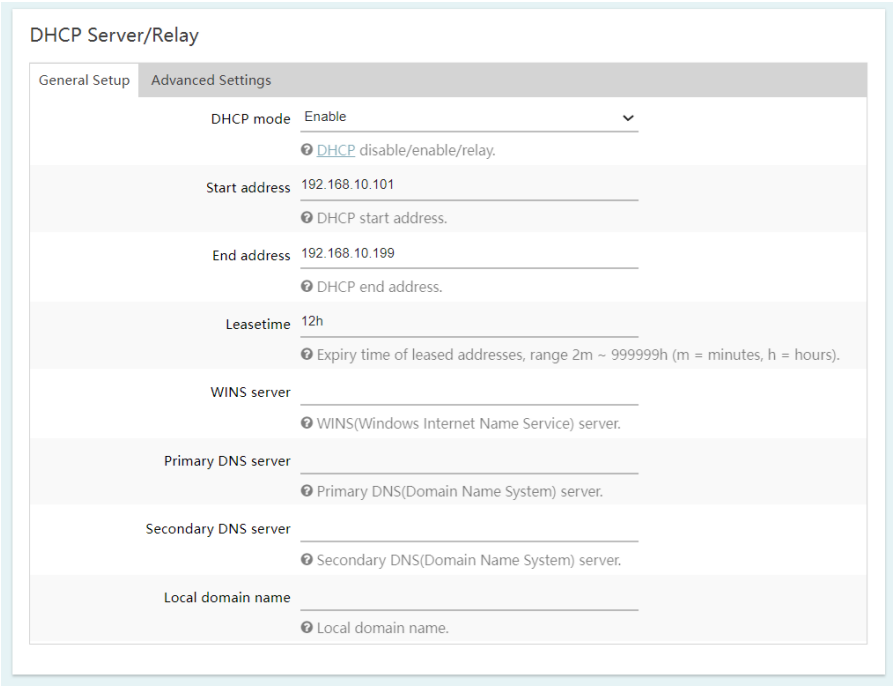
Network > LAN

Note: The internal DHCP server function is enabled by default on the LAN interface to automatically distribute IP address settings to network devices connected to the LAN and wireless LAN interfaces. The internal DHCP server only supports only the class C IP address range. The default IP range is 101 – 199 (192.168.10.101 – 192.168.10.199)

1. Log into your router management page

2. Click on **Network** and click **LAN**.

3. Under the DHCP Server/Relay section, you can modify or enter the new DHCP settings and click **Apply** to save and commit the changes.



• **DHCP mode –** Allows you to set the mode to Enable, Disable, or Relay.

- **Enable** – Using this setting enables the DHCP server function on the LAN interface.
- **Disable** - Using this setting disables the DHCP server function on the LAN interface.
- **Relay –** Using this setting allows you to use an external DHCP server instead of your router's internal DHCP server to distribute IP address settings on the LAN interface. If choosing this setting, enter the IP address of your external DHCP relay server.

• **Start address –** Enter the starting value of DHCP IPv4 address range. *(e.g. If your LAN IPv4 address is 192.168.50.1, entering 120 will define the first IP address of the DHCP pool is 192.168.50.120)*

• **End address –** Enter the ending value of DHCP IPv4 address range. *(e.g. If your LAN IPv4 address is 192.168.50.1, entering 200 will define the last IP address of the DHCP pool is 192.168.50.200)*

• **Leasetime –** Enter the lease time in hours (h) or minutes (m) DHCP clients will hold their IP address settings before automatically requesting a new lease (IP address settings) from the internal DHCP server. *(e.g. To specify 24 hours, enter 24h. To specify 480 minutes, enter 480m.)*

• **WINS server –** Enter the IPv4 address of your WINS (Windows Internet Name Server) for internal host name resolution on your local network to be distributed to DHCP clients. The WINS server provides the host name to IP address resolution for the NetBIOS naming service. This parameter is optional. *(e.g. 192.168.50.250)*

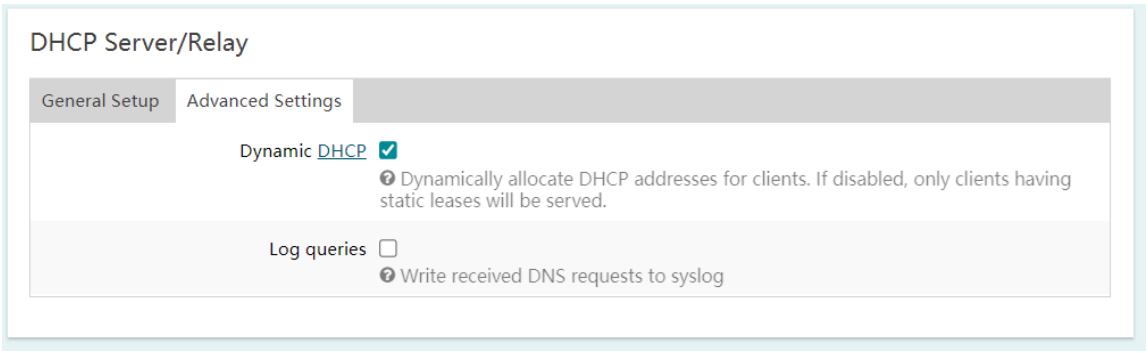
• **Primary DNS –** Enter the IPv4 address of your primary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. By default, the internal DHCP server uses DNS relay and provides the router LAN IPv4 address as the primary DNS server to DHCP clients. The DNS server provides the Internet domain name to IP address resolution when computers are accessing or browsing Internet websites. This parameter is optional. *(e.g. If entering 8.8.8.8, this DNS server will be provided DHCP clients instead of the router's LAN IPv4 address to resolve Internet domain names such as trendnet.com).*

• **Secondary DNS –** Enter the IPv4 address of your secondary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. If the primary DNS server cannot be reached, the secondary DNS server will be used. This parameter is optional. *(e.g. 8.8.4.4)*

• **Local domain name –** Enter a domain name to distribute to DHCP clients. This parameter is optional. *(e.g. trendnet.com)*

Below is a reference of the additional DHCP Server/Relay settings if you choose to make other configuration changes to these sections.

Advanced Settings



• **Dynamic DHCP –** Checking this option enables the DHCP server to distribute IPv4 address settings dynamically to clients. If this option is unchecked, IPv4 address settings will only be assigned to DHCP clients with a static DHCP reservation. Typically, this parameter does not need to be modified.

• **Log Queries –** Checking this option will enable logging to internal or syslog of any DNS queries. Typically, this parameter does not need to be modified.

4.2.8 Add static DHCP reservations

Network > LAN

1. Log into your router management page.

2. Click on **Network** and click **LAN**.

3. Under the Static Leases section, click **Add**.

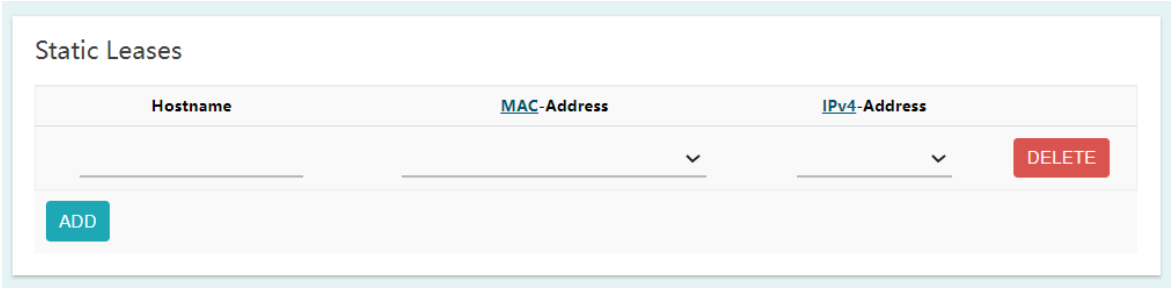
4. Enter the parameters for the static DHCP reservation and click **Apply** to save and commit the changes.

Note: The network device or computer the reservation is created for will need to release and renew the IPv4 address settings in order to obtain the new IP address settings.

• **Hostname –** Enter a name for the DHCP reservation. (e.g. trendnetpc)

• **MAC-Address –** Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. You can also click the drop-down list to select from a list of network devices detected by the router that have been assigned IPv4 address settings through DHCP. (e.g. AA:BB:CC:DD:EE:FF)

• **IPv4-Address –** Enter the IPv4 address to assign to the computer or network device for the reservation. You can also click the drop-down list to select from list of network devices detected by the router through DHCP. (e.g. 192.168.50.150)



4.2.9 Add static host name entries

Network > LAN

The router can be used for host name to IP address resolution of computers or network devices on your local network similar to a WINS server, however, entries will not dynamically populate and each entry must be manually entered. For clients to resolve the manually entered static entries, DHCP clients must use the router LAN IPv4 address as the WINS server.

1. Log into your router management page.

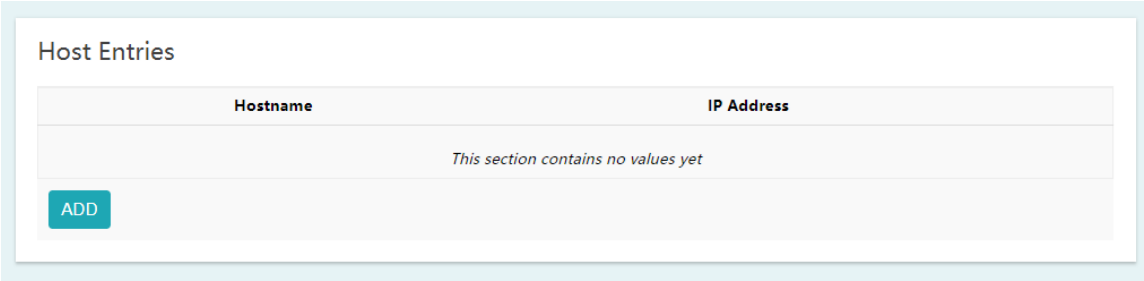
2. Click on **Network** and click **LAN**.

3. Under the Host Entries section, click **Add**.

4. Enter the parameters for the static host name entry and click **Apply** to save and commit the changes.

• **Hostname –** Enter the host name. (e.g. trendnetpc)

• **IP Address –** Enter the IPv4 address to resolve to host name. (e.g. 192.168.50.150)



4.2.10 Add static ARP entries

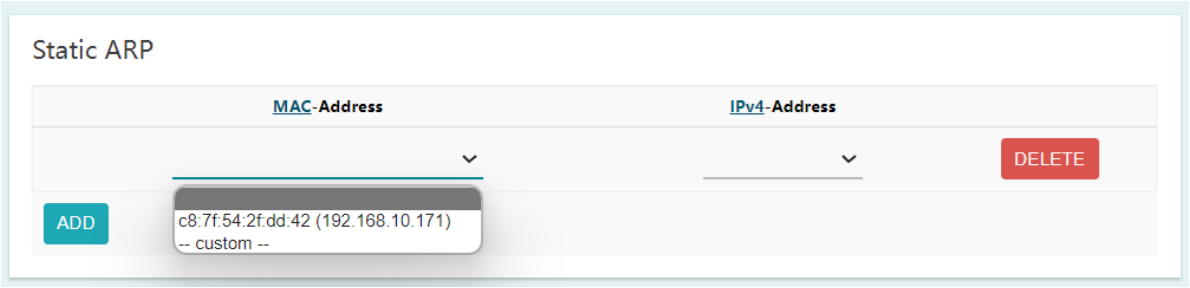
Network > LAN

ARP (Address Resolution Protocol) is the protocol responsible for resolving IP addresses to hardware MAC addresses. Typically, ARP entries are dynamically learned and refreshed in the ARP table however, in the case where your application requires static ARP entries to always be present in the router ARP table, you can manually enter and add them to the router. (ex. applications: WoL (Wake on LAN) or Wake on WAN)

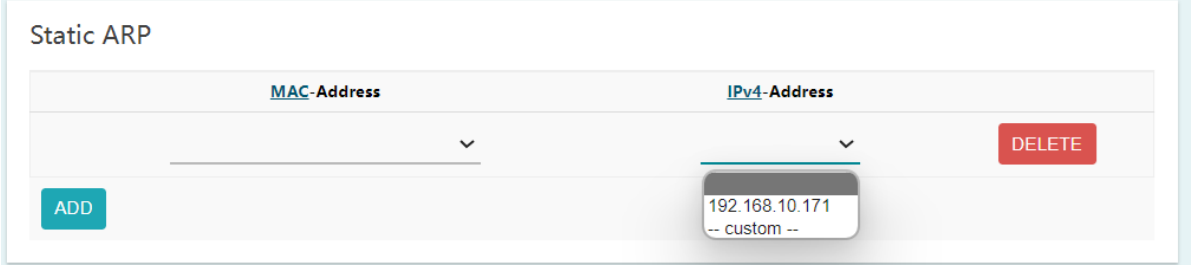
1. Log into your router management page.

2. Click on **Network** and click **LAN**.

3. Under the Static ARP section, click the **MAC-Address** drop-down list to select a MAC address from the list or select customer to manually enter a MAC address (format example: aa:bb:cc:dd:ee:ff).



4. Click the **IPv4-Address** drop-down list and select the IPv4 address to assign to the MAC address ARP table entry or select custom to manually enter an IPv4 address (format example: 192.168.10.129)

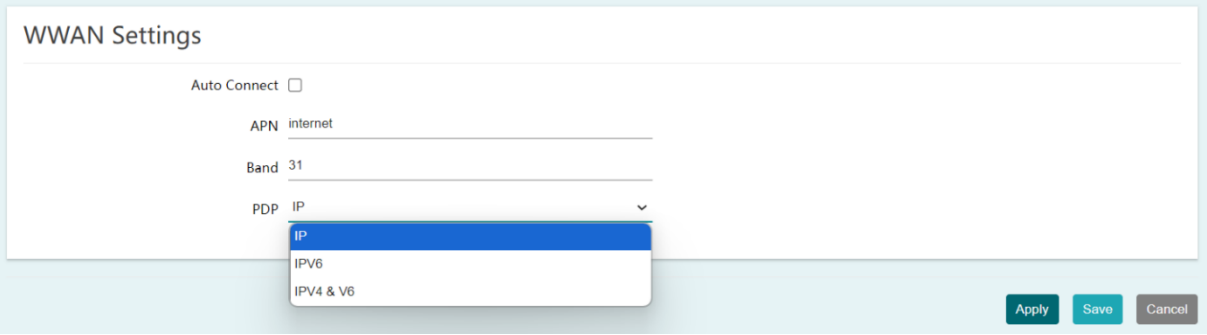


5. Click **Apply** to save and commit the changes.

Note: *You can specify additional static ARP entries by clicking* ***Add****. Delete existing entries by clicking the* ***Delete*** *button next to the entry to be removed.*

4.2.11 WWAN Settings

Network > WWAN Settings



1. The default setting for APN is Internet.

2. Enter the frequency band.

3. Click the **PDP** drop-down list and select the IP or IPV6 or IPV4 & V6.

4.2.12 Virtual LANs (VLANs)

Network > VLAN

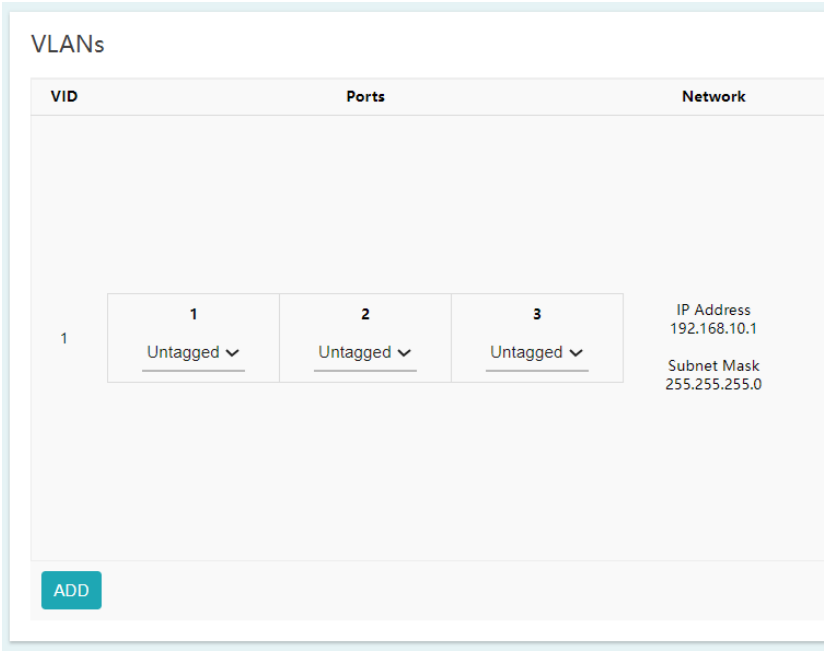
Your router supports port-based 802.1Q VLANs in addition to inter-VLAN routing. VLANs can be assigned different IP address interfaces in which the router can routed between VLAN IP subnets.

Create a port-based VLAN

1. Log into your router management page.

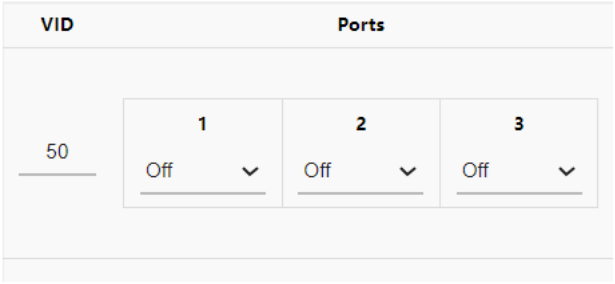
2. Click on **Network** and click **VLAN**.

3. Before assigning which untagged and tagged VLAN member ports are assigned to a new VLAN, the ports must be set to Off in the default VLAN VID: 1 (LAN). Also, click the Inter VLAN Routing drop-down list and select **Enabled** to enable communication between the LAN and other VLAN interfaces. Click **Apply** to save and commit the changes. Example: Below, we will remove port 3 from the default VLAN VID: 1 (LAN) interface so these ports can be re-assigned as untagged member ports of new VLANs.



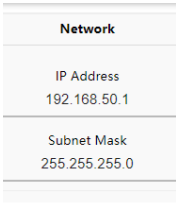
4. To create a new 802.1Q VLAN, under the VLANs section, click **Add**.

5. Under **VID,** enter the VLAN ID to assign to the new VLAN and set the untagged VLAN member ports. *Example: In the example below, we will create a new VLAN with VLAN ID: 50 and assign ports 2 as untagged member ports.*



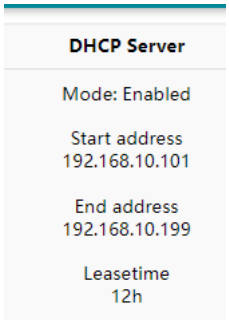
6. Enter the VLAN IP interface configuration under **IP Address** and **Subnet Mask.**

Example: In the example below, we will enter the VLAN 50 interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.



7. Under DHCP Server, click the **Mode** drop-down list and select **Enabled** to enable the DHCP server on the VLAN. Click **Apply** to save and commit the changes.

Example: In the example below, we will enable the DHCP server on VLAN 50 and leave IP address range and lease defaults. This will assign a DHCP IP range of 101-199 to ensure any devices connected to this VLAN obtain IP address information via DHCP.



If following the port-based VLAN configuration example, any computers or devices connecting to port 2 will obtain 192.168.50.x/255.255.255.0 address settings and use the VLAN 50 IP interface 192.168.50.1 as the Internet gateway and gateway to other local IP subnets.

VLAN 50

IP address: 192.168.50.1

Mask: 255.255.255.0

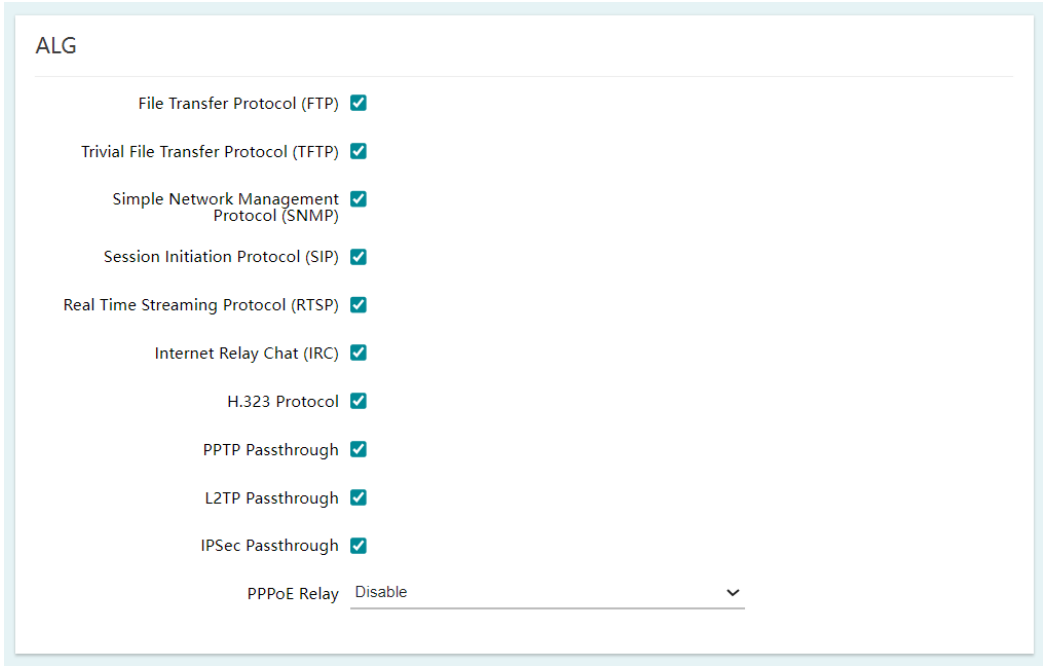
4.2.13 Application Layer Gateway (ALG)

Network > ALG

You may want to configure your router to allow computers the use of specific high layer applications or service sessions to pass through. Application Layer Gateways (ALG) allows you to easily enable or disable these applications to pass through your router.

Note: It is recommended to leave these settings enabled.

1. Log into your router management page.
2. Click on **Network** and click on **ALG**.
3. Review the applications. Click **Apply** to save and commit the changes.



4.2.14 UPnP and NAT-PMP

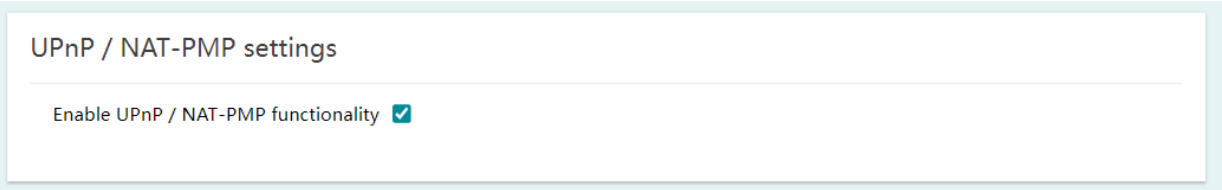
Services > UPnP

UPnP (Universal Plug and Play) and NAT-PMP (NAT Port Mapping Protocol) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP and NAT-PMP is disabled on your router by default and should only be enabled to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

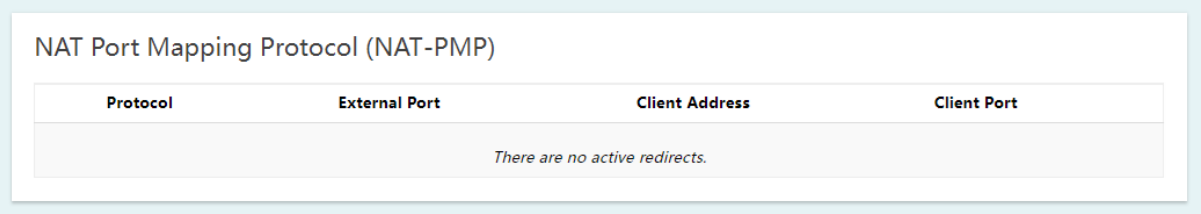
1. Log into your router management page.

2. Click on **Services** and click on **UPnP**.

3. Under the **UPnP** section, check the **Enable UPnP / NAT-PMP functionality** option. Click **Apply** to save and commit the changes.



Note: When UPnP/NAT-PMP is enabled, you can check the currently open connections in the UPnP/NAT-PMP entries table.



4.2.15 Quality of Service (QoS)

Network > QoS

The router supports up to four QoS priority queues for traffic classification and priority.

1. Log into your router management page.

2. Click on **Network** and click on **QoS**.

3. Under QoS settings, review the settings below. When complete, click **Apply** to save and commit your changes.

QoS Settings

• **Enable:** Check the enable option to **Enable** QoS.

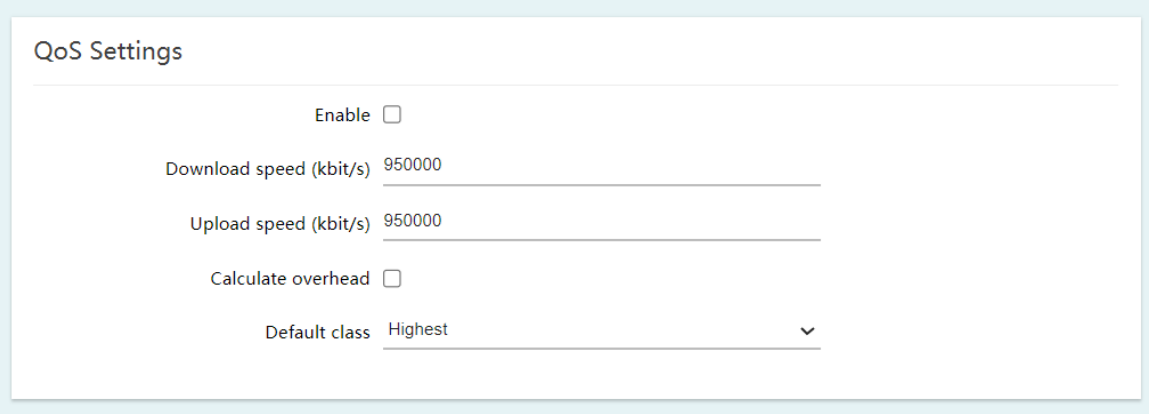
• **Download speed (kbit/s):** Enter the maximum download speed provided by your ISP in kilobits per sec. It is important to set this value accurately.

• **Upload speed (kbit/s):** Enter the maximum upload speed provided by your ISP in kilobits per sec. It is important to set this value accurately.

Note: *If your multiple mode is set to load balancing, you can combine the total upload bandwidth of both WAN connections.*

• **Calculate overhead** – Typically, when this option is unchecked/disabled, the overhead value will not be added to the upload and download speeds entered in the fields. When this option is checked/enabled, the total overhead calculation is included in the total upload/download speed specified to ensure the values entered are the absolute maximum value limits entered.

• **Default class** – When QoS is enabled, select the default priority class used for all other traffic after all specific QoS classification rules have been applied. You can typically set this to **Low**, **Medium, High** and **Highest**.



Classes – The QoS priority classes define the bandwidth maximum limits of total bandwidth that can be used and total bandwidth that can be shared for a particular class.

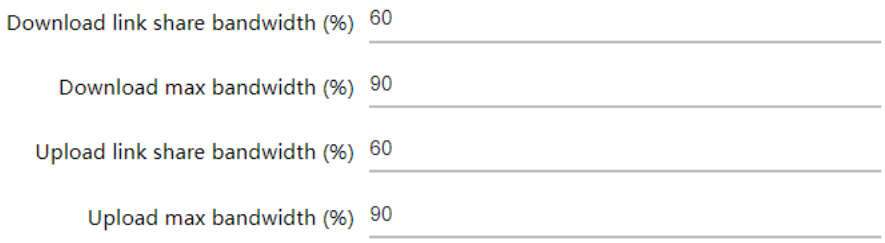
Note: *Typically, you do not need to modify the QoS priority class percentage settings.*

• **Download link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total download speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.

• **Download max bandwidth (%) –** This defines the maximum bandwidth % allowable from the total download speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.

• **Upload link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total upload speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.

• **Upload max bandwidth (%) –** This defines the maximum bandwidth % allowable from the total upload speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.



Classification Rules

Click Add to create a new QoS classification rule. When complete, click Apply to save and commit your changes.

• **Target** – Select the QoS priority class to apply to the rule.

• **Direction** – Select the direction of traffic in which to apply the QoS classification, Download (Inbound Traffic) or Upload (Outbound Traffic).

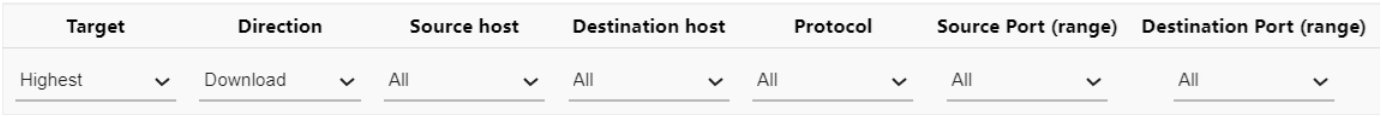
• **Source Host** – Click the drop-down list to select All (any IP address), a specific source host IP address from the list or select Custom to define a particular source IP address not listed.

• **Destination Host** – Click the drop-down list to select All (any IP address), a specific destination host IP address from the list or select Custom to define a particular destination IP address not listed.

• **Protocol** – Click the drop-down to select the type of traffic to apply the QoS classification rule. All/TCP/UDP/ICMP or custom to specify a particular protocol not listed.

• **Source Port** (range) – Enter the source port or source port range to apply the QoS classification rule.

• **Destination Port** (range) – Enter the source port or source port range to apply the QoS classification rule.



4.2.16 Dynamic DNS

Services > Dynamic DNS

When using a dynamic IP/DHCP WAN type from your ISP where your public IP or Internet IP address always changes, dynamic DNS provides a method of accessing your router or network remotely over the Internet for devices such as IP cameras, storage, or computers hosted on the local LAN side of your router. Dynamic DNS services do this by assigning a custom hostname or DNS name for you to reference. Your router will send updates to the dynamic DNS service provider if the WAN or Internet IP address(es) change providing the emulation of a virtual fixed IP address that you can always reference to access your router over the Internet.

Note: First, you will need to sign up for one of the DDNS service providers listed in the **Server Address** drop-down list**.**

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. no-ip.com, dyndns.org etc.)

2. Log into your router management page.

3. Click on **Services** and click on **Dynamic DNS**.

4. Review the **DDNS** settings below. When complete, click **Apply** to save and commit your changes.

• **Enabled** – Check the enabled option to enable dynamic DNS on the selected WAN interface.

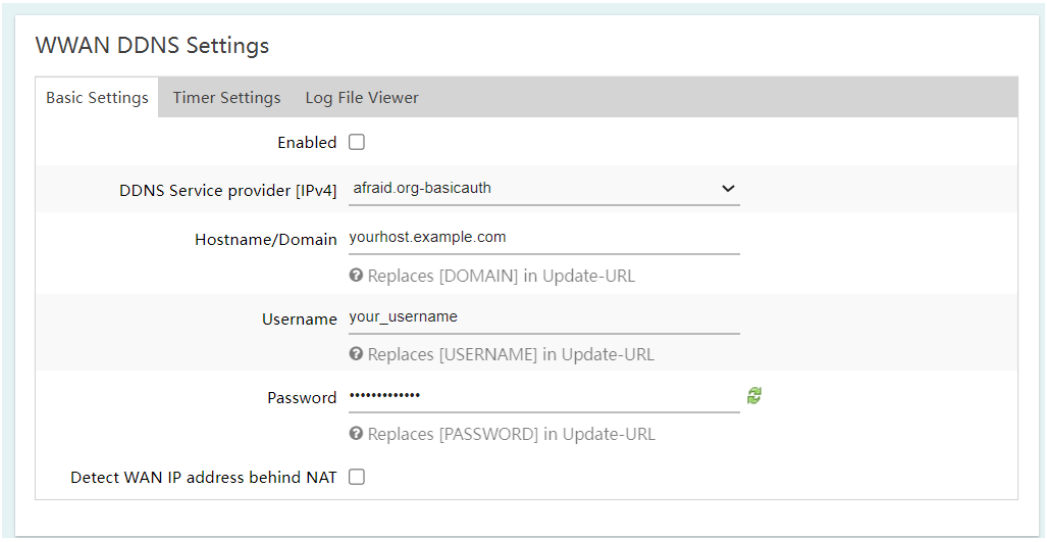
• **DDNS Provider [IPv4]:** Click the drop-down list Select your DDNS service.

• **Hostname/Domain:** Enter the custom hostname or DNS name you created with DDNS account. (e.g. trendnet.ddns.net)

• **Username:** This is the username required to login to your Dynamic DNS service account.

• **Password:** This is the password required to login to your Dynamic DNS service account.

• **Detect WAN IP address behind NAT:** This will allow your router to detect the IP address



Below is a reference of the additional Dynamic DNS settings if you choose to make other configuration changes to these sections.

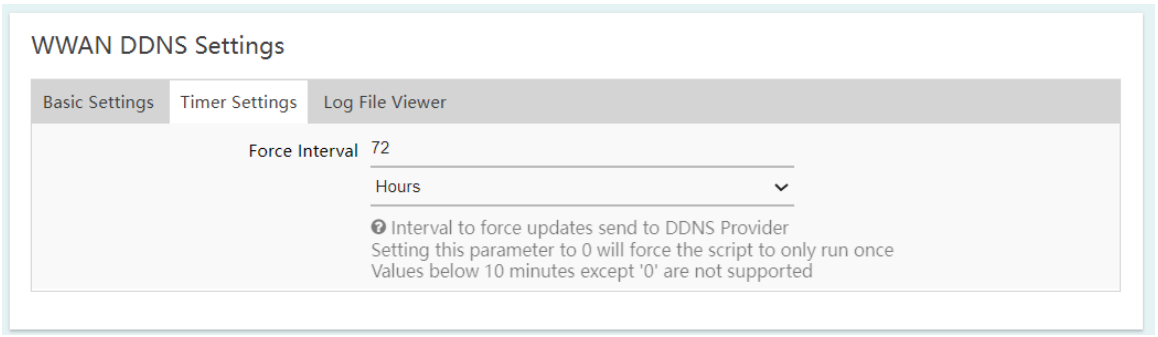
Timer Settings

Allows you to configure a specified interval to force your router to send a DDNS update to your DDNS service provider.

Note: *Please note that it is recommended not to set the interval too low and send updates too often as this may not meet the minimum requirements of your DDNS service provider client update policy.*

• **Force Interval –** Enter a value in days, hours, or minutes.

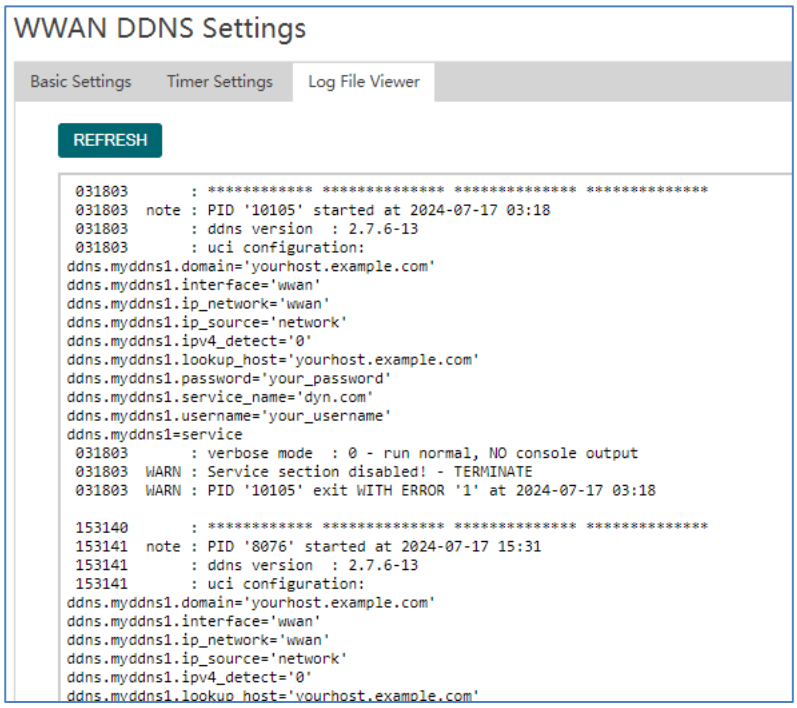
Note: The smallest interval allowed is 10 minutes. Setting the value to 0 will force your router to send a DDNS update only once and will not resend any more DDNS updates for the specified WAN.



Log File Viewer

Allows you to view the log status for Dynamic DNS of your router.

• Refresh – Clears any logged displayed and reload new logs



4.3 FIREWALL & SECURITY SETTINGS

4.3.1 General Settings

Network > Firewall > General Settings

1. Log into your router management page.

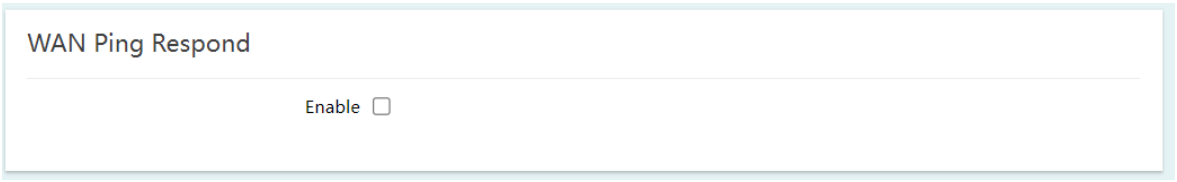
2. Click on **Network,** click on **Firewall,** and click on the **General Settings** tab.

3. Review the settings below. When complete, click **Apply** to save and commit your changes.

General Settings

WAN Ping Respond

• **Enable –** By default, this function is disabled to prevent the WAN port interfaces from responding to ping/ICMP requests. Enabling this option will set your WAN port interfaces to respond ping/ICMP requests from the Internet.



4.3.2 Port Forwarding rules

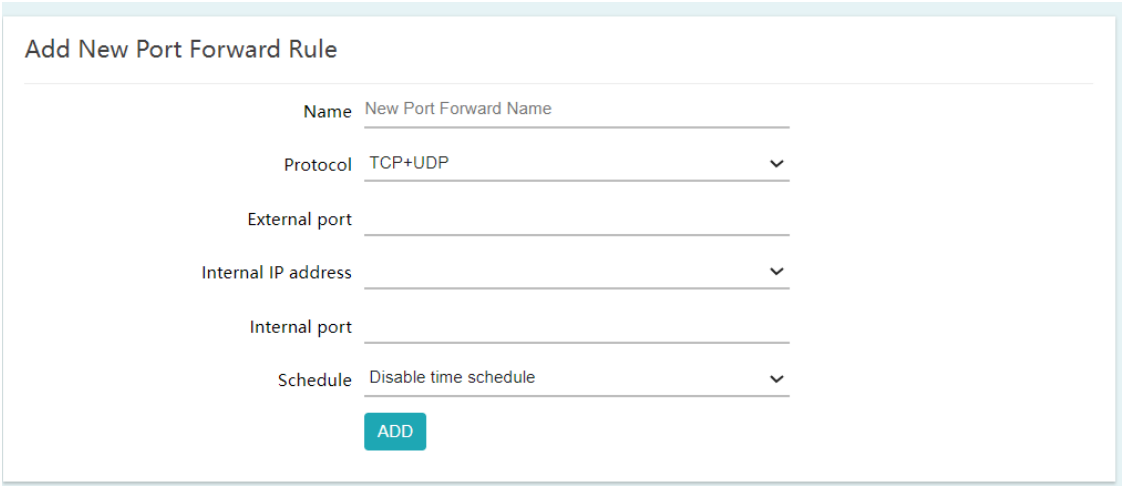
Network > Firewall > Port Forward

Port forwarding rules allow to create inbound rules from the WAN interfaces/Internet to your internal computers or devices for specific services/protocols such as a file server (FTP), IP camera, web server (HTTP/HTTPS), or remote access, etc.

1. Log into your router management page.

2. Click on **Network,** click on **Firewall,** and click on the **Port Forward** tab.

3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.



• **Name –** Enter a name for the new port forwarding rule.

• **Protocol –** Click the drop-down list to select the protocol for the service to allow: **TCP, UDP, TCP+UDP**, or **Other**.

• **External Port –** Enter the external port number for the service to allow.

Note: *You can also enter a consecutive range of ports in the following format: 80-90*

• **Internal IP address –** Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to forward the port/protocol service.

• **Internal Port –** Enter the internal port number for the service to allow.

Note: *You can also enter a consecutive range of ports in the following format: 80-90. Typically, the internal port or port range is same as the external port or port range.*

• **Schedule –** Allows you to select a schedule when the port forwarding rule should be enabled or disabled.

Note: *To restrict access to source IP address, after you have created the port forward rule, click* ***Edit*** *on the port forwarding entry in the list and enter the IP address in* ***Source IP address*** *field, then click* ***Apply.***

4.3.4 Port Trigger rules

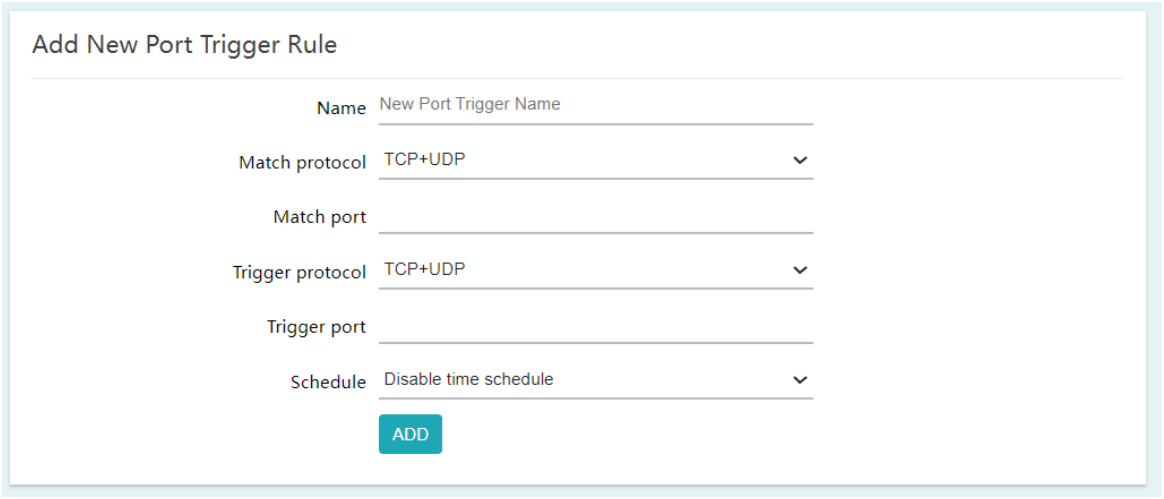
Network > Firewall > Port Trigger

Port triggering is typically used for applications that require a range of ports to be dynamically opened on request to an internal device on your network. The router will wait for a request on a specific port or range of ports (trigger port) from a device on your network and once a request is detected by your router, the router will forward a port or range of ports (match port) to the device on your network.

1. Log into your router management page.

2. Click on **Security,** click on **Firewall,** and click on the **Port Trigger** tab.

3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.



• **Name –** Enter a name for the new port trigger rule.

• **Match Protocol –** Click the drop-down list to select the match port protocol for the service to allow: **TCP, UDP,** or **TCP+UDP**.

• **Match Port –** Enter the match port number for the service to allow.

Note: *You can also enter a consecutive range of ports in the following format: 80-90*

• **Trigger Protocol –** Click the drop-down list to select the trigger port protocol for the service to allow: **TCP, UDP,** or **TCP+UDP**.

• **Trigger Port –** Enter the match port number for the service to allow.

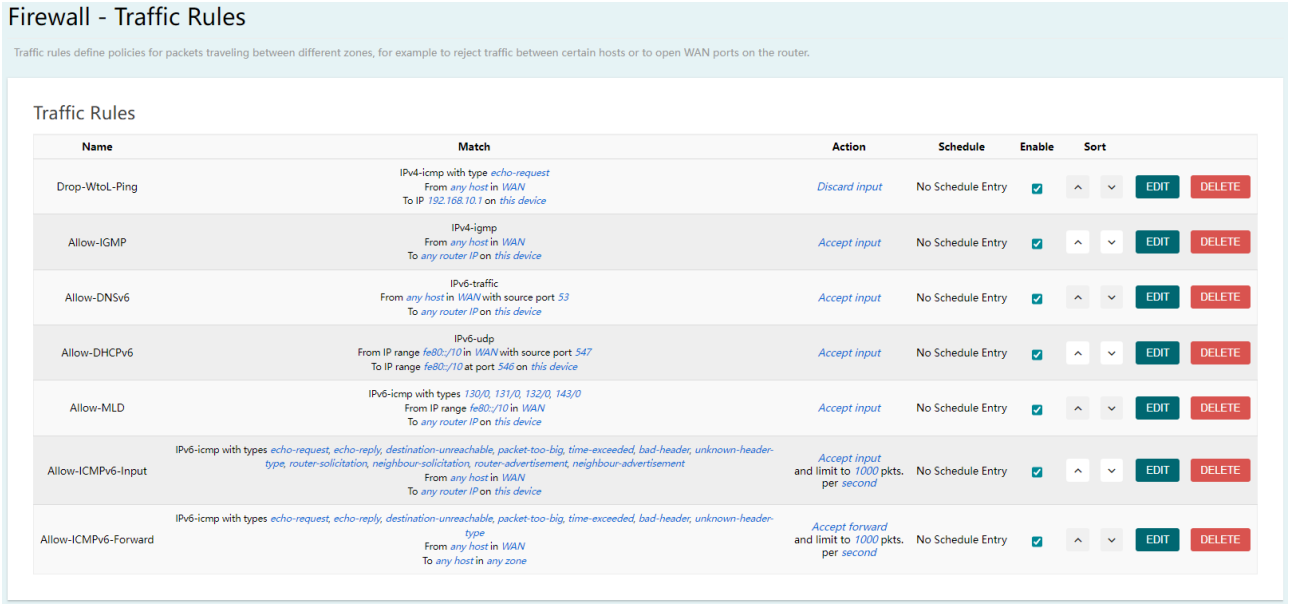
Note: *You can also enter a consecutive range of ports in the following format: 80-90*

• **Schedule –** Allows you to select a schedule when the port trigger rule should be enabled or disabled.

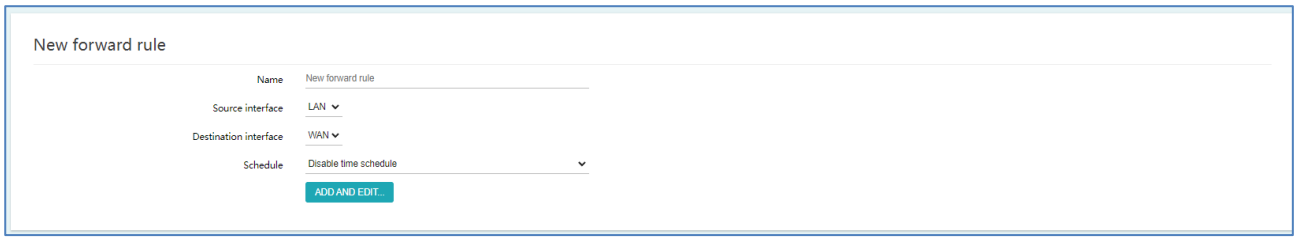
4.3.5 Traffic Rules

Network > Firewalls – Traffic rules

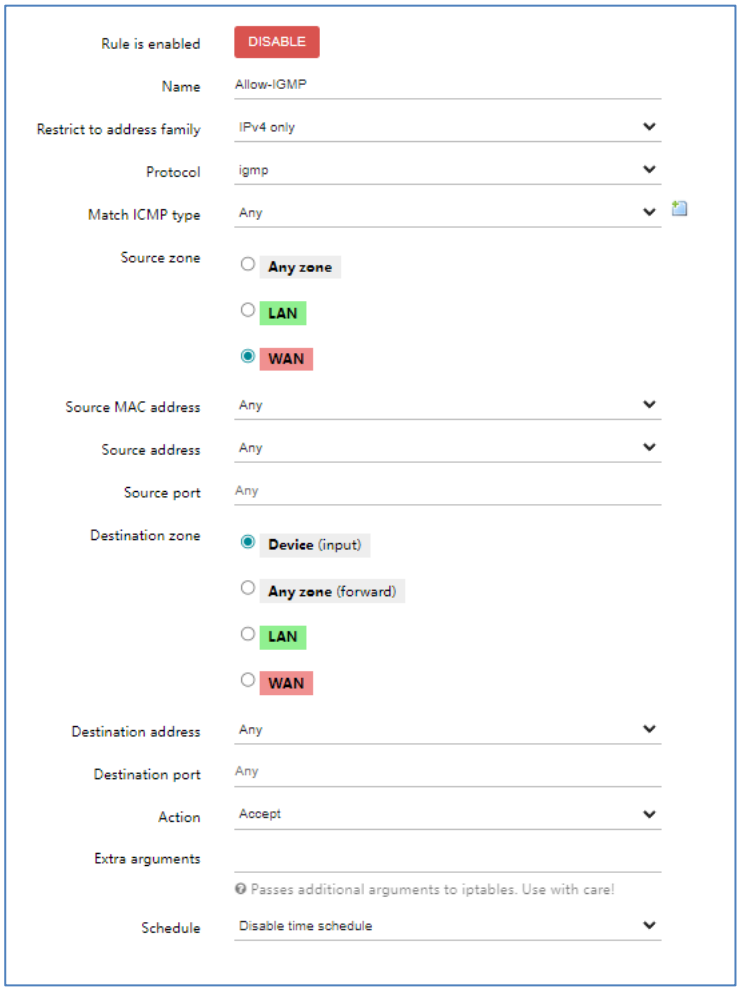
Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.



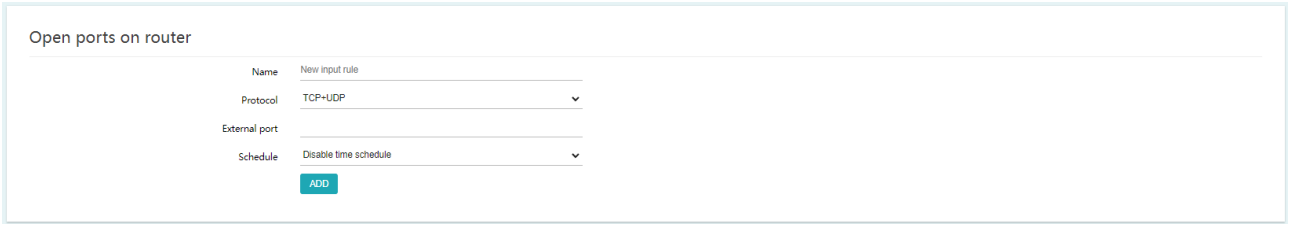
A new rule can be added



The rules can be edited or deleted or can be reordered.



If it is required to allow traffic with certain custom port number/(s), the ports can be opened on the router via “Open ports on router”.



4.3.6 Denial of Service (DoS) prevention

Network > Firewall > DoS Prevention

The router supports prevention against common denial of service (DoS) attacks. Malicious users use denial of service attacks to temporarily or permanently disrupt the availability of services from network resources such as your router. Typically, DoS attacks are achieved by flooding a specific network resource by excessively sending unnecessary requests which can cause the network device or resource to stop functioning.

1. Log into your router management page.

2. Click on **Network,** click on **Firewall,** and click on the **DoS Prevention** tab.

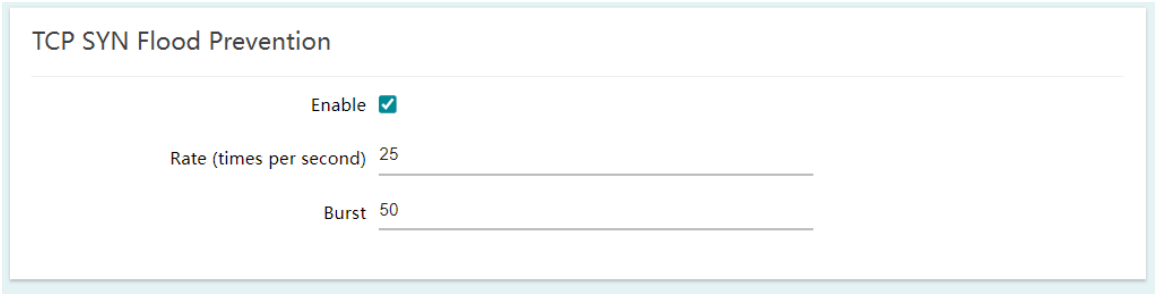
3. Review the settings below. When complete, **Apply** to save and commit your changes.

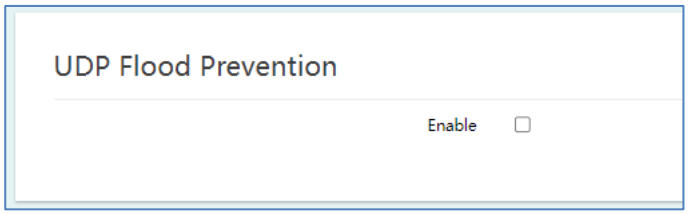
Choose the DoS prevention type to enable, TCP SYN flood, UDP flood, or ICMP flood.

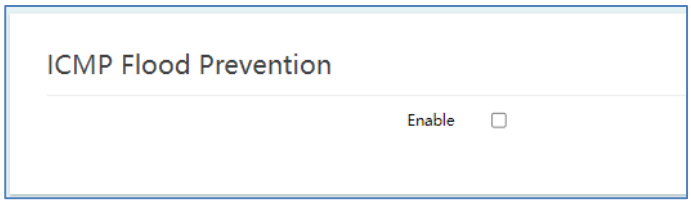
• **Enable –** Check this option to enable DoS prevention.

• **Rate (times per second) –** This value limits the number of packets that can be received by the router per second for a specific session.

• **Burst** – This value limits the total number of packets that can be received and stored in buffer memory for a specific session.







4.3.7 DMZ Host

Network > Firewall > DMZ Host

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards all ports to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet, however, it is a very insecure method and will open your local area network to greater threats from Internet attacks. It is recommended to use port forwarding instead to limit rules to specific ports/services only.

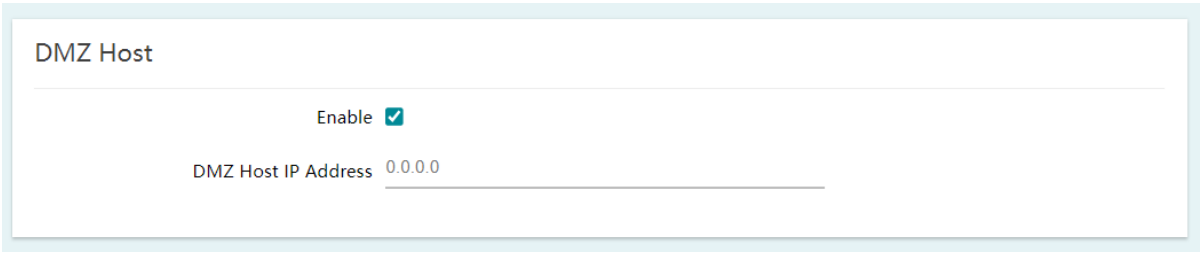
1. Log into your router management page.

2. Click on **Network,** click on **Firewall,** and click on the **DMZ Host** tab.

3. Review the settings below. When complete, **Apply** to save and commit your changes.

• **Enable –** Check this option to enable DMZ host.

• **DMZ Host IP Address -** Enter the IP address you assigned to the computer or network device to expose to the Internet. (e.g. 192.168.10.250)



4.3.8 One-to-One NAT

Network > Firewall > One-to-One NAT

If you have multiple static public WAN/Internet IP addresses assigned by your ISP, you can map the additional public IP addresses to a local computer or device on your network and allow all or specific ports or services similar to port forwarding

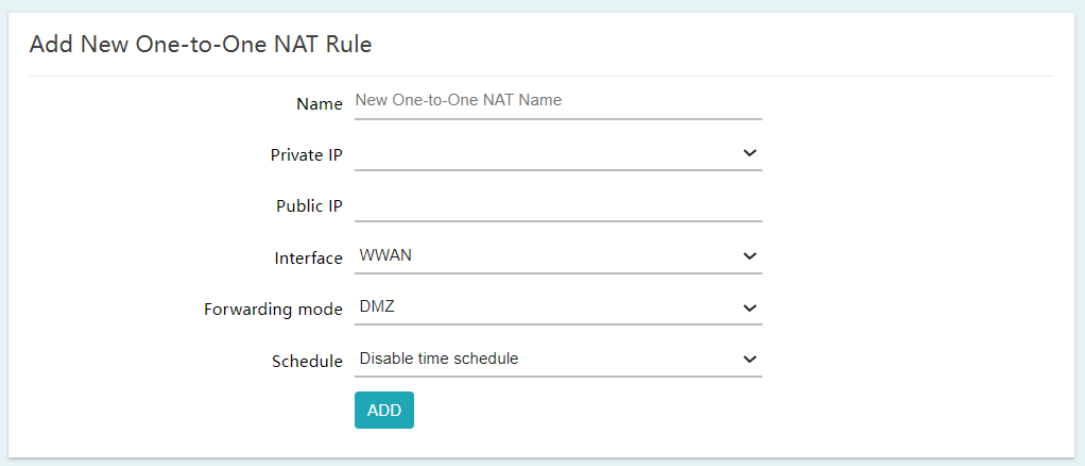
but using different public IP addresses through your router. Please check with your ISP if you have multiple static public IP addresses available that can be used to map to devices on your local network.

Note: This feature will only work when using a static IP address WAN type/protocol.

1. Log into your router management page.

2. Click on **Security,** click on **Firewall,** and click on the **One-to-One NAT** tab.

3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.



• **Name –** Enter a name for the new one-to-one NAT rule.

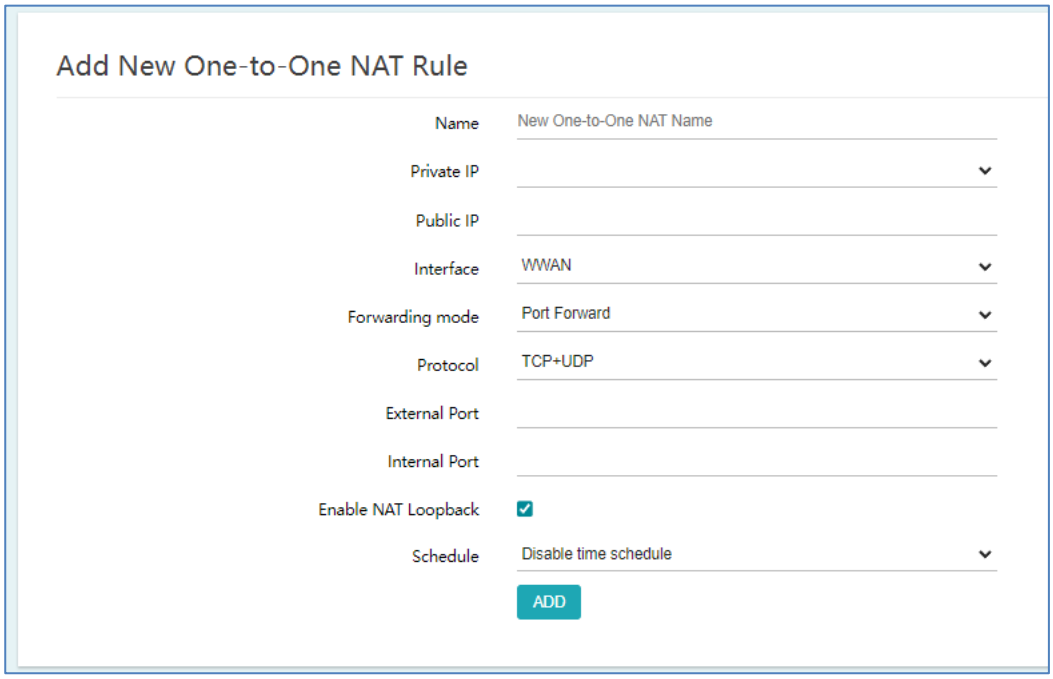
• **Private IP address –** Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to forward the port/protocol service.

• **Public IP –** Enter the additional static public Internet IP address you would like to map to the local/internal IP address.

• **Interface –** Click the drop-down list to select the external WAN interface(s) to allow: **WWAN**.

• **Forwarding Mode** - Select **DMZ** to forward all ports/protocols or **Port Forwarding** to specify which ports/protocols to allow.

- **DMZ –** Selecting this option will set the rule to forward all ports/protocols to the device's internal private IP address.
  - **Schedule –** Allows you to select a schedule when the port forwarding rule should be enabled or disabled.
- **Port Forward –** Selecting this option will allow to set the specific ports/protocols to allow for the rule.
- **Protocol –** Click the drop-down list to select the protocol for the service to allow: **TCP, UDP, TCP+UDP**, **ICMP**, or **Custom**.
  - **Schedule –** Allows you to select a schedule when the port forwarding rule should be enabled or disabled.


Add New One-to-One NAT Rule
Name
New One-to-One NAT Name
Private IP
Public IP
Interface
WWAN
Forwarding mode
Port Forward
Protocol
TCP+UDP
External Port
Internal Port
Enable NAT Loopback
Schedule
Disable time schedule
ADD

4.4 ROUTER MAINTENANCE AND MONITORING

4.4.1 Managing access to the router management interface

Administrator > Access Management

This section will allow you to restrict access router management access to specific interfaces. By default, management access to the web interface (HTTP) is restricted only to the LAN interface.

1. Log into your router management page.

2. Click on **Administrator** and click on **Access Management.**

3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Local Access Management

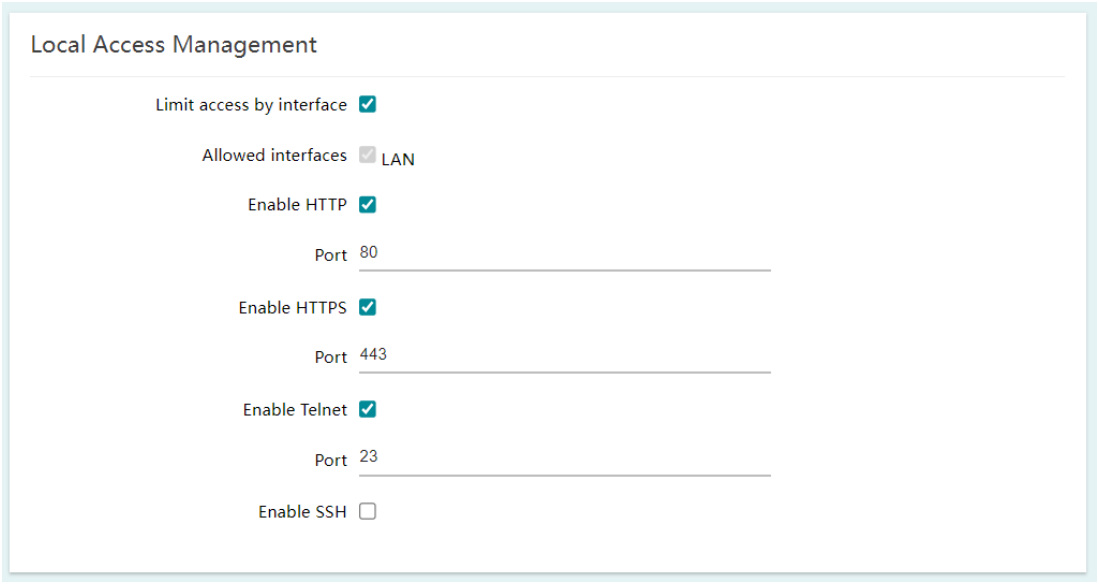
• **Limit access by interface –** Checking this option will allow you to select specific local interfaces (e.g. LAN, VLAN) that are allowed access to the router management interface.

o **Allowed interfaces –** The available local interfaces will be in this section. (e.g. Selecting LAN will only allow management access from the LAN and all other VLAN interfaces will be denied.)

• **Enable HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected local interfaces.

• **Enable Telnet –** Checking this option will enable command line interface access via Telnet on the selected local interfaces.

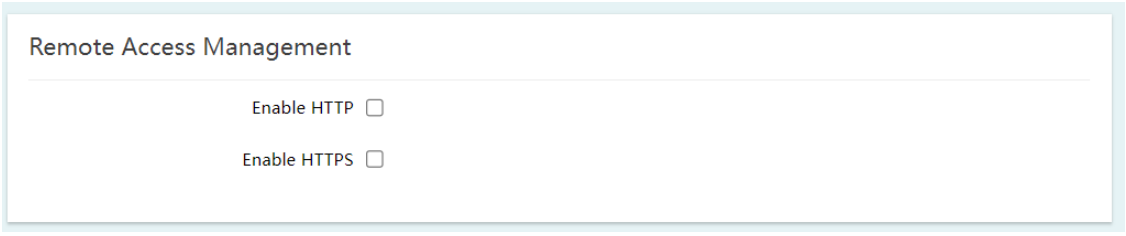
• **Enable SSH –** Checking this option will enable secure command line interface access via SSH (Secure Shell) on the selected local interfaces.



Remote Access Management

• Enable HTTPS – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected WAN interfaces.

• Enable SSH – Checking this option will enable secure command line interface access via SSH (Secure Shell) on the selected WAN interfaces.



4.4.2 Diagnostic tools

Administrator > Diagnostics

This section includes network tools and utilities for testing connectivity and troubleshooting.

1. Log into your router management page.

2. Click on **Administrator** and click on **Diagnostics.**

3. Review the settings below.

Network Utilities

• **Ping –** This tool conducts a basic ping/connectivity test to a host IP address or domain name. After selecting and entering all of the required parameters, click **PING** to start the connectivity test and the results will appear at the bottom of the page.

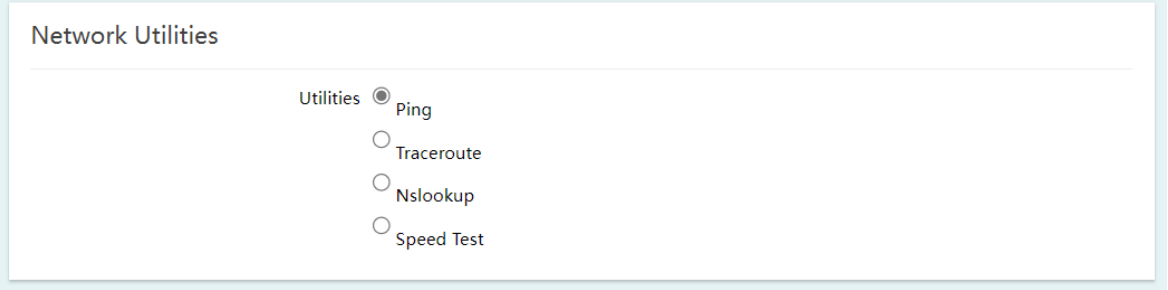
- **Protocol –** Select the IP protocol version for the connectivity test, IPv4 or IPv6.
- **Host –** Enter the host IP address or domain name to test connectivity.

• **Traceroute –** This tool conducts a test to check the routing path taken to reach a specific destination host IP address or domain name. After selecting and entering all of the required parameters, click **TRACEROUTE** to start the connectivity test and the results will appear at the bottom of the page.

- **Protocol –** Select the IP protocol version for the connectivity test, IPv4 or IPv6.
- **Host –** Enter the host IP address or domain name to test connectivity.

• **Nslookup –** This tool conducts a test to check domain name resolution to an IP address. After entering in the domain name to resolve, click **NSLOOKUP** to start the resolution test and the results will appear at the bottom of the page.

- **Host –** Enter the host IP address or domain name to test resolution.



Speed Test – This section allows for a speed test of your ISP connection with the option to specify **verbose** or **simple**.

4.4.3 Backup and restore your router configuration settings

Administrator>Backup / Flash Firmware

You may have added many customized settings to your router and in the case that you need to reset your router to factory defaults, all your customized settings will be lost. This will require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

To backup your router configuration:

1. Log into your router management page.

2. Click on **Administrator**, then click on **Backup / Flash Firmware**

3. Next to Download backup, click **Generate Archive**.

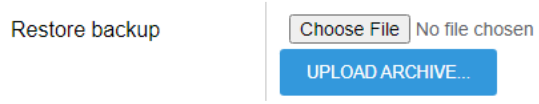
4. Depending on your web browser settings, you may be prompted to save the configuration file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: backup-TEW-929DRU-YYYY-MM-DD.dat)

To restore your router configuration:

1. Log into your router management page.

2. Click on **Administrator**, then click on **Backup / Flash Firmware.**

3. Next to Restore backup, click **Browse** or **Choose File**.



4. A separate file navigation window should open.

5. Select the router configuration file to restore and click **Upload Archive** (Default Filename: backup-TEW-929DRU-YYYY-MM-DD.dat). If prompted, click **Yes** or **OK**.

6. Wait for the router to restore settings.

To reset the firmware to its initial state:

1. click "Perform reset" 

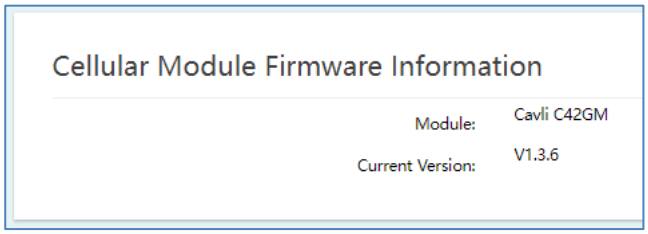
Administrator>Flash new firmware image

1. Click **Choose File**, then Select the FW file you want to use.

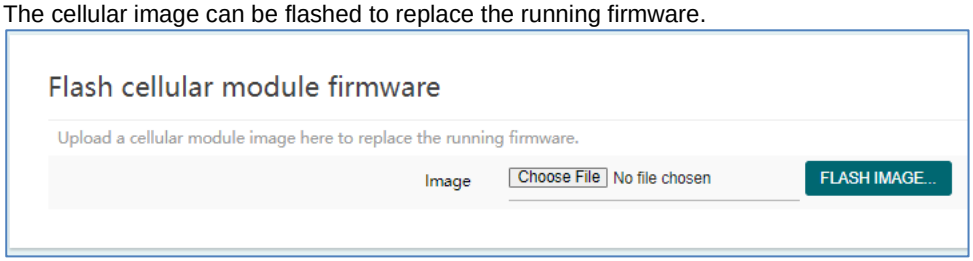
2. Click **Flash Image** and proceed with the FW update.

Cellular Module Firmware Information and Upgrade

The cellular current firmware information is displayed



The cellular image can be flashed to replace the running firmware.



4.4.4. Reboot your router

Administrator > Reboot

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

There are two methods that can be used to restart your router.

• **Turn the router** off for 10 seconds.

Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.

OR

• **Router Management Page** – This is also known as a soft reboot.

1. Log into your router management page.
2. Click on **Administrator**, then click on **Reboot.**
3. Next to Reboots the operating system, click **Perform Reboot**.

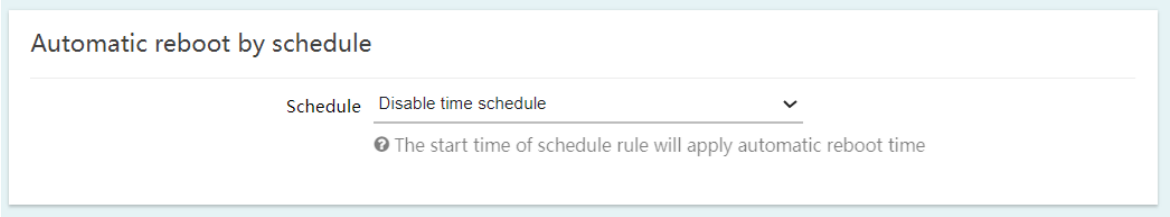
4. Wait for the device to reboot.

4.4.5 Scheduled automatic reboot

Administrator > Reboot > Setting

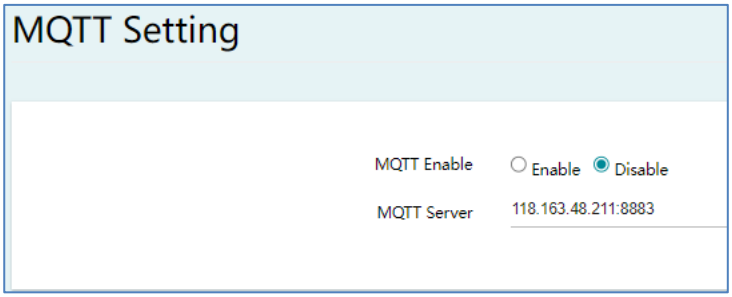
The scheduled automatic reboot feature allows you to set a daily or weekly schedule for the router to initiate an automatic reboot in an attempt to resolve any connectivity issues or intermittent problems that may occur with your device. Before using the scheduled automatic reboot feature, please ensure your Time settings are configured correctly and you have already created a time schedule for this function.

1. Log into your router management page.
2. Click on **Administrator,** click on **Reboot**, and click on **Setting** tab**.**
3. Click the Automatic reboot by schedule drop-down list and select the schedule used for the automatic device reboot function. Click **Apply** to save and commit the changes.



4.4.6 MQTT

Administrator > MQTT
The router provides the option to enable or disable an MQTT client to connect to a server for machine-to-machine communication.



4.4.7 Reset your router to factory details

Administrator > Backup / Flash Firmware

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting.

There are two methods that can be used to reset your router to factory defaults.

• **Reset Button** – Located on the front panel of your router. Use this method if you are encountering difficulties with accessing your router management page.

OR

• Router Administrator Page

1. Log into your router management page.
2. Click on **Administrator**, then click on **Backup / Flash Firmware.**
3. Next to Reset to defaults, click **Perform Reset**. When prompted to confirm this action, click **OK**.

4. Wait for the router settings to revert to factory default.

4.4.8 Ping Watchdog

Administrator > Ping Watchdog

The Ping Watchdog feature allows you configure your router to monitor connectivity to a specific host IP address. If connectivity is lost to the specified host IP address, the router will automatically initiate a device reboot in an automatic attempt to re-establish previously lost connectivity.

1. Log into your router management page.
2. Click on **Administrator** and click on **Ping Watchdog.**
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Local Access Management

• **Enable –** Check this option to enable the ping watchdog feature.

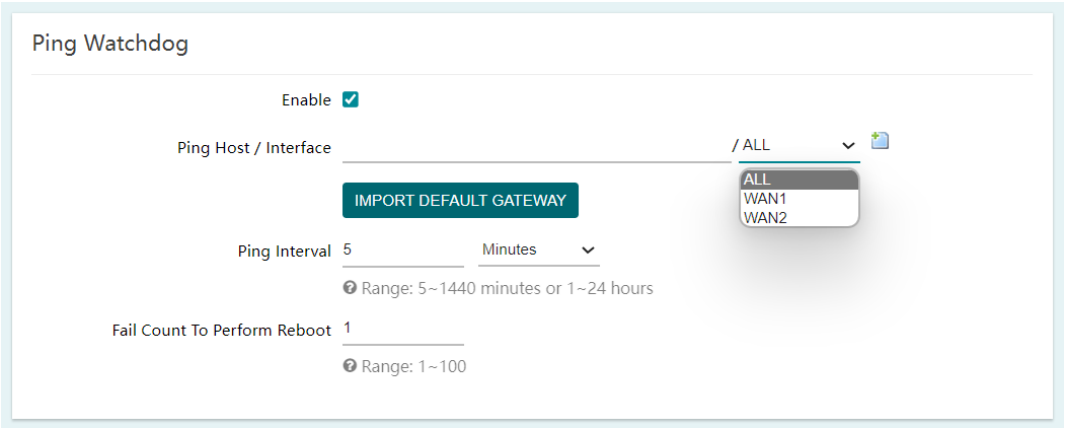
• **Ping Host / Interface –** Enter the IP address to monitor and send ping requests to check connectivity.

Note: You can add additional host IP address entries to monitor by clicking .

- **ALL –** Check all local and WAN interfaces for the specified host IP address.
- **WAN1 –** Check only the WAN1 interface for the specified host IP address.
- **WAN2 –** Check only the WAN2 interface specified host IP address.
- **Import Default Gateway –** Clicking this option will automatically attempt to copy both WAN interfaces default IP gateway to an available entry.

• **Ping Interval** – Enter interval time for the router to send ping and connectivity check. Example: Setting the interval to 5 Minutes will configure to send a ping and check connectivity every 5 minutes.

• **Fail Count to Perform Reboot –** Once ping/connectivity check fails, this sets the maximum number of attempts the router will attempt to check connectivity before initiating an automatic reboot.



4.4.9 Check the router status information

Status > Overview

You may want to check the system information of your router firmware, S/N, uptime, available memory, active connection, WAN interface information, wireless interface information, DHCP clients, connected wireless clients, dynamic DNS and active UPnP entries.

1. Log into your router management page.

2. Click on **Status** and click on **Overview.**

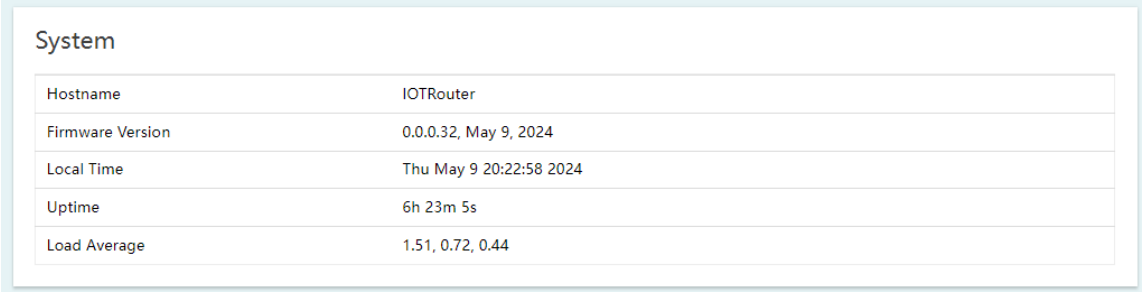
• System

o **Hostname –** Displays the currently assigned hostname of the router. This is the name other network devices identify the router by on the network.

o **Firmware Version –** Displays the currently loaded firmware version and date.

o **Local Time –** Displays the current device time and date.

o **Uptime –** Displays the total amount of time the router has been up and running without reboot.



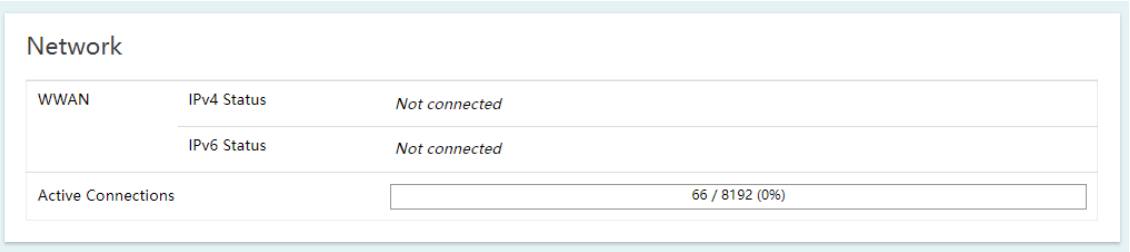
• Memory

Displays the available, free and buffered memory status.

• Network

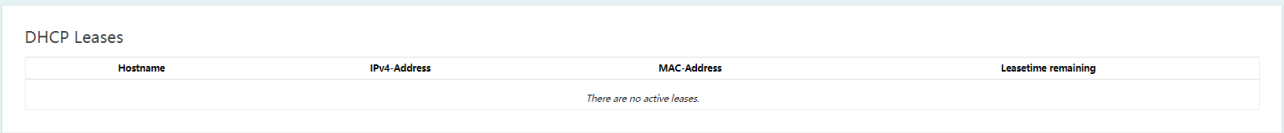
o **WWAN IPv4 Status** – Displays the current IPv4 status

o **WWAN IPv6 Status –** Displays the current IPv6 status



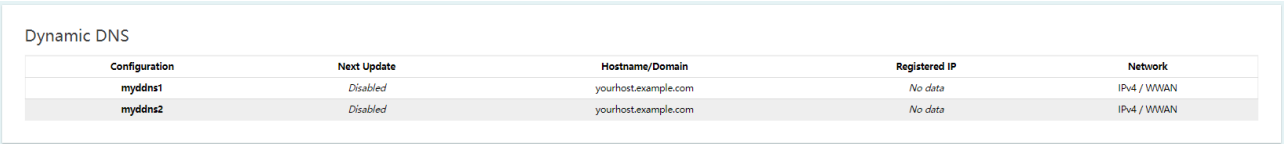
• DHCP Leases

This displays the current valid DHCP leases along with their remaining time.



• Dynamic DNS

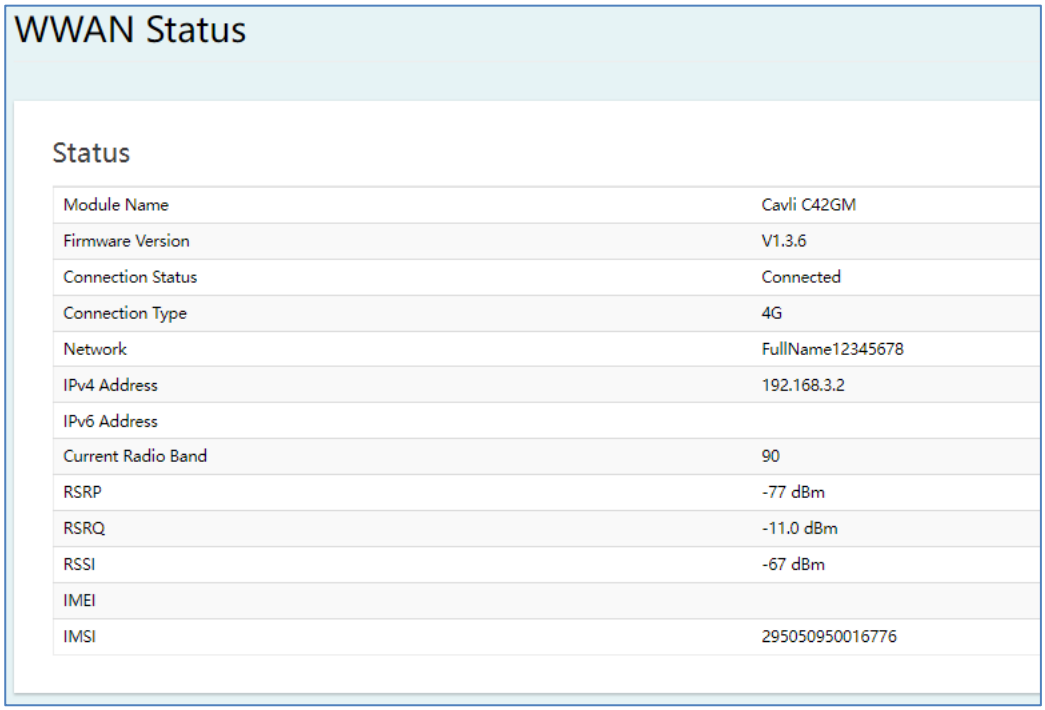
This displays the configured dynamic DNS and the registered IP information.



4.4.10 WWAN Status

Status > WWAN

This section displays the WWAN module and firmware information as well as its network and connection status. If the status is connected, it displays the connection KPIs RSSI, RSRP and RSRQ.



4.4.11 Real Time Graphs

Status > Realtime Graphs

This section displays the device real-time CPU load, traffic load, and connection/session information.

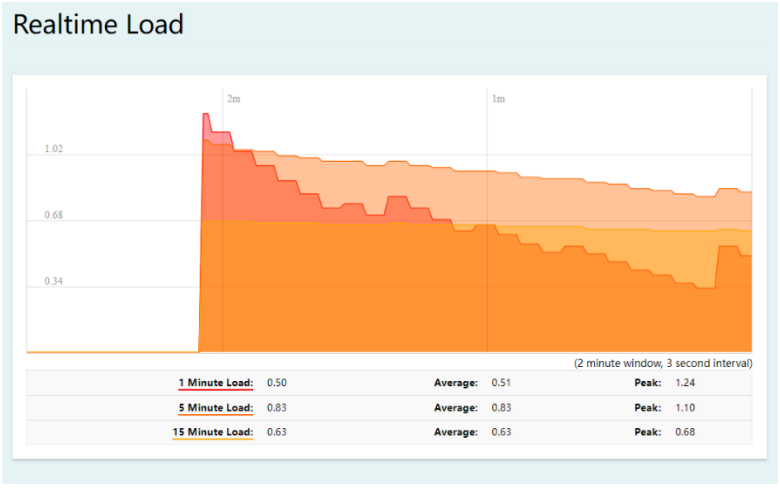
CPU Load

This chart shows the load of the CPU in 1 minute, 5 minutes, and 15 minutes intervals.

• Red graph: Displays the CPU load in the last 1 minute

• Orange graph: Displays the CPU load in the last 5 minutes

• Yellow graph: Displays the CPU load in the last 15 minutes

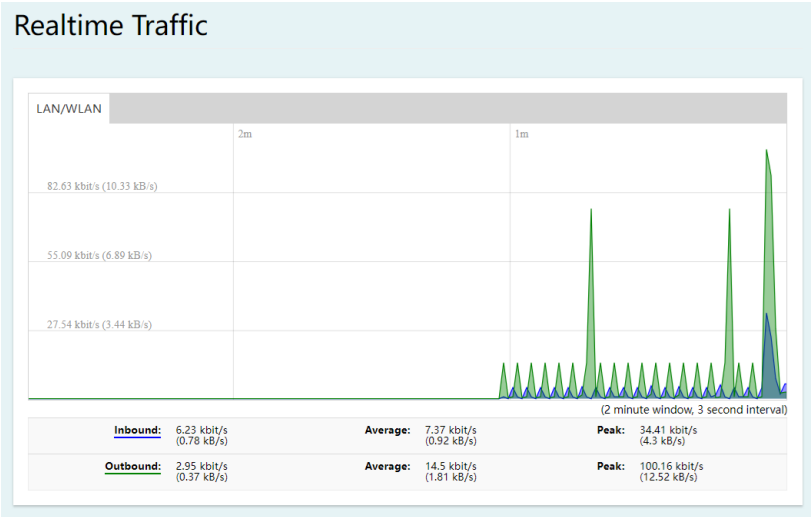


Traffic Load

This chart shows the real-time traffic load

• Blue graph: Displays the inbound traffic

• Green graph: Displays the outbound traffic



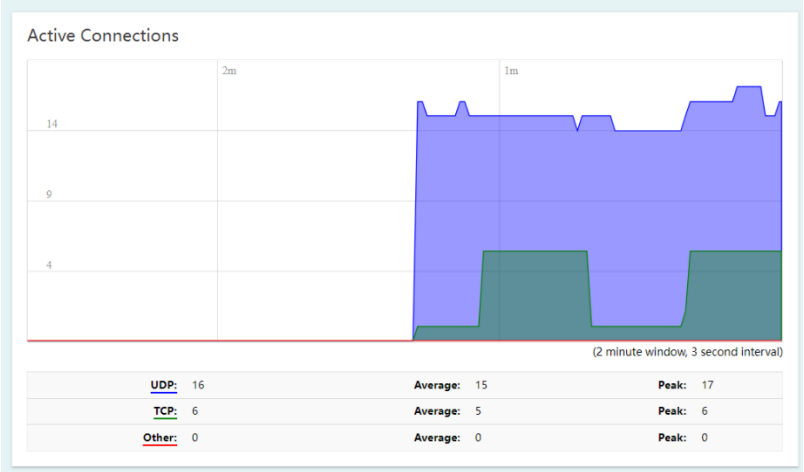
Connections

This chart shows the connection and session information

• Blue graph: Displays the connections with UDP protocol

• Green graph: Displays the connections with TCP protocol

• Red graph: Displays the connections that do not use UDP or TCP protocol



4.4.12 View routing table and ARP entries

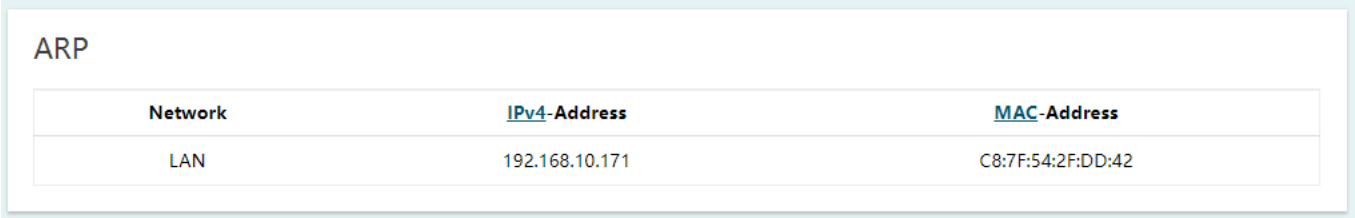
Status > Routes

You may want to check the current routing table and ARP entry information for troubleshooting or monitoring purposes.

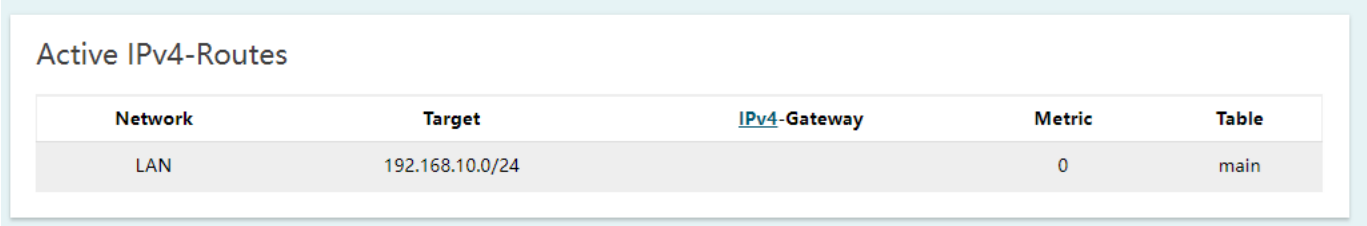
1. Log into your router management page.

2. Click on **Status** and click on **Routes.**

• **ARP –** Displays the router ARP table.



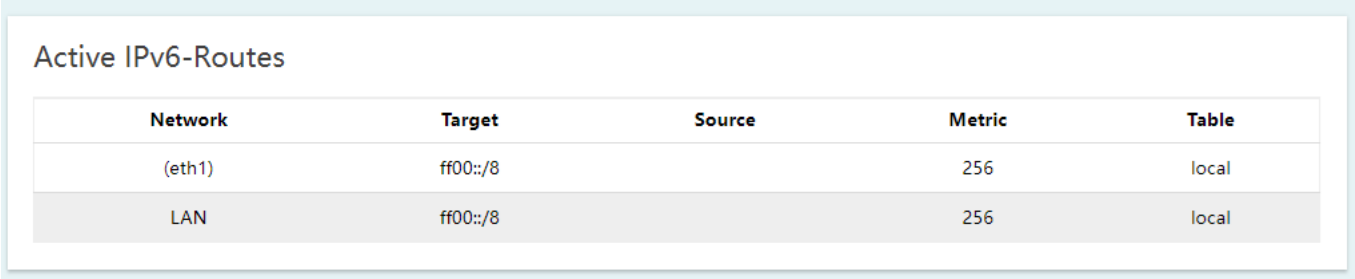
• **Active IPv4-Routes –** Displays the current IPv4 active routing table.



Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
LAN	192.168.10.0/24		0	main

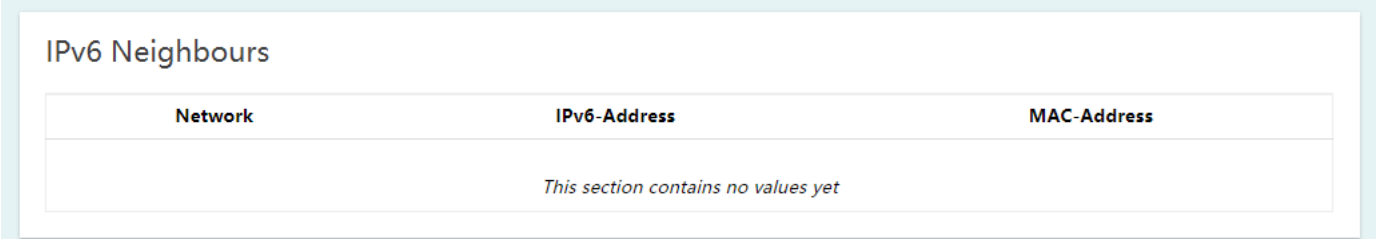
• **Active IPv6-Routes –** Displays the current IPv6 active routing table.



Active IPv6-Routes

Network	Target	Source	Metric	Table
(eth1)	ff00::/8		256	local
LAN	ff00::/8		256	local

• **IPv6 Neighbors –** Displays currently discovered/detected IPv6 neighbor devices.



IPv6 Neighbours

Network	IPv6-Address	MAC-Address
This section contains no values yet		

4.4.13 View your router logging

Status > System Log

Your router system log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page.

2. Click on **Status** and click on **System Log.**

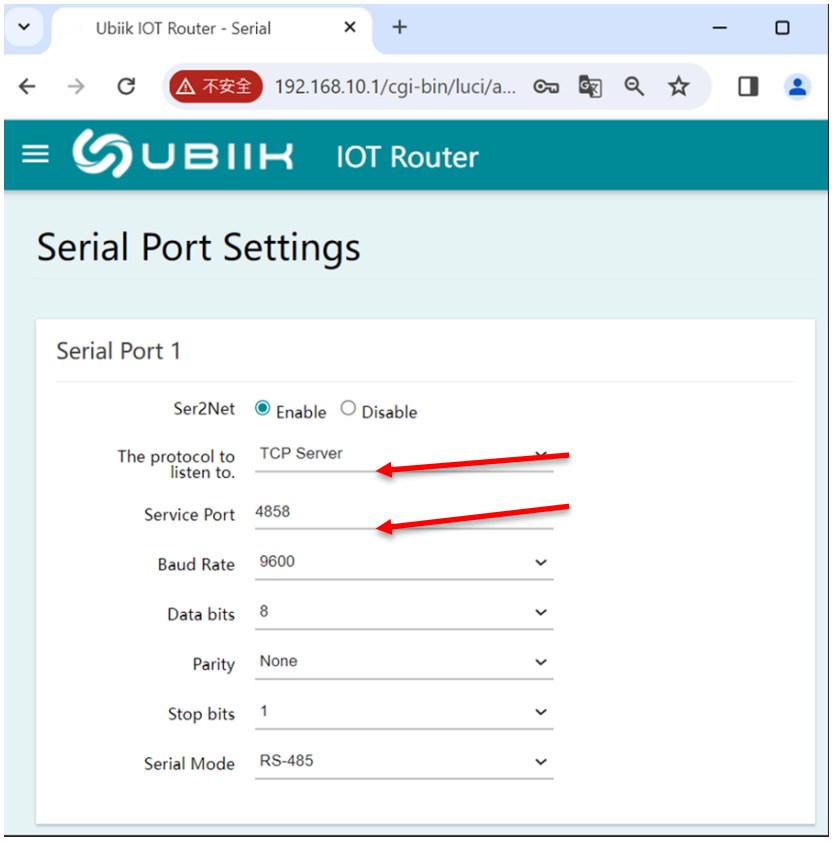
Note: The router system log will display the most recent entries in the list.

Time	Level	Source	Message
Type to filter	Type to filte	Type to filte	Type to filter
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-p PROXY => proxy=[USER:PASS@]PROXY:PORT
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-s SCRIPT => ip_script=SCRIPT; ip_source="script"
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-t => force_dnstcp=1 (default 0)
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-u URL => ip_url=URL; ip_source="web"
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-S SECTION SECTION to start
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-h => show this help and exit
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-L => use_logfile=1 (default 0)
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-v LEVEL => VERBOSE=LEVEL (default 0)
Thu May 9 20:27:09 2024	daemon.err	uhttpd[2527]	-V => show version and exit
Thu May 9 20:27:10 2024	daemon.err	uhttpd[2527]	dynamic_dns_lucihelper.sh: command 'get_registered_ip': 'lookup_host' not set
Thu May 9 20:27:10 2024	daemon.err	uhttpd[2527]	Usage:
Thu May 9 20:27:1	daemon.err	uhttpd[252	dynamic_dns_lucihelper.sh [options] -- command

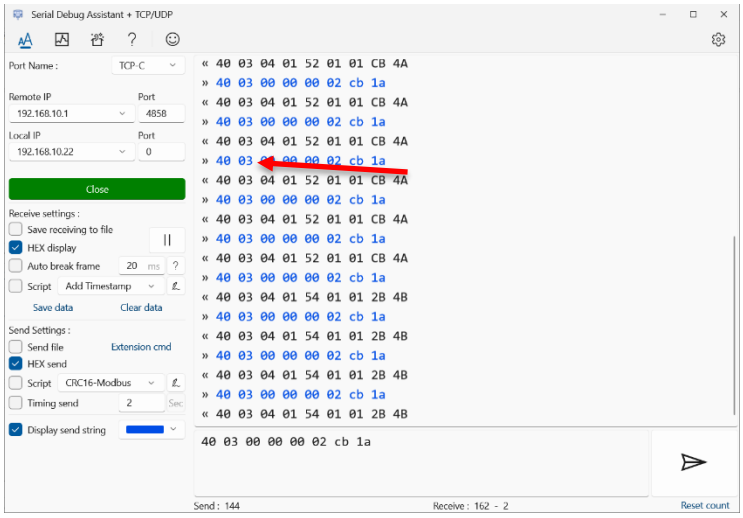
Serial Ports

In the webGUI, under the Network menu, enter to “serial” setting page to configure the Serial Port Settings.

- Enable the Serial port and choose the protocol to TCP Server and specify the Service port.
- Apply to save setting.

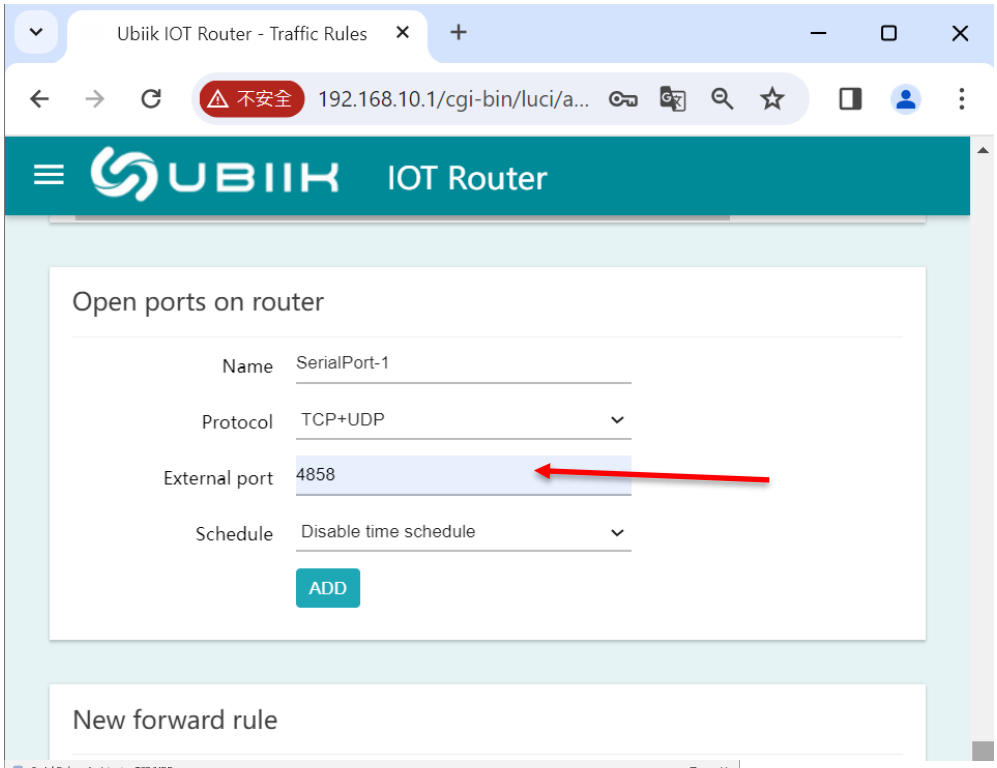

Ubiik IOT Router - Serial
不安全
192.168.10.1/cgi-bin/luci/a...
UBIIK
IOT Router
Serial Port Settings
Serial Port 1
Ser2Net
Enable
Disable
The protocol to listen to.
TCP Server
Service Port
4858
Baud Rate
9600
Data bits
8
Parity
None
Stop bits
1
Serial Mode
RS-485

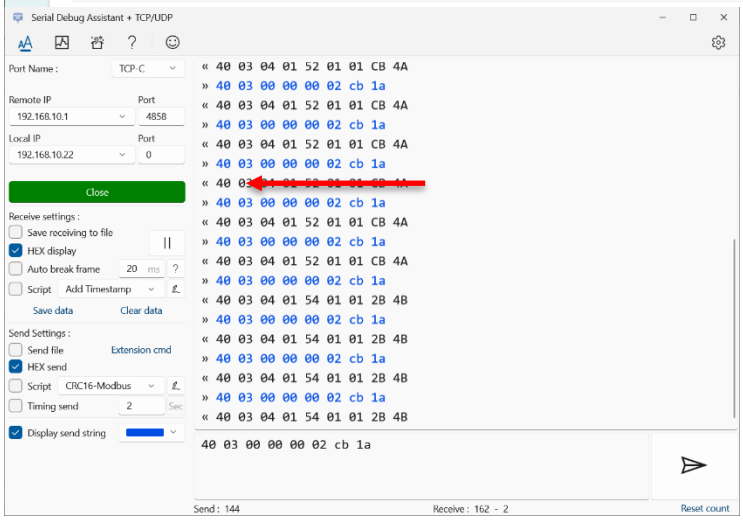
Use the Serial port access tool that supported TCP client mode, input the IP and port, the IP is device IP, the port is service port you configured in router.



If you want to remote connect from router's WAN IP, you need to configure the traffic rule on router. Under Firewall-Traffic Rules-Open the port on router page.

- Add the External port and apply the setting.

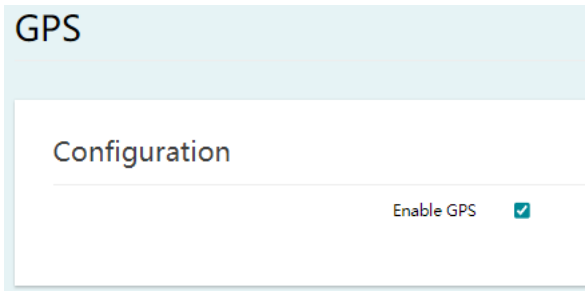


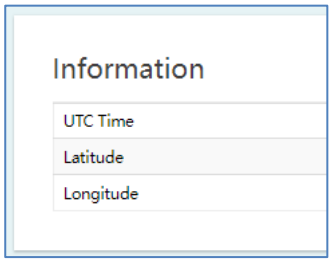


4.4.14 GPS

Status > GPS

GPS can be enabled on the router. Once synchronized, the GPS coordinates and time information is displayed.



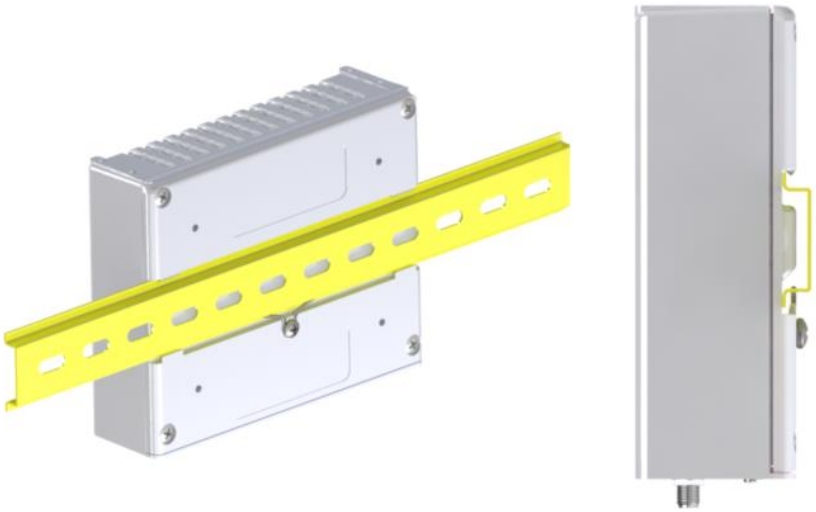

Information
UTC Time
Latitude
Longitude

5. INSTALLATION

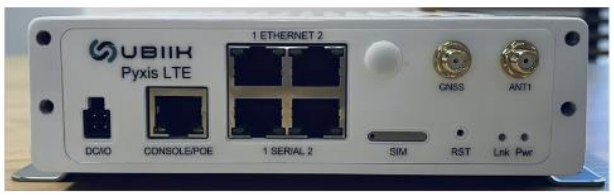
5.1 MOUNTING SOLUTIONS

Pyxis LTE radios can be mounted in several different ways to meet the customers application. These include:

DIN Rail Mounting



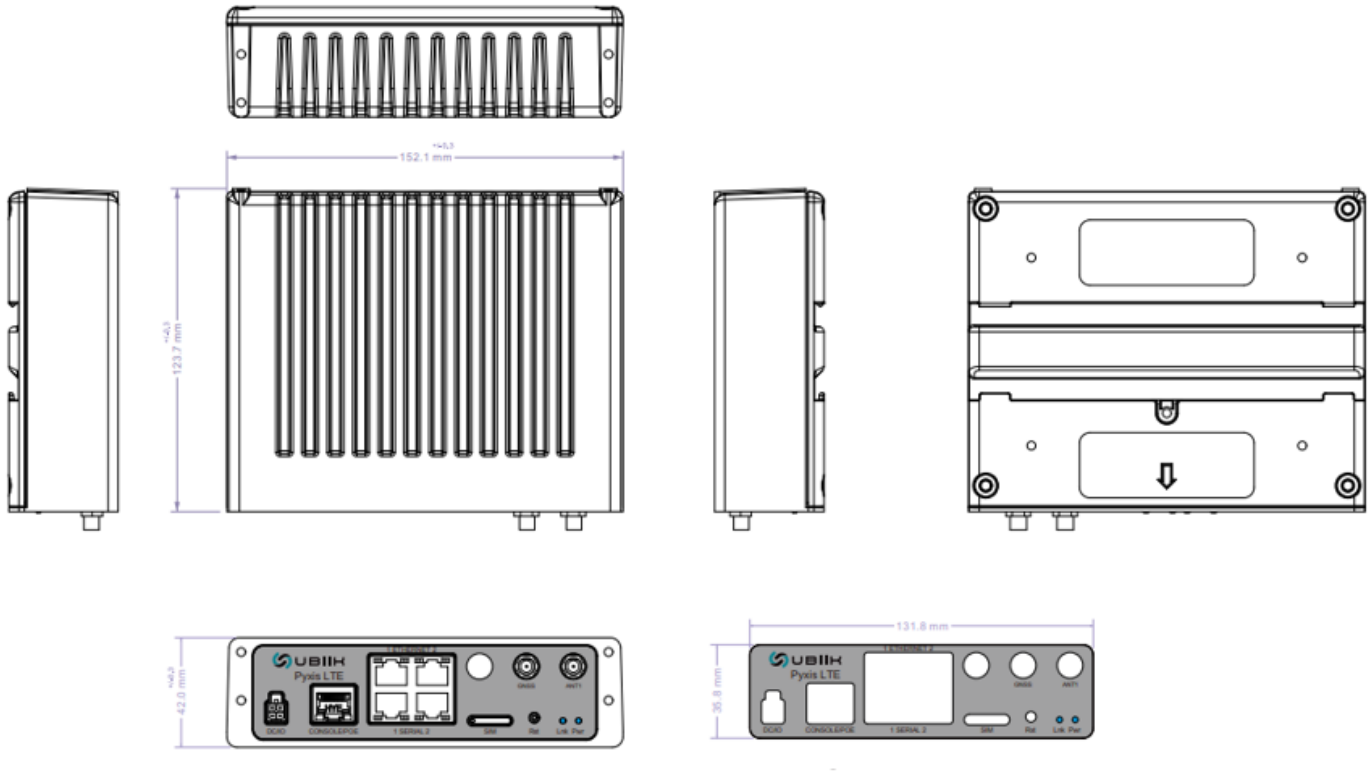
Wall / Surface Mounting



6 SPECIFICATIONS

Region	US
TECHNOLOGY	
Standards	LTE-M
Platform	Dual-core ARM 64bit A53@1.0GHz Processor 8GB eMMC + 512MB DRAM LTE miniPCIe: Sierra HL7810
Frequency Bands	ISM-FDD: DL 925-928MHz; UL: 902-915MHz B106：DL 936.5-939.5MHz; UL: 897.5-900.5MHz
Modulation	QPSK, 16QAM
Data Rate	>300 kbps
Transmit Power	+23dBm
INTERFACE	
Power Supply	PoE IEEE 802.3 AF 9-15V (nominal 12V)
I/O Interfaces	2x Ethernet 10/100/1000M Base-T (RJ45 connectors) 2x RS232/485 (RJ45 connectors) 1x Console Port or 802.3 af PoE (RJ45) GPIO (2 pins) DC-In (2 pins) 1x Nano SIM 1x Reset Button
LED Indicators	1x LED for System Power 1X LED for Network Connection
Antenna Connections	1x SMA Connector: LTE-M 1x GNSS (optional)
PHYSICAL	
Dimensions	4.87 x 5.98 x 1.65 inches (123.7 x 152.1 x 42mm)
Weight	670 grams
Power Consumption	Maximum: 5.14w Standby: 3.48 w
Operating Temperature	-4°F to +149°F
Storage Temperature	-40°F to +185°F
Humidity	5% to 90% non-condensing
Certification	FCC/ISED

6.1 MECHANICAL DIMENSIONS



Unit Total Width: 152.1mm / 5.98 inches

Unit Depth:123.7mm / 4.87 inches

Unit Height: 42.0mm / 1.65 inches

7 DOCUMENT HISTORY

Issue No.	Date	Description
1	7/19/2024	Document created
2	9/11/2024	Initial release
3	9/12/2024	- Modify chapter 1 content description. - Modify chapter 2.1.1 content description. - Modify chapter 2.1.2 & 2.2 & 2.3, correct the required distance between the human body and the antenna. - Modify chapter 3.5, add antenna list.