



ELPRO Technologies
645M-4
Industrial Cellular & WiFi IIoT Router
User Manual
V1.1



Table of Contents

1.	Product Introduction.....	6
1.1.	Product overview	6
1.2.	Application use.....	6
1.3.	Features.....	6
2.	Hardware Installation	7
2.1.	Ports	7
2.2.	Mounting.....	8
2.3.	Power up and SIM Card.....	8
2.4.	Grounding	8
2.5.	Terminal block	9
2.6.	Power Supply.....	10
2.7.	LED Description	10
3.	Modem configuration	11
3.1.	Overview	11
3.2.	How to log into the Router.....	11
3.3.	Log into the router	12
4.	Router status	12
4.1.	Status overview.....	12
4.2.	Network status.....	13
4.3.	Firewall status	14
4.4.	Routes	15
4.5.	System log	15
4.6.	Kernel log	15
	Realtime graphs	16
5.	System Configuration.....	17
5.1.	Setup wizard.....	17
5.2.	System	19
5.3.	Password	20
5.4.	NTP	20
5.5.	Backup/Restore	21
5.6.	Upgrade.....	21
5.7.	Reset.....	22
5.8.	Reboot.....	23
6.	Services configuration.....	23
6.1.	ICMP check.....	23
6.2.	VRRP	24
6.3.	Failover (link backup)	25
6.4.	DTU.....	26
6.5.	SNMP.....	28
6.6.	GPS	29
6.7.	SMS	30
7.	VPN.....	34
7.1.	IPSEC.....	34
7.2.	PPTP	35

7.3.	L2TP	36
7.4.	OpenVPN	37
7.5.	GRE tunnel.....	38
7.6.	DDNS	39
7.7.	Connect Radio Module.....	40
8.	Network Configuration.....	41
8.1.	Operation Mode.....	41
8.2.	Mobile configuration.....	42
8.3.	Cell mobile data limitation	43
8.4.	LAN settings.....	44
8.5.	Wired-WAN	46
8.6.	WiFi Settings.....	47
8.7.	WiFi General configuration	47
8.8.	WiFi Advanced Configuration.....	48
8.9.	WiFi Interface Configuration	48
8.10.	WiFi AP client	50
8.11.	Interfaces Overview	52
8.12.	Firewall	52
8.13.	Port Forwards.....	53
8.14.	Traffic rules.....	54
8.15.	DMZ.....	56
8.16.	Security.....	56
8.17.	Static Routes.....	57
8.18.	Switch	57
8.19.	DHCP and DNS.....	58
8.20.	Diagnostics	59
8.21.	Loopback Interface.....	59
8.22.	Dynamic Routing	60
8.23.	QoS.....	61
9.	Specifications	62

Copyright © ELPRO TECHNOLOGIES 2019

ELPRO is a registered trademark of ELPRO Technologies. Other brands used in this manual are trademarks of their registered holders.

Specifications are subject to change without notice. No part of this manual may be reproduced without the consent of ELPRO Technologies. All rights reserved.

ELPRO reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to. Performance data indicates typical values related to the particular product. Product updates may result in differences between the information provided in this manual and the product shipped. For access to the most current product documentation and application notes, visit www.elpro.com.au. Products offered may contain software which is proprietary to ELPRO. The offer or supply of these products and services does not include or infer any transfer of ownership.

WARNING:

Maintain a distance of at least 20 cm (8 inches) between the transmitter antenna and any person while in use. This modem is designed for use in applications that observe the 20 cm separation distance.

Interference issues:

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized
- Do not operate in locations where medical equipment or devices that the device could interfere with may be in use
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers

Mobile application safety

- Do not change parameters or perform other maintenance of the ELPRO 645M while driving
- Road safety is crucial. Observe National Regulations for cellular telephones and devices in vehicles
- Avoid potential interference with vehicle electronics by correctly installing the ELPRO 645M modem. ELPRO recommends installation by a professional

Follow instructions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment. Practice all plant and safety instructions and precautions. Failure to follow the instructions can cause personal injury and/or property damage.

Proper use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (1) constitute "misuse" and/or "negligence" within the meaning of the product warranty, thereby excluding warranty coverage for any resulting damage; and (2) invalidate product certifications or listings.

Product disposal

When your product reaches the end of its useful life, it is important to take care in the disposal of the product to minimize the impact on the environment.

Responsible disposal of equipment

Please consider the environment when disposing of this product at end of service life. This product contains recyclable materials and should be disposed through local electronics recycling facility.

Europe

In Europe, you can return the product to the place of purchase to have the product disposed in accordance with EU WEEE legislation.

Deployment of ELPRO products in customer environment

There is increasing concern regarding cybersecurity across industries, where companies are steadily integrating field devices into enterprise-wide information systems. This is why ELPRO has incorporated secure development life cycle in their product development to ensure that cybersecurity is addressed at all levels of development and commissioning of our products.

There is no protection method that is completely secure. Industrial Control Systems continue to be the target for attacks. The complexities of these attacks make it very difficult to have a complete secure system. A defence mechanism that is effective today may not be effective tomorrow as the ways and means of cyber-attacks constantly change. Therefore, it's critical that our customers remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerability of their products and systems in their environment.

At ELPRO we are focusing on analysing emerging threats and ensuring that we are developing secure products and helping our customers deploy and maintain our solutions in a secure environment. We continue to evaluate cybersecurity updates that we become aware of and provide the necessary communication on our website as soon as possible.

Release notice

This is the update release of the 645M-1 Cellular and WiFi IIoT Router, which applies to firmware version 3.2.208.

1. Product Introduction

1.1. Product overview

The ELPRO Technologies 645M-4 is an LTE CAT-1 industrial grade 3G/4G/4GX WiFi Modem Router, based on the latest OpenWrt platform. This low-cost and low-power LTE CAT-1 router, with download speeds of up to 10Mbps and upload speeds of up to 5Mbps, is an ideal replacement to 3G devices. This allows a smooth migration from 3G to 4G LTE, with the benefits of a lower latency and a much better network coverage.

The ELPRO Technologies 645M-4 is designed to suit Industrial applications. It is one of the few routers with wide Frequency Band allocation including the support of band B28 (700MHz). It enables users to quickly create a secure and fast wireless network. It features a built-in WiFi N300 with speeds of up to 300 Mbps, one Ethernet WAN port for fixed internet connection and one Ethernet LAN port, as well as a GPIO with four digital output ports. Other features include VPN IPSEC, PPTP, L2TP and Open VPN to establish a secure connection over the 3G/4G network.

The durable and rugged design makes the 645M-4 the router of choice for remote harsh environments. The compact design, easy integration and advanced built-in features make it suitable for a wide range of industrial M2M applications, including industrial automation, building automation, smart metering, security, surveillance, transportation, health, mining and environmental monitoring.

1.2. Application use

The ELPRO Technologies 645M-4 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). Being of Industrial grade with excellent temperature specifications examples of use are remote Well Head connectivity for Oil and Gas Applications. Providing backhaul data transfer and linking of municipals for Water and Irrigation applications. All these and more applications are handled either via Private or Public M2M IP networks with the added ability of providing secure VPN connectivity.

1.3. Features

The 645M-4 supports the following:

LTE FDD B1/B2/B3/B4/B5/B7/B8/B28 and LTE TDD B40 with 3G fallback to DC-HSPA+/HSPA+/HSPA/WCDMA B1/B2/B5/B8

IEEE802.11b/g/n N300 Wi-Fi AP function, WDS bridging, WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, Authenticated encryption mode

RS232 interface data transparent transmission and protocol conversion

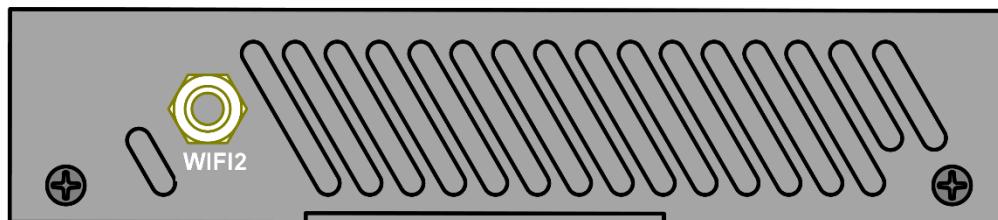
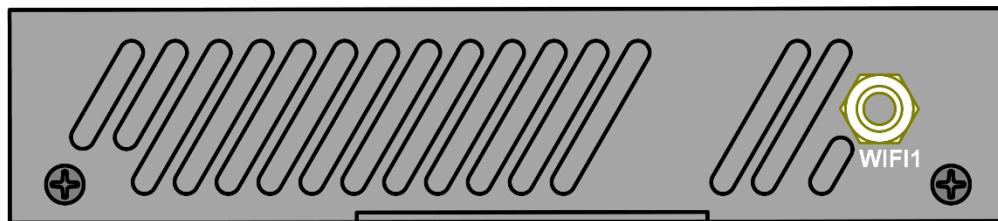
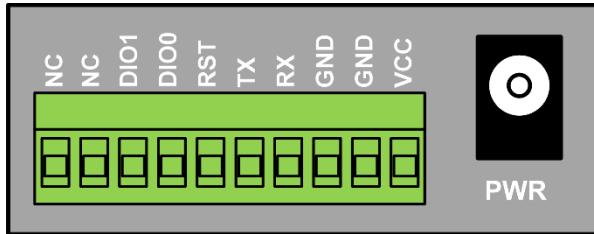
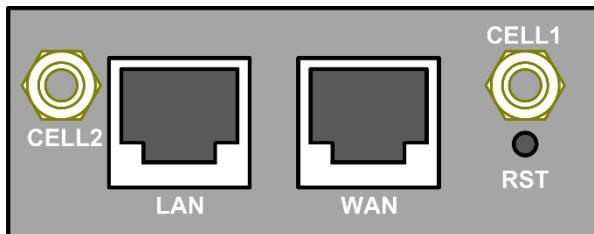
On-demand dialing, including time on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline TCP/IP protocol stack, Telnet, HTTP, SNMP, PPP, PPPoE, network protocol

VPN IPSEC, PPTP, L2TP and Open VPN

Configuration via a user-friendly interface using a web browser

2. Hardware Installation

2.1. Ports



LAN: LAN RJ45 Ethernet port

WAN: WAN RJ45 Ethernet port

RST: sys reset button

PWR: DC power socket. DC5~40V standard. (DC5~50V optional)

VCC: DC wire positive pole

GND: DC wire ground

GND: Serial ground

RX: Serial receive

TX: Serial transmit

RST: Reset

DIO0: Digital I/O Port 0

DIO1: Digital I/O Port 1

NC: DIO2 Digital I/O Port 2

NC: DIO3 Digital I/O Port 3

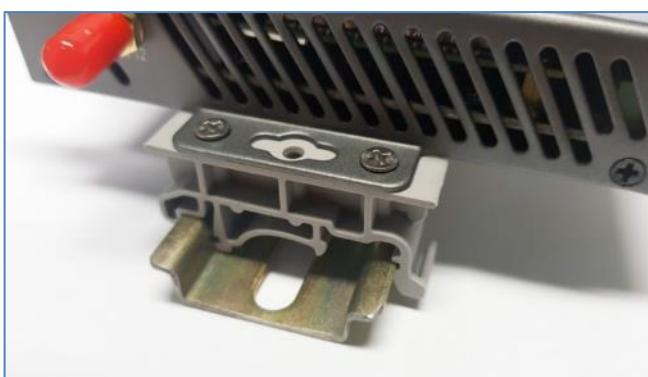
Antenna Connections Table

Antenna Connector	Marks
Cell 1	Primary cell antenna
Cell 2	Auxiliary cell antenna
WiFi 1	Primary WiFi-1 antenna
WiFi 2	Diversity WiFi-2 antenna
GPS	GPS antenna (optional)

2.2. Mounting

The modem can be mounted flat on a panel using the side plate mounting holes or by using DIN Rail mount clips which can be supplied as an accessory and are screwed to the side mounting plates.

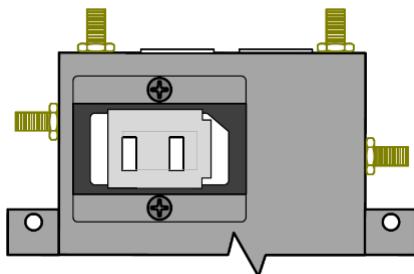
The mounting clips are screwed through the side plate mounting holes and provide a clip-on / clip-off mounting solution for “Type O” (Top Hat) 35mm (1.38”) x 7.5mm (0.3”) standard DIN Rail.



2.3. Power up and SIM Card

Please ensure the SIM card is inserted, and the antennas are connected before powering up the router.

The SIM card holder for the 645M-4 is located on the rear of the modem under the cover held in with 2 x screws and accommodates a standard 15 x 25mm SIM.

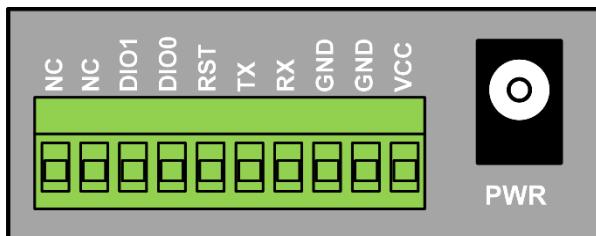


2.4. Grounding

To ensure a safe operation, the cabinet where the router is installed should be grounded properly.

2.5. Terminal block

Please refer to the following table on Pin description relating to the terminal block:



Signal	Description	Note
VCC	+5-40V DC Input, +5~50V optional	Current: 12V/1A
GND	Ground	
GND	Ground	
TX	Transmit Data	RS232 Serial TX
RX	Receive Data	RS232 Serial RX
RST	Reset	The Reset Pin has the same function as the reset button. Short both the RST and GND terminals for 3 seconds and the modem will restore to factory defaults. Holding for 1 second will reboot the modem.
DIO0	General Purpose I/O #0	Digital Input / Output #1
DIO1	General Purpose I/O #1	Digital Input / Output #2
NC	General Purpose I/O #2	Digital Input / Output #3
NC	General Purpose I/O #3	Digital Input / Output #4

Note: When powering the modem via the terminal block, the power cable should be wired with the correct voltage polarity. Wrong wiring may damage the modem. Pin 1 and Pin 2 are reserved for power, where Pin 2 is "GND" and Pin 1 is power input "Vin" (DC5~40V).

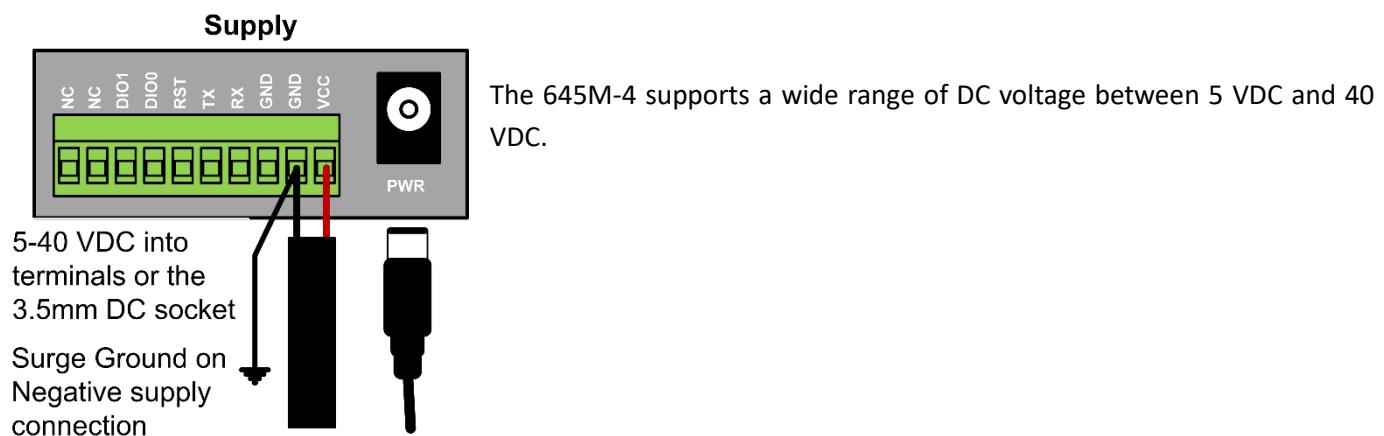
Note: The General Purpose I/O can be used as either Inputs or Outputs for SMS, Email or SNMP. When used as Digital Inputs they are voltage Free connections. Digital Outputs are a 0-3.3VDC Output and are not suitable for driving Relays.

For wiring instructions for the General Purpose, I/O please see Installation Guide for further details.

I/O Terminal on router	Serial port (RS232)
Port 3 (GND)	Pin 5
Port 4 (RX)	Pin 2
Port 5 (TX)	Pin 3

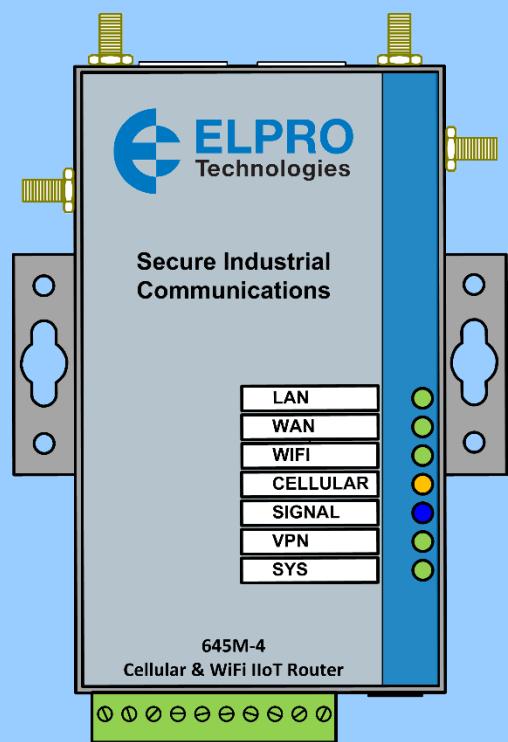
Note: See installation guide for the wiring between DTE and DCE Devices. The 645M-4 is a DCE device.

2.6. Power Supply



2.7. LED Description

Please refer to the following table for LED description.

LED	Indication Light	Description	Module
LAN	Blink	Ethernet data transmission	
	Off	No Ethernet connection	
	On	Ethernet is connected	
WAN	Blink	Ethernet data transmission	
	Off	No Ethernet connection	
	On	Ethernet is connected	
WIFI	On	WiFi enabled	
	Off	WiFi disabled	
CELLULAR	On	Cell connection is 'UP' and now you have access to the Internet	
Signal	Off	No signal, or signal checking is not ready	
	Blinks once every 4s	Signal bar is 1	
	Blinks once every 3s	Signal bar is 2	
	Blinks once every 2s	Signal bar is 3	
	Blinks once every 1s	Signal bar is 4	
	Blinks twice every 1s	Signal bar is 5	
VPN	On	VPN tunnel set-up	
	Off	VPN tunnel not set-up or VPN failure	
SYS	On for 25 seconds	On for 25 seconds after power up	
	Blink	System set-up normally	
	Off or still on after 25 seconds	System set-up failure	

3. Modem configuration

3.1. Overview

The 645M-4 router has a built-in WEB interface. Below are instructions on how to access the web interface and configure the router.

3.2. How to log into the Router

The router's default parameters are:

Default IP: 192.168.1.1

Subnet mask: 255.255.255.0

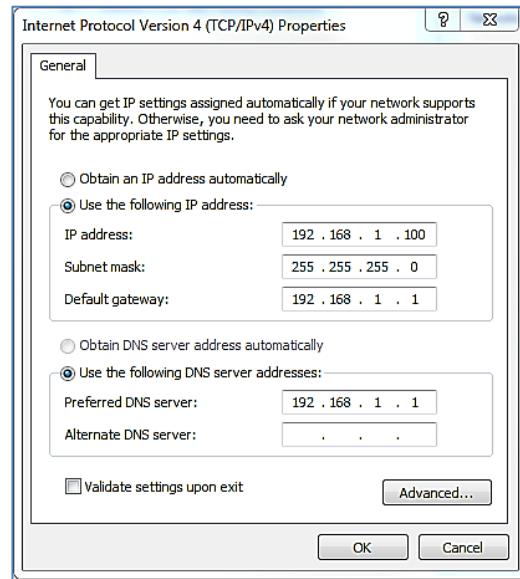
There are two ways to configure the IP address of your PC.

Manual settings

Set the PC IP to 192.168.1.xxx (xxx = 2~254), subnet mask:

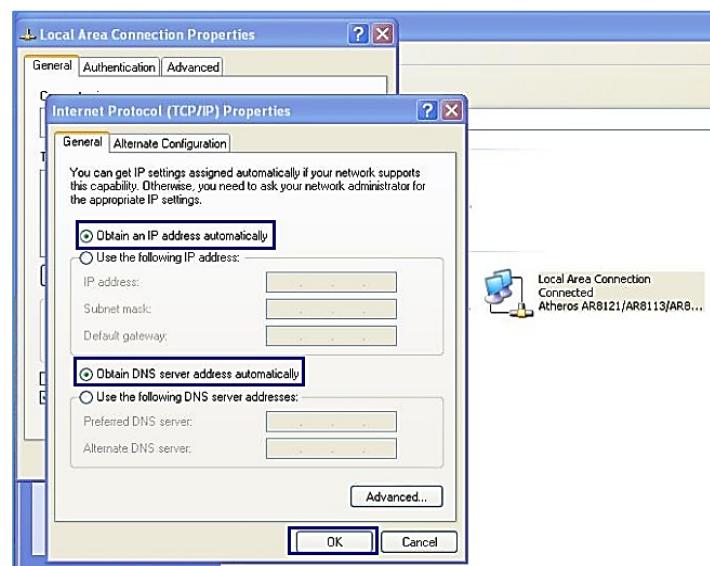
255.255.255.0, default gateway: 192.168.1.1, primary DNS:

192.168.1.1.



DHCP settings

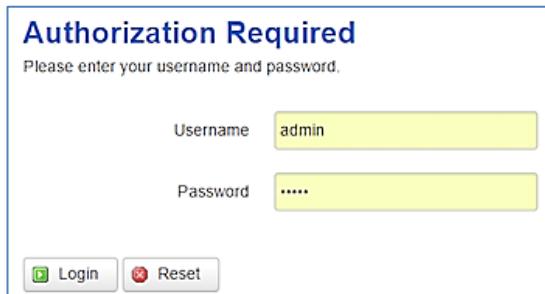
Choose "Obtain an IP address automatically" and "Obtain DNS server address automatically". Then click the 'OK' button.



3.3. Log into the router

Open a Web browser and type <http://192.168.1.1> into the address field, then press “Enter”.

Type in the username and password. Both Username and Password are “admin”. Then click on the “Login” button.



The form is titled "Authorization Required" and contains the following fields:

- Username: admin
- Password: (redacted)
- Buttons: Login (green icon), Reset (red icon)

To configure the router, you can skip the following section “Router status” and go straight to System> Setup wizard

4. Router status

4.1. Status overview

Click “Status” in the navigation bar, and then click “Overview”.

Status	
Overview	Status
Network	System
Firewall	Hostname 645M-4
Routes	SN 660420156A007260
System Log	Firmware Version 3.2.208
Kernel Log	Kernel Version 3.18.29
Reboot Log	Local Time Thu Aug 29 12:36:29 2019
Realtime Graphs	Uptime 0h 18m 45s
VPN	Load Average 0.96, 0.95, 0.61
System	Port Status  LAN1 LAN2 LAN3 LAN4 WAN
Services	Mobile 1
Network	Cellular Status Down
Logout	IP Address
	DNS 1
	DNS 2
	Cell Modem QUECTEL_EC21 (2C7C_0121)
	IMEI/ESN 864292040486951
	Sim Status SIM Ready
	Strength  14 / 31, dBm : -

4.2. Network status

The Network status page consists of 3 tabs, detailing information about the cell mobile interface, WAN and LAN.

Cell mobile interface page:

Mobile Status	
Mobile 1	
Cellular Status	Down
Cell Modem	QUECTEL_EC21 (2C7C_0121)
IMEI/ESN	864292040486951
Sim Status	SIM Ready
Strength	17 / 31
Selected Network	Automatic
Registered Network	Registered on Home network: ", ,
Sub Network Type	WCDMA
Location Area Code	FFFF
Cell ID	2DB05D6
MSISDN/IMSI	AT+CFUN=0 OK / 505016003061461

Connection Status	
Port	Mobile-eth
IPv4 Addr	10.96.89.89/30
DNS 1	10.4.149.70
DNS 2	10.4.130.164
Gateway	0h 0m 10s
Uptime	0h 13m 19s
RX	144.59 KB (537 Pkts.)
TX	111.93 KB (634 Pkts.)

WAN status page:

Status		Mobile	WAN	LAN																							
Overview																											
Network																											
WAN Status																											
<table> <tbody> <tr> <td>IPv4 WAN Status</td> <td>Port</td> <td>Wired-WAN</td> </tr> <tr> <td>Protocol:</td> <td colspan="2">dhcp</td> </tr> <tr> <td>Address:</td> <td colspan="2">0.0.0.0</td> </tr> <tr> <td>Netmask:</td> <td colspan="2">255.255.255.255</td> </tr> <tr> <td>Gateway:</td> <td colspan="2">0.0.0.0</td> </tr> <tr> <td>Mac Addr:</td> <td colspan="2">90:22:06:00:00:00</td> </tr> <tr> <td>RX</td> <td colspan="2">0.00 B (0 Pkts.)</td> </tr> <tr> <td>TX</td> <td colspan="2">182.30 KB (550 Pkts.)</td> </tr> </tbody> </table>				IPv4 WAN Status	Port	Wired-WAN	Protocol:	dhcp		Address:	0.0.0.0		Netmask:	255.255.255.255		Gateway:	0.0.0.0		Mac Addr:	90:22:06:00:00:00		RX	0.00 B (0 Pkts.)		TX	182.30 KB (550 Pkts.)	
IPv4 WAN Status	Port	Wired-WAN																									
Protocol:	dhcp																										
Address:	0.0.0.0																										
Netmask:	255.255.255.255																										
Gateway:	0.0.0.0																										
Mac Addr:	90:22:06:00:00:00																										
RX	0.00 B (0 Pkts.)																										
TX	182.30 KB (550 Pkts.)																										

LAN status page:

Status Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN System Services Network Logout	<div style="border-bottom: 1px solid black; margin-bottom: 5px;"> Mobile WAN LAN </div> <h3>LAN Status</h3> <h4>Status Overview</h4> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Uptime:</td> <td>0h 29m 0s</td> </tr> <tr> <td>Protocol:</td> <td>static</td> </tr> <tr> <td>Name:</td> <td>br-lan</td> </tr> <tr> <td>type:</td> <td>bridge</td> </tr> <tr> <td>Mac Addr:</td> <td>90:22:06:00:00:00</td> </tr> <tr> <td>IPv4 Addr:</td> <td>192.168.1.1/24</td> </tr> <tr> <td>IPv6 Addr:</td> <td>FDEF:1A1B:E9DC::1/60</td> </tr> <tr> <td>RX</td> <td>545.51 KB (4434 Pkts.)</td> </tr> <tr> <td>TX</td> <td>894.14 KB (3686 Pkts.)</td> </tr> </table> <h3>LAN Ports</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Port</th> <th>MAC-Addr</th> <th>RX</th> <th>TX</th> </tr> </thead> <tbody> <tr> <td>Wired-LAN</td> <td>90:22:06:00:03:6F</td> <td>691.42 KB (5329 Pkts.)</td> <td>984.10 KB (3915 Pkts.)</td> </tr> <tr> <td>WiFi</td> <td>90:22:06:00:03:6F</td> <td>0.00 B (0 Pkts.)</td> <td>109.41 KB (854 Pkts.)</td> </tr> </tbody> </table> <h3>DHCP Leases</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Hostname</th> <th>IPv4-Address</th> <th>MAC-Address</th> <th>Leasetime remaining</th> </tr> </thead> <tbody> <tr> <td>Lenovo-PC</td> <td>192.168.1.165</td> <td>f0:76:1c:62:f2:e5</td> <td>11h 52m 3s</td> </tr> </tbody> </table> <h3>DHCPv6 Leases</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Hostname</th> <th>IPv6-Address</th> <th>DUID</th> <th>Leasetime remaining</th> </tr> </thead> <tbody> <tr> <td colspan="4"><i>There are no active leases.</i></td> </tr> </tbody> </table>	Uptime:	0h 29m 0s	Protocol:	static	Name:	br-lan	type:	bridge	Mac Addr:	90:22:06:00:00:00	IPv4 Addr:	192.168.1.1/24	IPv6 Addr:	FDEF:1A1B:E9DC::1/60	RX	545.51 KB (4434 Pkts.)	TX	894.14 KB (3686 Pkts.)	Port	MAC-Addr	RX	TX	Wired-LAN	90:22:06:00:03:6F	691.42 KB (5329 Pkts.)	984.10 KB (3915 Pkts.)	WiFi	90:22:06:00:03:6F	0.00 B (0 Pkts.)	109.41 KB (854 Pkts.)	Hostname	IPv4-Address	MAC-Address	Leasetime remaining	Lenovo-PC	192.168.1.165	f0:76:1c:62:f2:e5	11h 52m 3s	Hostname	IPv6-Address	DUID	Leasetime remaining	<i>There are no active leases.</i>			
Uptime:	0h 29m 0s																																														
Protocol:	static																																														
Name:	br-lan																																														
type:	bridge																																														
Mac Addr:	90:22:06:00:00:00																																														
IPv4 Addr:	192.168.1.1/24																																														
IPv6 Addr:	FDEF:1A1B:E9DC::1/60																																														
RX	545.51 KB (4434 Pkts.)																																														
TX	894.14 KB (3686 Pkts.)																																														
Port	MAC-Addr	RX	TX																																												
Wired-LAN	90:22:06:00:03:6F	691.42 KB (5329 Pkts.)	984.10 KB (3915 Pkts.)																																												
WiFi	90:22:06:00:03:6F	0.00 B (0 Pkts.)	109.41 KB (854 Pkts.)																																												
Hostname	IPv4-Address	MAC-Address	Leasetime remaining																																												
Lenovo-PC	192.168.1.165	f0:76:1c:62:f2:e5	11h 52m 3s																																												
Hostname	IPv6-Address	DUID	Leasetime remaining																																												
<i>There are no active leases.</i>																																															

4.3. Firewall status

The Firewall status page shows the IPv4 and IPv6 rules and counters. Here, you can reset the counters and restart the firewall functionality.

Status Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN System Services Network Logout	<div style="border-bottom: 1px solid black; margin-bottom: 5px;"> IPv4 Firewall IPv6 Firewall </div> <h3>Firewall Status</h3> <h4>Actions</h4> <ul style="list-style-type: none"> • Reset Counters • Restart Firewall <h4>Table: Filter</h4> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="10">Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)</th> </tr> <tr> <th>Rule #</th> <th>Pkts.</th> <th>Traffic</th> <th>Target</th> <th>Prot.</th> <th>Flags</th> <th>In</th> <th>Out</th> <th>Source</th> <th>Destination</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>3091</td> <td>276.99 KB</td> <td>delegate_input</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>-</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="10">Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)</th> </tr> <tr> <th>Rule #</th> <th>Pkts.</th> <th>Traffic</th> <th>Target</th> <th>Prot.</th> <th>Flags</th> <th>In</th> <th>Out</th> <th>Source</th> <th>Destination</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1688</td> <td>401.12 KB</td> <td>delegate_forward</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>-</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="10">Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)</th> </tr> </thead> </table>	Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)										Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options	1	3091	276.99 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-	Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)										Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options	1	1688	401.12 KB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-	Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)									
Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)																																																																											
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options																																																																	
1	3091	276.99 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-																																																																	
Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)																																																																											
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options																																																																	
1	1688	401.12 KB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-																																																																	
Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)																																																																											

4.4. Routes

The Routes page shows rules which are currently active on the router. An ARP table is displayed as well.

Status	Routes					
	The following rules are currently active on this system.					
	ARP					
	IPv4-Address	MAC-Address	Interface			
System Log	10.96.89.90	4c:54:99:45:e5:d5	usb0			
Kernel Log	192.168.1.165	f0:76:1c:62:f2:e5	br-lan			
Realtime Graphs						
VPN						
System						
Services						
Network						
Logout						
Active IPv4-Routes						
	Network	Target	IPv4-Gateway	Metric		
	ifmobile	0.0.0.0/0	10.96.89.90	0		
	ifmobile	10.96.89.88/30		0		
	ifmobile	10.96.89.90		0		
	lan	192.168.1.0/24		0		

4.5. System log

This page shows the system log from system boot up. The system log resets when the router is restarted. You can export the system log by clicking the button “Export Syslog”.

System Log	
Status	
Overview	Export syslog
Network	
Firewall	
Routes	
System Log	
Kernel Log	
Reboot Log	
Realtime Graphs	
VPN	
System	
Services	
Network	
Logout	


```
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.000000] NR_IRQS:256
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.000000] CPU Clock: 360MHz
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.000000] systick: running - mult: 214748, shift: 32
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.010000] Calibrating delay loop... 239.61 BogoMIPS (lpj=1198080)
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.080000] pid_max: default: 32768 minimum: 301
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.090000] Mount-cache hash table entries: 1024 (order: 0, 4096 bytes)
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.100000] Mountpoint-cache hash table entries: 1024 (order: 0, 4096 bytes)
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.110000] pinctrl core: initialized pinctrl subsystem
Wed Sep 28 23:08:11 2016 kern.info kernel: [ 0.120000] NET: Registered protocol family 16
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] r2880-pinmux pinctrl: try to register 28 pins ...
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 0 (io0) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 1 (io1) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 2 (io2) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 3 (io3) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 4 (io4) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 5 (io5) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 6 (io6) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 7 (io7) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 8 (io8) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 9 (io9) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 10 (io10) on r2880-pinmux
Wed Sep 28 23:08:11 2016 kern.debug kernel: [ 0.130000] pinctrl core: registered pin 11 (io11) on r2880-pinmux
```

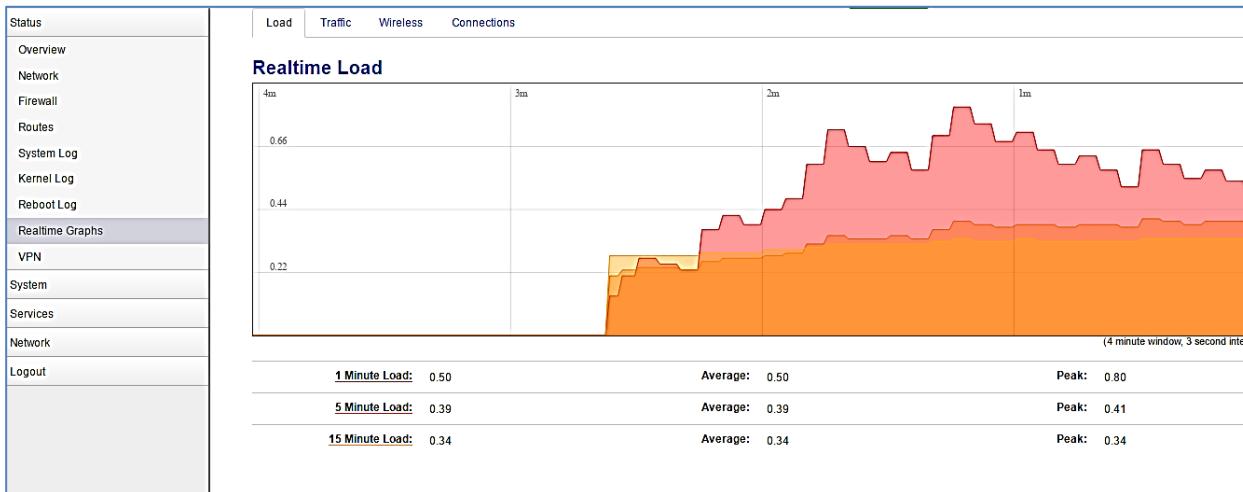
4.6. Kernel log

This page shows the kernel log from system boot up. This log is not saved when the router is restarted. It can be exported by clicking the button “Export Log”.

Status Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN System Services Network Logout	<h3>Kernel Log</h3> <p>Export log</p> <pre>[0.00000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r49294)) #933 Wed Sep 28 21:07:09 CST 2016 [0.00000] SoC Type: Ralink RT5350 id:1 rev:3 [0.00000] bootconsole [early0] enabled [0.00000] CPU0 revision is: 0001964c (MIPS 24KEc) [0.00000] MIPS: machine is rt5350_model [0.00000] Determined physical RAM map: [0.00000] memory: 04000000 @ 00000000 (usable) [0.00000] initrd not found or empty - disabling initrd [0.00000] Zone ranges: [0.00000] Normal [mem 0x00000000-0x03ffff] [0.00000] Movables zone start for each node [0.00000] Early memory node ranges [0.00000] node 0: [mem 0x00000000-0x03ffff] [0.00000] Initmem setup node 0 [mem 0x00000000-0x03ffff] [0.00000] On node 0 totalpages: 16384 [0.00000] free_area_init_node: node 0, pgdat 80300190, node_mem_map 81000000 [0.00000] Normal zone: 128 pages used for memmap [0.00000] Normal zone: 0 pages reserved [0.00000] Normal zone: 16384 pages, LIFO batch:3 [0.00000] Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes. [0.00000] Primary data cache 16kB, 4-way, VIPT, no aliases, linesize 32 bytes [0.00000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768 [0.00000] pcpu-alloc: [0] 0 [0.00000] Built 1zonelists in Zone order, mobility grouping on. Total pages: 16256 [0.00000] Kernel command line: console=ttyS1,57600 rootfs_type=squashfs,jffs2 [0.00000] PID hash table entries: 256 (order: -2, 1024 bytes) [0.00000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes) [0.00000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)</pre>

Realtime graphs

The real time graphs page shows the system load and interfaces traffic in realtime.



5. System Configuration

5.1. Setup wizard

When you login to the router for the first time, you will need to configure the Setup Wizard page. This page consists of 4 sections: General, Mobile, LAN & WiFi.

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p style="text-align: center;"> Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi </p> <p>Step - General</p> <p>First, let's change your router password from the default one.</p> <p>Password Settings</p> <p>New password: <input type="password"/> </p> <p>Confirm new password: <input type="password"/> </p> <p>System Settings</p> <p>Current system time: Thu Aug 29 12:40:17 2019 <input checked="" type="checkbox"/> Sync with browser</p> <p>Timezone: <input type="button" value="Australia/Melbourne"/></p> <p>Hostname: <input type="text" value="645M-4"/></p> <p>Language: <input type="button" value="English"/></p> <p style="text-align: right;"> Skip Wizard Save & Next </p>
---	---

Fill in the appropriate parameters as required, then click “Save & Next”.

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p style="text-align: center;"> Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi </p> <p>Mobile Configuration</p> <p>Mobile Configuration</p> <p>SIM 1</p> <p>Enable: <input checked="" type="checkbox"/></p> <p>Mobile connection: <input type="button" value="DHCP mode"/></p> <p>APN: <input type="text" value="telstra.internet"/></p> <p>PIN code: <input type="text"/></p> <p>Dialing number: <input type="text" value="*99#"/></p> <p>Authentication method: <input type="button" value="None"/></p> <p>Network Type: <input type="button" value="automatic"/></p> <p>MTU: <input type="text" value="1500"/></p> <p>Online mode: <input type="button" value="Keep Alive"/></p> <p style="text-align: right;"> Skip Wizard Save & Next </p>
---	--

Enable: Enable mobile network;

Mobile connection: Select a suitable mode for the mobile connection. The default value is ‘DHCP mode’;

APN: Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

PIN code: Most SIM cards don’t have a PIN code, in which case you leave this field blank;

Dialing number: Fill in the related value. The default value is *99#. This can be obtained from your carrier or SIM Card Provider;

Authentication method: There are three options to choose from (None, PAP, CHAP). Please confirm with your carrier the type of authentication. Default is *None*;

Username: Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

Note: If your SIM card has no username, please input the default value, otherwise the router may not dialup. If the Authentication method is 'None', this option will not appear.

Password: Fill in the related value. This can be obtained from your carrier or SIM Card Provider.

Network Type: Different Cell Modems support different types. The default value is *Automatic*.

MTU: Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500. Please configure it to optimise your own network.

When finished, click "Save & Next"

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p style="margin-top: 10px;"> Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi </p> <p>Step - LAN</p> <p>Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.</p> <p>General Configuration</p> <p>IP address: 192.168.1.1 Netmask: 255.255.255.0 Enable DHCP: <input checked="" type="checkbox"/> Start: 100 Limit: 150 Lease time: 12h</p> <p style="text-align: right;"> Skip Wizard Save & Next </p>
---	--

Fill in parameters as required. When finished, click "Save & Next"

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p style="margin-top: 10px;"> Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi </p> <p>Step - Wireless</p> <p>Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. you will lose connection.)</p> <p>WiFi Configuration</p> <p>Enable wireless: <input checked="" type="checkbox"/> SSID: ELPRO_645M-4 Transmit Power: 20 dBm (100 mW) Band: 2.4GHz (802.11g+n) HT mode (802.11n): disabled Channel: 11 (2.462 GHz) Encryption: WPA2-PSK Cipher: auto Key: Country Code: 00 - World</p> <p style="text-align: right;"> Skip Wizard Finish </p>
---	--

Fill in parameters as required, then press "Finish". Note: pressing the button "Save & Next" will save the configuration of the current page and jump to the next page. All configurations will be applied when you click the button "Finish" on this last page (WiFi).

5.2. System

General Settings

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p>System</p> <p>Here you can configure the basic aspects of your device like its hostname or the timezone.</p> <p>System Properties</p> <p>General Settings Logging Language</p> <p>Local Time Thu Aug 29 12:41:04 2019 <input type="button" value="Sync with browser"/></p> <p>Hostname: <input type="text" value="645M-4"/></p> <p>Timezone: <input type="button" value="Australia/Melbourne"/></p> <p><input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/></p>
---	--

Local Time

This page shows the system time. You can sync the time with the browser by clicking the button “Sync with browser”.

Hostname

It is the router’s name. The default name is “645M-4”

Time zone

Select a suitable time zone. The default value is “Australia/Melbourne”

Logging

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p>System</p> <p>Here you can configure the basic aspects of your device like its hostname or the timezone.</p> <p>System Properties</p> <p>General Settings Logging Language</p> <p>System log buffer size: <input type="text" value="64"/></p> <p>External system log server: <input type="text" value="0.0.0.0"/></p> <p>External system log server port: <input type="text" value="514"/></p> <p>Log output level: <input type="button" value="Debug"/></p> <p>Cron Log Level: <input type="button" value="Normal"/></p> <p><input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/></p>
---	--

System log buffer size

The unit is KB. The default value is 64 KB. If the actual log size exceeds the set value, then the first lines of data will be lost.

External system log server

Here you enter the IP address of the external log server. You can setup a Linux machine with “syslogd” run as a log server.

External system log server port

This is the UDP port of the external log server.

Log output level

This is the Log level. The default is ‘Debug’ with highest level. Emergency is the lowest level.

Cron log level

It is the log level to process “Crond”.

Language and Style

Language	English	▼
----------	---------	---

The default language is “English”.

5.3. Password

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<div style="display: flex; justify-content: space-around; font-size: small;"> Web Account SSH Account Guest Account </div> <div style="margin-top: 10px;"> Web Account <small>Changes the administrator username and password</small> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> Current username <input type="text"/> </div> <div style="width: 45%;"> New username <input type="text"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> Password <input type="password"/> </div> <div style="width: 45%;"> Confirmation <input type="password"/> </div> </div> <div style="text-align: right; margin-top: 20px;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div> </div>
---	--

Here you can change the administrator’s password for accessing the device. Click the “eye button” to show the new password you entered. Also available is the addition of entering in Guest account and if using SSH the same again a username and password. It is recommended that Primary Admin account is not shared amongst users and the use of a Guest account is used for all other users.

5.4. NTP

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<div style="display: flex; justify-content: space-between; font-size: small;"> NTP NTP Configuration </div> <div style="margin-top: 10px;"> Time Synchronization <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> Enable NTP client <input checked="" type="checkbox"/> </div> <div style="width: 45%;"> Provide NTP server <input type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> NTP sync count <input type="text" value="0"/> </div> <div style="width: 45%;"> NTP sync interval(min) <input type="text"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> NTP server candidates <ul style="list-style-type: none"> 0.au.pool.ntp.org 1.au.pool.ntp.org 2.au.pool.ntp.org 3.au.pool.ntp.org </div> <div style="width: 45%;"> </div> </div> <div style="text-align: right; margin-top: 20px;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div> </div>
---	---

NTP is Network Timing Protocol.

Enable NTP client

The default value is checked. The router acts as a NTP client.

Provide NTP server

The default value is unchecked. The router acts as a NTP server.

NTP server candidates

It is the NTP server list. Multiple NTP servers are accepted. You can click the  button to delete an entry or click the  button to add a new entry.

5.5. Backup/Restore

Status		
System		
System		
Setup Wizard		
Password		
NTP		
Backup/Restore		
Upgrade		
Reset		
Reboot		
Services		
Network		
Logout		

Configuration files operations

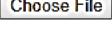
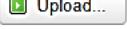
Backup

Download a tar archive of the current configuration files.

Download backup configuration archive : 

Restore

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup configuration archive :  No file chosen 

To backup the configuration files, click the button “Download”. Then an archive file will be generated and downloaded to your PC automatically.

To restore the configuration files, click the button “Choose File” and select an archived configuration file. Click the button “Upload”. The system will upload the file and then restart the router.

5.6. Upgrade

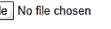
Status		
System		
System		
Setup Wizard		
Password		
NTP		
Backup/Restore		
Upgrade		
Reset		

System upgrade

Upload a sysupgrade-compatible image here to replace the running firmware. Check “Keep settings” to retain the current configuration (requires a compatible firmware image).

Keep settings:

Safe upgrade:

Image:  No file chosen 

Upload a system compatible firmware to replace the current firmware. The default value for “Keep settings” is checked, which means the existing configuration will be kept after the system upgrade, otherwise the router will be reset to factory settings. We recommend to un-check “Keep settings” to prevent conflicting parameters after the firmware upgrade.

Click the button “Choose File” and select a compatible firmware, then click the button “Upload image”. The router will run a basic check of the file. If it is an incompatible file, an error message will appear like this one below:

System upgrade

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

Keep settings:

Image: no file selected

The uploaded image file does not contain a supported format. Make sure that you choose the generic image format for your Router.

If the firmware file is ok, a verification message will appear. Click the button "Proceed", and the system will restart after a few minutes.

Upgrade Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the upgrade procedure.

- Checksum: d49e4e53a837a6eca830ff8cad9c0c41
- Size: 10.25 MB (15.00 MB available)
- Configuration files will be kept.

5.7. Reset

Factory Reset can be performed one of three ways.

1. From the web page (see below)

Status	System Reset <small>Resets all configurations to factory default</small> <small>Warning: All configurations will be reset to factory default while resetting!</small> <input type="button" value="Reset"/>
System	
System	
Setup Wizard	
Password	
NTP	
Backup/Restore	
Upgrade	
Reset	

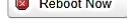
This button resets all configurations to factory default. After clicking the "Reset" button, a message will appear prompting you to confirm. By clicking "OK", the router will reset to factory default and the system will restart.

2. The Reset Pin on the terminal strip. Short the RST and GND terminals for 3 seconds and the modem will restore to factory defaults. Holding for 1 second will reboot the modem.
3. Hold in the "RST" button, just below "CELL 1" on the Antenna end of the modem for approx. 5 seconds.

Note: There is no immediate indication that the reset has been performed. Release the button and after about 5 seconds you will see all the Led's go OFF then the WAN & LAN will come ON briefly then go OFF.

The LAN will come ON and flicker with traffic, the SYS led will come ON for approx. 25 seconds then start to flash and the Wi-Fi LED will come on. This is good indication that the modem has reset as the Wi-Fi is enabled by default.

5.8. Reboot

Status System System Setup Wizard Password NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	<p>Reboot Settings</p> <p>Reboot At Time Settings</p> <p>Reboot at time <input type="checkbox"/></p> <p>Time(H.M.S) <input type="text" value="16"/> <input type="text" value="15"/> <input type="text" value="00"/></p> <p>Reboot Timer Settings</p> <p>Reboot when timeout <input type="checkbox"/></p> <p>Timer(min) <input type="text" value="1440"/></p> <p>Reboot Reboots the operating system immediately Warning: There are unsaved changes that will be lost while rebooting!</p> <p> Reboot Now</p> <p style="text-align: right;">Save & Apply Save Reset</p>
---	---

The 645M-4 has the ability for programmed Reboot at specific times or under timer to provide mechanism in the event of a partial disconnection to the Cellular provider. It is recommended that a periodic time is set to allow for recovery of the modem to the network in the event of partial disconnection from the Carrier.

Reboot Button - Click the button “Reboot” and the system will restart.

6. Services configuration

6.1. ICMP check

For a stable operation, we suggest you enable ICMP check. With this feature, the router will periodically ping a hostname and automatically restart when a problem is detected.

Status System Services ICMP Check VRRP Failover DTU SNMP GPS SMS VPN DDNS Connect Radio Module NMS Captive Portal WEB Filter Network	<p>ICMP Check</p> <p>Enable <input type="checkbox"/></p> <p>Host1 to ping <input type="text" value="www.google.com"/> ipv4 or hostname</p> <p>Host2 to ping <input type="text" value="8.8.8.8"/></p> <p>Ping timeout <input type="text" value="4"/> seconds (range [1 - 10])</p> <p>Max retries <input type="text" value="10"/> (range [3 - 1000])</p> <p>Interval between ping <input type="text" value="2"/> minutes (range [1 - 1440])</p> <p>Reconnect <input type="checkbox"/></p> <p>Action when failed <input type="button" value="Restart module"/></p>
---	--

Enable: Enable ICMP check feature

Host1 to ping / Host2 to ping: The domain name or IP address for checking the network connection.

Ping timeout: After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.

Max retries: When the number of failed pings reaches the “Max retries”, this will trigger the action configured in item “Action when failed”.

Interval between pings: The time between two pings in minutes.

Action when failed: the options are “Restart module” and “Restart router”. “Restart module” will restart the radio module. “Restart router” will restart the whole system including the radio module.

6.2. VRRP

Status
System
Services
ICMP Check
VRRP
Failover
DTU
SNMP
GPS
SMS
VPN
DDNS
Connect Radio Module
NMS
Captive Portal
WEB Filter
Network
Logout

VRRP Configuration

VRRP LAN Configuration Settings

Enable	<input type="checkbox"/>
Virtual ID	1
Virtual IP address	192.168.1.253 
Priority	100
Advertisement interval	1  s
Password	<input type="password"/> 
Track interface	<input type="button" value="None"/>
Track IP/Host	<input type="text"/>
Track Interval	10  s
Track Weight	10
Status	

Enable: Enable VRRP (Virtual Router Redundancy Protocol) for LAN.

IP address: Virtual IP address for LAN’s VRRP cluster. IP address entry can be deleted by clicking the  button, or added by clicking the  button.

Virtual ID: Routers with the same IDs will be grouped in the same VRRP cluster. The legal number is from 1 to 255.

Priority: The router with the highest priority in the same VRRP cluster will act as a master. The legal number is from 1 to 255.

6.3. Failover (link backup)

Status System Services ICMP Check VRRP Failover DTU SNMP GPS SMS VPN DDNS Connect Radio Module NMS Captive Portal WEB Filter Network Logout	<input type="radio"/> Failover <input checked="" type="radio"/> Advanced	
	Failover Configuration	
	Failover Settings	
	Enable <input type="checkbox"/> Back To High priority <input checked="" type="checkbox"/>	
	Current interface primary	
	Primary Configuration	
	Primary	<input type="button" value="Wired_wan"/>
	Host1 to ping	<input type="text"/>
	Host2 to ping	<input type="text"/>
	Ping timeout	<input type="text" value="1"/>
	Max Retries	<input type="text" value="10"/>
	Interval between ping	<input type="text" value="30"/>
	NAT	<input type="button" value="Default"/>

	Secondary Configuration	
	Secondary	<input type="button" value="Wired_wan"/>
	Host1 to ping	<input type="text"/>
	Host2 to ping	<input type="text"/>
	Ping timeout	<input type="text" value="1"/>
	Max Retries	<input type="text" value="10"/>
	Interval between ping	<input type="text" value="30"/>
	Third Configuration	
	Third	<input type="button" value="None"/>
	Host1 to ping	<input type="text"/>
	Host2 to ping	<input type="text"/>
	Ping timeout	<input type="text" value="1"/>
	Max Retries	<input type="text" value="10"/>
	Interval between ping	<input type="text" value="30"/>

Enable: Enable failover feature

Back to high priority: If “back to high priority” is checked, the router will go back to the selected “high priority” WAN interface when available. The priorities can be set to primary, secondary and third priority. There are four options to choose from: Wired-WAN, Wifi_client, Cell_mobile, and None.

Host1 to ping / Host2 to ping: The domain name or IP address for checking the network connection.

Ping timeout: After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.

Max retries: When the number of failed pings reaches the “Max retries”, this will confirm that the WAN interface is unavailable.

Interval between pings: The time between two pings in seconds.

6.4. DTU

Notes:

- 1) This feature is for the 645M-4 with DTU option only.
- 2) This feature conflicts with the “Connect Radio module” and “GPS send to serial” features. Please disable “DTU” when using either of the above two functions.

System <hr/> Services <hr/> ICMP Check <hr/> VRRP <hr/> Failover <hr/> DTU <hr/> SNMP <hr/> GPS <hr/> SMS <hr/> VPN <hr/> DDNS <hr/> Connect Radio Module <hr/> NMS <hr/> Captive Portal <hr/> WEB Filter <hr/>	<div style="background-color: #f0f0f0; padding: 10px;"> <p>DTU Configuration</p> <p>Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Enable</td> <td style="width: 85%;"><input type="checkbox"/></td> </tr> <tr> <td>Send DTU ID</td> <td><input type="checkbox"/></td> </tr> <tr> <td>DTU ID</td> <td>660420156A007260</td> </tr> <tr> <td>Send DTU ID on initial connection</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Forward delay</td> <td>200 milliseconds (range[10,10000])</td> </tr> <tr> <td>Terminate character(s)</td> <td><input type="text"/></td> </tr> <tr> <td>Debug</td> <td><input type="button" value="Error"/></td> </tr> </table> <p>Serial Setting</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Serial baudrate</td> <td style="width: 85%;"><input type="button" value="115200 bps"/></td> </tr> <tr> <td>Serial parity</td> <td><input type="button" value="None"/></td> </tr> <tr> <td>Serial databits</td> <td><input type="button" value="8 bits"/></td> </tr> <tr> <td>Serial stopbits</td> <td><input type="button" value="1 bits"/></td> </tr> </table> </div>	Enable	<input type="checkbox"/>	Send DTU ID	<input type="checkbox"/>	DTU ID	660420156A007260	Send DTU ID on initial connection	<input type="checkbox"/>	Forward delay	200 milliseconds (range[10,10000])	Terminate character(s)	<input type="text"/>	Debug	<input type="button" value="Error"/>	Serial baudrate	<input type="button" value="115200 bps"/>	Serial parity	<input type="button" value="None"/>	Serial databits	<input type="button" value="8 bits"/>	Serial stopbits	<input type="button" value="1 bits"/>
Enable	<input type="checkbox"/>																						
Send DTU ID	<input type="checkbox"/>																						
DTU ID	660420156A007260																						
Send DTU ID on initial connection	<input type="checkbox"/>																						
Forward delay	200 milliseconds (range[10,10000])																						
Terminate character(s)	<input type="text"/>																						
Debug	<input type="button" value="Error"/>																						
Serial baudrate	<input type="button" value="115200 bps"/>																						
Serial parity	<input type="button" value="None"/>																						
Serial databits	<input type="button" value="8 bits"/>																						
Serial stopbits	<input type="button" value="1 bits"/>																						

	<p>Network Setting</p> <p>Protocol: <input type="button" value="TCP"/></p> <p>Service mode: <input type="button" value="Client"/></p> <p>Enable Heartbeat: <input type="checkbox"/></p> <p>Heartbeat Interval: <input type="text" value="5"/></p> <p>Heartbeat Content: <input type="text"/></p> <p>DTU center configuration</p> <p>CENTER1</p> <p>Center enable: <input checked="" type="checkbox"/></p> <p>Center IP: <input type="text" value="192.168.1.171"/></p> <p>Center Port: <input type="text" value="5000"/></p> <p>New center name: <input type="text"/> <input type="button" value="Add"/></p> <p style="text-align: right;"><input type="button" value="Delete"/></p>
	<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>

Enable: Enable DTU feature.

Send DTU ID: Send DTU ID at the front of the packet.

DTU ID: The default DTU ID is the SN of the router. You can change it if required.

Forward delay: This unit is in milliseconds. It is the time delay when sending data between the serial port and the network.

Serial baudrate: Supports 300/1200/2400/4800/9600/19200/38400/57600/115200bps

Serial parity: Can be none, odd or even

Serial databits: Can be 7 bits or 8 bits

Serial stopbit: Can be 1 bit or 2 bits

Protocol: Both TCP and UDP are supported

Service mode: Client and Server are supported.

Enable heartbeat: The heartbeat is used to maintain the “keep alive” connection.

Heartbeat interval: The time between two heartbeat packets.

Heartbeat content: The content of heartbeat packets.

DTU center Configuration: The DTU centre is the DTU server. Simply input the centre name and click the button “Add”.

If the centre is not needed, you can delete it by clicking the button “Delete”, or set it to ‘Disabled’.

Notes:

The maximum number of DTU centers is 32.

6.5. SNMP

Enable SNMP: Enable the SNMP feature

Remote Access: Allow SNMP remote access. If it is unchecked, only the LAN subnet can access SNMP.

Contact: Set the contact information here.

Location: Set the router's physical address.

Name: Set the router's name in SNMP.

Port: SNMP service port, the default value is 161.

SNMP Configuration

General Settings

Enable SNMP

Remote Access

Contact

Location

Name

Port

Get Community: The username for SNMP get. The default value is 'public'. SNMP get is read-only.

Get Host/Lan: The network range to get the router via SNMP, default is '0.0.0.0./0'

Set Community: The username for SNMP set. The default value is 'private'. SNMP set is read-write.

Set Host/Lan: The network range to set the router via SNMP, default is '0.0.0.0./0'

SNMP v1 and v2c Settings

Get Community

Get Host/Lan

Set Community

Set Host/Lan

User: SNMPv3 username

Security Mode: Three options: None, Private and Authorised. If it is set to 'None', there is no password required. If it is set to 'Authorised', only Authentication method and password are required.

Authentication: Authentication method with two options: MD5 and SHA.

Encryption: Encryption method DES and AES supported.

Authentication password: SNMPv3 authentication password is at least 8 characters long.

Encryption password: SNMPv3 encryption password is at least 8 characters long.

SNMP v3 Settings

User

Security Mode

Authentication

Encryption

Authentication Password 

Encryption Password 

After all items are setup, click the button "Save & Apply" to enable SNMP functionality.

6.6. GPS

Status	GPS Configuration	
System	Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time	
Services	<input checked="" type="checkbox"/> Enable	
ICMP Check	<input type="checkbox"/> Prefix SN No.	
VRRP	<input type="checkbox"/> Only GPRMC	
Failover		
DTU	Send interval <input type="text" value="10"/>	
SNMP	GPS send to <input type="button" value="TCP"/>	
GPS	Server IP/Domain <input type="text" value="192.168.1.100"/>	
SMS		
VPN		
DDNS	Server port <input type="text" value="6000"/>	
Connect Radio Module		

Enable: Check this button to enable GPS.

Only GPRMC: If checked, it will only send GPRMC data info (Longitude Latitude altitude)

Prefix SN No.: If checked, it will add the router's SN to the data packet.

Send interval: Set the frequency of GPS data packets being sent.

GPS Send to: Choose between "Serial" and "TCP/IP". The router will only receive the GPS signal and will not process it. It will send this GPS signal to your GPS processor devices or servers. If the GPS processor device is connected to the 645M-4 Router via a Serial Port, please choose "Serial".

If the GPS processor device is a remote server, please choose "Serial".

GPS to TCP/UDP Settings

Server IP: Fill in the correct destination server IP or domain name.

Server port: Fill in the correct destination server port.

Serial baudrate:

9600/19200/38400/57600/115200bps

Serial parity:

none/odd/even

Serial databits:

7/8

Serial stopbits:

1/2

Serial flow control:

none/hardware/software

GPS send to	<input type="button" value="Serial"/>
Serial baudrate	<input type="button" value="115200 bps"/>
Serial parity	<input type="button" value="None"/>
Serial databits	<input type="button" value="8 bits"/>
Serial stopbits	<input type="button" value="1 bits"/>
Serial flow control	<input type="button" value="None"/>
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>	

6.7. SMS

SMS Command

SMS Command	
Enable	<input type="checkbox"/>
SMS ACK	<input type="checkbox"/>
Reboot Router Command	reboot
Get Cell Status Command	cellstatus
Set Cell link-up Command	cellup
Set Cell link-down Command	celldown
DIO_0 Set Command	dio01
DIO_0 Reset Command	dio00
DIO_1 Set Command	dio11
DIO_1 Reset Command	dio10
DIO Status Command	diosstatus
Wifi On Command	wifion
Wifi Off Command	wifioff

Enable: Check it to enable the SMS command feature.

SMS ACK: If checked, the router will send the command feedback to the sender's mobile phone number.

Reboot Router Command: Input the command for "reboot" operation, default is "reboot".

Get Cell Status Command: Input the command for "router cell status" operation, default is "cellstatus".

Set cell link-up Command: Input the command for "router cell link up" operation, default is "cellup". If the router gets this command, the Router Cell will go online.

Set cell link-down Command: Input the command for "router cell link down" operation, default is "celldown". If the router gets this command, the Router Cell will go offline.

DIO_0 Set Command: Input the command for I/O port 0. For SMS feature, please keep the default parameters.

DIO_0 Reset Command: Input the command for I/O port 0. For SMS feature, please keep the default parameters.

DIO_1 Set Command: Input the command for I/O port 1. For SMS feature, please keep the default parameters.

DIO_1 Reset Command: Input the command for I/O port 1. For SMS feature, please keep the default parameters.

DIO Status Command: Input the command for I/O port status. For SMS feature, please keep the default parameters.

Wifi on Command: input the command for turning on WiFi. For SMS feature, please keep the default parameters.

Wifi off Command: input the command for turning off WiFi. For SMS feature, please keep the default parameters.

SMS alarm

SMS Alarm: Enable the SMS alarm feature.

Enable Signal Quality Alarm: Enable Signal Quality Alarm feature.

Signal Quality Threshold: Set the signal quality threshold.

Failed Times Threshold: If the failed counter exceeds this threshold, a signal alarm will be generated.

Success Times Threshold: If a signal alarm is generated, and the success counter is greater or equal to the Success Times Threshold, this will clear the signal alarm.

SMS Alarm

SMS Alarm

RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm

Signal Quality Threshold

Failed Times Threshold

Success Times Threshold

Phone Number

Add Phone number: Input a name and click the button “Add” to add a new Phone number.

Delete Phone number: Click the button “Delete”.

SMS command: Enable the SMS command feature on this phone number.

SMS alarm: This phone number can receive SMS alarms.

Phone Number

Phone Number Configuration

NUM1

SMS Command

SMS Alarm

Phone Number

Send SMS

Receiver Phone Number: The phone number that receives SMS messages.

Message: Message content.

Submit: Click the button “Submit” to send the message immediately.

Send SMS

Receiver Phone Number

Message

DIO Mail

System		
Services		
ICMP Check		
VRRP		
Failover		
DTU		
SNMP		
GPS		
SMS		
VPN		
DDNS		
Connect Radio Module		
NMS		
Captive Portal		
WEB Filter		
Network		
Logout		

Mail Configuration
Send email to specified address when DIO changed

Enable

SMTP server

Port

Username/Account

SMTP Authentication

Password 

TLS

StartTLS

Check server certificate

TLS trust file No file chosen

Mail format	<input type="button" value="System template"/>
DIO_0 name	<input type="text" value="DIO0"/>
DIO_0 high text	<input type="text" value="1"/>
DIO_0 low text	<input type="text" value="0"/>
DIO_1 name	<input type="text" value="DIO1"/>
DIO_1 high text	<input type="text" value="1"/>
DIO_1 low text	<input type="text" value="0"/>
DIO_2 name	<input type="text" value="DIO2"/>
DIO_2 high text	<input type="text" value="1"/>
DIO_2 low text	<input type="text" value="0"/>
DIO_3 name	<input type="text" value="DIO3"/>
DIO_3 high text	<input type="text" value="1"/>
DIO_3 low text	<input type="text" value="0"/>

Receiver Configuration

This section contains no values yet

New group name 

DIO Default

Status System Services ICMP Check VRRP Failover DTU SNMP GPS SMS VPN DDNS Connect Radio Module NMS Captive Portal WEB Filter <hr/> Network <hr/> Logout	SMS Command	SMS Alarm	Phone Number	SMS	DIO Mail	DIO Default	DIO sms
	DIO Configuration						
	DIO trap <input type="checkbox"/>						
	Set DIO to high for a period of time <input type="text" value="0"/> s						
	DIO_0 default value <input type="text" value="Low"/>						
	DIO_1 default value <input type="text" value="Low"/>						
	DIO_2 default value <input type="text" value="Low"/>						
	DIO_3 default value <input type="text" value="Low"/>						
	DIO_0 Value <input type="text" value="0"/>						
	DIO_1 Value <input type="text" value="0"/>						
	DIO_2 Value <input type="text" value="0"/>						
	DIO_3 Value <input type="text" value="0"/>						
	DIO_0 Function <input type="text" value="None"/>						
	DIO_1 Function <input type="text" value="None"/>						
	DIO_2 Function <input type="text" value="None"/>						
DIO_3 Function <input type="text" value="None"/>							

DIO SMS

Status System Services ICMP Check VRRP Failover DTU SNMP GPS	SMS Command	SMS Alarm	Phone Number	SMS	DIO Mail	DIO Default	DIO sms
	DIO SMS configuration						
	send user defined SMS alarm when DIO changed						
	Enable self-defined DIO SMS alarm <input type="checkbox"/>						
	<input type="button" value="Save &"/>						

7. VPN

7.1. IPSEC

Enable: Enable IPSEC feature

Exchange mode: IKEv1-Main, IKEv1-Aggressive and IKEv2-Main modes are supported.

Authentication method: Client and Server. Client is the machine which starts the IPSEC connection.

Remote VPN endpoint: Domain name or IP address of the remote endpoint. This needs to be accessed over the internet.

Preshared Keys: This is known as PSK. The length is 16 to 32.

Local subnet: The local subnet which connects to the IPSEC VPN.

Remote subnet: The remote subnet which connects to the IPSEC VPN.

IPsec

IPsec Configuration

Enable

Exchange mode IKEv1-Main

Authentication method Server

Remote VPN endpoint

Preshared Keys

Local subnet 192.168.1.0/24

Remote subnet 192.168.10.0/24

Note:

All configurations in Phase 1 Proposal and Phase 2 Proposal must match with the remote endpoint to establish an IPSEC connection.

Phase 1 Proposal

The phase must match with another incoming connection to establish IPsec

Encryption algorithm 3DES

Hash algorithm SHA1

DH group MODP1024

Phase 2 Proposal

The phase must match with another incoming connection to establish IPsec

Encryption algorithm AES 128

PFS group MODP1024

Authentication HMAC_SHA1

7.2. PPTP

This page shows a list of configured PPTP instances and their state. Click the button “Edit” to make changes to an instance or click the button “Delete” to delete it.

Point-to-Point Tuneling Protocol

PPTP Configuration

Below is a list of configured PPTP instances and their state.

Name	Type	Enable	
	Server	No	 
New instance name:	<input type="text"/> Role: <input type="button" value="Client"/> <input style="background-color: #0070C0; color: white; border: none; font-weight: bold;" type="button" value="Client"/> <input type="button" value="Server"/>		

PPTP Client configuration

Enable: Enable this instance.

Server: Domain name or IP address of PPTP server.

Username: Server authentication username.

Password: Server authentication password.

MTU: Maximum Transmission Unit.

Keep Alive: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.

Use default gateway: If unchecked, no default route is configured.

Use DNS servers advertised by peer: If unchecked, the advertised DNS server addresses are ignored.

PPTP Client Instance: Aaaa

Main Settings

Enable

Server

Username

Password 

MTU

Keep Alive

Use default gateway

Use DNS servers advertised by peer

PPTP Server Configuration

Local IP: Indicates the server’s IP address.

Remote IP: The remote IP address lease start.

Remote IP end: The remote IP address lease end.

ARP Proxy: If the remote IP has the same subnet as the LAN, check it for connecting with each other.

Debug: For PPTP server debug, the log can be monitored in the system log.

Username: Server authentication username

Password: Server authentication password.

PPTP Server Instance:

Main Settings

Enable

Local IP

Remote IP

Remote IP end

ARP Proxy

Debug

Username	Password
<input type="text" value="youruser"/>	<input type="password"/> 

 Add

7.3. L2TP

This page shows a list of configured L2TP instances and their state. Click the button “Edit” to make changes to an instance or click the button “Delete” to delete it.

IPSec	PPTP	L2TP	OpenVPN	GRE Tunnel
-------	------	------	---------	------------

Layer 2 Tunneling Protocol

L2TP Configuration

Name	Type	Enable
L2tpd_server	Server	No

New instance name: Role: Client

L2TP NAT enable

L2TP Client configuration

Enable: Enable this L2TP instance.

Server: Domain name or IP address of L2TP server.

Username: Server authentication username.

Password: Server authentication password.

MTU: Maximum Transmission Unit.

Keep Alive: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.

Checkup Interval: Number of seconds to pass before checking if the interface is not up since the last setup attempt and retry the connection otherwise. Set it to a value sufficient for a successful L2TP connection for you. It's mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.

L2TP Client Instance: Bbbbb

Main Settings

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
MTU	<input type="text"/> 1500
Keep Alive	<input type="text"/>
Checkup Interval	<input type="text"/>

L2TP Server configuration

Local IP: Indicates the server's IP address.

Remote IP range begin: The remote IP address lease start.

Remote IP range end: The remote IP address lease end.

Remote LAN IP: L2TP client IP.

Remote LAN netmask: The mask of L2TP client IP, the default value is 255.255.255.0

Username: Server authentication username.

Password: Server authentication password.

L2TP Server Instance: L2tpd_server

Main Settings

Enable	<input type="checkbox"/>
Local IP	<input type="text"/> 192.168.0.1
Remote IP range begin	<input type="text"/> 192.168.0.20
Remote IP range end	<input type="text"/> 192.168.0.30
Remote LAN IP	<input type="text"/>
Remote LAN netmask	<input type="text"/> 255.255.255.0

Username	Password
<input type="text"/> user	<input type="password"/> 

7.4. OpenVPN

This page is a list of configured OpenVPN instances and their state. Click the button “Edit” to make changes to an instance or click the button “Delete” to delete it. Click the button “Start” or “Stop” to start or stop a specific instance.

OpenVPN

OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	 start	tun	1194	udp	 Edit  Delete
sample_server	No	no	 start	tun	1194	udp	 Edit  Delete
sample_client	No	no	 start	tun	1194	udp	 Edit  Delete



Note: For OpenVPN configuration help, hover the cursor over the item to get more information. If the item you need is not shown on the main page, please check the “Additional Field” dropdown list at the bottom of the page.

Overview » Instance "sample_server"

[« Switch to basic configuration](#)

Configuration category: [Service](#) | [Networking](#) | [VPN](#) | [Cryptography](#)

Service

enabled	<input type="checkbox"/>
verb	<input type="text" value="3"/>
mlock	<input type="checkbox"/>
disable_occ	<input type="checkbox"/>

-- Additional Field --
cd
chroot
log
log_append
nice
echo
remap_usr1
status_version
mute
up
up_delay
down
route_up
setenv
tls_verify
client_connect
learn_address
auth_user_pass_verify

7.5. GRE tunnel

Enable: Enable GRE tunnel feature.

TTL: Time-to-live.

MTU: Maximum Transmission Unit.

Peer IP address: Remote WAN IP address.

Remote LAN subnet: Remote LAN subnet address.

Remote LAN Netmask: Remote LAN subnet mask.

Metric: Route Metric, generally configured as 1

Local Interface: Allows you to choose a specific interface or all interfaces (default)

Local Tunnel IP: Virtual IP address. This cannot be in the same subnet as the LAN network.

Local Tunnel Mask: Virtual IP mask.

Keepalive: Allows Keepalives (periodic status message used to monitor the integrity of the tunnel). Received, Send and Received or None. Keepalives should be used with care as it will utilize some data

Keepalive interval: Time interval (in seconds) between transmitted keepalive packets.

Keepalive Retries: Defines the number of times to retry after failed keepalives before determining that the tunnel endpoint is down.

GRE Tunnel

GRE Instance: Gre_tunnel

Enable

TTL 255

MTU 1500

Peer IP Address

Remote LAN subnet

Remote LAN netmask

Metric 0

Local Interface All

Local Tunnel IP

Local Tunnel Mask

Keepalive Send and receive

Keepalive interval 60

Keepalive Retries 5

7.6. DDNS

DDNS allows a router to be reached via a fixed domain name while having a dynamically changing IP address.

Status System Services ICMP Check VRRP Failover SNMP DTU GPS SMS VPN DDNS Connect Radio Module Network Logout	<h3>Dynamic DNS</h3> <p>Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.</p> <h4>Overview</h4> <p>Below is a list of configured DDNS configurations and their current state. If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Configuration</th> <th>Hostname/Domain Registered IP</th> <th>Enabled</th> <th>Last Update Next Update</th> <th>Process ID Start / Stop</th> </tr> </thead> <tbody> <tr> <td>example_ipv4</td> <td>yourhost.example.com No data</td> <td><input type="checkbox"/></td> <td>Never Disabled</td> <td>[Edit] [Delete]</td> </tr> <tr> <td>myddns_ipv6</td> <td>yourhost.example.com No data</td> <td><input type="checkbox"/></td> <td>Never Disabled</td> <td>[Edit] [Delete]</td> </tr> </tbody> </table> <p style="text-align: center;">Add</p> <p style="text-align: right; margin-top: -10px;">Save & Apply Save Reset</p>	Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	example_ipv4	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	[Edit] [Delete]	myddns_ipv6	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	[Edit] [Delete]
Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop												
example_ipv4	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	[Edit] [Delete]												
myddns_ipv6	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	[Edit] [Delete]												

Enabled: Enable this instance.

IP address version: IPv4 and IPv6 supported.

DDNS Service provider: Select a suitable provider.

Hostname/Domain: The Domain name to remotely access the router.

Details for: example_ipv4

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
<p>Enabled <input checked="" type="checkbox"/></p> <p>IP address version <input checked="" type="radio"/> IPv4-Address <input type="radio"/> IPv6-Address</p> <p>DDNS Service provider [IPv4] dyndns.org</p> <p>Hostname/Domain comsetsupport.dvrdns.org</p> <p>Username techsupport</p> <p>Password ***** </p>			
Back to Overview			

IP address source: Defines the source of the systems IPv4-Address which will be sent to the DDNS provider. We recommend the option 'Network'.

Network: Defines the network of the systems IPv4-Address.

DNS-server: OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'. IP address and domain name are required.

Log to syslog: Writes log messages to the syslog. Critical errors will always be written to the syslog.

Log to file: Writes detailed messages to the log file. File will be truncated automatically.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
<p>IP address source [IPv4] Network</p> <p>Network [IPv4] ifmobile</p> <p>DNS-Server mydns.lan</p> <p>PROXY-Server user:password@myproxy.lan:8080</p> <p>Log to syslog Notice</p> <p>Log to file <input checked="" type="checkbox"/></p>			

Check Interval: The minimum check interval is 1 minute=60seconds.

Force interval: The minimum check interval is 1 minute=60seconds.

Error Retry Counter: On Error, the script will stop execution after a given number of retries. The default settings of '0' will retry indefinitely.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
Check Interval	10	minutes	
Force Interval	72	hours	
Error Retry Counter	0		
Error Retry Interval	60	seconds	

Read the log file of DDNS.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
Read / Reread log file			
<pre>/var/log/ddns/example_ipv4.log Please press [Read] button</pre>			

7.7. Connect Radio Module

The Connect Radio Module feature is used for exchanging data between Radio module and serial.

Note:

This feature conflicts with the “DTU” and “GPS sent to serial” functions. Please make sure the other two features are disabled before enabling the Connect Radio Module. Otherwise, the following error will appear:

Connect Mode: Serial only

Modem to Serial Settings

Serial baudrate: 9600/19200/38400/57600/115200bps

Serial parity: none/odd/even

Serial databits: 7 bits/ 8 bits

Serial stopbit: 1 bit/ 2 bits

Serial Flow Control: none/hardware/software

Connect Radio Module Configuration

Exchange data between radio module and serial

Enable	<input checked="" type="checkbox"/>
Connect mode	Serial
Serial baudrate	115200 bps
Serial parity	None
Serial databits	8 bits
Serial stopbits	1 bits

• Enable: conflict with DTU, please disable DTU firstly

8. Network Configuration

8.1. Operation Mode

Status System Services Network Operation Mode Mobile LAN Wired WAN WAN IPv6 Interfaces Wi-Fi Firewall Switch	<p>Operation mode configuration</p> <p>You may configure the operation mode suitable for your environment.</p> <p>Operation mode <input type="radio"/> Bridge mode All ethernet and wireless interfaces are bridged into a single bridge interface.</p> <p><input checked="" type="radio"/> Gateway mode The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.</p> <p><input type="radio"/> AP client mode The wireless ap client interface is treated as WAN port</p> <p>Wired-WAN port role <input checked="" type="radio"/> Wired-WAN port acts as WAN <input type="radio"/> Wired-WAN port acts as LAN</p> <p>NAT enable <input checked="" type="checkbox"/></p> <p style="text-align: right;">Save & Apply Save Reset</p>
---	--

Operation mode

Bridge: All Ethernet and wireless interfaces are bridged into a single bridge interface.

Gateway: The first Ethernet port is treated as a WAN port. The second Ethernet port and the wireless interface are bridged together and are treated as LAN ports.

AP Client: The wireless ap client interface is treated as a WAN port and the wireless AP interface and the Ethernet ports are treated as LAN ports.

NAT Enabled

Network Address Translation. Default is *Enabled*.

Ethernet WAN port:

Wired-WAN port acts as WAN

Wired-WAN port acts as LAN

The default operation is in “Gateway mode”.

8.2. Mobile configuration

The router supports several cell modems. If you replace the original cell modem with a different one, the router will automatically detect the new modem.

Network Operation Mode Mobile LAN Wired WAN WAN IPv6 Interfaces Wi-Fi Firewall Switch DHCP and DNS Diagnostics Dynamic Routing Loopback Interface Hostnames Guest LAN(Guest WiFi) Static Routes QoS Logout	<div style="border-bottom: 1px solid black; margin-bottom: 10px;"> SIM 1 </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Enable: <input checked="" type="checkbox"/> </div> <div style="width: 45%;"> Mobile connection: <input type="button" value="DHCP mode"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> PIN code: <input type="text"/> </div> <div style="width: 45%;"> Dialing number: <input type="text" value="*99#"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> APN: <input type="text" value="telstra.internet"/> </div> <div style="width: 45%;"> Authentication method: <input type="button" value="None"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Dual APN support: <input type="checkbox"/> </div> <div style="width: 45%;"> Network Type: <input type="button" value="automatic"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> MTU: <input type="text" value="1500"/> </div> <div style="width: 45%;"> Online mode: <input type="button" value="Keep Alive"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Metric: <input type="text" value="0"/> </div> <div style="width: 45%;"> IPv4 netmask: <input type="text"/> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Default route: <input checked="" type="checkbox"/> </div> <div style="width: 45%;"></div> </div>
--	---

Enable: Enable mobile network;

Mobile connection: Select a suitable mode for the mobile connection. The default value is DHCP mode;

APN: Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

PIN number: Most SIM cards don't have a PIN number, in which case you leave this field blank;

Dialing number: Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

Authentication method: There are three options to choose from (None, PAP, CHAP). Please confirm with your carrier the type of authentication. Normally select *None*;

Username: Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

Note: If your SIM card has no username, please input the default value, otherwise the router may not dialup. If the authentication method is 'None', this option will not appear.

Password: Fill in the related value. This can be obtained from your carrier or SIM Card Provider.

Network Type: Different Cell Modems support different types. The default value is *Automatic*.

MTU: Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500. Please configure it to optimise your own network.

Online Mode

Keep Alive: Means always online. The router will keep online whether there is data for transmission or not.

On Demand: The router will dialup only when there is data for transmission.

Idle time (minutes): Fill in the time. For example, if you fill in 5, the router will go offline after 5 minutes if there is no data for transmission.

Scheduled: The router will dialup or go offline depending on the schedule.

8.3. Cell mobile data limitation

Enable data limitation:

Period: Month, Week or Day.

Start day: The first day of the period.

SIM data limit (MB): The maximum data that can be used during this period. If it is exceeded, the router will terminate the cell mobile connection.

Enable alarm: Enable 'data limitation' alarm.

Phone number: The phone number that receives the data limitation alarm SMS.

Warning percent of data used: If the used data reaches this level, a data limitation alarm SMS will be sent.

Used (MB): The data that has been consumed so far during this period.

General	Data Limitation	
Data Limitation Configuration		
Enable data limitation	<input type="checkbox"/>	
Period	Month	
Start day	1	
SIM data limit(MB)	0	
Enable alarm	<input type="checkbox"/>	
Phone number		
Warning percent of Data Used	90 %	
Used(Bytes)	6474236	

8.4. LAN settings

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Status	br-lan	Uptime: 0h 16m 51s MAC-Address: 90:22:06:00:00:00 RX: 1.38 MB (7506 Pkts.) TX: 1.10 MB (5224 Pkts.) IPv4: 192.168.1.1/24 IPv6: fdef1a1b:e9dc::1/60	
Protocol	Static address		
Really switch protocol?	<input checked="" type="checkbox"/> Switch protocol		
IPv4 address	192.168.1.1		
IPv4 netmask	255.255.255.0		
IPv4 gateway			
IPv4 broadcast			
Use custom DNS servers			
IPv6 assignment length	60		

Protocol: Only static address is supported for LAN.

Use custom DNS servers: Multiple DNS servers are supported.

IPv6 assignment length: Assign a part of given length of every public IPv6-prefix to LAN interface.

IPv6 assignment hint: Assign prefix parts using this hexadecimal sub prefix ID for LAN interface.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot	<input checked="" type="checkbox"/>		
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Override MAC address	90:22:06:80:02:01		
Override MTU	1500		
Use gateway metric	0		

Bring up on boot: If checked, the LAN interface will be set to 'up' upon system boot-up. If unchecked, the LAN interface will be 'down'. Don't uncheck it if not required.

Use built-in IPv6-management: The default is checked. If IPv6 is not needed, it can be unchecked.

Override MAC address: Overrides LAN MAC address.

Override MTU: Maximum Transmission Unit.

Use gateway metric: The LAN subnet's metric to gateway.

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

Bridge interfaces

Enable STP

- Interface Wired-LAN (lan)
 Wired-WAN (wan, wan6)
 Mobile-eth
 WiFi (lan)

Bridge interfaces: LAN bridges wired-LAN and WiFi in the same LAN subnet.

Enable STP: Enable Spanning Tree Protocol on LAN. The default value is unchecked.

DHCP Server

General Setup Advanced Settings IPv6 Settings

Ignore interface

Start

Limit

Leasetime

Ignore interface: If it is unchecked, this will disable DHCP on LAN.

Start: Lowest leased address as offset from the network address.

Limit: Maximum number of leased addresses.

Leasetime: Expiry time of leased addresses, minimum is 2 minutes (2m).

DHCP Server

General Setup Advanced Settings IPv6 Settings

Dynamic DHCP

Force

IPv4-Netmask

DHCP-Options



Dynamic DHCP: Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force: Force DHCP on this network even if another server is detected.

IPv4-Netmask: Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options: Define additional DHCP options. (For example, '192.168.2.1 and 192.168.2.2' which advertises different DNS servers to clients.)

DHCP Server

General Setup Advanced Settings IPv6 Settings

Router Advertisement-Service	server mode
DHCPv6-Service	server mode
NDP-Proxy	disabled
DHCPv6-Mode	stateless + stateful
Always announce default router	<input type="checkbox"/>
Announced DNS servers	<input type="text"/> + x
Announced DNS domains	<input type="text"/> + x

Router Advertisement-Service: Four options: disabled, server mode, relay mode and hybrid mode.

DHCPv6-Service: Same options as above.

NDP-Proxy: Three options: disabled, relay mode and hybrid mode.

Always announce default router: Announce as default router even if no public prefix is available.

8.5. Wired-WAN

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces. INTERFACE.VLANNR (e.g., eth0.1).

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

Status	eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:00:65:FC RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)
Protocol	DHCP client	
Hostname to send when requesting DHCP	645M-4	

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

Protocol: The default protocol is DHCP client. If you need to change it to a different protocol (i.e. PPPoE), select the protocol from the drop-down menu, then click the button “Switch protocol”.

Note: the ‘Advanced Settings’ is different for different protocols. Move the mouse over the title to get help information. We recommend you use Google Chrome.

8.6. WiFi Settings

Wi-Fi Overview

Generic MAC80211 802.11bgn (radio0)		Channel: 11 (2.462 GHz) Bitrate: 65 Mbit/s	<input type="button"/> WiFi Restart	<input type="button"/> AP Client	<input type="button"/> Add
	SSID: Cell_AP_00036f Mode: Master BSSID: 90:22:06:00:03:6F Encryption: WPA2 PSK (CCMP)		<input checked="" type="button"/> Disable	<input type="button"/> Edit	<input checked="" type="button"/> Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cell_AP_00036f	E8:50:8B:21:F2:28	?	-50 dBm	0 dBm	6.0 Mbit/s, MCS 0, 20MHz	65.0 Mbit/s, MCS 6, 20MHz

Wifi Restart: turn WiFi off then on.

AP Client: Scan all frequencies to get the WiFi network information.

Add: Add a new wireless network.

Disable: Disable a wireless network.

Edit: Modify settings of the wireless network.

Remove: Delete a wireless network.

Associated Stations: This is a list of connected wireless stations.

8.7. WiFi General configuration

Device Configuration

General Setup **Advanced Settings**

Status 85% Mode: Master | SSID: Cell_AP_00036f
 BSSID: 90:22:06:00:03:6F | Encryption: WPA2 PSK (CCMP)
 Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm
 Signal: -50 dBm | Noise: 0 dBm
 Bitrate: 72.2 Mbit/s | Country: 00

Wi-Fi network is enabled Disable

Operating frequency Mode: 11g/n mixed | Channel: 11 (2462 MHz) | Width: 20 MHz

Transmit Power 20 dBm (100 mW)

Status: Shows the WiFi signal strength, mode, SSID.

Operating frequency Mode: Supports 802.11b/g/n. the Legacy means 802.11b/g. "N" means 802.11n.

Channel: Channel 1-11.

Width: 20MHz and 40MHz.

Transmit Power: From 0dBm to 20dBm.

8.8. WiFi Advanced Configuration

Device Configuration

General Setup	Advanced Settings
Country Code	00 - World
Distance Optimization	
Fragmentation Threshold	
RTS/CTS Threshold	

Country Code: Use ISO/IEC 3166 alpha2 country codes.

Distance Optimization: Distance to furthest network member in meters.

Fragmentation Threshold

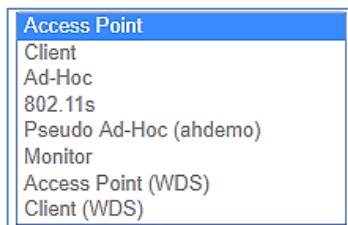
RTS/CTS Threshold

8.9. WiFi Interface Configuration

General Setup

ESSID: Extended Service Set Identifier. It is the broadcast name.

Mode: Supported options.



Network: Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

Hide Extended Service Set Identifier: ‘Hide SSID’ means this WiFi cannot be scanned by others.

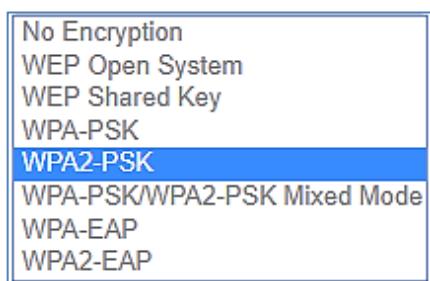
WMM Mode

Interface Configuration

General Setup	Wireless Security	MAC-Filter
ESSID	ELPRO_645M-4	
Mode	Access Point	
Network	<input type="checkbox"/> ifmobile:  <input checked="" type="checkbox"/> lan:  <input type="checkbox"/> wan:  <input type="checkbox"/> wan6:  <input type="checkbox"/> create: <input type="text"/>	
Hide Extended Service Set Identifier	<input type="checkbox"/>	
WMM Mode	<input checked="" type="checkbox"/>	

Wireless Security

Encryption:



Key: It is the password to join the wireless network. If the Encryption is set to "No Encryption", no password is needed.

Interface Configuration

General Setup	Wireless Security	MAC-Filter
Encryption: WPA2-PSK		
Cipher: auto		
Key: 		
Enable WPS pushbutton, requires WPA(2)-PSK <input checked="" type="checkbox"/>		

MAC Filter

MAC-Address Filter: MAC Address Access Policy.

Disabled: disable MAC-address filter functionality.

Allow list: Only the MAC addresses in the list are forwarded.

Deny list: All packets can be forwarded except MAC address in the list.

MAC-List: Click button  to delete a MAC address from list, click button  to add a new MAC address to the list.

Interface Configuration

General Setup	Wireless Security	MAC-Filter
MAC-Address Filter: Allow list		
MAC-List:		
00:1E:10:1F:00:00 (10.223.164) 		
68:A8:6D:48:77:5E (dentydeME) 		
90:22:06:80:02:01 (Cell_Router) 		

8.10. WiFi AP client

Steps 1) Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.

Join Network: Wireless Scan

 MERCURY_FE2A Channel: 3 Mode: Master BSSID: 8C:F2:28:FD:FE:2A Encryption: mixed WPA/WPA2 - PSK	<input type="button" value="Join Network"/>
<input type="button" value="Back to overview"/> <input type="button" value="Repeat scan"/>	

Step 2) If the WiFi you want to join is on the list, click the button “Join Network” accordingly. If it is not, click “Repeat Scan” until you find the WiFi that you want to join.

Join Network: Settings

<input checked="" type="checkbox"/> Replace wireless configuration	
WPA passphrase	<input type="text" value="*****"/> 
Name of the new network <input type="text" value="wwan"/>	
<input type="button" value="Submit"/> <input type="button" value="Back to scan results"/>	

Step 3) Join Network Settings

Replace wireless configuration: An additional wireless network will be created if it is unchecked. Otherwise it will replace the old configuration.

WPA passphrase: Specify the secret encryption key here.

Name of the new network: The default value is ‘wwan’. Please change it if it conflicts with other interfaces.

Step 4) Click ‘Submit’ if everything is configured. The below is the Wi-Fi configuration page. Don’t change the operating frequency. Make sure the ESSID and BSSID are for the Wi-Fi you want to join.

Device Configuration

<input type="button" value="General Setup"/>	<input type="button" value="Advanced Settings"/>						
<div style="display: flex; justify-content: space-between;"> Status <div style="flex-grow: 1;"> Mode: Client SSID: MERCURY_FE2A BSSID: 8C:F2:28:FD:FE:2A Encryption: - Channel: 11 (2.462 GHz) Tx-Power: 0 dBm Signal: 0 dBm Noise: 0 dBm Bitrate: 0.0 Mbit/s Country: 00 </div> </div>							
Wireless network is enabled <input type="button" value="Disable"/>							
Operating frequency <table style="margin-left: auto; margin-right: auto;"> <tr> <th>Mode</th> <th>Channel</th> <th>Width</th> </tr> <tr> <td>N</td> <td>3 (2422 MHz)</td> <td>20 MHz</td> </tr> </table>		Mode	Channel	Width	N	3 (2422 MHz)	20 MHz
Mode	Channel	Width					
N	3 (2422 MHz)	20 MHz					
Transmit Power <table style="margin-left: auto; margin-right: auto;"> <tr> <td>20 dBm (100 mW)</td> <td style="text-align: right;">▼</td> </tr> </table>		20 dBm (100 mW)	▼				
20 dBm (100 mW)	▼						

Interface Configuration

General Setup Wireless Security

ESSID	MERCURY_FE2A
Mode	Client
BSSID	8C:F2:28:FD:FE:2A
Network	<input type="checkbox"/> ifmobile:  <input type="checkbox"/> lan:  <input type="checkbox"/> wan:  <input type="checkbox"/> wan6:  <input checked="" type="checkbox"/> wwan:  <input type="checkbox"/> create: <input type="text"/>

Step 5) Click the button “Save & Apply” to start the AP client.

Wireless Overview

	Generic MAC80211 802.11bgn (radio0) Channel: 3 (2.422 GHz) Bitrate: 150 Mbit/s	 Wifi Restart  AP Client  Add
	68% SSID: Cell_AP_0002b2 Mode: Master BSSID: 90:22:06:00:02:B3 Encryption: None	 Disable  Edit  Remove
	85% SSID: MERCURY_FE2A Mode: Client BSSID: 8C:F2:28:FD:FE:2A Encryption: WPA2 PSK (CCMP)	 Disable  Edit  Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
 Cell_AP_0002b2	68:A8:6D:48:77:5E	?	-62 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	58.5 Mbit/s, MCS 6, 20MHz
 MERCURY_FE2A	8C:F2:28:FD:FE:2A	192.168.1.1	-50 dBm	0 dBm	135.0 Mbit/s, MCS 7, 40MHz	150.0 Mbit/s, MCS 7, 40MHz

8.11. Interfaces Overview

The “Interfaces Overview” page shows all Interfaces status, including uptime, MAC-address, RX, TX and IP address.

Interfaces

Interface Overview

Network	Status	Actions
LAN  br-lan	Uptime: 0h 50m 35s MAC-Address: 90:22:06:80:02:01 RX: 945.69 KB (9759 Pkts.) TX: 2.35 MB (6976 Pkts.) IPv4: 192.168.10.1/24 IPv6: fd90:5065:78e::1/60	 Connect  Stop  Edit
IFMOBILE  eth1	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	 Connect  Stop  Edit
WAN  eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:C0:02:01 RX: 0.00 B (0 Pkts.) TX: 480.27 KB (1433 Pkts.)	 Connect  Stop  Edit
WAN6  eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:C0:02:01 RX: 0.00 B (0 Pkts.) TX: 480.27 KB (1433 Pkts.)	 Connect  Stop  Edit
WWAN  Client "MERCURY_FE2A"	Uptime: 0h 5m 46s MAC-Address: 90:22:06:00:02:B2 RX: 243.14 KB (980 Pkts.) TX: 236.01 KB (1861 Pkts.) IPv4: 192.168.1.105/24	 Connect  Stop  Edit

8.12. Firewall

	General Settings	Port Forwards	Traffic Rules	DMZ	Security
--	------------------	---------------	---------------	-----	----------

Firewall - General Settings

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

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: reject

8.13. Port Forwards

This page includes the “Port Forwards” list and how to add new “Port Forwards” rules.

General Settings	Port Forwards	Traffic Rules	DMZ	Security																																				
Firewall - Port Forwards Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.																																								
Port Forwards <table border="1"> <thead> <tr> <th>Name</th> <th>Match</th> <th>Forward to</th> <th>Enable</th> <th>Sort</th> </tr> </thead> <tbody> <tr> <td colspan="5"><i>This section contains no values yet</i></td> </tr> <tr> <td colspan="5"> New port forward: <table border="1"> <thead> <tr> <th>Name</th> <th>Protocol</th> <th>External zone</th> <th>External port</th> <th>Internal zone</th> <th>Internal IP address</th> <th>Internal port</th> </tr> </thead> <tbody> <tr> <td>New port forward</td> <td>TCP+UDP</td> <td>ope</td> <td></td> <td>lan</td> <td></td> <td></td> </tr> <tr> <td colspan="7"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </td> </tr> </tbody> </table> </td> </tr> </tbody> </table>					Name	Match	Forward to	Enable	Sort	<i>This section contains no values yet</i>					New port forward: <table border="1"> <thead> <tr> <th>Name</th> <th>Protocol</th> <th>External zone</th> <th>External port</th> <th>Internal zone</th> <th>Internal IP address</th> <th>Internal port</th> </tr> </thead> <tbody> <tr> <td>New port forward</td> <td>TCP+UDP</td> <td>ope</td> <td></td> <td>lan</td> <td></td> <td></td> </tr> <tr> <td colspan="7"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </td> </tr> </tbody> </table>					Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	New port forward	TCP+UDP	ope		lan			<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>						
Name	Match	Forward to	Enable	Sort																																				
<i>This section contains no values yet</i>																																								
New port forward: <table border="1"> <thead> <tr> <th>Name</th> <th>Protocol</th> <th>External zone</th> <th>External port</th> <th>Internal zone</th> <th>Internal IP address</th> <th>Internal port</th> </tr> </thead> <tbody> <tr> <td>New port forward</td> <td>TCP+UDP</td> <td>ope</td> <td></td> <td>lan</td> <td></td> <td></td> </tr> <tr> <td colspan="7"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </td> </tr> </tbody> </table>					Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	New port forward	TCP+UDP	ope		lan			<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>																					
Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port																																		
New port forward	TCP+UDP	ope		lan																																				
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>																																								

Name: Port Forward instance name.

Protocol: TCP+UDP, UDP and TCP can be chosen.

External zone: The recommended option is ‘wan’.

External port: Match incoming traffic directed at the given destination port on this host.

Internal zone: The recommended zone is ‘lan’.

Internal IP address: Redirect matched incoming traffic to the specific host.

Internal port: Redirect matched incoming traffic to the given port on the internal host.

8.14. 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.

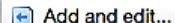
The traffic rules overview page contains the following functionalities:

Traffic rules list:

Traffic Rules					
Name	Match	Action	Enable	Sort	
Allow-DHCP-Renew	IPv4-UDP From <i>any host in wan</i> To <i>any router IP at port 68 on this device</i>	Accept input	<input checked="" type="checkbox"/>	 	 
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host in wan</i> To <i>any host in any zone</i>	Accept forward	<input checked="" type="checkbox"/>	 	 
Allow-IGMP	IPv4-IGMP From <i>any host in wan</i> To <i>any router IP on this device</i>	Accept input	<input checked="" type="checkbox"/>	 	 
Allow-DHCPv6	IPv6-UDP From IP range <i>fe80::/10 in wan</i> with source port 547 To IP range <i>fe80::/10 at port 546 on this device</i>	Accept input	<input checked="" type="checkbox"/>	 	 
Allow-MLD	IPv6-ICMP with types <i>130/0, 131/0, 132/0, 143/0</i> From IP range <i>fe80::/10 in wan</i> To <i>any router IP on this device</i>	Accept input	<input checked="" type="checkbox"/>	 	 
Allow-ICMPv6-Input	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> From <i>any host in wan</i> To <i>any router IP on this device</i>	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	 	 
Allow-ICMPv6-Forward	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type</i> From <i>any host in wan</i> To <i>any host in any zone</i>	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	 	 

Open ports on router and create 'new forward rules':

Open ports on router:			
Name	Protocol	External port	
New input rule	TCP+UDP		

New forward rule:			
Name	Source zone	Destination zone	
New forward rule	Ian	wan	

Source NAT list and create source NAT rule:

Source NAT					
Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.					
Name	Match	Action	Enable	Sort	
<i>This section contains no values yet</i>					
New source NAT:					
Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	Ian	wan	-- Please cho	Do not rewrite	

Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Firewall - Traffic Rules - forwardtest

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	<input checked="" type="checkbox"/> Disable
Name	forwardtest
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	<input type="radio"/> Any zone <input checked="" type="radio"/> lan: lan:  <input type="radio"/> openvpn: (empty) <input type="radio"/> vpnzone: (empty) <input type="radio"/> wan: wan:  wan6:  ifmobile:  wwan: 

Source MAC address	any
Source address	any
Source port	any
Destination zone	<input type="radio"/> Device (input) <input type="radio"/> Any zone (forward) <input checked="" type="radio"/> lan: lan:  <input type="radio"/> openvpn: (empty) <input type="radio"/> vpnzone: (empty) <input type="radio"/> wan: wan:  wan6:  ifmobile:  wwan: 

Destination address	any
Destination port	any
Action	accept
Extra arguments	

Name: Traffic rule entry name.

Restrict to address family: IPv4+IPv6, IPv4 and IPv6 can be selected. Specify the matched IP address family.

Protocol: Specify the protocol matched in this rule. "Any" means any protocol is matched.

Source zone: It is the zone that the traffic comes from.

Source MAC address: Traffic rule check if the incoming packet's source MAC address is matched.

Source address: Traffic rule check if the incoming packet's source IP address is matched.

Source port: Traffic rule check if the incoming packet's TCP/UDP port is matched.

Destination zone: The zone that the traffic will go to.

Destination address: Traffic rule check if the incoming packet's destination IP address is matched.

Destination port: Traffic rule check if the incoming packet's TCP/UDP port is matched.

Action: If traffic is matched, the system will handle traffic according to the Action (accept, drop, reject, don't track).

Extra argument: Passes additional argument to the "iptables".

8.15. DMZ

General Settings	Port Forwards	Traffic Rules	DMZ	Security
------------------	---------------	---------------	-----	----------

DMZ Configuration

You may setup a Demilitarized Zone(DMZ) to separate internal network and Internet.

Enable DMZ

IP address

Protocol

In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

IP Address: Please Enter the IP address of the computer which you want to set as DMZ host

Protocol: All protocols, TCP+UDP, TCP, UDP.

Note: When DMZ host is settled, the computer is completely exposed to the external network; the firewall will not influence this host.

8.16. Security

SSH access from WAN: Allow or deny users to access the router from remote side.

Ping from WAN to LAN: Allow or deny ping from remote side to the internal LAN subnet.

HTTPS access from WAN: Allow or deny access to the router web management page from the remote side.

Remote network: Any IP Address, Single IP address, Subnet.

IP address: Fill a remote IP address that can access the router's web management page.

Netmask: 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.

General Settings	Port Forwards	Traffic Rules	DMZ	Security
------------------	---------------	---------------	-----	----------

System security configuration

SSH access from WAN

Ping from WAN to LAN

HTTPS Remote Access

HTTPS access from WAN

Remote network

IP address

Netmask

HTTP Remote Access

HTTP access from WAN

Remote network

8.17. Static Routes

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
lan	<input type="text"/>	255.255.255.255	<input type="text"/>	0	1500

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
This section contains no values yet				



Interface: You can choose the corresponding interface type.

Target: The destination host IP or network.

Gateway: IP address of the next router.

Notice:

The Gateway and LAN IP of this router must belong to the same network segment.

If the destination IP address is that of a host, then the Netmask must be 255.255.255.255.

If the destination IP address is an IP network segment, it must match with the Netmask. For example, if the destination IP is 10.0.0.0, and the Netmask is 255.0.0.0.

8.18. Switch

VLANs on "switch0" (rt305x-esw)

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	Port 5	CPU
1	untagged	untagged	untagged	untagged	off	off	tagged
2	off	off	off	off	untagged	off	tagged



Note:

1. Port 4 is Wired-WAN port, port 0, port 1, port 2, port 3 are LAN ports.
2. “Untagged” means the Ethernet frame transmits from this port without VLAN tag.
3. “Tagged” means the Ethernet frame transmits from this port with VLAN tag.
4. “Off” means this port does not belong to VLAN. For default settings, port 0 belongs to VLAN1, but does not belong to VLAN 2.

8.19. DHCP and DNS

Domain required: Don't forward DNS-requests without DNS-Name.

Authoritative: This is the only DHCP on the local network.

Local server: Local domain specifications. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only.

Local domain: Local domain suffix appended to DHCP names and hosts file entries.

Log queries: Write received DNS requests to syslog.

DNS forwarding's: List of DNS servers to forward requests to.

Rebind protection: Discard upstream RFC1918 responses.

Allow localhost: Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services.

Domain whitelist: List of domains to allow RFC1918 responses for.

Suppress logging: Suppress logging of the routine operation of these protocols.

Allocate IP sequentially: Allocate IP addresses sequentially, starting from the lowest available address.

Filter private: Do not forward reverse lookups for local networks.

Filter useless: Do not forward requests that cannot be answered by public name servers.

Localise queries: Localise hostname depending on the requesting subnet if multiple IPs are available.

Expand hosts: Add local domain suffix to names served from hosts files.

No negative cache: Do not cache negative replies, e.g. for non existing domains.

Strict order: DNS servers will be queried in the order of the resolv file.

Bogus NX Domain Override: List of hosts that supply bogus NX domain results.

DNS server port: Listening port for inbound DNS queries.

DNS query port: Fixed source port for outbound DNS queries.

Max DHCP leases: Maximum allowed number of active DHCP leases.

Max edns0 packet size: Maximum allowed size of EDNS.0 UDP packets.

Max concurrent queries: Maximum allowed number of concurrent DNS queries.

DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

Server Settings

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
<input checked="" type="checkbox"/> Domain required			
<input checked="" type="checkbox"/> Authoritative			
Local server	/lan/		
Local domain	lan		
<input type="checkbox"/> Log queries			
DNS forwardings	/example.org/10.1.2.3		
<input checked="" type="checkbox"/> Rebind protection			
<input checked="" type="checkbox"/> Allow localhost			
Domain whitelist	ihost.netflix.com		

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
<input type="checkbox"/> Suppress logging			
<input type="checkbox"/> Allocate IP sequentially			
<input checked="" type="checkbox"/> Filter private			
<input type="checkbox"/> Filter useless			
<input checked="" type="checkbox"/> Localise queries			
<input checked="" type="checkbox"/> Expand hosts			
<input type="checkbox"/> No negative cache			
<input type="checkbox"/> Strict order			
Bogus NX Domain Override	67.215.65.132		
DNS server port	53		
DNS query port	any		
Max. DHCP leases	unlimited		
Max. EDNS0 packet size	1280		
Max. concurrent queries	150		

8.20. Diagnostics

Diagnostics

Network Utilities

<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>
<input type="button" value="IPv4"/>	<input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>
		<input type="button" value="Nslookup"/>

Ping: It is a tool used to test the reachability of a host on an Internet Protocol (IP) network.

Traceroute: It is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

Nslookup: It is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

For example if you want to ping www.google.com, type the target domain name or IP address, then click the button "Ping". Wait a couple of seconds, the result will be shown as below.

Diagnostics

Network Utilities

<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>
<input type="button" value="IPv4"/>	<input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>
		<input type="button" value="Nslookup"/>


```
PING www.google.com (93.46.8.89): 56 data bytes
--- www.google.com ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

8.21. Loopback Interface

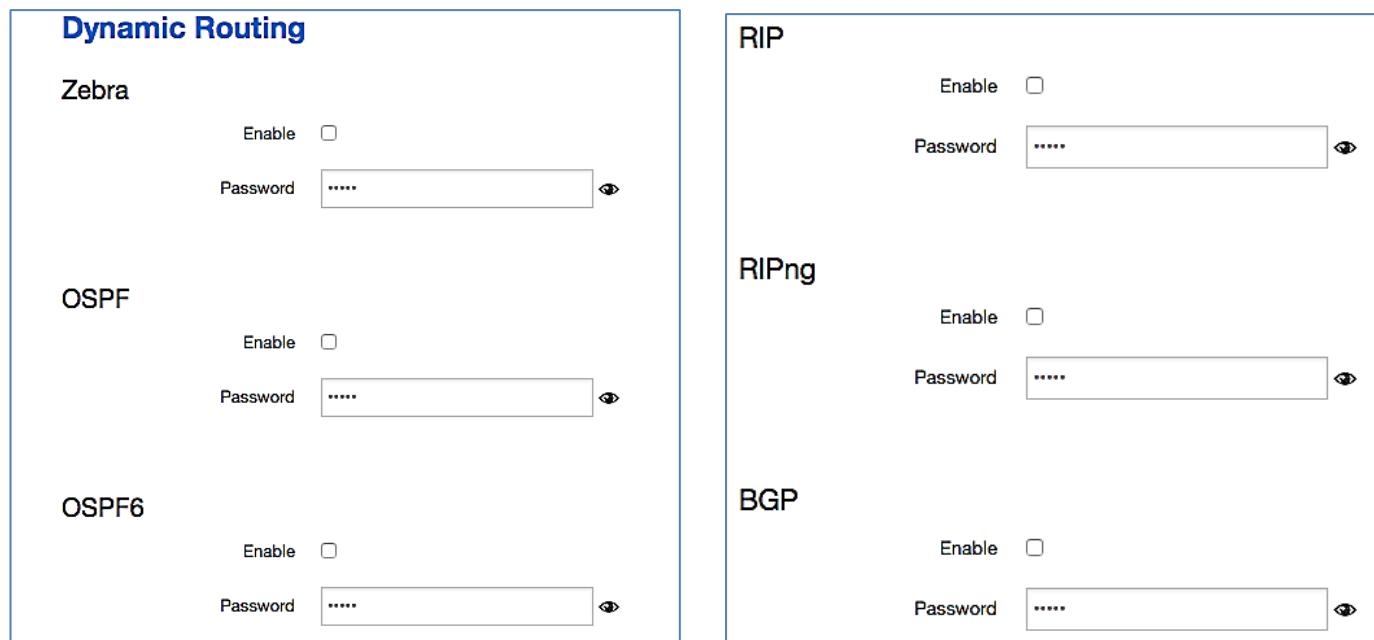
Loopback Interface Configuration

IP address	<input type="text" value="127.0.0.1"/>
Netmask	<input type="text" value="255.0.0.0"/>

The default Loopback interface has IP address 127.0.0.1. You can change it if required.

8.22. Dynamic Routing

Dynamic Routing is implemented by quagga-0.99.22.4. Dynamic Routing services can be enabled:



Dynamic Routing	
Zebra	Enable <input type="checkbox"/> Password <input type="text" value="....."/>
OSPF	Enable <input type="checkbox"/> Password <input type="text" value="....."/>
OSPF6	Enable <input type="checkbox"/> Password <input type="text" value="....."/>
RIP	Enable <input type="checkbox"/> Password <input type="text" value="....."/>
RIPng	Enable <input type="checkbox"/> Password <input type="text" value="....."/>
BGP	Enable <input type="checkbox"/> Password <input type="text" value="....."/>

Zebra: Zebra is an IP routing manager. Telnet port number is 2601.

OSPF: Open Shortest Path First. Telnet port number is 2604.

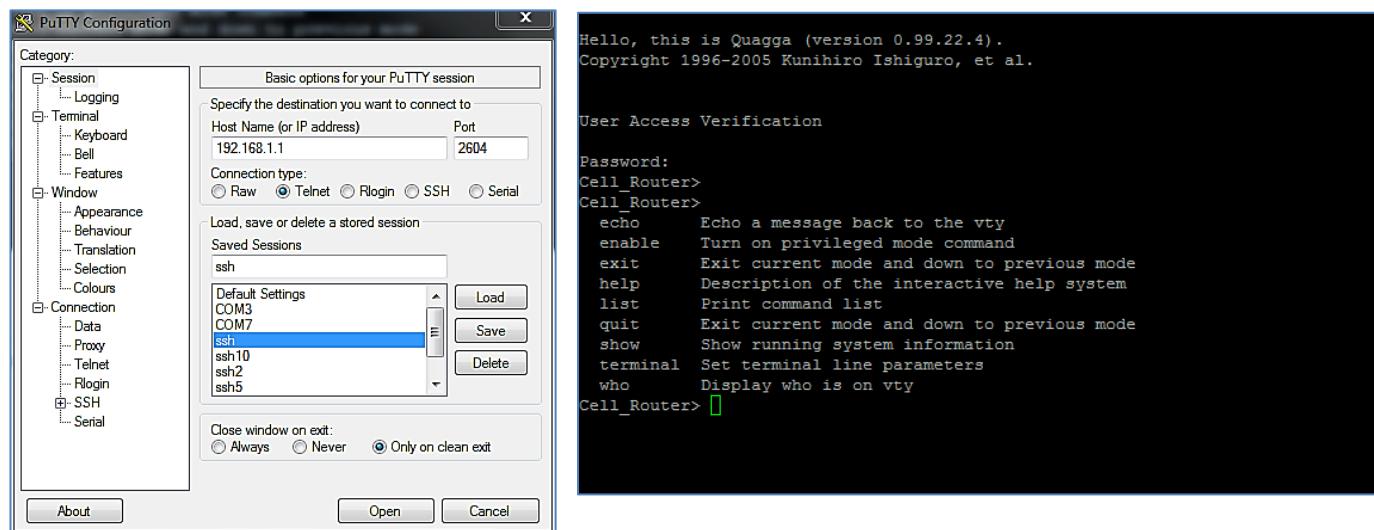
OSPF6: Open Shortest Path First for IPv6. Telnet port number is 2606.

RIP: Routing Information Protocol. Telnet port number is 2602.

RIPng: It is an IPv6 reincarnation of the RIP protocol. Telnet port number is 2603.

BGP: Border Gateway Protocol. Telnet port number is 2605.

Example: The router's LAN IP is 192.168.10.1. If we want to configure OSPF, we need to set OSPF to "Enable" first, then open putty in windows:



PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type: Telnet Raw Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions: ssh

Default Settings: COM3, COM7, ssh1, ssh10, ssh2, ssh5

Close window on exit: Always Never Only on clean exit

Terminal Window Output:

```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Cell_Router>
Cell_Router> echo    Echo a message back to the vty
Cell_Router> enable   Turn on privileged mode command
Cell_Router> exit     Exit current mode and down to previous mode
Cell_Router> help    Description of the interactive help system
Cell_Router> list    Print command list
Cell_Router> quit    Exit current mode and down to previous mode
Cell_Router> show    Show running system information
Cell_Router> terminal Set terminal line parameters
Cell_Router> who     Display who is on vty
Cell_Router> [ ]
```

Input the password of OSPF. Then press key "?" for help.

8.23. QoS

QoS (Quality of Service) can prioritise network traffic selected by addresses, ports or services.

Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

		<input type="button" value="Delete"/>
WAN		
Enable	<input checked="" type="checkbox"/>	
Classification group	<input type="button" value="default"/>	
Calculate overhead	<input type="checkbox"/>	
Half-duplex	<input type="checkbox"/>	
Download speed (kbit/s)	<input type="text" value="1024"/>	
Upload speed (kbit/s)	<input type="text" value="128"/>	
<input type="button" value=""/>		<input type="button" value="Add"/>

Enable: Enable QoS on this interface.

Classification group: Specify class group used for this interface.

Calculate overhead: Decrease upload and download ratio to prevent link saturation.

Download speed: Download limit in kilobits/second.

Upload speed: Upload limit in kilobits/second.

Classification Rules

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Comment
priority	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="22,53"/>	<input type="button" value=""/>	<input type="button" value="ssh, dns"/>
normal	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="TCP"/>	<input type="button" value="20,21,25,80,110,443,993,995"/>	<input type="button" value=""/>	<input type="button" value="ftp, smtp, http(s), imap"/>
express	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="all"/>	<input type="button" value="5190"/>	<input type="button" value=""/>	<input type="button" value="AOL, iChat, ICQ"/>
<input type="button" value=""/>							<input type="button" value="Add"/>

Each section defines one group of packets and which target (i.e. bucket) this group belongs to. All the packets share the bucket specified.

Target: The four defaults are: priority, express, normal, low.

Source host: Packets matching this source host(s) (single IP or in CIDR notation) belong to the bucket defined in target.

Destination host: Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in target.

Protocol: Matching packets belong to the bucket defined in target.

Ports: Matching packets belong to the bucket defined in target. If more than 1 port is required, they must be separated by a comma.

Number of bytes: Matching packets belong to the bucket defined in target.

9. Specifications

Specification	Description	Specification	Description
Cellular - Radio			
Frequency - Bands	4G LTE FDD MHz 2100 (B1), 1900 (B2), 1800 (B3) 1700 (B4), 850 (B5), 2600 (B7) 900 (B8) 700 (B28) 4G LTE TDD MHz 2300 (B40) UMTS/HSPA/HUSPA,HSPA+/DC-HSPA+ 850/900/1900/2100MHz Quad Band EGSM 850/ 900/ 1800/ 1900MHz	LAN	2 x 10/100M RJ45
WiFi	802.11b/g/n; 300Mbps RF Power; 20dBm 100mW Access Point/ Client / WDS	Serial	1 x RS232 Terminal Interface
Networking			
VPN	OpenVPN, IPSec, L2TP, PPTP Server and Client Supported	Antenna	2 x WiFi SMA (Diversity Support)
Protocols Supported	TCP, UDP, SMTP, POP, ICMP, FTP, PPP, PPPoE, DHCP, DDNS, DNS, SNMP, WPS, DMZ, Syslog (local and remote), NAT, xDSL, NTP, QoS, SNMP, Dynamic routing (OSPF, OSPF6, RIP, RIPng, BGP)	I/O	2 x Cellular SMA 4 x DIO Input or Output (0-3.3VDC) SMS Monitor & Control
Security	64/128 bits WEP, 802.1x, WPA and WPA2, TKIP, AES encryption, WPA1/2- 802.1x, EAP-TLS, TTLS, LEAP, PEAP, Username and password, Access control base WAN/LAN, Access control base source IP, PAP and CHAP, IP filtering, Radius Client	LED	SYS, VPN, SIGNAL, CELL, WAN, LAN, WiFi
VLAN	ID Tagging supported	Power	
Fail over redundancy	Auto-dial feature, keep alive link Cellular (2G/3G/4G), RJ45 WAN (xDSL, DHCP, Fixed IP), WiFi client	Input Power	5-40VDC
Serial Server	RS232 terminal to IP Server	Current Consumption	Idle 122mA@12VDC Max 208mA@12VDC
SMS	SMS call to control router to be online, offline, reboot, status info, alarm, IO, WiFi on, WiFi off	Power Connection	2.5mm DC Jack or Terminal block
Physical			
		Operating Temperature	-40 to +85deg Celsius
		Humidity	95% non condensating
		Weight	220grams
		Dimensions	100mm x 60mm x 21mm
		Warranty	3 Years
		Mounting	Panel mount (optional DIN rail mount)
Compliance			
		Regulatory	RCM, CE, RoHS

Contact Information

ELPRO Technologies

29 Lathe St Virginia,
QLD, Australia, 4014

Phone: +61 7 3352 8600

Email : sales@elpro.com.au

Web: <http://www.elpro.com.au>

ELPRO Technologies Inc.

Address: 2028 East Ben White Blvd, #240-5656
Austin, TX 78741-6931
USA

Phone: +855 443 5776

E-mail: sales@elpro.com.au

Web: www.elpro.com.au