Complies with IMDA Standards DA108743

TeaM1-5GM Modem/Router

TM1-5GM2020SG

USER GUIDE

Updated 07 July 2021

Page 1 | 47

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

SN	Description	Quantity	Part No.	Photo	Remarks
1.1	TeaM1-5GM Modem/Router Unit	1	TM1- 5GM2020SG	100 · · ·	
1.2	Power cable	1	5GM-H1-B		Length 1m with open ended
1.3	IO cable (Serial ports, DIOs)	1	5GM-H2-B	P	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

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

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	and a second	
2.2	Power cable	1	5GM-H1-B		Length 1m with open ended
2.3	IO cable (Serial ports, DIOs)	1	5GM-H2-B	P	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	P	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 iss Customized length and/or t	sued. 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	N	Cable length 1m and SMA terminal
Plea	ase contact supplier for	customization of	functions and accessories	S

Table of Contents

1	Overview	.6
	.1 Cellular Network Connection	.6
	.2 Protocols and Data Security	.6
	.3 Characteristic and Features	.6
2	Installation Guide and Connection	.7
	.1 Dimensions / Size / Mounting Holes	.7
	.2 Panels / External Connectors	.8
	.3 Panel LEDs	.9
	.4 Antenna Frequency Bands Information	.9
	.5 External Cables and Connector Pin Assignment1	0
	2.5.1 Panel Connector J1 and External Cable H11	0
	2.5.2 Panel Connector J2 and External Cable H21	11
	2.5.3 Panel Connector J3 and External Cable H3	2
	2.5.4 Panel Connector J4 and External Cable H4	12
	6 SIM Card Plug / Removal	13
3	System Power Lin & Setun	14
U	1 Connection Diagram	14
	2 Power Lin	
Л	General Web Portal Settings	15
-	1 Log Into Your Router Running OpenWrt	15
	2 Status Page	16
	3 Network and Granhs	17
	1 3 1 Load	17
	4.3.2 Traffic	17
	4.3.2 Trainc	. / Q
	4.3.4 Porformance Graph	0
	4.5.4 Penoimance Graph	
5	Administration	. ອ >∩
5	Authinistiation	20
		20
	5.2.1 Stops to Access The Modern Operating System Using SSU:	20
	3.2.1 Steps to Access The Modern Operating System Using SST	- T 2 /
		24)/
G	.4 Laliyuaye	24)5
0	Connyulation2	20
	6.1.1 bonID Configuration Ontions	20
	6.1.2 Logging of Bonnod Bookets	20
		10 70
		-7 7
	6.2.2 LED Configuration for Signal Strangth	-7 7
	6.2.2 LED Configuration for Signal Strength	-1 7
	0.2.3 MOde	27
	.5 SelOverivel	29
		29
		19
		51
	0.3.4 LINKS	<u>></u> د
-	0.3.5 KemoteGPIU	54 57
1		55
	.1 LAN	55
		55
	7.1.2 Edit LAN Setting	56
	7.1.3 DHCP Server	37
	7.1.4 Static Routes	37

72 W/	AN	38
721	Port Forward	30
72 Eir	owoll	40
7.3 11	Conorol Sotting	
7.3.1		
7.3.2	I raffic Rules	
7.3.3	NAT Rules	
7.4 uH	TTPd	41
7.4.1	Features	41
7.4.2	Configuration	41
7.5 SN	IMPD	
7.5.1	SNMPD	
7.5.2	Com2Sec	
7.5.3	Access	
8 Status		43
8.1 Lo	gs	43
9 Logout	~	43
10 Appen	dix	
10.1	Optional Enterprise 5G/4G+GNSS Integrated RF Antenna (IP69K)	
10.2	Optional Low Profile 5G/4G+GNSS Integrated RE Antenna (IP69K)	45
10.2.1	Mounting options for M670 and M970	46
10.2.1	Intional Heavy Duty 5G/AG+GNSS Integrated RF Antenna (IP60K)	0+ ۸۸
10.0	Optional Heavy Duty 50/40+0100 integrated RE Antenna (IP09K)	4040
10.4	Julional rieavy Duty 50/46+6135 integrated KF Antenna (IP09K)	

Table 1: Panel Connectors	8
Table 2: Panel Connectors and External Cable	
Table 3: Panel Connectors J1 and External Cable H1	
Table 4: Panel Connectors J2 and External Cable H2	
Table 5: Panel Connectors J3 and External Cable H3	
Table 6: Panel Connectors J4 and External Cable H4	

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 3G/4G will automatically fallback to 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



2.2 Panels / External Connectors



Table 1: Panel Connectors

SN	Description	Remarks
ANT3	5G Antenna 1, SMA 50 Ω	
ANT4	5G Antenna 2, SMA 50 Ω	
ANT5	5G Antenna 3, SMA 50 Ω	4x4 MIMO, N77776/79 SGNR
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	
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
мімо	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 $\pm 2/3$ 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 [®] Class 2 (26 dBm +2/-3 dB) for 5G NR n41/n77/n78 bands HPUE [®]
--------------	---	---

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

2.5.2 Panel Connector J2 and External Cable H2

Panel C	onnector		Cable connector	Cable
J2: D389	999/24WD35SN	Signal Description	D38999/26WD35PN	labelling
Pin No.			Pin No.	
Pin 1	RS422 connection	RS422A (RX+)	Pin 1	1
Pin 2	from	RS422B (RX-)	Pin 2	2
Pin 4	TeaM1- 5GM	RS4222 (1X-)	Pin 4	4
Pin 5		RS422Y (1X+)	Pin 5	5
Pin 18	RS485 connection	RS485A (D+)	Pin 18	18
Pin 19		RS485B (D-)	Pin 19	19
Pin 20	RS232-1 connection	DGND	Pin 20	20
Pin 21	from TeaM1- 5GM	RS232-1-TXD	Pin 21	21
Pin 22		RS232-1-RXD	Pin 22	22
Pin 23	RS232-2 connection	DGND	Pin 23	23
Pin 24	from TeaM1- 5GM	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.	Input 0	Pin 28	28
Pin 29	VIH > 6V	Input 1	Pin 29	29
Pin 32	VIL < 4V	Input 2	Pin 32	32
Pin 33	9~48V.	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	Vout L1	Pin 7	7
Pin 9	TeaM1	Vout L2	Pin 9	9
Pin 11	5GM.	Vout_L3	Pin 11	11
Pin 13	Max. Current: 0.5A @ 48V	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.	WARN EXT2, warning signal	Pin 14	14
Pin 15*	LVCMOS3.3V output.	Data_safety_Ext, data safety warning signal	Pin 15	15
Pin 16*	*Do not connect. ** Contact supplier if	HB_EXT, heart-beating signal, device health condition	Pin 16	16
Pin 17*	required	Warn_EXT1, warning signal	Pin 17	17
			P	

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

2.5.3 Panel Connector J3 and External Cable H3

Panel Connector			Cable connector		
J3: MRJ	R-8F81-01	Signal Description	RJ45 plug	Cable labelling	
Pin No.			Pin No.		
Pin 1		BI_DA+	Pin 1	Whit/green	
Pin 2	Gigabit Ethornot	BI_DA-	Pin 2	Green	
Pin 3	Connection. Cat.5e or Cat.6 cable.	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	
C	J3	*RJ45 water-proof accessory available upon request.	Contraction of the second seco		

Table 5: Panel Connectors J3 and External Cab	ole H3
---	--------

2.5.4 Panel Connector J4 and External Cable H4

Table 6: Panel Connectors J4 and External Cable H4

Panel Connector			Cable connector		
J3: MUSBR-E151-30		Signal Description	Mini-USB-AB plug	Cable labelling	
Pin No.			Pin No.		
Pin 1		USB_VBUS	Pin 1		
Pin 2	USB cable	USB_D-	Pin 2		
Pin 3		USB_D+	Pin 3		
Pin 4		USB_DGND	Pin 4		
0	4	*Mini-USB waterproof accessory available upon request.			

2.6 SIM Card Plug / Removal



Ш

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 <u>http://192.168.1.1/</u>. At that page you should see a login page: (correct as of Barrier Breaker)

TEAM1-5GM		
No password set! There is no password set on this router. Please configure a root passw	vord to protect the web interface.	
Authorization Required		
Please enter your username and password.		
Username	root	
Password	[]
		Login Reset

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.

TEAM1-5GM					Refreshing
General Overview Network Graphs Device List Administration Configuration Network	No password s There is no passwo Status System Inform	et! rd set on this router. Pl nation	lease configure a root passwo	rd to protect the web interface.	
Status	Model		TI AM5716 Modem		
Logout	Serial Number		ARMv7 Processor rev 2 (v7l)		
	Firmware Version			ab1b7dd9 / LuCI Master git-20.302.26354-bb62854	
	Local Time		2000-01-04 02:08:19		
	Uptime		2d 18h 8m 22s		
	Memory Usag	e			
	Total Available		774.91 MB / 99910 MB (77%)		
	Used		233.79 MB / 999.10 MB (23%)		
	Buffered		5.21 MB / 999.10 MB (0%)		
	Cached		55.60 MB / 999:10 MB (5%)		
	Network				
	Active Connections			86 / 16384 (0%)	
	Active DHCP L	eases			
	Hostname	IPv4-Address	MAC-Address	Lease time remaining	
	-	192.168.1.143		11h 48m 56s	
	-	192.168.1.115		11h 39m 30s	
	Active DHCPv	6 Leases			
	Host	IPv6-Address	DUID	Lease time remaining	9
				11h 48m 49s	
				5h 46m 42s	

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.

TEAM1-5GM						Refreshing
General Overview Network Graphs Device List	Load <u>Traffic</u> Conne eth0 usb0 wwan0	ections Performance (eth1	Əraphs			
Administration	3m		2m		Im	1
Configuration						
Network	2.34 MbH/s (300.00 KE/s)					
Status						
Logout	1.68 Misi/s (200.00 (Gl/s)					
	800.00 Kbit/s (100.00 KB/s)					
					(3 minute wi	ndow, 8 second intervo
	Inbound:	15.22 Kbit/s (1.90 KB/s)	Average:	10.30 Kbit/s (1.29 KB/s)	Peak:	322.32 Kbit/s (40.29 KB/s)
	Outbound:	4.99 Kbit/s (639 B/s)	Average:	52.22 Kbit/s (6.53 KB/s)	Peak:	2.93 Mbit/s (374.99 KB/s)

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.

TEATT1-5GM						Refreshing
General Overview	Load Traff	ic Connect	ions Performance Graphs			
Network Graphs		3m		2m	1m	
Administration	75					
Configuration						
Network	50					
Status	50					
Logout						
	25					
					(3 minu	ute window, 3 second interval)
			0	Average: 67		Poak: 90
		TOP: 0		Average: 07	F	Peak: 6
		Other 0	, ,	Average: 3		
		Other: 0)	Average: 0	ŀ	eak: 0
						Enable DNS lookups
	Network	Protocol	Source		Destination	Transfer
	IPV4	TCP	192.168.1.143:51129		192.168.1.1:443	363.14 KB (702 Pkts.)
	IPV4	TCP	192.168.1.143:51148		192.168.1.1:443	109.78 KB (90 Pkts.)
	IPV4	TCP	192.168.1.143:51146		192.168.1.1:443	93.38 KB (86 Pkts.)
	IPV4	TCP	192.168.1.143:51147		192.168.1.1:443	43.02 KB (49 Pkts.)
	IPV4	TCP	192.168.1.143:51149		192.168.1.1:443	2.97 KB (13 Pkts.)
	IPV6	UDP	[fd7b:bbf6:7767:0:8c50:775f:5	658:3605]:57186	[fd7b:bbf6:7767::1]:53	776 B (8 Pkts.)
	IPV6	UDP	[fd7b:bbf6:7767:0:8c50:775f:5	658:3605]:59220	[fd7b:bbf6:7767::1]:53	776 B (8 Pkts.)
	IPV6	UDP	[fd7b:bbf6:7767:0:8c50:775f:5	658:3605]:58792	[fd7b:bbf6:7767::1]:53	776 B (8 Pkts.)
	IPV6	UDP	[fd7b:bbf6:7767:0:8c50:775f:5	658:36051:59301	[fd7b:bbf6:7767::11:53	776 B (8 Pkts.)

4.3.4 Performance Graph

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





TEATTI-5GM



4.4 Device List

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

TEATTI-5GM					
General Overview Network Graphs	Connected De	vices	MAC-Address	Lease time remaining	
Device List Administration		192.168.1.143		11h 40m 11s	
Configuration					
Network Status					
Logout					

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.

TEAM-5GM					
General Administration	The system password has been successfully changed	d.	Dismiss		
System Upgrade and Restore	Router Password SSH Access SSH-Keys Logging	Language			
Reboot	Router Password				
Network	Changes the administrator password for accessing the device				
Status	Password				
Logout	Confirmation	••••••			
		Password strength: Weak			
			Save		

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.

General	Router Password SSH Access SSH-Keys	Logging Language	
Administration System	SSH Access		
Upgrade and Restore Reboot	Dropbear offers SSH network shell access and ar	n integrated SCP server	
Configuration	Dropbear Instance		
Network	and and		Delete
Status	Interface	unspecified	Tified on all
Logout	Port		
	Password authentication	wan:	
	Allow root logins with password	 Allow the root user to login with 	password
	Gateway Ports	Allow remote hosts to connect to	b local SSH forwarded ports
	Add instance		

5.2.1 Steps to Access The Modem Operating System Using SSH:

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.

Adapter connection. Oser can install the driver norm the

- 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

← Settings	
ம் Home	Windows Update
Find a setting	You're up to date
Update & Security	Check for updates
C Windows Update	View optional updates
当 Delivery Optimization	Pause updates for 7 days Visit Advanced options to change the pause period
Windows Security	san consistent abran in entrille nut home betten
T Backup	Change active hours Currently 8:00 AM to 5:00 PM
C Troubleshoot	See update history See updates installed on your device

- f. Expand the "Driver updates" category
- g. Tick "USB Ethernet/RNDIS Gadget"

← Settings	_		×
命 Optional updates			
Choose the updates you want and then select Download and install.			
\checkmark Driver updates			
If you have a specific problem, one of these drivers might help. Otherwise, automatic updates wi up to date.	ll keep y	our driv	ers
INTEL - System - 1/1/1970 12:00:00 AM - 10.1.1.42			
Intel Corporation - Display - 26.20.100.7463			
NVIDIA - Display - 26.21.14.4137			
Acer Incorporated Other hardware - USB Ethernet/RNDIS Gadget			
Download and install			

- 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.

Real PuTTY Configuration		? ×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Basic options for your PuTTY set Specify the destination you want to connect Host Name (or IP address) 192.168.1.1 Connection type: Raw Ielnet Rlogin SSH Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never Only on close	ssion ct to <u>Port</u> 22 Serjal <u>Load</u> <u>Save</u> <u>D</u> elete
<u>A</u> bout <u>H</u> elp	<u>O</u> pen	<u>C</u> ancel

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

ß	192.168	.1.1 - F	PuTTY					\times
2	login	as:	root					\sim
								~

6. Enter the password

🖉 192.168.1.1 - PuTTY		×
🚰 login as: root 🛃 root@192.168.1.1's password: 🗧		^
		\sim

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.

TEAM1-5GM				Unsaved Changes: 9
General	Router Password SSH Access SSH-Keys Logging	Language		
Administration System	Logging			
Upgrade and Restore	System log buffer size	64		
		kiB		
Configuration Network	External system log server	0.0.0.0]	
Status	External system log server port	514		
Logout	External system log server protocol	UDP	~	
	Write system log to file	/tmp/system.log		
	Log output level	Debug	~]	
	Cron Log Level	Debug	~]	
	2		Save & A	pply - Save Reset

5.4 Language

Time zone and Language settings.

TEAM1-5GM				Unsaved Changes: 9
General Administration	Router Password SSH Access SSH-Keys Logging	Language		
System	Language and Style			
Reboot	Local Time	1/1/2000, 9:34:12 AM		
Configuration		Sync with browser	Sync with NTP-Server	
Network	Timezone	Asia/Singapore	v]	
Status	Language	auto		
Logout	×			
			Save & App	ly • Save Reset

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.

ТЕАПП-56М		
General	Overview IPSet-Lookup RIPE-Lookup View Logfile	e Advanced
Administration	IP Filter	
Configuration banIP	Enable IP Filter	
Cellular SerOverNet RemoteGPIO	Automatic WAN Interface Detection	0
Network		Save & Apply
Status		
Logout		

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

TEAM-5GM			
General Administration Configuration	General LED Configuration Mode	10	
baniP Cellular SerOverNet RemoteGPIO			Save & Apply V Save
Network			
Status Logout			

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

ТЕАПП-56М					
General Administration	General LED Configu	ration Mode			
Configuration	Name	Weak	Medium	Strong	
baniP	4G	-93	-86	-80	Edit
Cellular SerOverNet RemoteGPIO	5G	-93	-86	-80	Edit
Network					
Status					
Logout					

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

TEATTI-5GM				
General	General LED Configuration Mode			
Administration	Mode:	AUTO	~	
Configuration banIP	Enable:	Enable ALL	~	
Cellular SerOverNet				
RemoteGPIO				ave Reset
Network				
Status				
Logout				

TEAM1-5GM			
General Administration	General LED Configuration Mode		
Configuration banIP Cellular SerOverNet RemoteGPIO	Enable:	AUTO NR5G LTE WCDMA	Save & Apply 🔹 Save Reset
Network Status			
Logout			

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

TEAM1-5GM			
General	General LED Configuration Mode		
Administration	Mode:	AUTO	.
Configuration banIP Cellular SerOverNet	Enable:	Enable ALL Enable ALL Disable SA	
RemoteGPIO		Disable NSA	Save & Apply V Save Rese
Status			
Logout			

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).

TEATT1-5GM										Unsaved Changes: 1
General Administration Configuration banIP Cellular SerOverNet RemoteGPIO	SerOv Genera Globals: Reconner	erNe al ct Inter (>=0):	ə t val (>=0):			globals 15 180	5			
Network Status	Serial									
Logout	Name		Device	Ba	ud Rate	Data Bits	Stop E	Bits Parity	DE/RE	
	RS232_2		/dev/ttyS4	115:	200	8	1	NOPARIT	Y -1	
	RS485		/dev/ttyS1	115:	200	8	1	NOPARIT	Y 77	Edit
	RS422		/dev/ttyS3	115:	200	8	1	NOPARIT	Y 238	Edit
	Nets									
	Nets	Туре	Local Port	SSL	SSL Verify	Cert File	CA File	Remote Address	Remote Port	
	Client1	top	0	false	false	client.pem	server.crt	128.106.109.191	50000	Edit Delete
	Client2	tcp	123	false	false	123	123	123	123	Edit Delete
	Client3	top	12312	false	false	12312	12321	123	12312	Edit Delete
	Add									
	Links									
	Name		Serial		Net		In Use			
	LINK1		RS232_1		Client	1	true			Edit Delete
	LINK2		RS232_2		Client	:1	true			Edit Delete
	LINK3		RS422		Client	:1	true			Edit Delete
	LINK4		RS485		Client	1	true			Edit Delete
	Add									
									Save & App	oly - Save Reset

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	E Edit
RS232_2	/dev/ttyS4	115200	8	1	NOPARITY	-1	E Edit
RS485	/dev/ttyS1	115200	8	1	NOPARITY	77	E 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

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.

Nets	Туре	Local Port	SSL	SSL Verify	Cert File	CA File	Remote Address	Remote Port	
Client1	tcp	0	false	false	client.pem	server.crt	128.106.1	50000	Edit Delete
Add									

Steps to set Net for serial port

1. Click 'Add' button

SerOverNet	
Nets	[
Туре	Please choose
Local Port	
SSL	Please choose
SSL Verify	Please choose
Cert File	[
CA File	
Remote Address	
Remote Port	[

2. Set the name of the Net

SerOverNet	
Nets	Name_of_the_net
Туре	Please choose •
Local Port	[
SSL	Please choose •
SSL Verify	Please choose 🔻
Cert File	[
CA File	
Remote Address	
Remote Port	

3. Select type of the Net

	Please choose	•
Please	choose	
tcp		
tcp6		
udp		
udp6		
tcp-lister	ı	
tcp6-liste	en	
udp-liste	n	
udp6-list	en	
custor	n	

4. Set the local port

SerOverNet	
Nets	Name_of_the_net
Туре	tcp
Local Port	Your_local_port
SSL	Please choose
SSL Verify	Please choose
Cert File	
CA File	
Remote Address	
Remote Port	

5. Set SSL, SSL verify if needed (here leave it as default)

6. Set the Cert File and CA File is needed

SerOverNet	
Nets	Name_of_the_net
Туре	tcp
Local Port	Your_local_port
SSL	Please choose
SSL Verify	Please choose
Cert File	client.perm
CA File	server.crt
Remote Address	128.108.xxx.xxx
Remote Port	xxxx

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

SerOverNet	
Name	[Link1
Serial	Please choose
Net	Please choose
In Use	Please choose

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

SerOverNet		
Name	Link1]
Serial	R\$232_1	•
Net	Please choose	•
In Use	Please choose	•]

3. Assign a Net for the serial port

SerOverNet		
Name	Link1	
Serial	R\$232_1	•
Net	Client1	•
In Use	Please choose	•

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

SerOverNet		
Name	Link1	
Serial	R\$232_1	•]
Net	Client1	•
In Use	true	•

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

Links

Name	Serial	Net	In Use	
LINK1	RS232_1	Client1	true	Edit Delete
LINK2	RS232_2	Client1	true	Edit Delete
LINK3	R\$422	Client1	true	Edit Delete
LINK4	RS485	Client1	true	Edit Delete



6.3.5 RemoteGPIO

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

TEAM1-5GM			
General	Input/ Output		
Administration	Configuration - RemoteGPIO		
baniP	Input		
SerOverNet	Values Rendered Below are the updated values of	/sys/class/gpio/gpia\$(num)/value	
RemoteGPIO	INPUTO		
Status	Name	INPUTO	
Logout	Num	480	
	Value	1	
	INPUT1		
	Name	INPUT1	
	Num	481	
	Value	1	
	INPUT2		
	Name	INPUT2	
	Num	482	
	Value	1	
	INPUT3		
	Name	INPUT3	
	Num	483	
	Value	1	

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

Name	Value	
VOUT1	1	Edit
VOUT2	1	Edit
VOUT3	0	Edit
VOUT4	0	Edit

Save

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.

TEATTI-5GM		
General Administration	LAN Static Routes	
	Network - LAN	
Add new interface	Drotood Statio address	
Name	New interface name	e
Protocol	DHCP client	
Bridge interfaces	Oreates a bridge over specified interface(s)	
Interface	unspecified •	et l
		Cancel Create interface
		_
Add new interface		
Name	New interface name	
Protocol	DHCP client 🗸	
Bridge interfaces	DHCP client MBIM Cellular PPP	
Interface	DHCPv6 client PPPoE	
	QCM Cellular	Cancel Create interface
	Static address Unmanaged	

Add new interface		
Name	New interface name	
Protocol	DHCP client	~
Bridge interfaces	Creates a bridge over specified interface(s	(e)
Interface	unspecified	•
	unspecified	
	Ethernet Adapter: "eth0" (lan) Ethernet Adapter: "usb0" (usb)	
	Ethernet Adapter: "wwan0"	
	🖉 Ethernet Adapter: "eth1"	
	🔝 Alias Interface: "@lan"	
	🛃 Alias Interface: "@usb"	
	🖉 Alias Interface: "@wan"	
	custom	

7.1.2 Edit LAN Setting

Detail refers to official document

TEAM-5GM	
General LAN Static Routes Administration Configuration	
Interfaces » LAN	
General Settings Advanced Settings Physical Settings Firewal	Il Settings DHCP Server
Status	Device: eth0 Uptime:1h:2m:8a MAC: 94 E3 e5D:08:D58:00 ₹ RX: 30:00 Ficts.) TX: 1722 MB (2000 Ficts.) TX: 1722 MB (2000 Ficts.) TV: 1722 MB (2000 Ficts.) TV: 1725 MB (2000 Fic
Protocol	Static address 🔹
Bring up on boot	•
IPv4 address	192.168.1.1
IPv4 netmask	255,255,0
IPv4 gateway	
IPv4 broadcast	1921681.255
Use custom DNS servers	•
IPv6 assignment length	60 •
	Assign a part of given length of every public IPv6-prefix to this interface
IPv6 assignment hint	
IPv6 suffix	Assign prefix parts using this nexadecimal subpremult for this interface. [±1] Optional. Allowed values: 'eui64', 'random', fixed value like ':1' or :::12'. When IPv6 prefix (like 'abcd::) is received from a delegating server, use the suffix (like ':1') to form the IPv6 address ('abcd::') for the IPv6 address ('abcd::')
	Dismiss Save

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:

. Choose an interface for	the static route.	
General Settings Advanced Settings		
Interface	lan: 🛃	•
arget	lan: 🖉	
∂v4-Netmask	wan: 100 200.200.200.0	
	if target is a network	
⁵ v4-Gateway	192.168.1.1	
		Dismiss

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

Add new interface	
Name	Name_interface
Protocol	QCM Cellular

- 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:

Interraces » WAN		
General Settings Advanced Settings Firewall Settings		
Status	Device: qom-won RX: 0 B (0 Picts.) TX: 0 B (0 Picts.)	
Protocol	QCM Cellular	~
Bring up on boot		
Modem device	/dev/cdc-wdm0	•]
IFname	wwan0]
APN	sunsurf]
PIN)
Authentication Type	NONE	~]
PDP Type	IPv4	~

- 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 LuCl interface (Network \rightarrow WAN \rightarrow 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.

TEAM1-5GM					
	WAN Port Forwards	Match		Action	Enable
- Unnamed forward					
General Settings Advanced Settin	gs				
Name		Unnamed forwa	ird]	
Protocol		TCP	UDP	•]	
Source zone		wan won:		•	
External port					
		Match incoming tr	affic directed	at the given des	stination port or port range on this host
Destination zone		lan lan: 🧾 usb: 🖉)	•	
Internal IP address			any	•]	
Internal port		Redirect matched	incoming traff	ic to the specifi	ed internal host
		Redirect matched	incomina trafi	; ic to the aiven r	port on the internal host
					Dismiss

7.3 Firewall

7.3.1 General Setting

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

TEAM-5GM									
General Administration Configuration Network LAN WAN	General Settings Traffic R Firewall - Zone Set The firewall creates zones over General Settings	ules NAT Rul tings ryour network in	es nterfo	ces to cont	trol netw	ork traffic flo	SW:		
Firewall uHTTPd	Enable SYN-flood protectio Drop invalid packets	n		0					
Status	Input			9	accept			~	
Logodi	Forward				accept reject			~	
	Routing/NAT Offloa Experimental feature. Not fully	ding compatible wit	:h QoS	/SQM.					
	Software flow offloading) Software	based offloo	iding f	or routing/NAT	
	Zones								
	Lone ⇒ Forwardings	accept	•]	accept	•]	accept	*		Edit Delete
		reject	~	accept	~	reject	*	۲	
								Save 8	Apply V Save Reset

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 <u>running Lua in-process</u>, 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 <u>UCI</u>, 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 <u>the uHTTPd UCI configuration page</u>. 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 Com2	Sec 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	vl	ro	Edit Delete
public	v2c	ro	Edit Delete
public	usm	ro	Edit Delete
private	vl	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'.

General	System Log Kernel Log
Administration	System Log
Configuration	Cystam Log
Network	Sat Jan 1 11:20:38 2000 user.info banIP-0.3.12[16468]: banIP is currently disabled, please set ban_enabled to '1' to use this service Sat Jan 1 11:20:43 2000 doemon.notice Hoolub_GUI[582]: at-genge"servingcell"
Status	Sat Jan 1 11:20:43 2000 daemon.notice Module_UUI[362]: UK Sat Jan 1 11:20:43 2000 daemon.notice Module GUIFS821: at-genge"neighbourcell"
D. (Sat Jan 1 11:20:43 2000 daemon.notice Module_GUI[582]: OK
Performance Graphs	Sat Jan 1 11:20:44 2000 daemon.notice Module_GUI[582]: at+creg?
Logs	Sat Jan 1 11/20:44 2000 daemon.notice Module_OU[S2]: +CRkG: 2,2
	Sat Jan 1 11:20:44 2000 deemon.notice Module GUISS21: at+gosloc=1
Logout	Sat Jan 1 11:20:44 2000 daemon.notice Module GUI[582]: +CME ERROR: 516
	Sat Jan 1 11:20:46 2000 user.notice root: qcm bringup failed, retry in 5s
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: Network device 'wwan0' link is down
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: Interface 'wan' has link connectivity loss
	Sat Jan 1 11:20:46 2000 daemon.notice netifid: wan (16/4/): command railed: Permission denied
	Sat Jan 1 11:20:40 2000 definition definition anternace wan' is disabled
	Sat Jan 1 11:20:46 2000 deamon.notice netifd: Interface 'wan' is enabled
	Sat Jan 1 11:20:46 2000 kern.info kernel: [12049.578893] 8021q: adding VLAN 0 to HW filter on device wwan0
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: Network device 'wwan0' link is up
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: Interface 'wan' has link connectivity
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: Interface 'wan' is setting up now
	Sat Jan 1 11:20:46 2000 daemon.notice netifd: wan (16756): qcm[16756] connecting
	Sat Jan 1 11:20:47 2000 Gaemon.notice netific wan (16/56); [01-01_11:20:47:612] Quectel_QConnectWanager_Linux_V.6.0.16
	Sat Jan 111:20:47 2000 datmini.notice metrid: Wah (10/20) sh. chi ci ce et / systemssinet/wwahd/moin/infin/ink_state. Honexisten: directory
	Sat Jan 1 11:20:47 2000 daemon.notice netifd: Interface 'wan' has link connectivity loss
	Sat Jan 1 11:20:47 2000 daemon.notice netifd: wan (16806): Command failed: Permission denied
	Sat Jan 1 11:20:47 2000 daemon.notice netifd: Interface 'wan' is now down
	Sat Jan 1 11:20:47 2000 daemon.notice netifd: Interface 'wan' is disabled
	Sat Jan 1 11:20:47 2000 kern.info kernel: [12050.734900] 8021q: adding VLAN 0 to HW filter on device wwwan0
	Sat Jan 1 11:20:47 2000 daemon.notice netida: Internace wan' is enabled
	Sat Jan 1 11/2014/ 2000 daemon.notice netifa: Network device 'wwand' ink is up Sat Jan 1 11/2014/ 2000 daemon.notice netifa: Interface 'wan' has link connectivity
	Sat Jan 1 11:20:47 2000 demon.notice netifici. Interface 'wan' is setting un now
	Sat Jan 1 11:20:47 2000 daemon.notice netifd: wan (16825); gcm[16825] connecting
	Sat Jan 1 11:20:50 2000 user.info banIP-0.3.12[16989]: banIP is currently disabled, please set ban_enabled to '1' to use this service
	Sat Jan 1 11:20:54 2000 daemon.notice Module_GUI[582]: at+qeng="servingcell"
	Sat Jan 1 11:20:54 2000 daemon.notice Module_GUI[582]: OK
	Sat Jan 1 11:20:54 2000 daemon.notice Module_GUI[582]: at+qeng="neighbourcell"
	Sat Jan 1 11/20154 2000 daemon.notice Module_UUL[Sat]: UK
	Sat Jan 1 11:00:54 2000 deemon.httl:t Puoude_uoujacj: artitegr
	Sat Jan 11:20:54 2000 daemon notice Module GUTSA21: 0K

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")

10.2.1Mounting options for M670 and M970

Aluminum L-Bracket Mount Kit w/U-Bolt



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