Complies with
IMDA Standards
DA108743

TeaM1-5GM Modem/Router

TM1-5GM2020SG

USER GUIDE

Updated 07 July 2021

Purchase list of TeaM1-5GM modem/router & accessories

1. Harsh Environment Package 1 (TeaM1-5GM-H1)

SN	Description	Quantity	Part No.	Photo	Remarks
1.1	TeaM1-5GM Modem/Router Unit	1	TM1-5GM2020SG		
1.2	Power cable	1	5GM-H1-B		Length 1m with open ended
1.3	IO cable (Serial ports, DIOs)	1	5GM-H2-B		Length 1m with open ended
1.4	Integrated 3G, 4G, 5G and GNSS antenna (IP69K)	1	5GM-ANT-M670-BB-6CG		Cable length 4.5m

2. Harsh Environment Package 2 (TeaM1-5GM-H2)

SN	Description	Quantity	Part No.	Photo	Remarks
2.1	TeaM1-5GM Modem/Router Unit	1	TM1-5GM2020SG		
2.2	Power cable	1	5GM-H1-B		Length 1m with open ended
2.3	IO cable (Serial ports, DIOs)	1	5GM-H2-B		Length 1m with open ended
2.4	Low-Profile integrated 3G, 4G, 5G and GNSS antenna (IP69K)	1	5GM-ANT-M970-BB-6CG		Cable length 4.5m

3. Basic Package (TeaM1-5GM-B)

SN	Description	Quantity	Part No.	Photo	Remarks
3.1	TeaM1-5GM Modem/Router Unit	1	TM1-5GM2020SG		
3.2	Power cable	1	5GM-H1-B		Length 1m with open ended
3.3	IO cable (Serial ports, DIOs)	1	5GM-H2-B		Length 1m with open ended
3.4	Integrated 3G, 4G, 5G antenna (IP67)	1	5GM-ANT-YB0007AA		Cable length 0.5m
3.5	4G and 5G antenna (IP67)	2	5GM-ANT-GSA.8835		Cable length 1m

4. Optional & Customized Accessories

SN	Description	Part No.	Remark	
4.1	Power cable	5GM-H1-C-XX	XX: customization code issued. Customized length and/or termination available	
4.2	IO cable	5GM-H2-C-XX	XX: Customization code issued. Customized length and/or termination available	
4.3	IP67 Cat.5e/6 Ethernet cable	5GM-H3-C-XX		Options: Cable length with IP67 shielded cable and mounting.
4.4	IP67, USB2.0HS cable	5GM-H4-XX		Options: Cable length with IP67 shielded cable and mounting.
4.5	IP67 GNSS active antenna	5GM-ANT - GNSS - YLY001CA		Cable length 1m and SMA terminal
Please contact supplier for customization of functions and accessories				

Table of Contents

1 Overview

TeaM1-5GM is an industrial standard 5G modem to support 3G, 4G, 5GNR and GNSS. The robust mechanical enclosure design of modem/router makes it suitable to operate in harsh environment. Powered by 9~48V DC power supply, the device is suitable for vehicle, train, maritime, railway and outdoor applications.

1.1 Cellular Network Connection

TeaM1-5GM is able to provide connection between local devices and the internet through mobile 3G/4G/5GNR (Sub-6GHz) network supported by mobile ISP. The device is able to connect to a 5GNR Sub- 6GHz network by default in either SA or NSA mode. In the case of the field that does not have 5G coverage from specific ISP or cellular network signal quality is not good enough to support essential data connection, the device will automatically fallback to 3G/4G connection. 5G network shall have the priority to be used when the device is within the area of co-existing 3G/4G/5G network coverage.

1.2 Protocols and Data Security

Connection with 2x pre-configured destination IP address could be established upon powered on. Device authentication and data encryption using appropriate Transport Layer Security (TLS/SSL) cryptographic protocol shall be implied between device/remote site operating over the cellular network.

1.3 Characteristic and Features

Frequency Band

5GNR bands:

- n41/ n77/ n78/ n79

4G-LTE bands:

- LTE: B1/ 3/ 5/ 7/ 8/ 18/ 19/ 20/ 28/ 32/ 34/ 38/ 39/ 40/ 41/ 42/ 43

Characteristic and Key Features

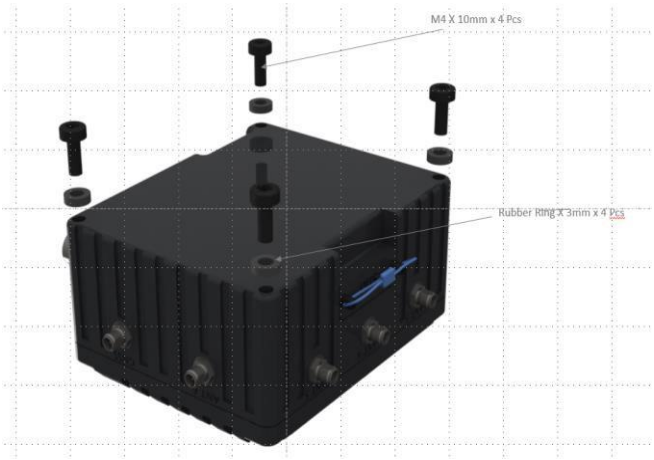
- CPU AM5715
- OpenWrt Operating system Firewall
- GNSS
- Data Logger 4 x MIMO
- Delay 2 - 5ms
- TCP/UDP/FTP/HTTP
- UL: 200 Mbps
- DL: 1.0 Gbps

Interface

- 1x Ethernet
- 1x USB 2.0 HS
- 2x RS232
- 1x RS485
- 1x RS422
- 4x Discrete Input 4x Discrete output
- 1x USB2.0 Engineering port

2 Installation Guide and Connection

2.1 Dimensions / Size / Mounting Holes



Size: 120mm x 97mm x 59mm

Weight: 600g

Vibration: 10g-PK random

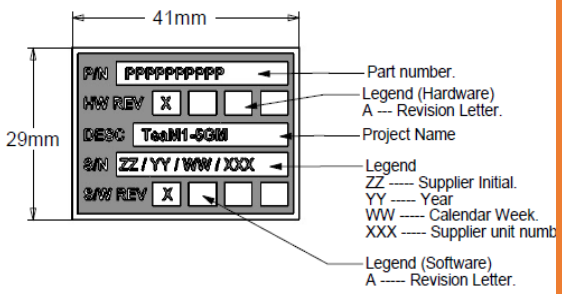
Shock: 20g impulse

Waterproof: IP67

Surface: AL6061, Black anodizing

Mounting: 4 x M4 x 10mm screw mounting

Product Serial Tag:



2.2 Panels / External Connectors

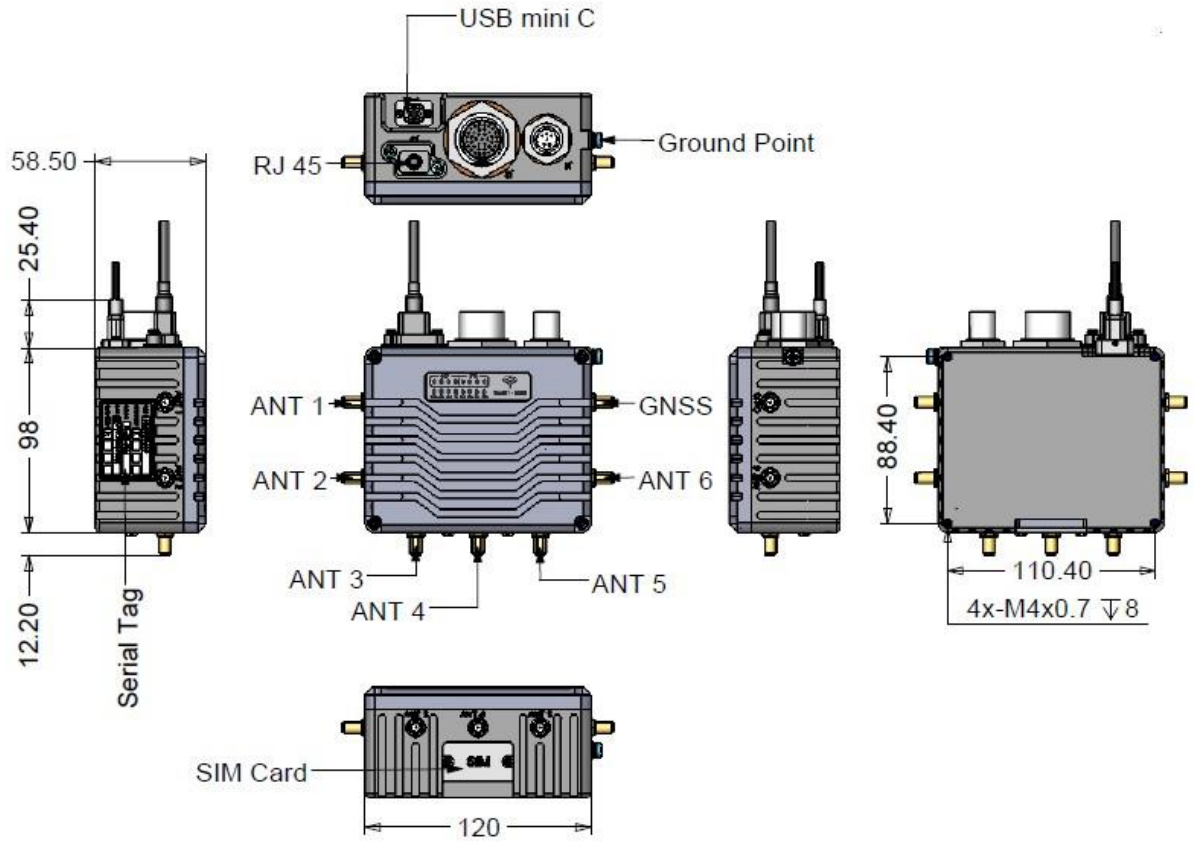
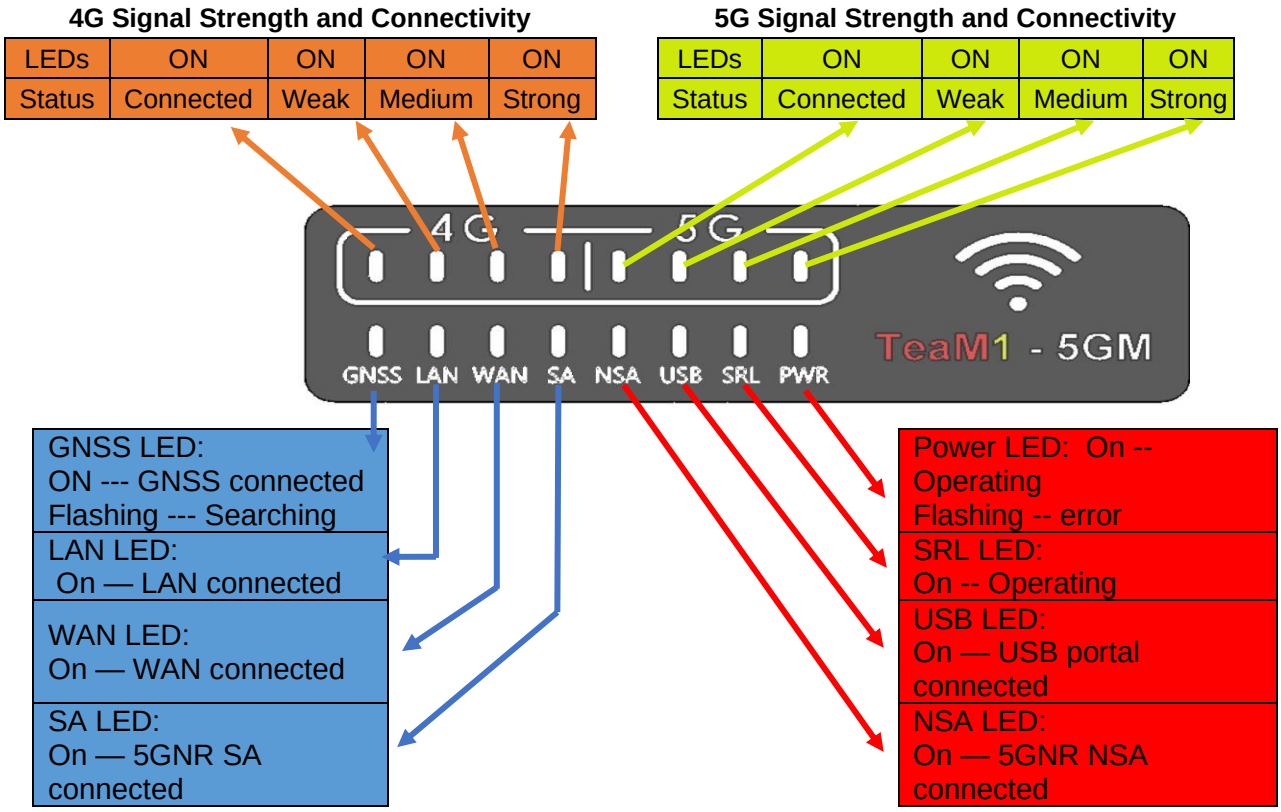


Table 1: Panel Connectors

SN	**Description**	**Remarks**
ANT3	5G Antenna 1, SMA 50 Ω	4x4 MIMO, N77/78/79 5GNR
ANT4	5G Antenna 2, SMA 50 Ω	
ANT5	5G Antenna 3, SMA 50 Ω	
ANT6	5G Antenna 4, SMA 50 Ω	
ANT1	4G/3G Antenna 1, SMA 50 Ω	
ANT2	4G/3G Antenna 2, SMA 50 Ω	
GNSS	GNSS antenna	Passive/active antenna
J1	Power input, engineering port, D38999/24WA6PN	Optional accessory: external cable H1
J2	2xRS232, 1xRS422, 1x RS485, 4x DI, 4x DO ports, D38999/24WD35SN	Optional accessory: external cable H2
J3	1x Gigabit Ethernet LAN. RJ45 (ruggedized), MRJR-8F81-01	Optional accessory: external cable H3
J4	Portal connector USB2.0 HS. Mini-USB-AB, MUSBR-E151-30	Optional VLAN connection.
GP	4x M4 x 10mm screw, Ground point.	Connect to earth
SIM	SIM card cover, 2x M3 x 10mm screw, with rubber gasket.	For IP67 sealing. Nano-SIM.

2.3 Panel LEDs



2.4 Antenna Frequency Bands Information

Frequency Bands[1]	
5G NR NSA	n1/n3/n5/n7/n8/n20/n28/n38/n40/n41/n77/n78/n79
5G NR SA	n1/n3/n5/n7/n8/n20/n28/n38/n40/n41/n77/n78/n79
LTE-FDD	B1/B3/B5/B7/B8/B18/B19/B20/B26/B28/B32
LTE-TDD	B34/B38/39/B40/B41/B42/B43
LAA	-
WCDMA	B1/B3/B5/B6/B8/B19
MIMO	DL: 4 × 4 UL[2]: 2 × 2
GNSS	GPS/GLONASS/BeiDou/Galileo/QZSS (optional)

Above table shows the operating band in the TeaM1-5GM. Any 50 Ohm RF antenna working in the bands shall be applicable for the device. The TeaM1-5GM uses SMA socket on its panel, and the respective antennas shall be terminated with SMA plug accordingly. The maximum transmission RF power from the device is illustrated as in table below.

Output Power	Class 3 (24 dBm +1/-3 dB) for WCDMA bands Class 3 (23 dBm ±2 dB) for LTE bands Class 3 (23 dBm ±2 dB) for 5G NR bands Class 2 (26 dBm ±2 dB) for LTE B38/B40/B41/B42 bands HPUE[4] Class 2 (26 dBm +2/-3 dB) for 5G NR n41/n77/n78/n79 bands HPUE[4]	Class 3 (24 dBm +1/-3 dB) for WCDMA bands Class 3 (23 dBm ±2 dB) for LTE bands Class 3 (23 dBm ±2 dB) for 5G NR bands Class 2 (26 dBm ±2 dB) for B41/B48 bands HPUE[4] Class 2 (26 dBm +2/-3 dB) for 5G NR n41/n77/n78 bands HPUE[4]

The antennas selected shall be complaint with above power rating requirements. For CA bands, see document Quectel_RG50xQ_Series_CA&EN-DC_Features. Optional antennas refer to Appendix.

2.5 External Cables and Connector Pin Assignment

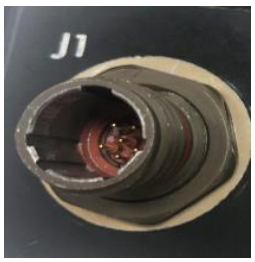
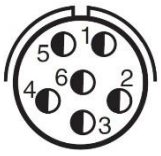
External panel connectors used on TeaM1-5GM are listed as in below table:

Table 2: Panel Connectors and External Cable

Panel Connector	Description and part number	External cable and terminal connector PN.
J1	Power input, engineering port, D38999/24WA6PN	Optional accessory: external cable H1 Connector: D38999/26WA6SN
J2	2xRS232, 1xRS422, 1x RS485, 4x DI, 4x DO ports, D38999/24WD35SN	Optional accessory: external cable H2 Connector: D38999/26WD35PN
J3	1x Gigabit Ethernet LAN. RJ45 (ruggedized), MRJR-8F81-01	Optional accessory: external cable H3 RJ45 plug (optional accessories if necessary)
J4	Portal connector USB2.0 HS. Mini-USB-AB, MUSBR-E151-30	Optional VLAN connection. (Offline or Online) Connector Mini-USB-AB plug.

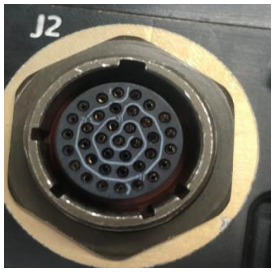
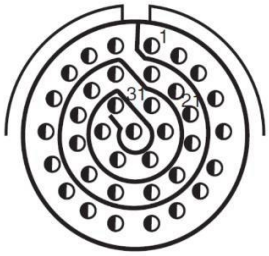
2.5.1 Panel Connector J1 and External Cable H1

Table 3: Panel Connectors J1 and External Cable H1

Panel Connector		**Signal Description**	**Cable connector**	**Cable labelling**
J1: D38999/24WA35PN			**D38999/26WA35SN**	
Pin No.	**Description**		**Pin No.**	
Pin 1	9~48V power in >16W peak.	9~48V power in Vin+	Pin 1	1 (RED)
Pin 2		Power Ground Vin-	Pin 2	2 (Black)
Pin 3	Engineering USB2.0 port (Optional device)	USB _DGND	Pin 3	3 (Optional)
Pin 4		USB_D-	Pin 4	4 (Optional)
Pin 5		USB_D+	Pin 5	5 (Optional)
Pin 6		USB_VBUS	Pin 6	6 (Optional)
				

2.5.2 Panel Connector J2 and External Cable H2

Table 4: Panel Connectors J2 and External Cable H2

Panel Connector J2: D38999/24WD35SN Pin No.		Signal Description	Cable connector D38999/26WD35PN Pin No.	Cable labelling
Pin 1	RS422 connection from TeaM1- 5GM	RS422A (RX+)	Pin 1	1
Pin 2		RS422B (RX-)	Pin 2	2
Pin 4		RS422Z (TX-)	Pin 4	4
Pin 5		RS422Y (TX+)	Pin 5	5
Pin 18	RS485 connection	RS485A (D+)	Pin 18	18
Pin 19		RS485B (D-)	Pin 19	19
Pin 20	RS232-1 connection from TeaM1- 5GM	DGND	Pin 20	20
Pin 21		RS232-1-TXD	Pin 21	21
Pin 22		RS232-1-RXD	Pin 22	22
Pin 23	RS232-2 connection from TeaM1- 5GM	DGND	Pin 23	23
Pin 24		RS232-2-TXD	Pin 24	24
Pin 25		RS232-2-RXD	Pin 25	25
Pin 26		DGND	Pin 26	26
Pin 27		DGND	Pin 27	27
Pin 28	Discrete input. VIH > 6V VIL < 4V 9~48V.	Input 0	Pin 28	28
Pin 29		Input 1	Pin 29	29
Pin 32		Input 2	Pin 32	32
Pin 33		Input 3	Pin 33	33
Pin 30		DGND	Pin 30	30
Pin 31		DGND	Pin 31	31
Pin 34		DGND	Pin 34	34
Pin 7	OD output from TeaM1 5GM. Max. Current: 0.5A @ 48V	Vout_L1	Pin 7	7
Pin 9		Vout_L2	Pin 9	9
Pin 11		Vout_L3	Pin 11	11
Pin 13		Vout_L4	Pin 13	13
Pin 6		+5VDC @0.1A output	Pin 6	6
Pin 8		+12VDC @0.2A output	Pin 8	8
Pin 10		+3.3VDC @0.1A output	Pin 10	10
Pin 12		9~48V@0.5A output (Power supply input)	Pin 12	12
Pin 14*	Optional. LVCMOS3.3V output. *Do not connect. ** Contact supplier if required	WARN_EXT2, warning signal	Pin 14	14
Pin 15*		Data_safety_Ext, data safety warning signal	Pin 15	15
Pin 16*		HB_EXT, heart-beating signal, device health condition	Pin 16	16
Pin 17*		Warn_EXT1, warning signal	Pin 17	17
				

*** Please contact supplier if customized cable is required, with specific termination and length.

2.5.3 Panel Connector J3 and External Cable H3

Table 5: Panel Connectors J3 and External Cable H3

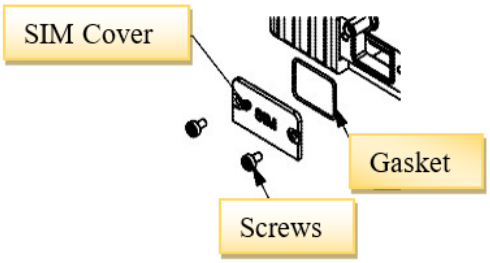
Panel Connector		**Signal Description**	**Cable connector**	**Cable labelling**
J3: MRJR-8F81-01			**RJ45 plug**	
Pin No.			**Pin No.**	
Pin 1	Gigabit Ethernet connection. Cat.5e or Cat.6 cable.	BI_DA+	Pin 1	Whit/green
Pin 2		BI_DA-	Pin 2	Green
Pin 3		BI_DB+	Pin 3	White/Orange
Pin 4		BI_DC+	Pin 4	Blue
Pin 5		BI_DC-	Pin 5	White/Blue
Pin 6		BI_DB-	Pin 6	Orange
Pin 7		BI_DD+	Pin 7	White/Brown
Pin 8		BI_DD-	Pin 8	Brown
		*RJ45 water-proof accessory available upon request.		

2.5.4 Panel Connector J4 and External Cable H4

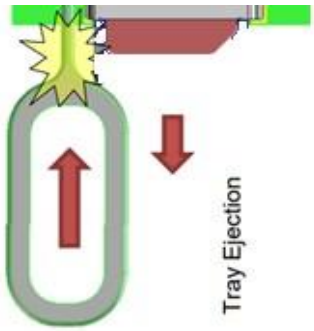
Table 6: Panel Connectors J4 and External Cable H4

Panel Connector		**Signal Description**	**Cable connector**	**Cable labelling**
J3: MUSBR-E151-30			**Mini-USB-AB plug**	
Pin No.			**Pin No.**	
Pin 1	USB cable	USB_VBUS	Pin 1	
Pin 2		USB_D-	Pin 2	
Pin 3		USB_D+	Pin 3	
Pin 4		USB_DGND	Pin 4	
		*Mini-USB waterproof accessory available upon request.		

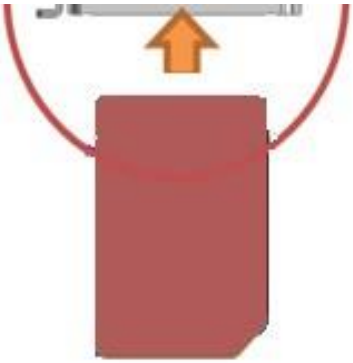
2.6 SIM Card Plug / Removal



1.Untighten the two screws on SIM card cover



2. Using needle to eject the SIM card out from the Connector.

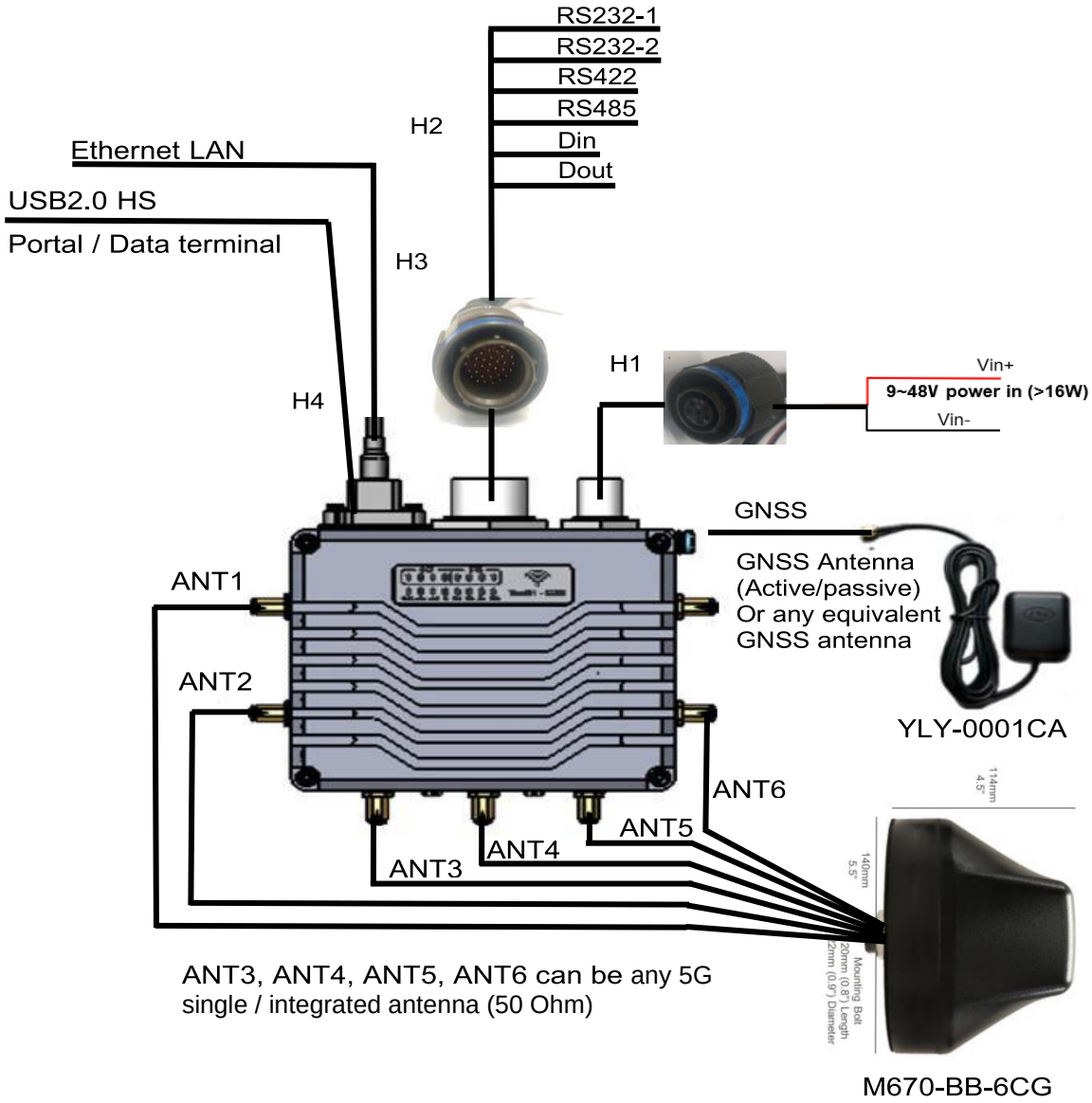


3. Insert the Nano-SIM card into the SIM card connector

Notes: SIM card cover shall be put back with sealing gasket

3 System Power Up & Setup

3.1 Connection Diagram



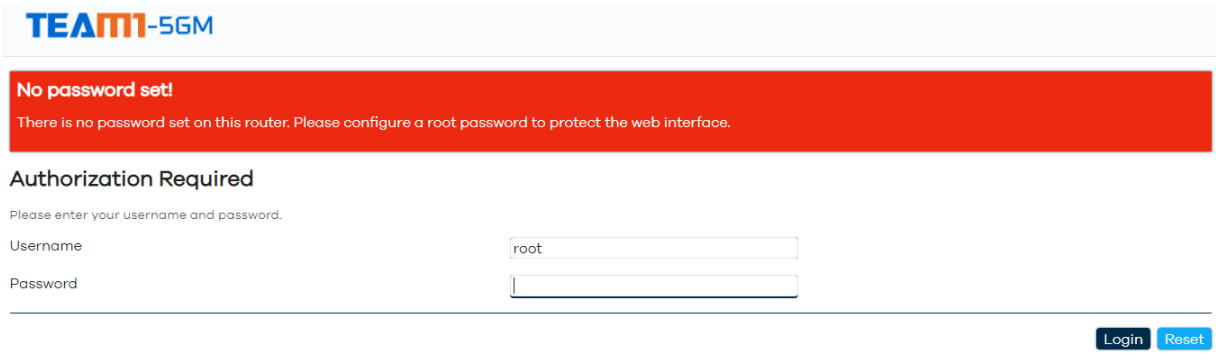
3.2 Power Up

After connecting H1 to the power supply, it normally takes 20-25s for the system to boot up. When the 'PWR' LED lights up, it means system is booted.

4 General Web Portal Settings

4.1 Log Into Your Router Running OpenWrt

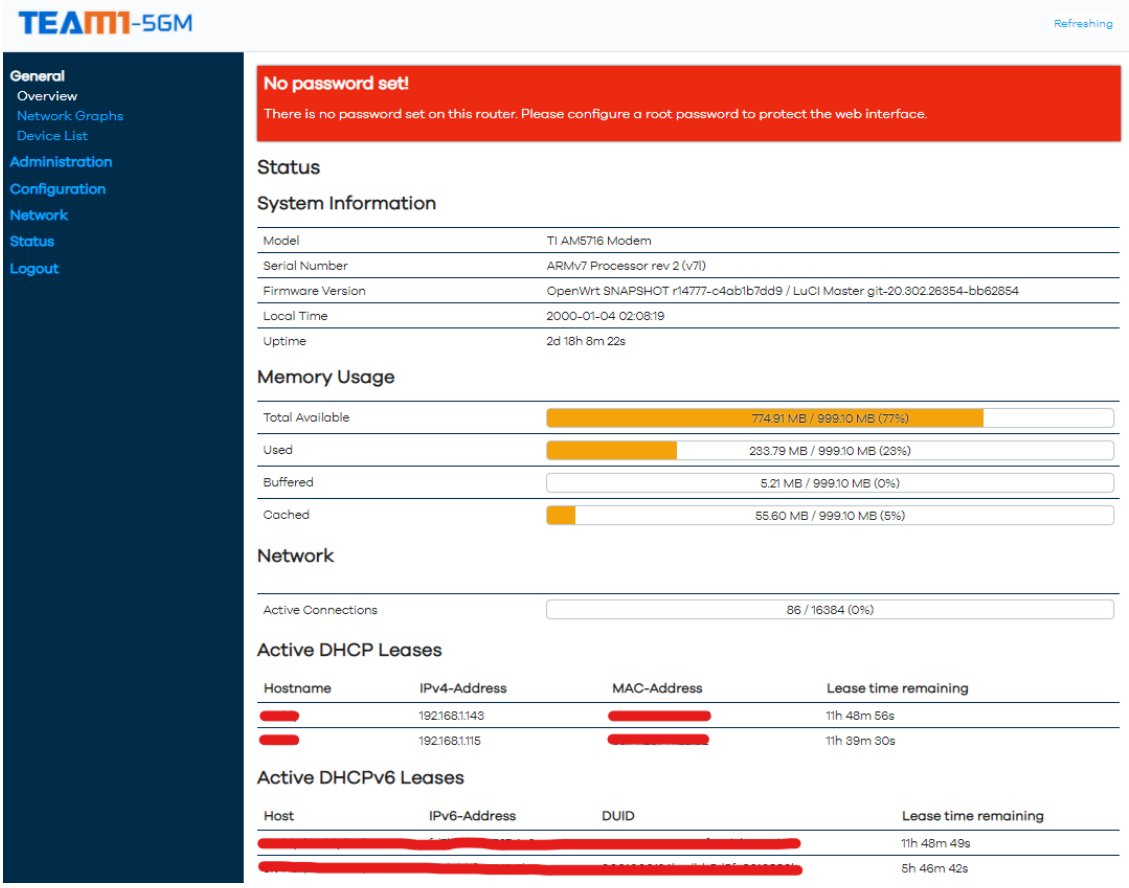
We've installed OpenWrt but now is time to get our router configured. Visit your router's administration page. No matter what the address was before, OpenWrt simplifies this by setting the administration address to be http://192.168.1.1/. At that page you should see a login page: (correct as of Barrier Breaker)



As you'll see, there's a notification that “root” user's password is not set. root is the username of the main administrative user on OpenWrt. We'll need to set that after we login. Log in with the username of **root** and leave the password field empty. Note: If you have installed a “tiny” build or a “snapshot” build, LuCI web interface will likely not be present and you will need to use ssh to login as root@192.168.1.1 (telnet is no longer supported by OpenWrt-project builds) Note: If the configuration of your router prior to flashing was somewhat exotic (e.g., router previously at 192.168.17.1), your PC (or whatever) might struggle to reconnect. If in doubt, consider simply rebooting the PC, or any other way to reset the connection.

4.2 Status Page

Once you have logged in, you will see the ‘General’ – ‘Overview’ page. From here you can get the detail information from the high-level view of your router’s status.



In the figure, you can see some basic system information like the version of OpenWrt and the web interface packages of OpenWrt, which is named LuCI. Additionally, you can see the uptime for the router since last reboot, the current clock time on the router and how much of the router's processor is used (“load”). Let's scroll down a little, you can see the router's memory usage. As services are started on the router, the “total available memory” will go down. In the case of the figure, there's lot of memory still available. If the amount is very low, the router could slow down and behave erratically. In that case, one would need to stop and disable services on the router. That's beyond the scope of this walkthrough but it's important to know.

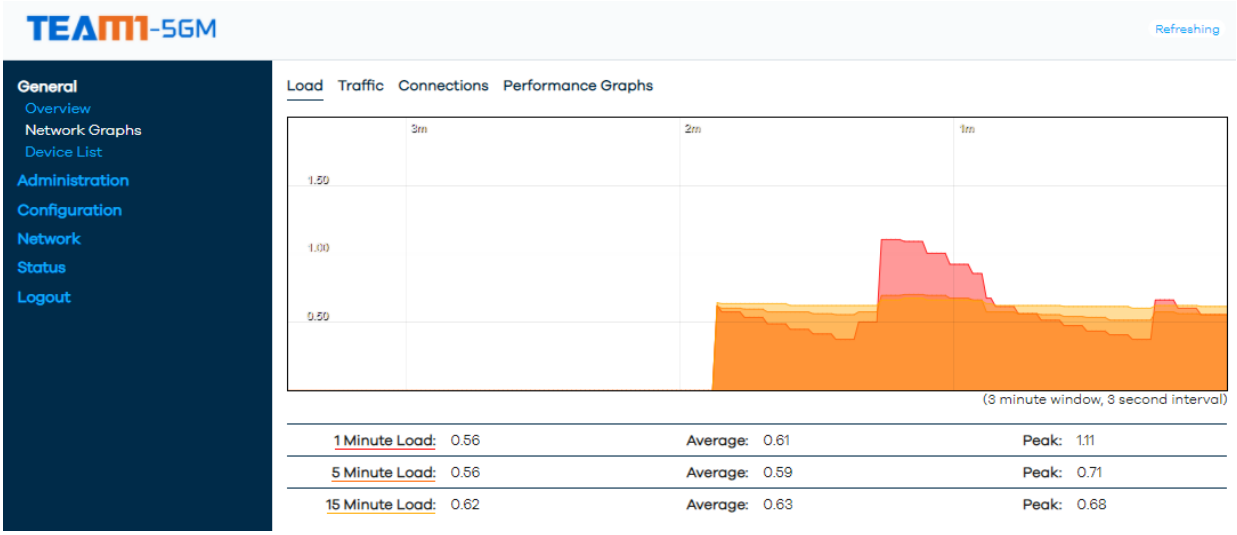
Next, we will see the Network section. The Network section shows information of the network interface of the router, particularly as it applies to IP addresses.

At the end of the screen shot, you'll see the DHCP leases computers on the router. Without getting into details, DHCP leases represent temporary IP addresses that the router will give out to client computers

4.3 Network and Graphs

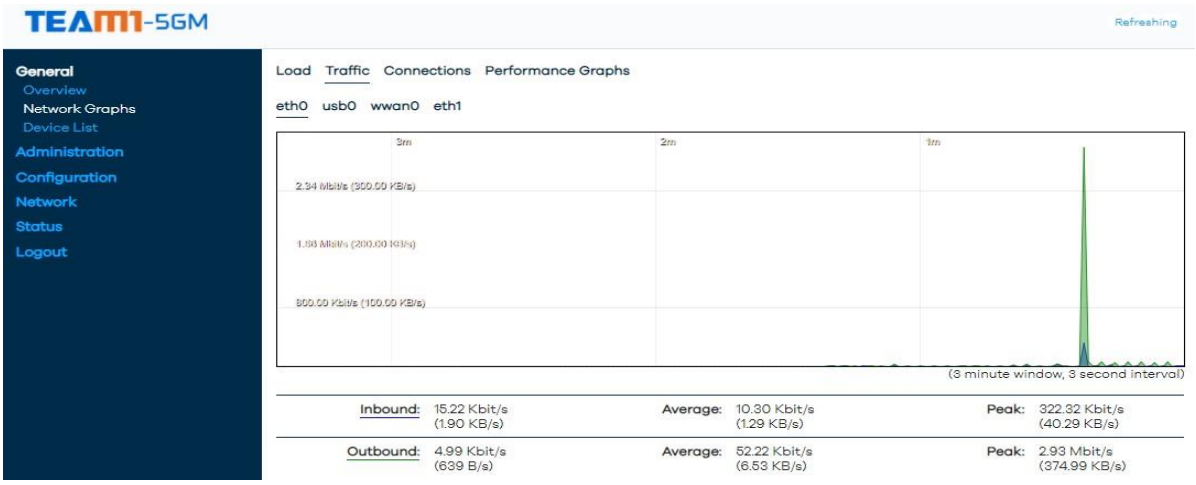
4.3.1 Load

Next, in the 'Network Graphs' section, there is an overall loading status of the system as shown in the screen shot below, and it is categorized in 1 min Load, 5 min Load and 15 min Load.



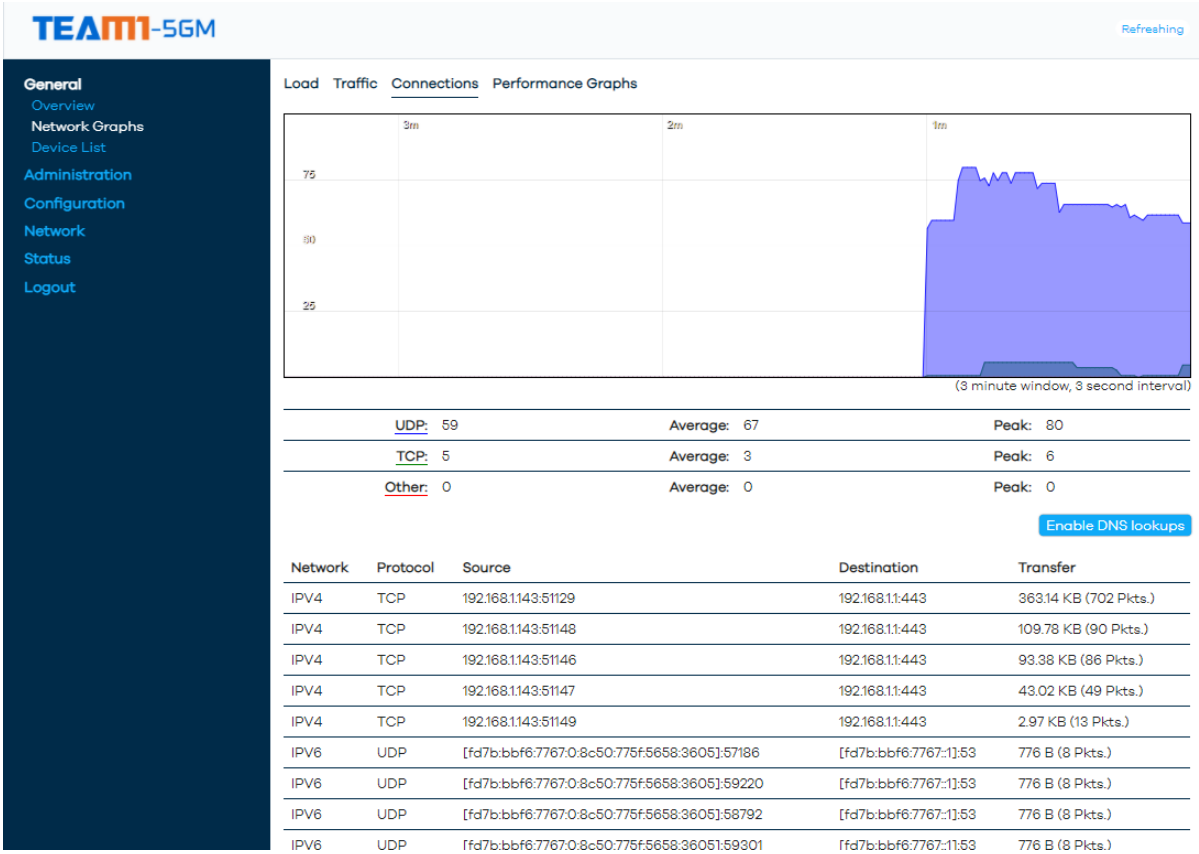
4.3.2 Traffic

Next is the 'Traffic' section, it shows the current traffic status of the system. In detail, it shows the current speed, average speed and peak speed of each interface.



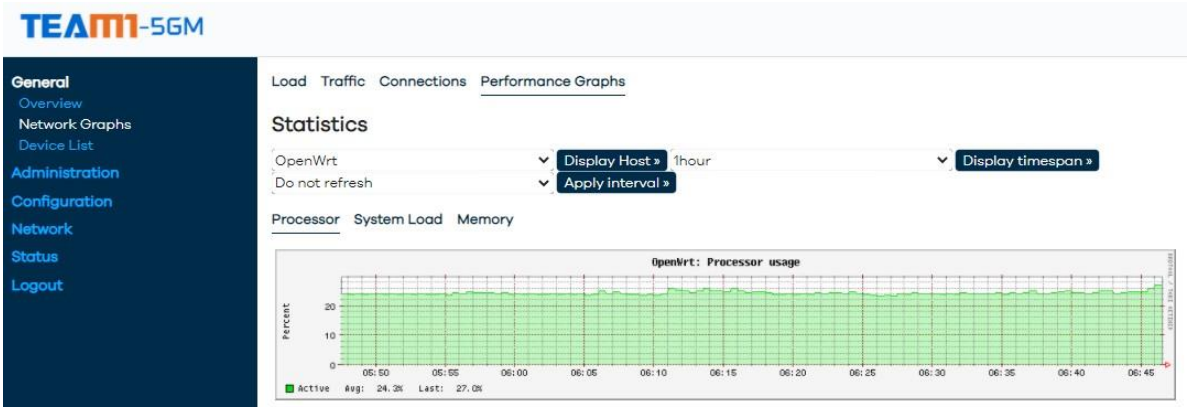
4.3.3 Connection

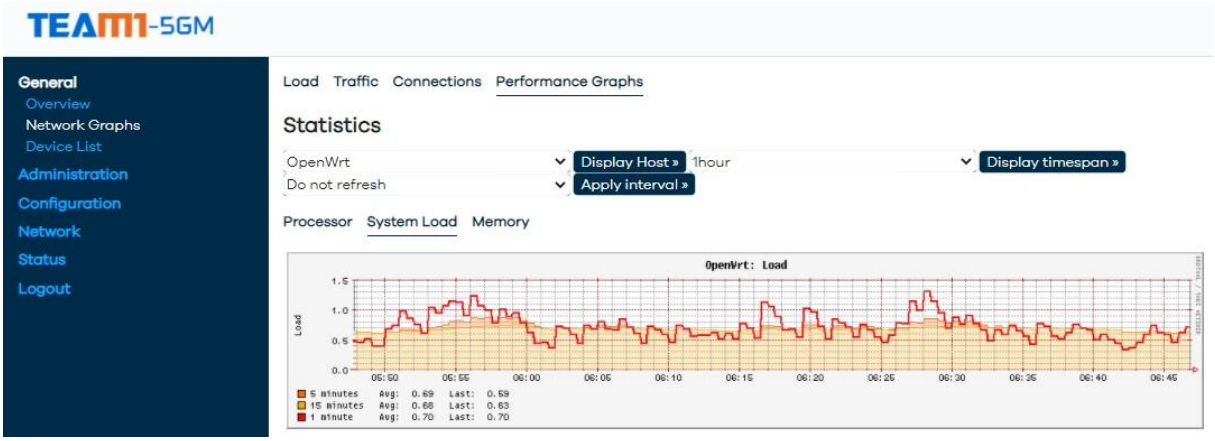
This section is the ‘Connections’ section, it contains the current UDP, TCP and other connections currently, and their average speed and peak speed.

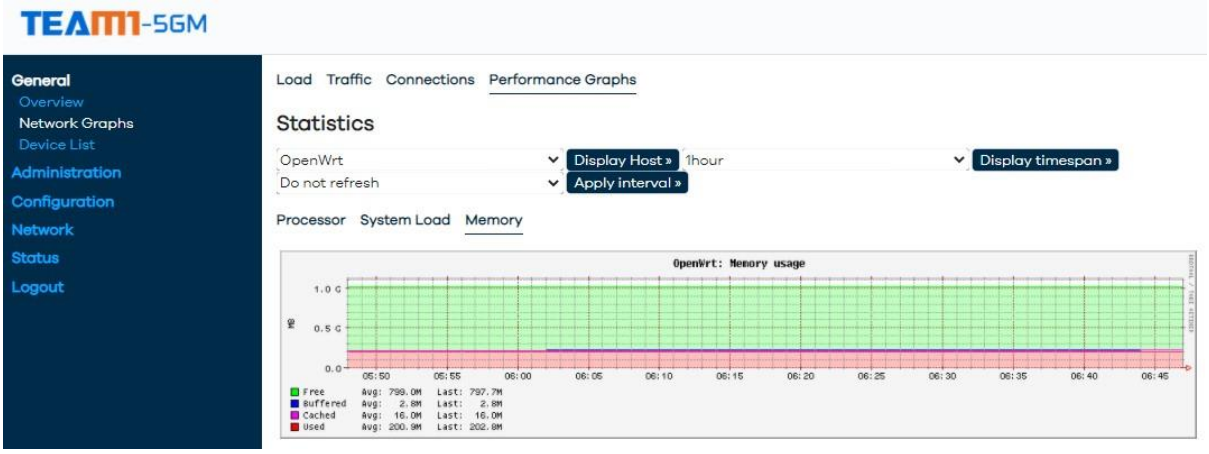


4.3.4 Performance Graph

There are three graphs in this section, processor usage percentage, system load and memory usage.

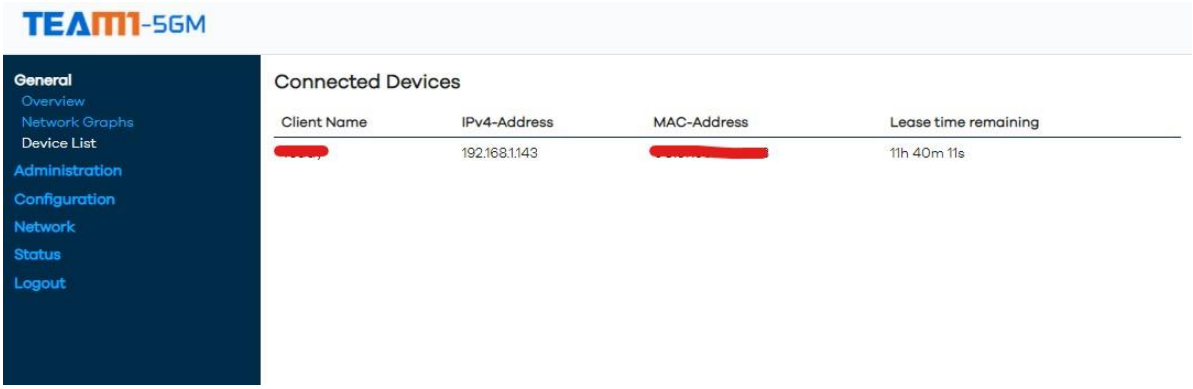






4.4 Device List

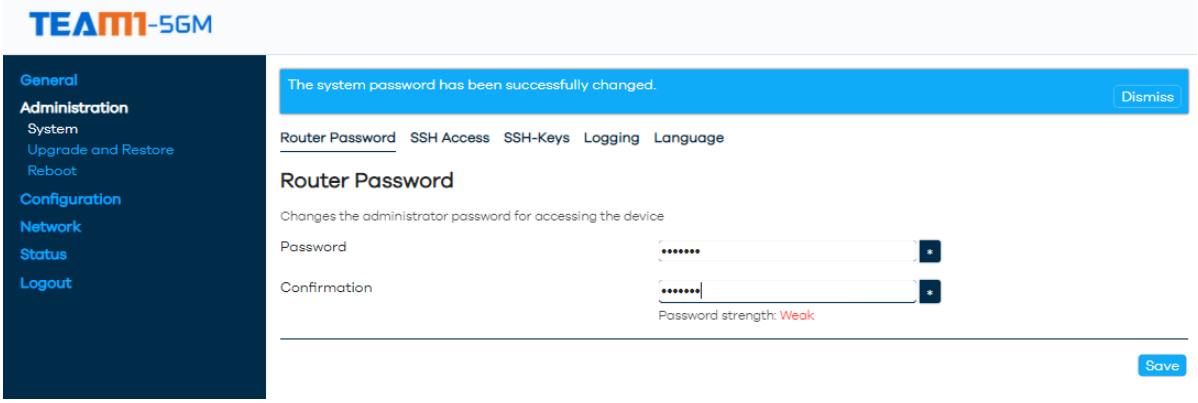
In the ‘Device list’, any connected device will be displayed here.



5 Administration

5.1 Set Up Root Password

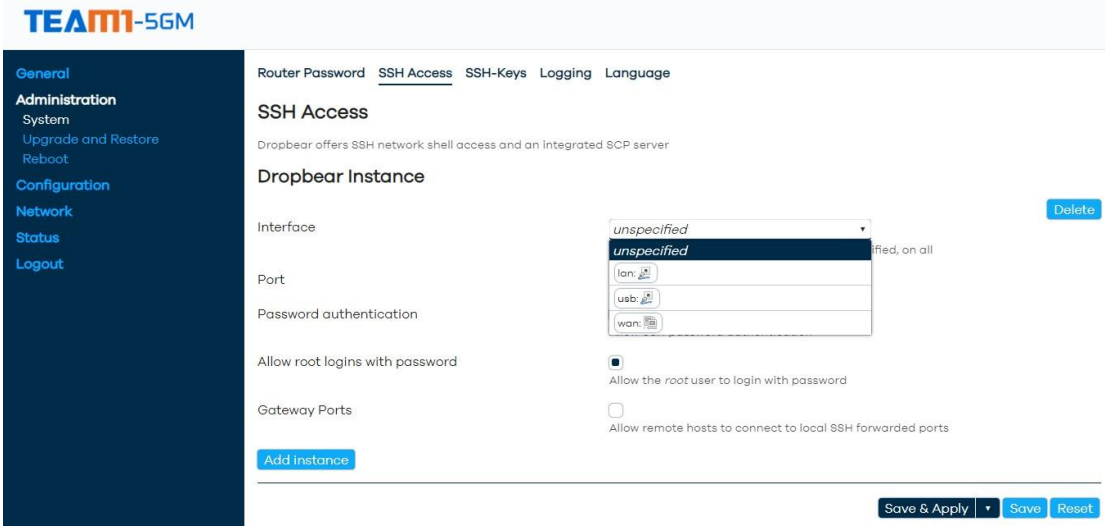
Now that we have a sense of the information on the status section, we need to fix that lack of a root password. We can do that in ‘Administration’ – ‘System’ – ‘Router Password’. Since this is an extremely powerful account, we need to provide a strong password that you'll remember. Once you have a new password, type it into the “password” field and then repeat it into the “confirmation” field. Make sure to remember this password; when you log into the router again, you'll need this password.



Lastly, we click “Save” to finalize our changes on this page.

5.2 SSH – Access

In this section, user can define which interface is preferred when using SSH to access the modem. For security concern, user can also add SSH-Key in the next section if needed.

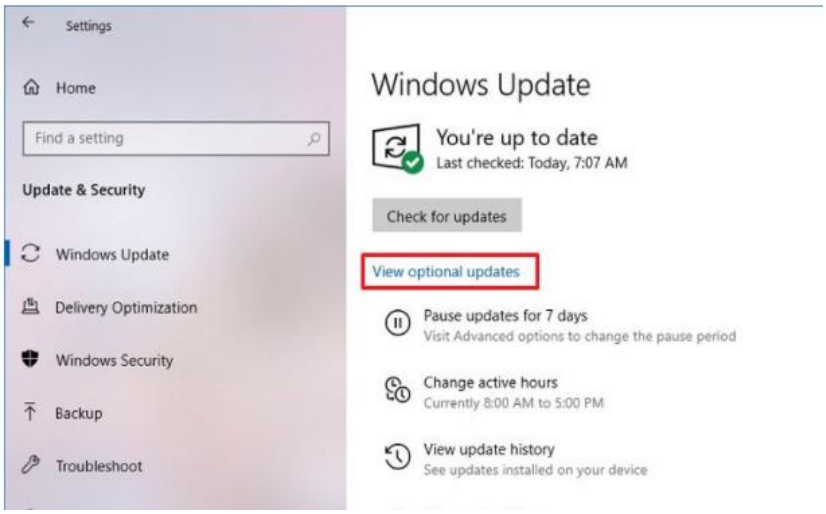


5.2.1 Steps to Access The Modem Operating System Using SSH:

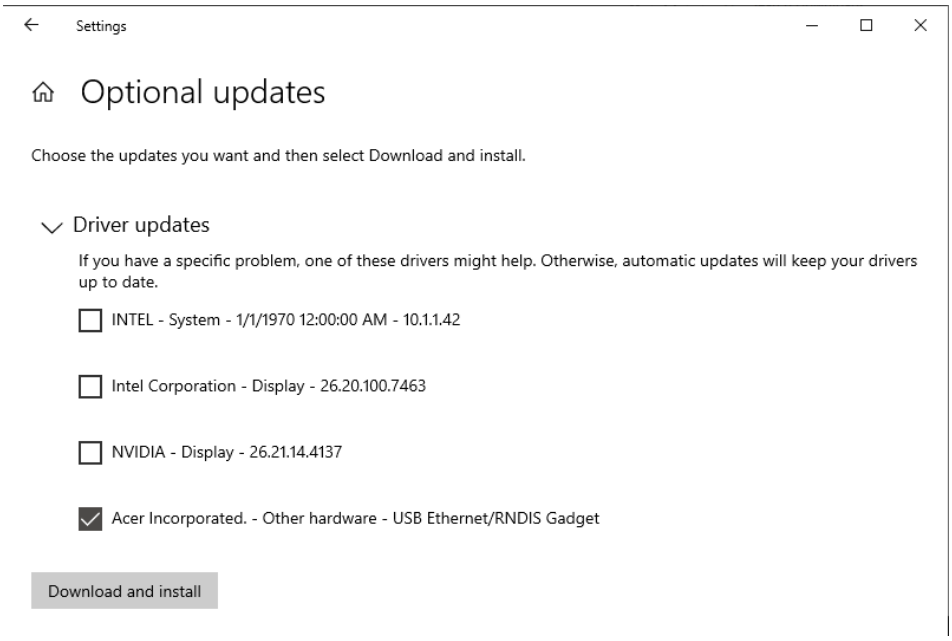
1. Connect H3(Ethernet cable) or H4(USB cable) to computer

   Notes: Connect H4 to computer needs to install driver to enable USB – Ethernet Adapter connection. User can install the driver from the windows update.

   a. Plug in H4 to computer
   b. Open “Settings” on Windows 10
   c. Click on “Update & Security”
   d. Click on “Windows Update” and click on “Check for updates”
   e. Click the “Views optional updates” option



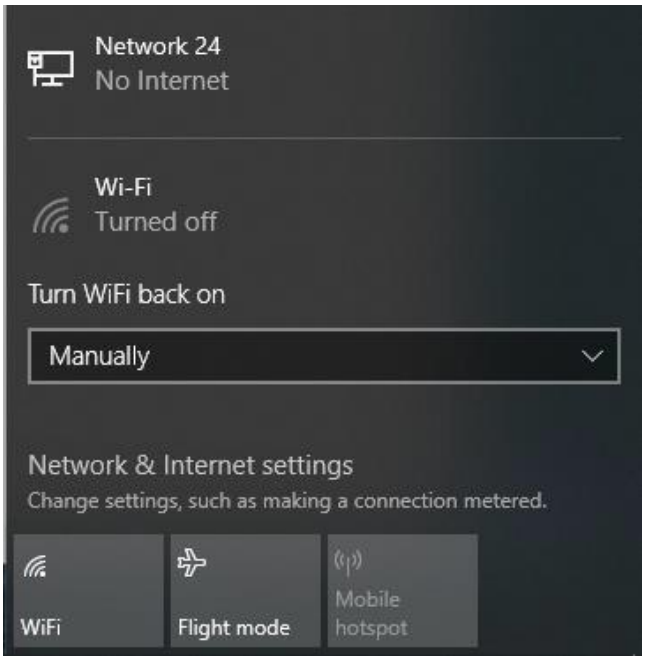
   f. Expand the “Driver updates” category
   g. Tick “USB Ethernet/RNDIS Gadget”



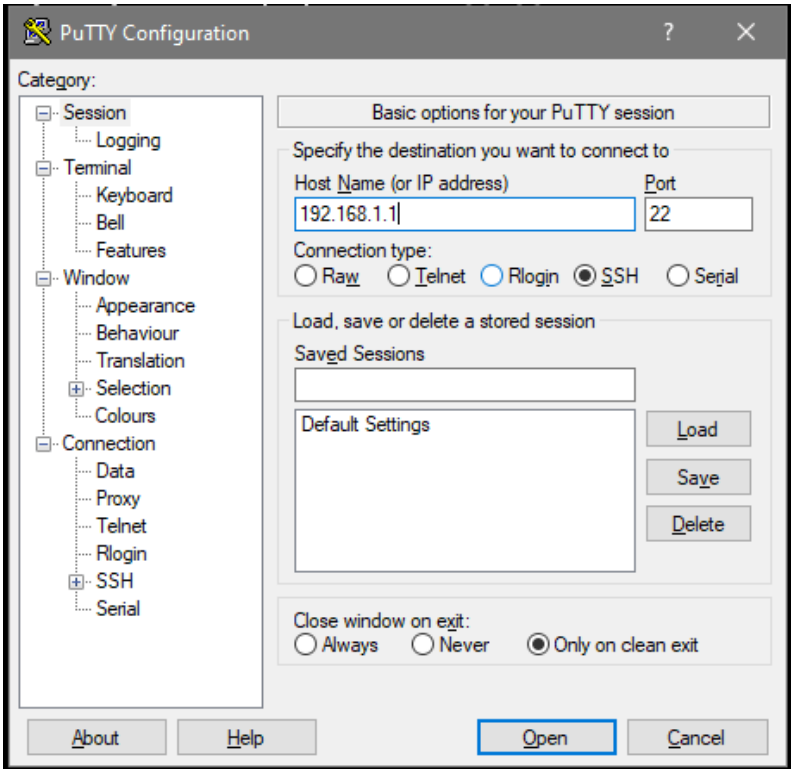
   h. Click “Download and install” button.

2. Turn off any other connection if any.

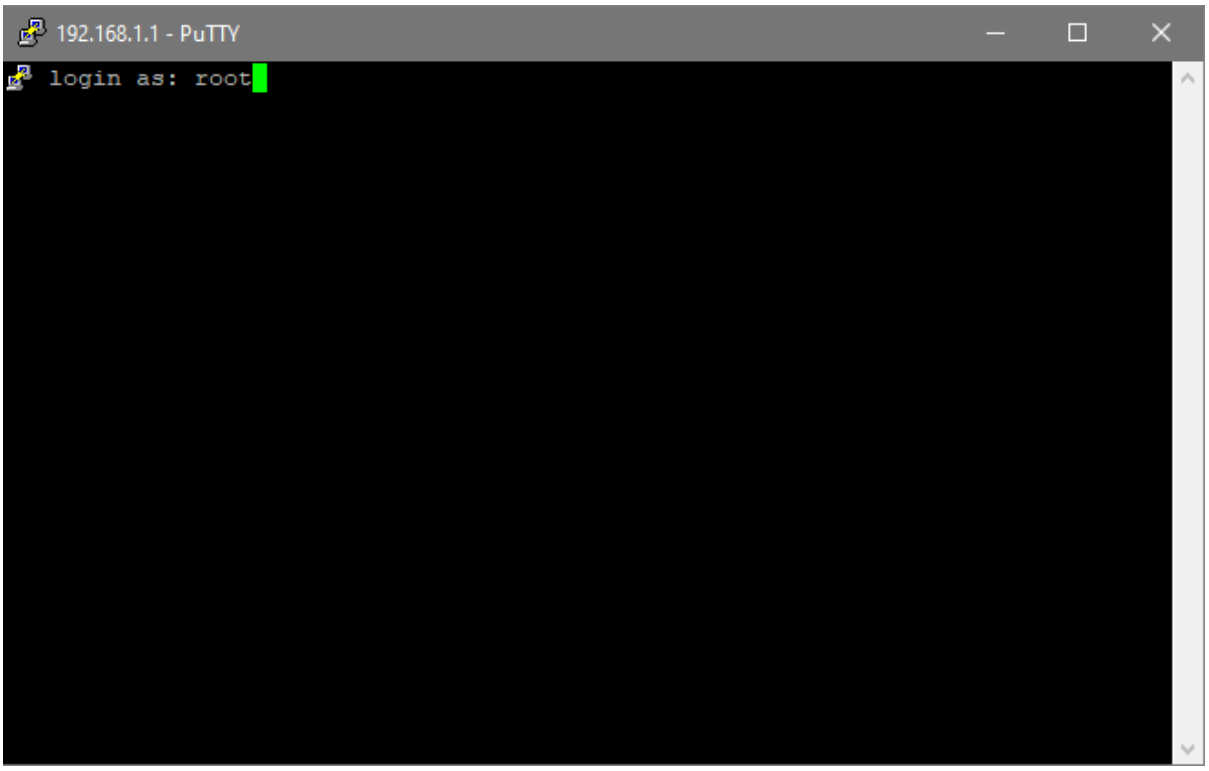
3. After a short while the Ethernet connection will appear in the system task bar as shown.



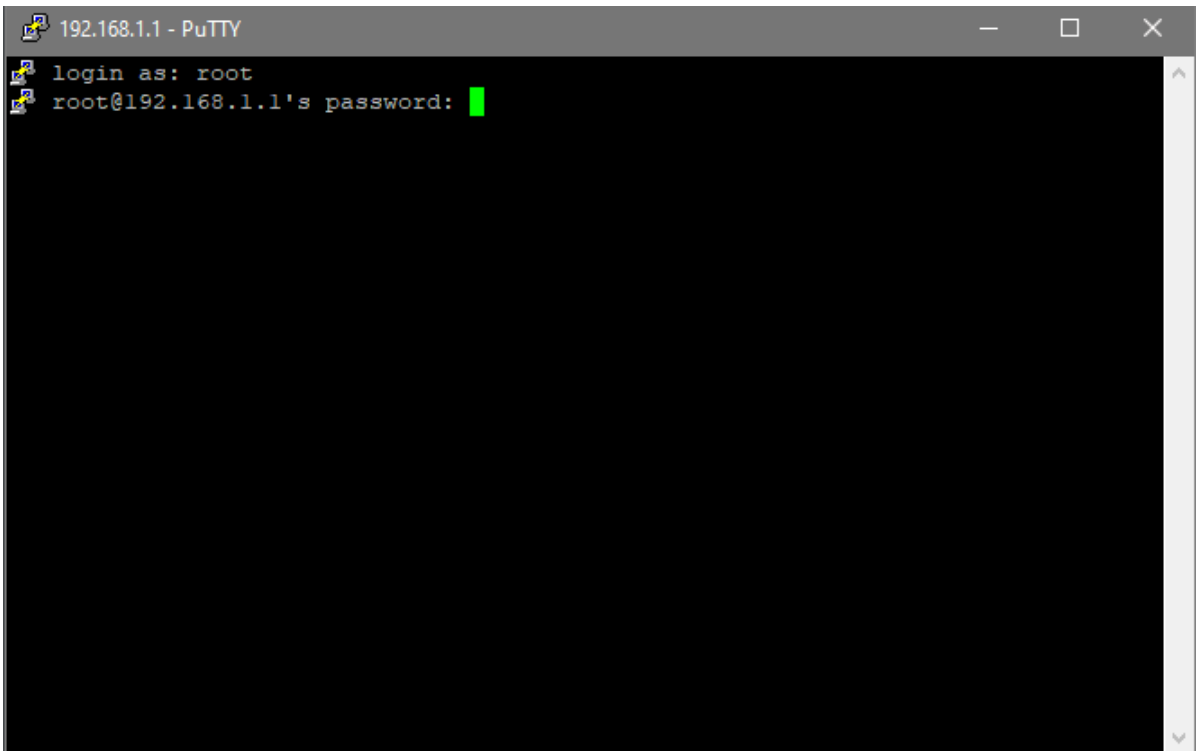
4. Next user a software that supports SSH, here is an example using 'Putty'. The default gateway of the modem is 192.168.1.1 port 22.



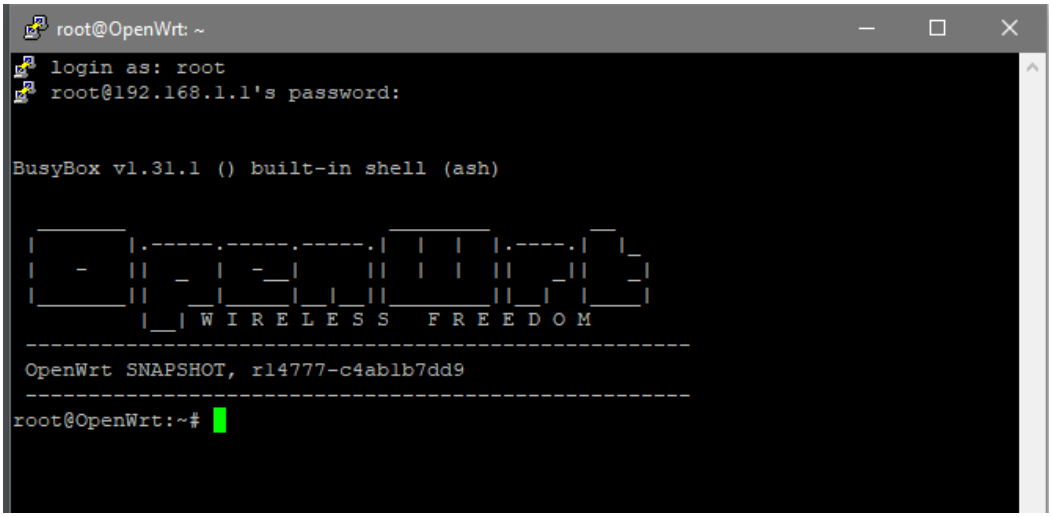
5. Click ‘Open’ and a window will appear, here we login as ‘root’



6. Enter the password

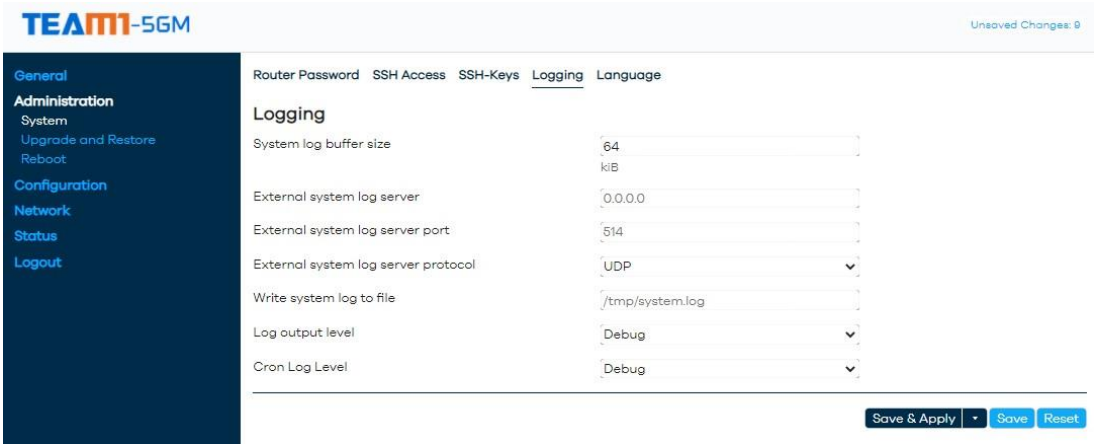


7. Now we are in



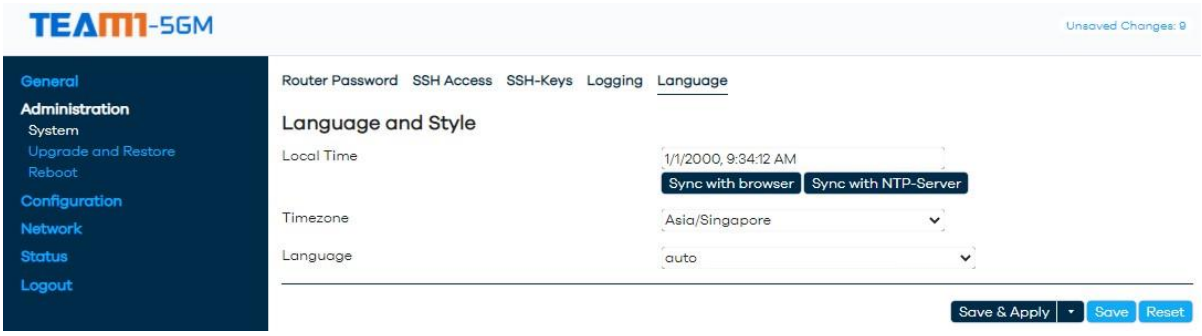
5.3 Logging

This section is for user to configure the log feature, which is able to record and store the system log to specified location.



5.4 Language

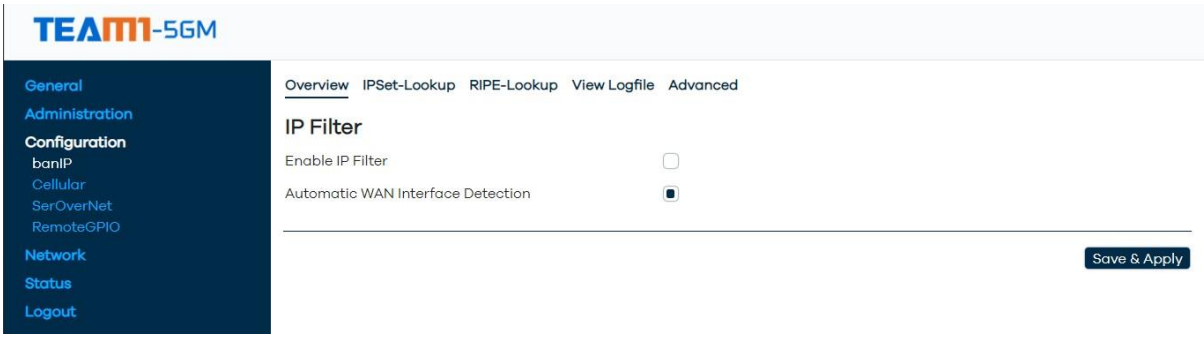
Time zone and Language settings.



6 Configuration

6.1 banIP

This section is used to ban incoming and/or outgoing IP addresses via ipsets. IP address blocking is commonly used to protect against brute force attacks, prevent disruptive or unauthorized address(es) from access or it can be used to restrict access to or from a particular geographic area. Any action or configuration take upon this section is strictly at users own risk.



6.1.1 banIP Configuration Options

Caution: Edit this section at your own risk.

- usually, the pre-configured banIP setup works quite well and no manual overrides are needed
- the following options apply to the 'global' config section:
  - ban_enabled => main switch to enable/disable banIP service (bool/default: '0', disabled)
  - ban_automatic => determine the L2/L3 WAN network device automatically (bool/default: '1', enabled)
  - ban_iface => space separated list of WAN network interface(s)/device(s) used by banIP (default: not set, automatically detected)
  - ban_realtime => a small log/banIP background monitor to block SSH/LuCI brute force attacks in realtime (bool/default: 'false', disabled)
  - ban_target_src => action to perform when banning inbound IPv4 packets ('DROP'/'REJECT', default: 'DROP')
  - ban_target_src_6 => action to perform when banning inbound IPv6 packets ('DROP'/'REJECT', default: 'DROP')
  - ban_target_dst => action to perform when banning outbound IPv4 packets ('DROP'/'REJECT', default: 'REJECT')
  - ban_target_dst_6 => action to perform when banning outbound IPv6 packets ('DROP'/'REJECT', default: 'REJECT')
  - ban_log_src => switch to enable/disable logging of banned inbound IPv4 packets (bool/default: '0', disabled)
  - ban_log_dst => switch to enable/disable logging of banned outbound IPv4 packets (bool/default: '0', disabled)

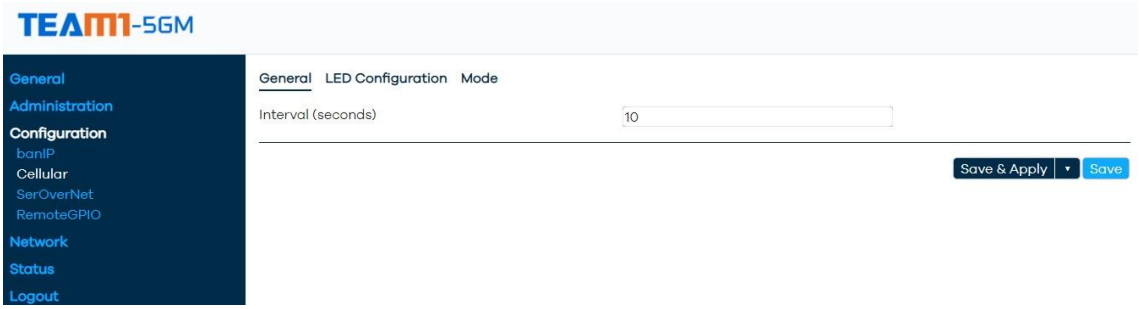
- the following options apply to the 'extra' config section:
  - ban_debug => enable/disable banIP debug output (bool/default: '0', disabled)
  - ban_nice => set the nice level of the banIP process and all sub- processes (int/default: '0', standard priority)
  - ban_triggerdelay => additional trigger delay in seconds before banIP processing begins (int/default: '2')
  - ban_backupdir => target directory for banIP backups (default: '/tmp')
  - ban_sshdaemon => select the SSH daemon for logfile parsing, 'dropbear' or 'sshd' (default: 'dropbear')
  - ban_starttype => select the used start type during boot, 'start', 'refresh' or 'reload' (default: 'start')
  - ban_maxqueue => size of the download queue to handle downloads & IPSet processing in parallel (int/default: '4')
  - ban_fetchutil => name of the used download utility: 'uclient-fetch', 'wget', 'curl', 'aria2c' (default: not set, automatically detected)
  - ban_fetchparm => special config options for the download utility (default: not set)
  - ban_autoblacklist => store auto-addons temporary in ipset and permanently in local blacklist as well (bool/default: '1', enabled)
  - ban_autowhitelist => store auto-addons temporary in ipset and permanently in local whitelist as well (bool/default: '1', enabled)

6.1.2 Logging of Banned Packets

- by setting ban_log_src=1 / ban_log_dst=1 in the config options, banIP will log banned inbound / outbound packets to syslog.
- example of a logged inbound (dst) and outbound (src) packet:
- to change the default logging behavior, the following options can be added to the 'global' config section:
  - ban_log_src_opts => IPv4 iptables LOG options for banned inbound packets (default: '-m limit --limit 10/sec')
  - ban_log_src_opts_6 => IPv6 iptables LOG options for banned inbound packets (default: '-m limit --limit 10/sec')
  - ban_log_src_prefix (default: '<ban_target_src>(src banIP) ', typically 'DROP(src banIP) ')
  - ban_log_src_prefix_6 (default: '<ban_target_src_6>(src banIP) ', typically 'DROP('src banIP)')
  - ban_log_dst_opts => IPv4 iptables LOG options for banned outbound packets (default: '-m limit --limit 10/sec')
  - ban_log_dst_opts_6 => IPv6 iptables LOG options for banned outbound packets (default: '-m limit --limit 10/sec')
  - ban_log_dst_prefix (default: '<ban_target_dst>(dst banIP) ', typically 'REJECT(dst banIP) ')
  - ban_log_dst_prefix_6 (default: '<ban_target_dst_6>(dst banIP) ', typically 'REJECT('dst banIP)')

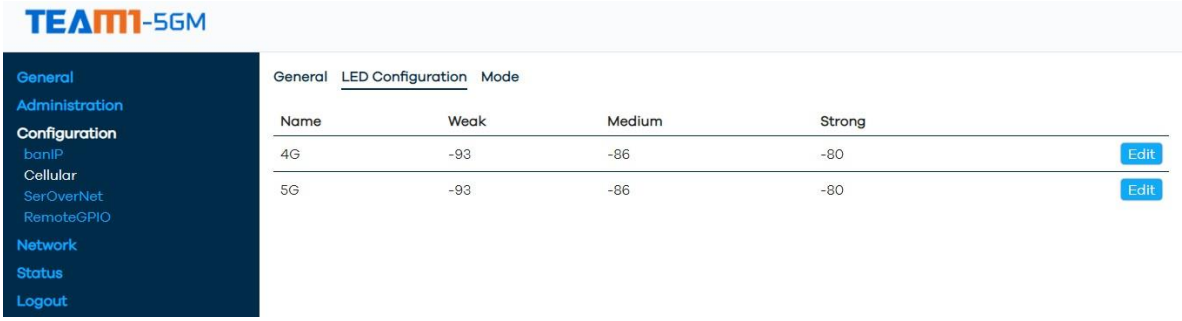
6.2 Cellular

6.2.1 Interval



The time interval of retrieving status of 5GM (in second), specifically the interval of sending 'AT commands' in the system background.

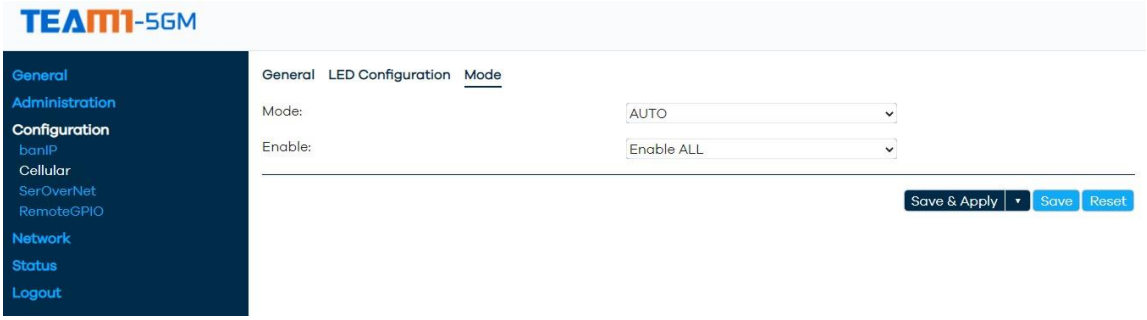
6.2.2 LED Configuration for Signal Strength

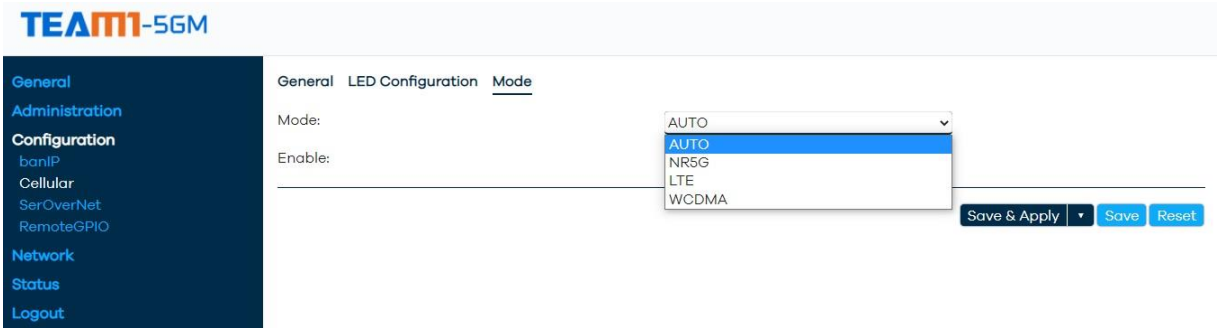


Customized threshold of signal strength according to various scenario, which means users have the right to decide how to classify the signal strength.

6.2.3 Mode

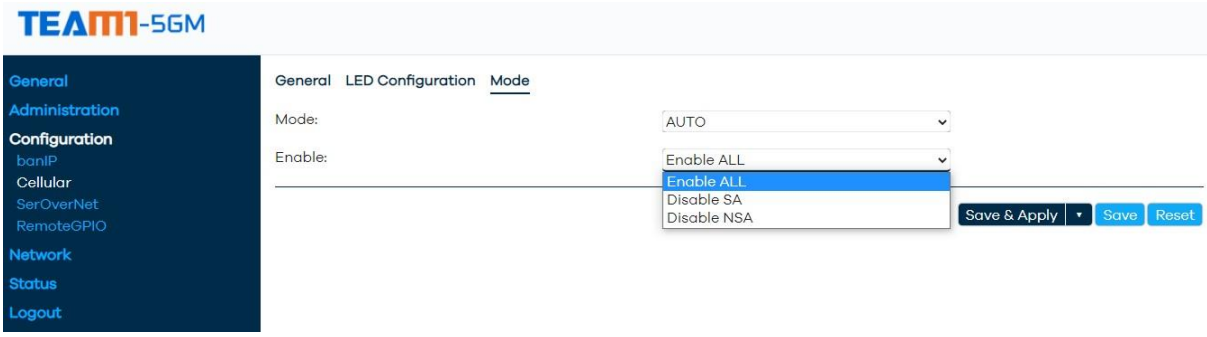
Set the operating mode of 5GM





Mode: This allows user to set the operation mode of 5GM, which contains:

- Auto: The modem will automatically choose operating mode
- NR5G: 5G mode
- LTE: 4G mode
- WCDMA: 3G mode



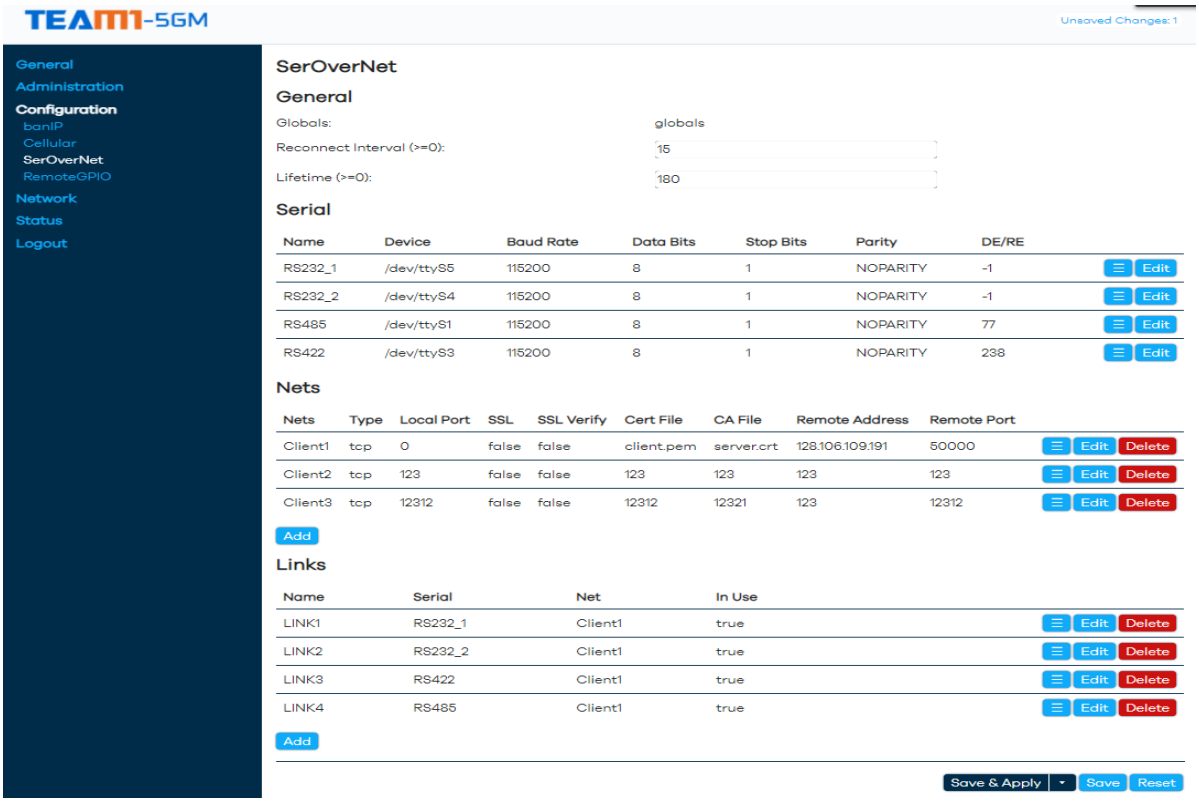
Enable: This option is specially for 5G mode, which will not take effect when user is using 4G/3G mode.

- Enable ALL: Enable SA and NSA mode.
- Disable SA: The modem only operates in NSA mode
- Disable NSA: The modem only operates in SA mode

6.3 SerOverNet

6.3.1 Overview

This section is designed for the feature called 'Serial over Network'. 5GM has 4 serial ports available, 2 x RS232 ports, 1 x RS422 port and 1 x RS485 port. In the general setting, user can set reconnect interval and connection lifetime (in second).



6.3.2 List of Ports

In this segment, the only 4 serial ports are listed. By clicking the 'Edit' Button user can change the settings of each port.

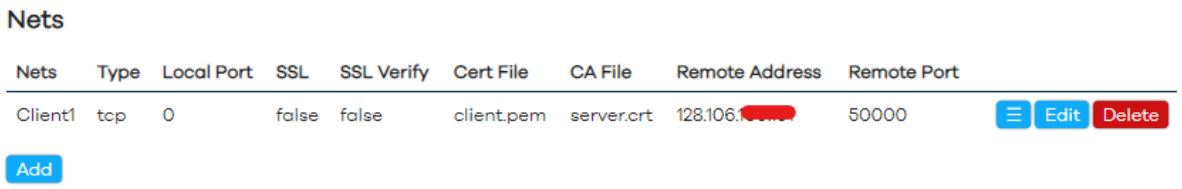
Serial

Name	Device	Baud Rate	Data Bits	Stop Bits	Parity	DE/RE	
RS232_1	/dev/ttyS5	115200	8	1	NOPARITY	-1	Edit
RS232_2	/dev/ttyS4	115200	8	1	NOPARITY	-1	Edit
RS485	/dev/ttyS1	115200	8	1	NOPARITY	77	Edit
RS422	/dev/ttyS3	115200	8	1	NOPARITY	238	Edit


SerOverNet
Name
RS232_1
Device
/dev/ttyS5
Baud Rate
115200
Data Bits
8
Stop Bits
1
Parity
NO PARITY
DE/RE
-1
Dismiss
Save

6.3.3 Nets

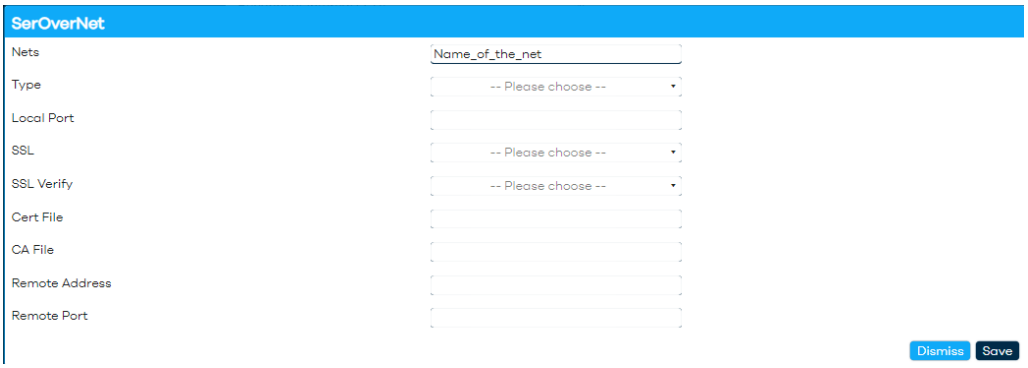
In this section, user can set the destination where the serial port connects to. The connection can be encrypted by SSL and Certificate file.



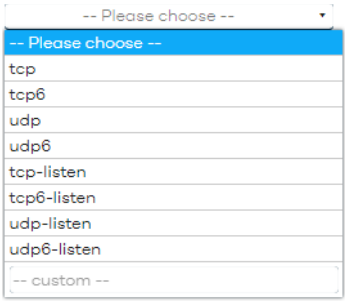
Steps to set Net for serial port

1. Click 'Add' button

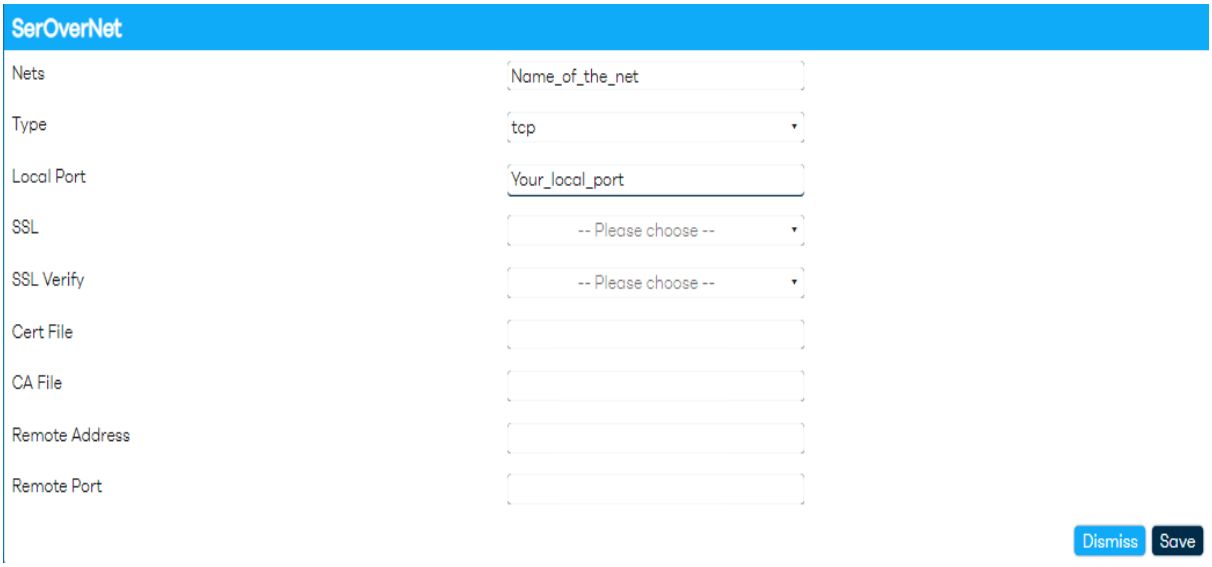
2. Set the name of the Net



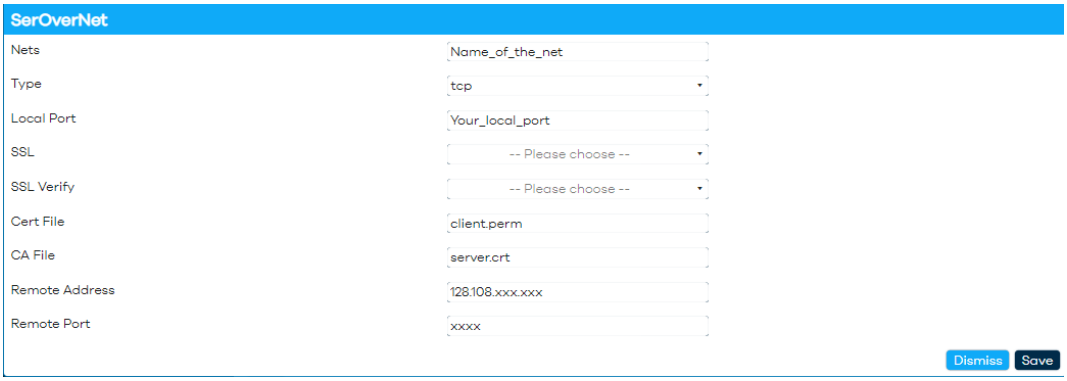
3. Select type of the Net



4. Set the local port



5. Set SSL, SSL verify if needed (here leave it as default)
6. Set the Cert File and CA File is needed



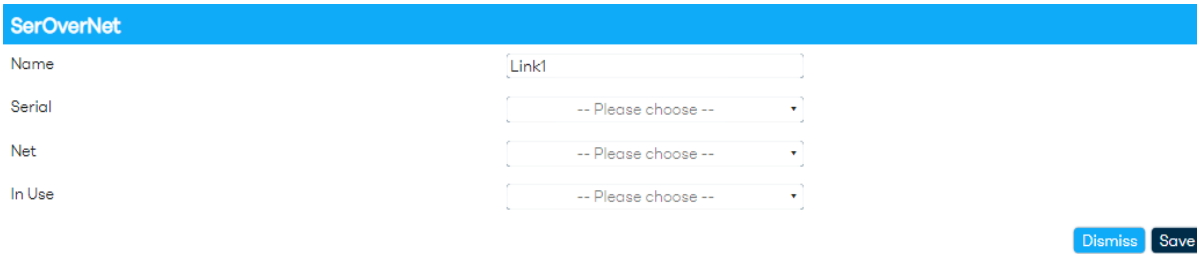
7. Click ‘Save’ to apply the setting

6.3.4 Links

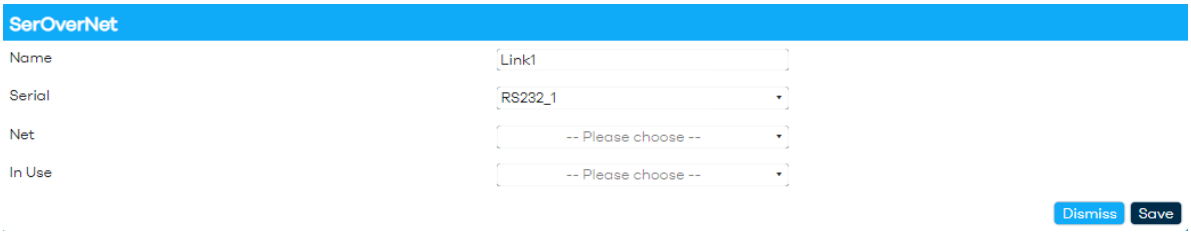
This section links the serial ports to nets that we set above. Steps to link the ports:

Click the ‘Add’ button

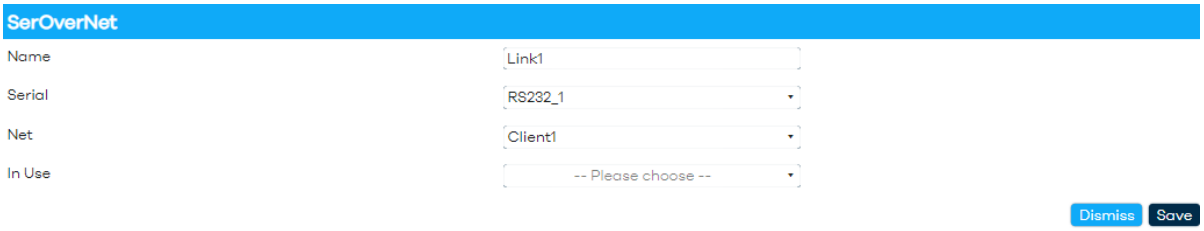
1. Set a name for the link



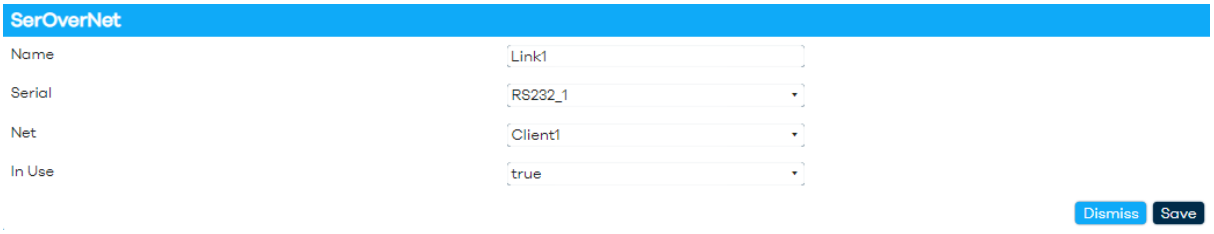
2. Choose a serial port to link (eg. RS232_1)



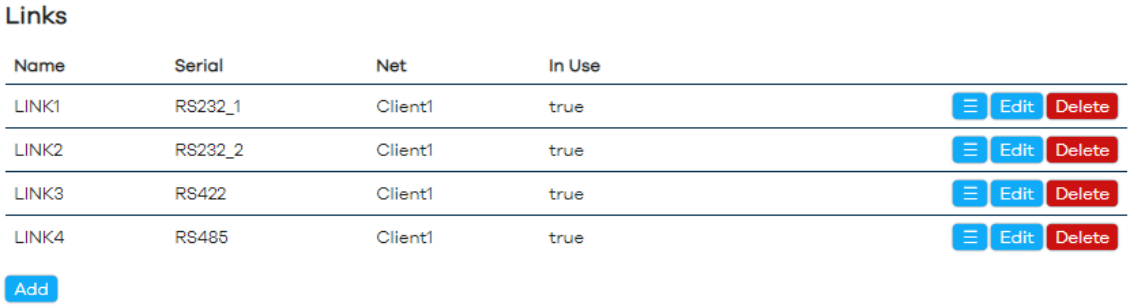
3. Assign a Net for the serial port



4. Set true for 'In Use' option. (eg. Once set, RS232_1 cannot be used by other Net.)

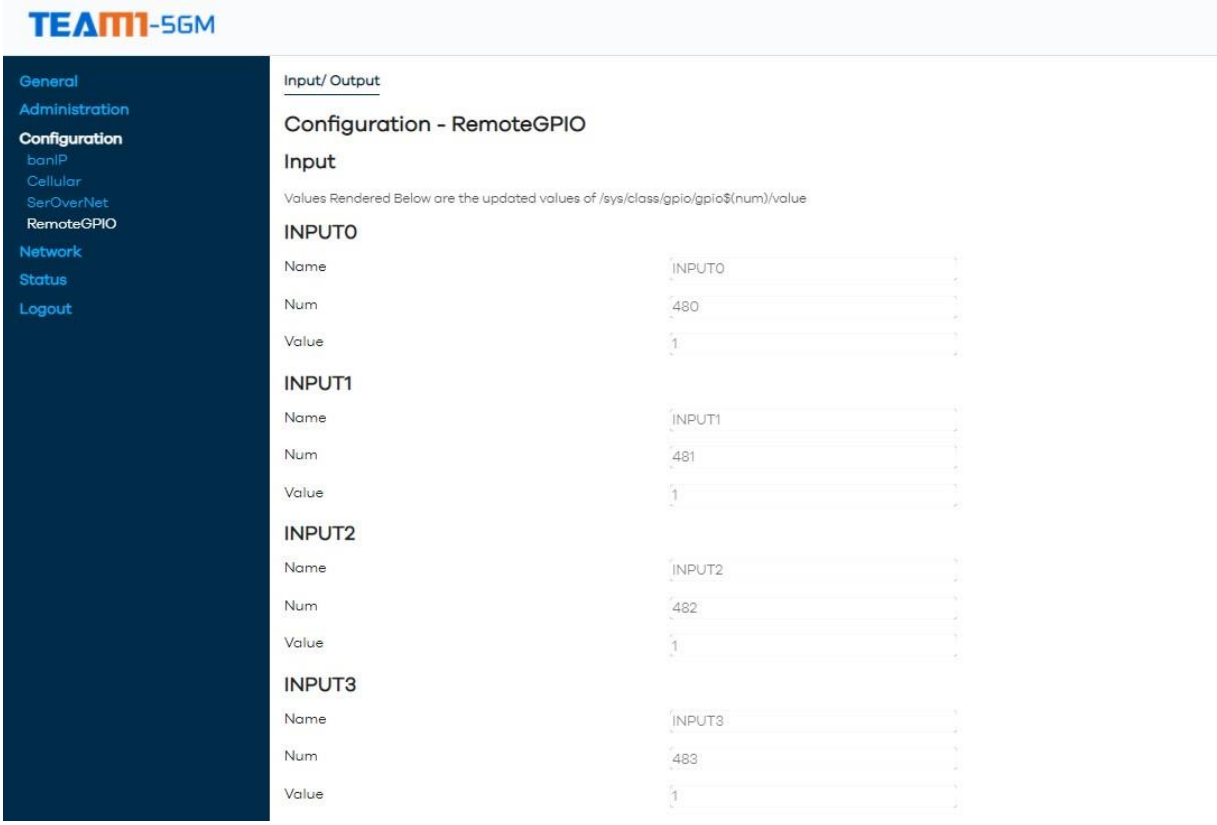


5. Click 'Save' to apply the setting (eg. Set multiple ports to one Net)



6.3.5 RemoteGPIO

In this section, the four available GPIO are listed here with their attribute displayed.



Click on 'Edit' and input value to write to /sys/class/gpio/gpio$(num)/value

Click ‘Save’ to apply to changes.

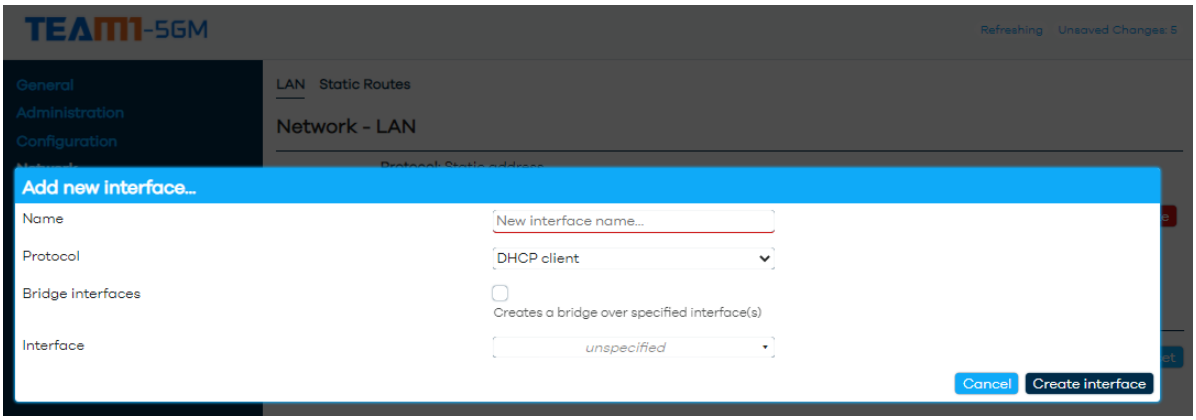
7 Network Interfaces

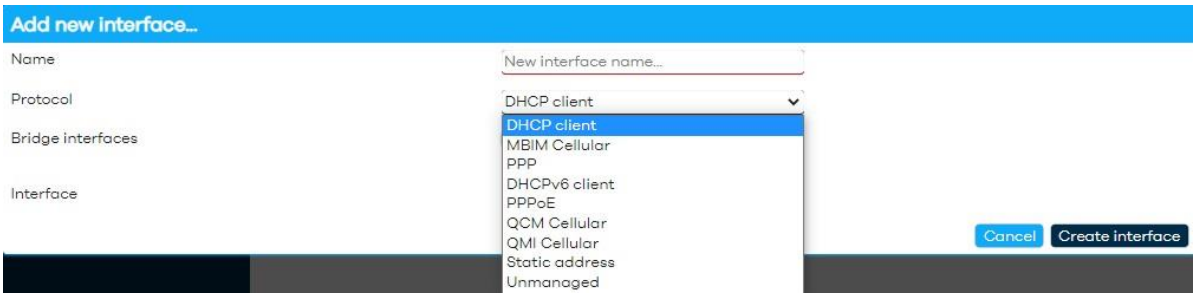
7.1 LAN

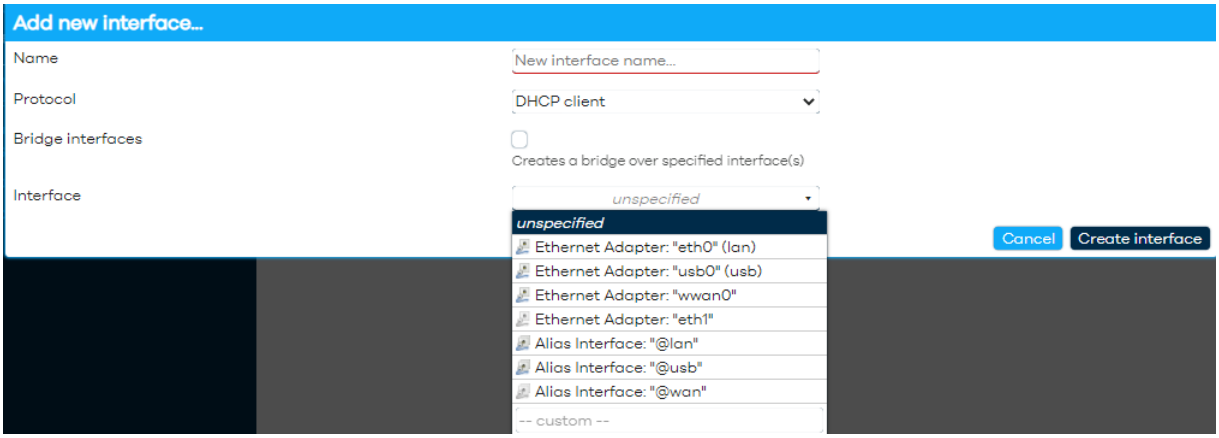
7.1.1 Add LAN Interface

In 'Network' – 'LAN' section, all of existing LAN interfaces will be listed here. There are four operations that user can perform, which are 'Restart', 'Stop', 'Edit' and 'Delete'. After each operation has been done, user must Click 'Save & Apply' button for the changes to take effect.

Click the 'Add new interface…' button to add a new interface. Enter the name and choose the 'Protocol' for the corresponding 'Interface' that is needed, and click 'Create interface' button.

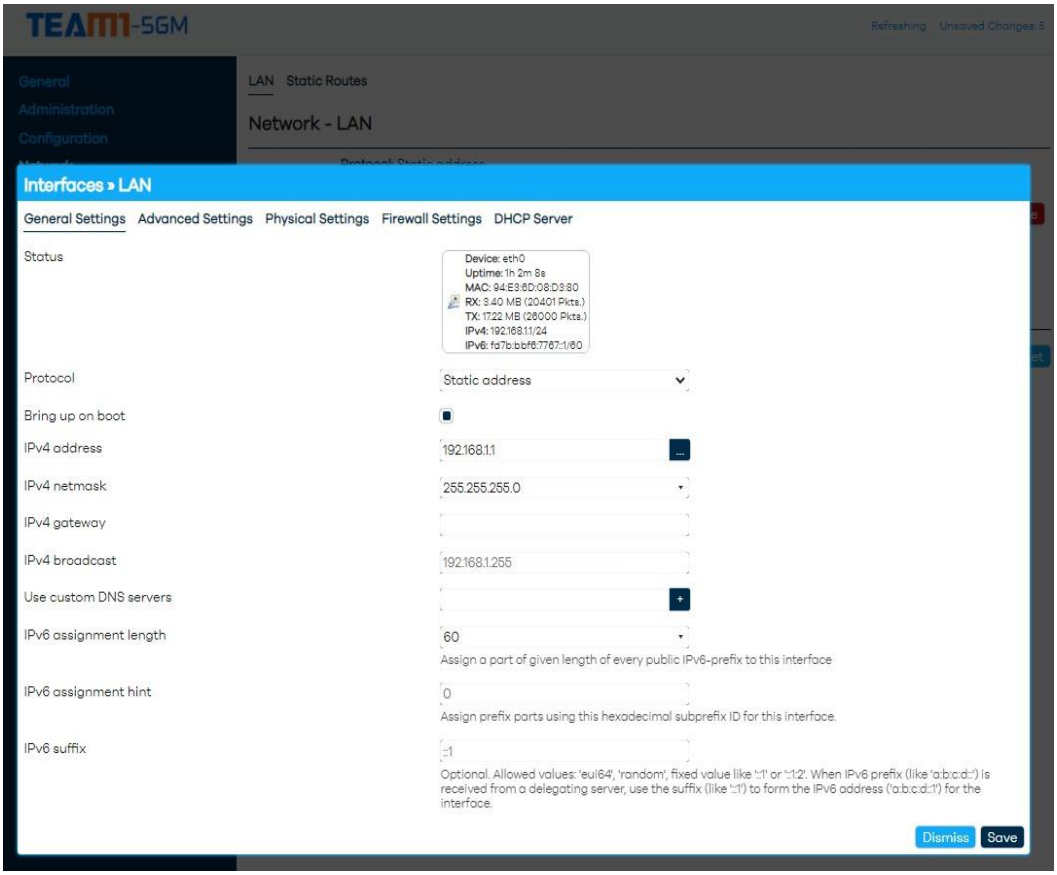






7.1.2 Edit LAN Setting

Detail refers to official document



IPV4 Address: 192.168.1.1, here you have to put your new IP address. **IPV4 Netmask:** choose the netmasks from the list as per your IP address. **Gateway IPV4:** you can add your gateway as per your choice.

The IPV4 Broadcast: leave it as default.

7.1.3 DHCP Server

If you are using the OpenWrt as AP mode it is not necessary to enable the DHCP server, but if you are using the OpenWrt as a router then DHCP has to enable. For Ignore interface option Disable DHCP for this interface.

- If the checkbox is checked it means DHCP server is disabled.
- If the checkbox is not checked it means DHCP server is enabled.

Start: this IP server start providing from this number. Limit: this will be last IP server will provide to client. Lease time: this is the expire time of leased addresses.

And click on save the changes and apply.

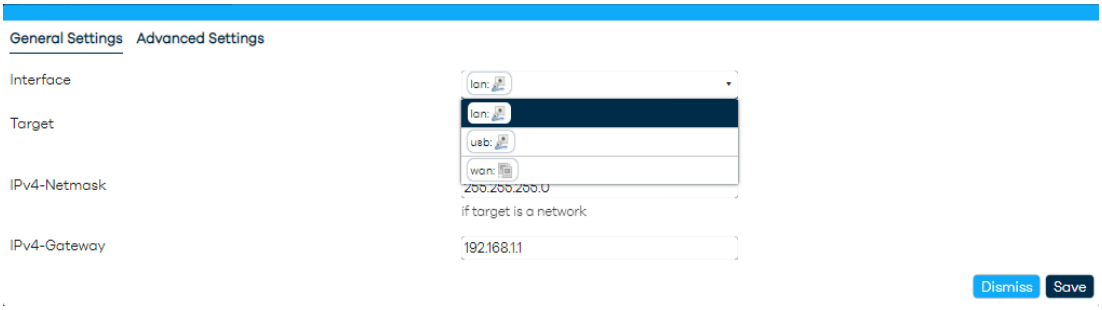
By this you can configure the OpenWrt LAN and DHCP server.

7.1.4 Static Routes

Typically, you do not need to add static routes unless you use multiple routers or multiple IP subnets on your network.

Steps to set a static route:

1. Choose an interface for the static route:



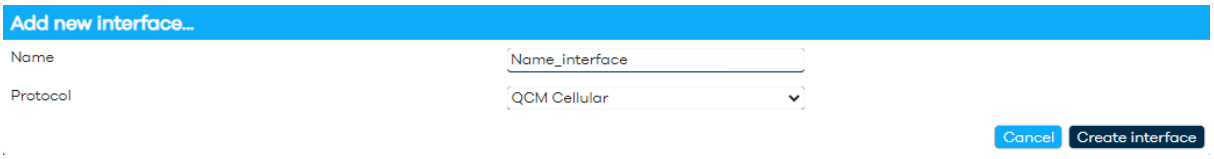
2. Enter the IP address for the final destination of the route in the ‘Target’ textbox
3. Enter the IP subnet mask for the final destination of the route. If the destination is a single host, enter 255.255.255.255
4. Enter the IP address of the gateway
5. The IP address of the gateway must be on the same LAN segment as the router
6. Click ‘Save’ to apply the changes

7.2 WAN

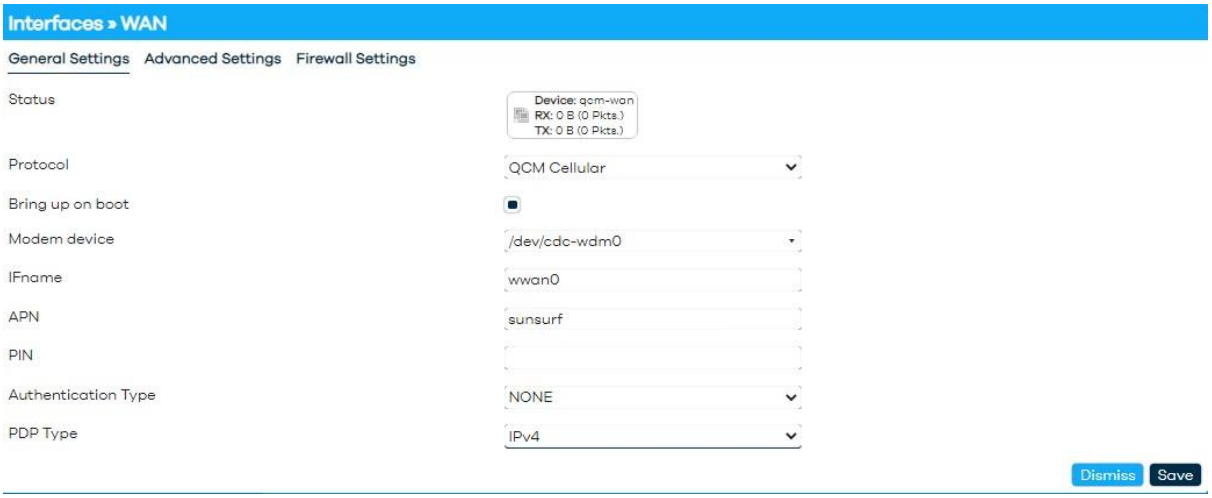
Add WAN interface and configuration

For 5GM to operate correctly, this section is the most essential part. Steps:

1. Click the ‘Add new interface…’ button



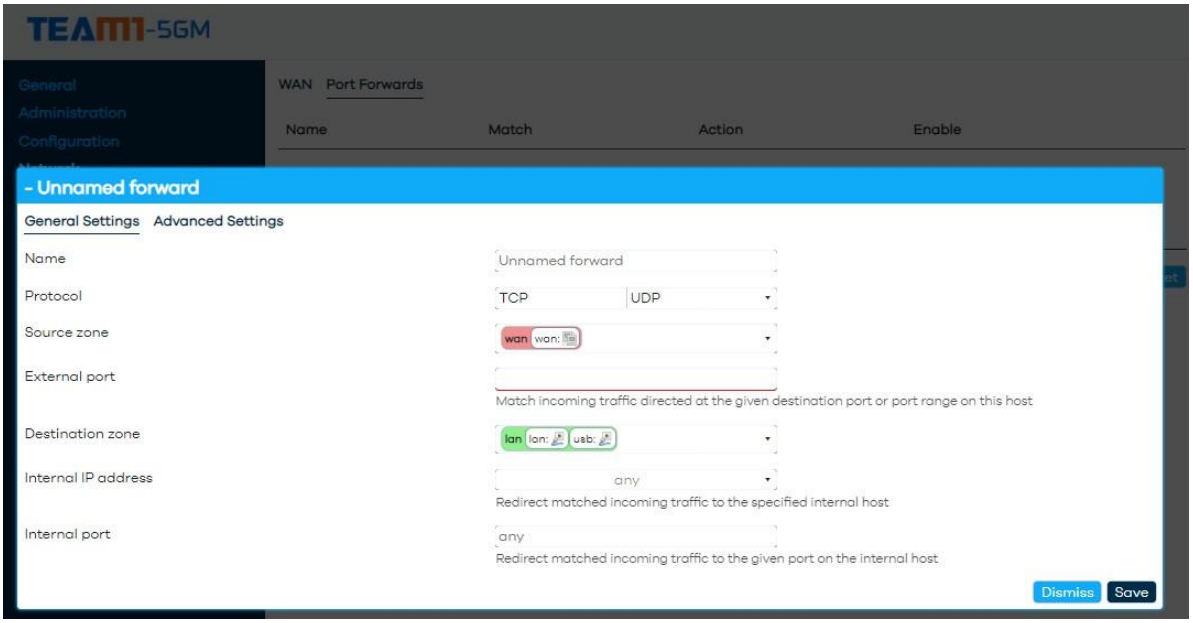
2. Give a name the interface
3. Choose a protocol for the interface. In most of the cases, an 4G/5G SIM card is used to set up a WAN interface, here is an example of using QCM Cellular as the protocol.
4. Click ‘Create interface’ button
5. Next, click ‘Edit’ to configure the details:



6. Check the ‘Bring up on boot’ option
7. Select the available modem device
8. Set wwan0 as IFname
9. Set the APN, different ISP has different APN, contact ISP for details if needed.
10. Enter the PIN of the SIM card if any.
11. Authentication Type is set to NONE as default, choose accordingly if needed.
12. PDP type set as IPV4 as default.
13. Click ‘Save’ to apply the changes.

7.2.1 Port Forward

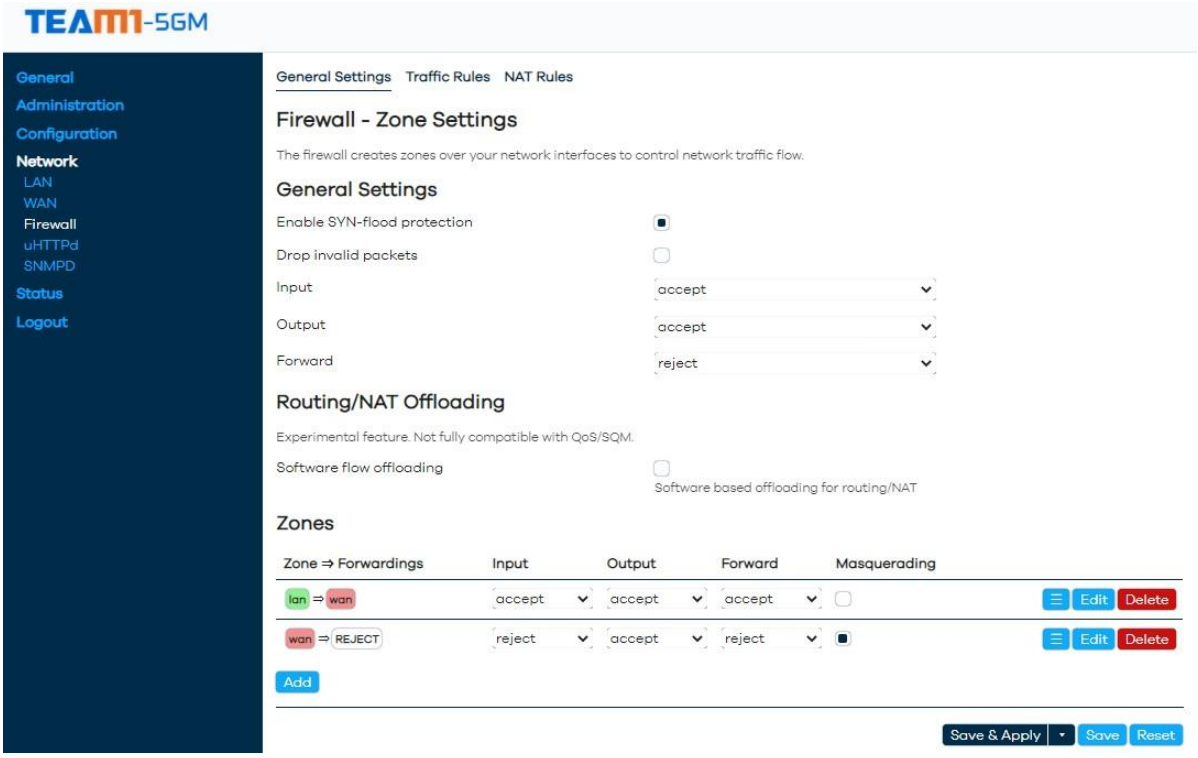
This page is a lite version of Port Forwards comparing with that in the usual LuCI interface (Network → WAN → Port Forwards). Port forwarding allows remote
computers on the Internet to connect to a specific computer or service within the private LAN. This version deletes Source Zone and Destination Zone, on the other hand, a default value was set to them. Source Zone: wan, destination Zone: lan. Furthermore, the users don't have to enter a new window to modify a server, that means, they can manipulate on the showing page, which simplifies the use of the interface.



7.3 Firewall

7.3.1 General Setting

The firewall creates zones over your network interfaces to control network traffic flow.



7.3.2 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.

7.3.3 NAT Rules

NAT rules allow fine grained control over the source IP to use for outbound or forwarded traffic.

7.4 uHTTPd

uHTTPd is configured to be the default LuCI web interface for OpenWrt. It is a web server written to be an efficient and stable server, suitable for lightweight tasks commonly used with embedded devices and proper integration with OpenWrt's configuration framework (UCI). In addition, it provides all the functionality expected of present-day web servers.

7.4.1 Features

Built as a general-purpose HTTP daemon, uHTTPd is not merely intended for running the OpenWrt's web interface but has functionality up to par with any other modern web server. Included is support for TLS (SSL), CGI and Lua. It is single threaded but supports multiple instances (i.e., multiple listen ports, each with its own document root and other features).
uHTTPd is built by default (since r35295 in Jan2013) to support the usage of TLS (HTTPS) via a libustream-* SSL library (on top of an actual SSL library: polarssl, mbedtls, cyalssl, openssl). Previously the package uhttpd-mod-tls was required, but it is not needed any more as long as you have installed a libustream library variant. Since Dec2016 luci-ssl installs by default libustream-mbedtls.
In contrast to many other web servers, it also supports running Lua in-process, which can speed up Lua CGI scripts. Note that LuCI, which depends on Lua, is not configured in this manner by default

7.4.2 Configuration

Configuration of uHTTPd integrates nicely with OpenWrt's user interface system, through standard UCI, provided since OpenWrt 10.03 (Backfire). The UCI configuration file is /etc/config/uhttpd. Since uHTTPd depends on this file directly, there is no second configuration file that gets written by UCI when settings are committed (like is the case with many other applications, such as Samba). Since uHTTPd is configured as part of the UCI system, refer to the uHTTPd UCI configuration page.
uHTTPd also properly provides an init script /etc/init.d/uhttpd to start or stop the service and enable it at boot time.

7.5 SNMPD

7.5.1 SNMPD

7.5.2 Com2Sec

SNMPD Com2Sec Security Access

Name	secname	source	community	
public	ro	default	public	Edit
private	rw	localhost	private	Edit

Save & Apply Save Reset

7.5.3 Access

SNMPD Com2Sec Security Access

Groups

group	version	secname	
public	v1	ro	Edit Delete
public	v2c	ro	Edit Delete
public	usm	ro	Edit Delete
private	v1	rw	Edit Delete
private	v2c	rw	Edit Delete
private	usm	rw	Edit Delete

Add

System

Values used in the MIB2 System tree

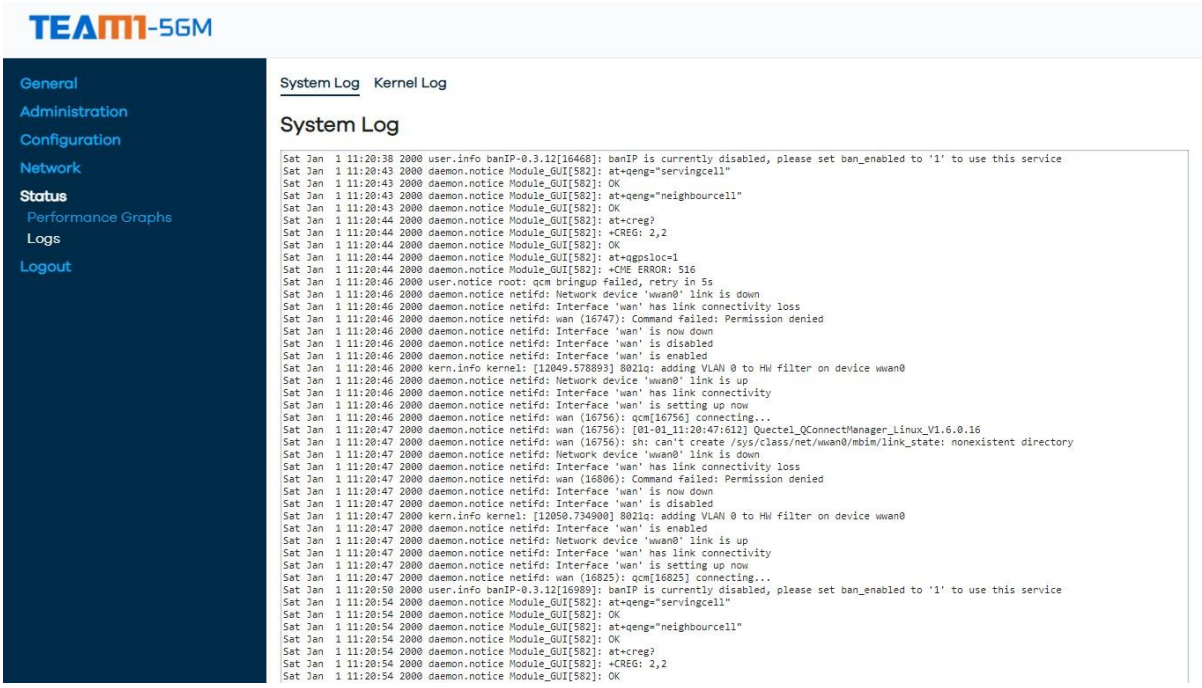
sysLocation	sysContact	sysName	
office	bofh@example.com	HeartOfGold	Edit

Save & Apply Save Reset

8 Status

8.1 Logs

There are two segments in this section, which are ‘System Log’ and ‘Kernel Log’.



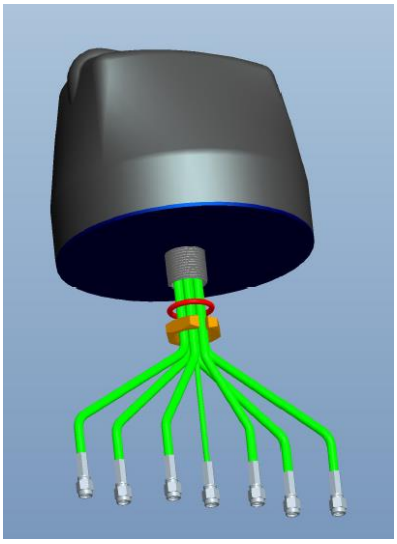
9 Logout

Click this section, the router will be logged out.

10 Appendix

10.1 Optional Enterprise 5G/4G+GNSS Integrated RF Antenna (IP69K)

5GM-ANT- M670-BB-6CG

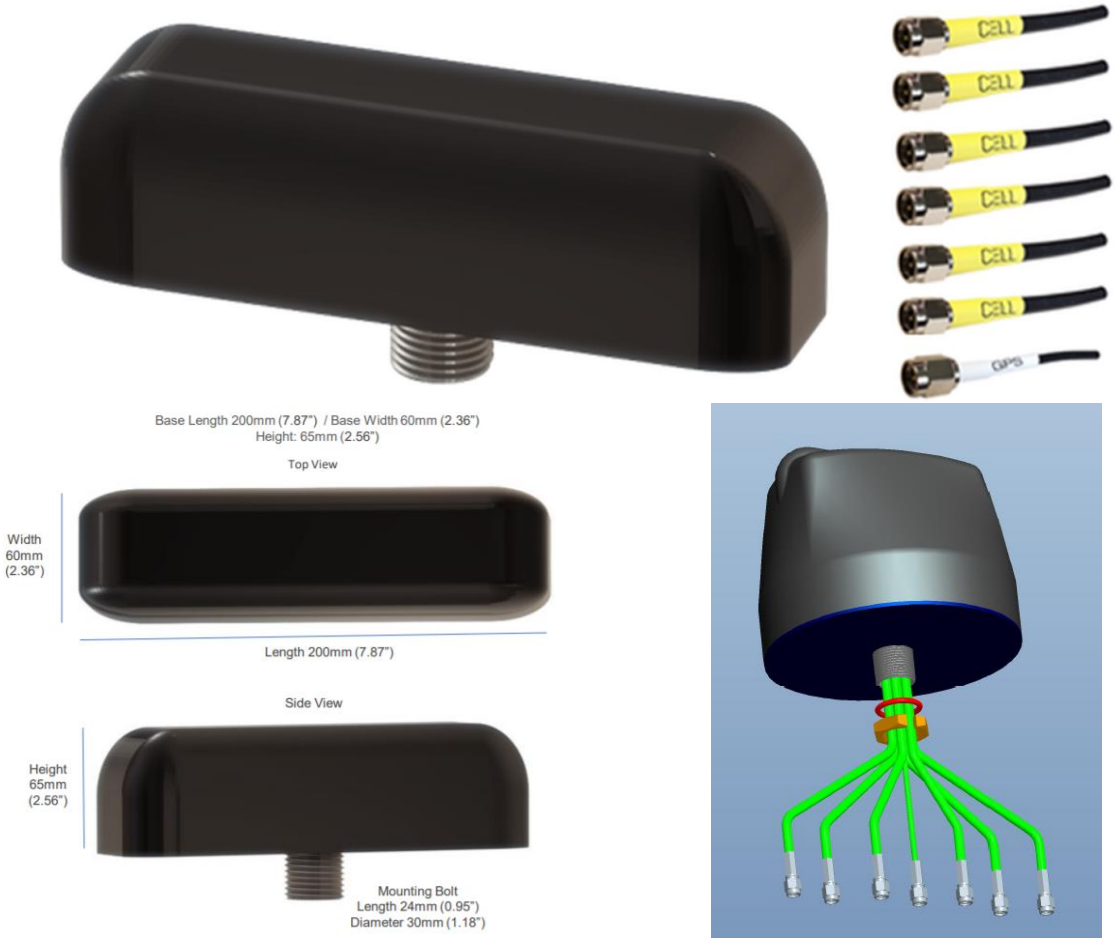


Specification / Features

- All in one 6+1 MIMO Cellular 4G/5G + GNSS/GPS
- Antenna Cellular Frequency 600 to 6000MHz
- GNSS Frequency Range 1562-1612MHz
- 50Ω Nominal Impedance
- Operation Temperature -40 to 80 °C
- IP69K Water Ingress Protection
- High Impact UV Stable ABS Polymer Antenna Housing
- Antenna Housing Height: 114mm (4.5") / Base Diameter: 140mm (5.5")

10.2 Optional Low Profile 5G/4G+GNSS Integrated RF Antenna (IP69K)

5GM-ANT- M970-BB-6CG



Specification / Features

- All in one 6+1 MIMO Cellular 4G/5G + GNSS/GPS
- Antenna Cellular Frequency 600 to 6000MHz
- GNSS Frequency Range 1562-1612MHz
- 50Ω Nominal Impedance
- Operation Temperature -40 to 80 °C
- IP69K Water Ingress Protection
- High Impact UV Stable ABS Polymer Antenna Housing
- Antenna Housing Height: 65mm (2.56”) / Base Length: 200mm (7.87”) / Base Width: 60mm (2.36”)

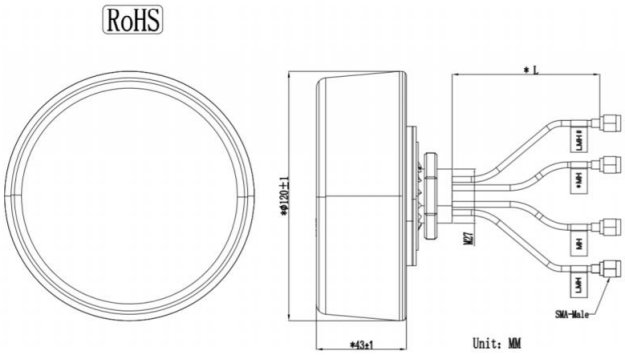
10.2.1 Mounting options for M670 and M970

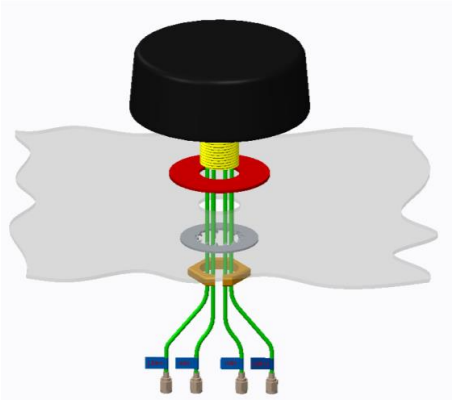
Aluminum L-Bracket Mount Kit w/U-Bolt

Adjustable Magnetic Mount Base

10.3 Optional Heavy Duty 5G/4G+GNSS Integrated RF Antenna (IP69K)

5GM-ANT- YB0007AA



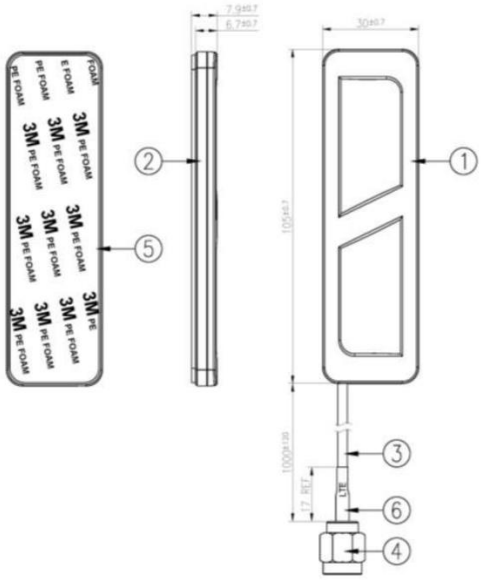


Specification / Features

- 4x MIMO Cellular 4G/5G
- Antenna Cellular Frequency 600 to 5000MHz
- 50Ω Nominal Impedance
- Operation Temperature -20 to 80 °C
- IP67 Water Ingress Protection
- KIBILAC® ASA material of Antenna Housing/shell
- Antenna Housing Height: 43mm / Base Diameter: 120mm

10.4 Optional Heavy Duty 5G/4G+GNSS Integrated RF Antenna (IP69K)

5GM-ANT- GSA.8835



Specification / Features

- Cellular 4G/5G
- Antenna Cellular Frequency 600 to 6000MHz
- 50Ω Nominal Impedance
- Operation Temperature -40 to 85 °C
- IP67 Water Ingress Protection
- PC+ABS Antenna Housing
- Antenna Housing Height: 7.9mm / Base Length: 105mm / Base Width: 30mm