

Industrial Grade 3G 4G 4GX Cellular Router

User Manual

CM685V-4



Comset: 37/ 125 Highbury Rd, Burwood VIC 3125, Australia

Table of Contents

1 Product Introduction	5
1.1 Product overview	5
1.2 Typical Application Diagram	5
1.3 Features	6
2 Hardware Installation	7
2.1 Overall Dimensions	7
2.2 Ports	8
2.3 Powering up the CM685V-4	9
2.4 SIM/UIM card	9
2.5 Terminal block	9
2.6 Grounding	11
2.7 Power Supply	11
2.8 LED Description	11
3 Software configuration	14
3.1 Overview	14
3.2 How to log into the Router	14
3.3 Router status	17
3.3.1 Status overview	17
3.3.2 Network status	18
3.3.3 Firewall status	21
3.3.4 Routes	21
3.3.5 System log	22
3.3.6 Kernel log	22
3.3.7 Realtime graphs	23
3.4 System Configuration	24
3.4.1 Setup wizard	24
3.4.2 System	28
3.4.3 Password	30
3.4.4 NTP	30
3.4.5 Backup/Restore	31
3.4.6 Upgrade	31
3.4.7 Reset	33
3.4.8 Reboot	34
3.5 Services configuration	34
3.5.1 ICMP check	34
3.5.2 VRRP	36
3.5.3 Failover (link backup)	37
3.5.4 DTU	39
3.5.5 SNMP	41
3.5.6 GPS (optional)	43

3.5.7 SMS	45
3.5.8 VPN	48
3.5.8.1 IPSEC	48
3.5.8.2 PPTP	49
3.5.8.3 L2TP	52
3.5.8.4 OpenVPN	53
3.5.8.5 GRE tunnel	55
3.5.9 DDNS	56
3.5.10 Connect Radio Module	58
3.6 Network Configuration	60
3.6.1 Operation Mode	60
3.6.2 Mobile configuration	61
3.6.3 Cell mobile data limitation	62
3.6.4 LAN settings	63
3.6.5 Wired-WAN	66
3.6.6 WiFi Settings	67
3.6.6.1 Wifi General configuration	68
3.6.6.2 WiFi Advanced Configuration	69
3.6.6.3 WiFi Interface Configuration	70
3.6.6.4 WiFi AP client	72
3.6.7 Interfaces Overview	74
3.6.8 Firewall	75
3.6.8.1 General Settings	75
3.6.8.2 Port Forwards	75
3.6.8.3 Traffic rules	76
3.6.8.4 DMZ	80
3.6.8.5 Security	81
3.6.9 Static Routes	82
3.6.10 Switch	82
3.6.11 DHCP and DNS	83
3.6.12 Diagnostics	85
3.6.13 Loopback Interface	86
3.6.14 Dynamic Routing	86
3.6.15 QoS	88

Copyright © COMSET 2017

Comset is a registered trademark of Comset. 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 Comset. All rights reserved.

WARNING: Keep at least a 20 cm distance between the user's body and the modem router device.

Address: 37/ 125 Highbury Road, Burwood VIC 3125, Australia

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

Phone: +61 3 9001 9720

Fax: +61 3 9888 7100

Chapter 1

1 Product Introduction

1.1 Product overview

The Comset CM685V-4 is an industrial grade 3G/4G/4GX LTE WiFi Modem Router based on the latest OpenWrt platform. With download speeds of up to 150 Mbps and upload speeds of up to 50 Mbps, it is one of the few routers on the Australian market that supports band B28 (700MHz).

The Comset CM685V-4 is designed to suit Australian conditions. It supports the latest LTE Advanced Technology that performs fast and reliable data communication. 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 two 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 CM685V-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 Typical Application Diagram

The Comset CM685V-4 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). A good example is the connection of ATM machines and POS systems back to a server over a secure 4G connection using a secure VPN IPSEC tunnel.



1.3 Features

The CM685V-4 supports the following:

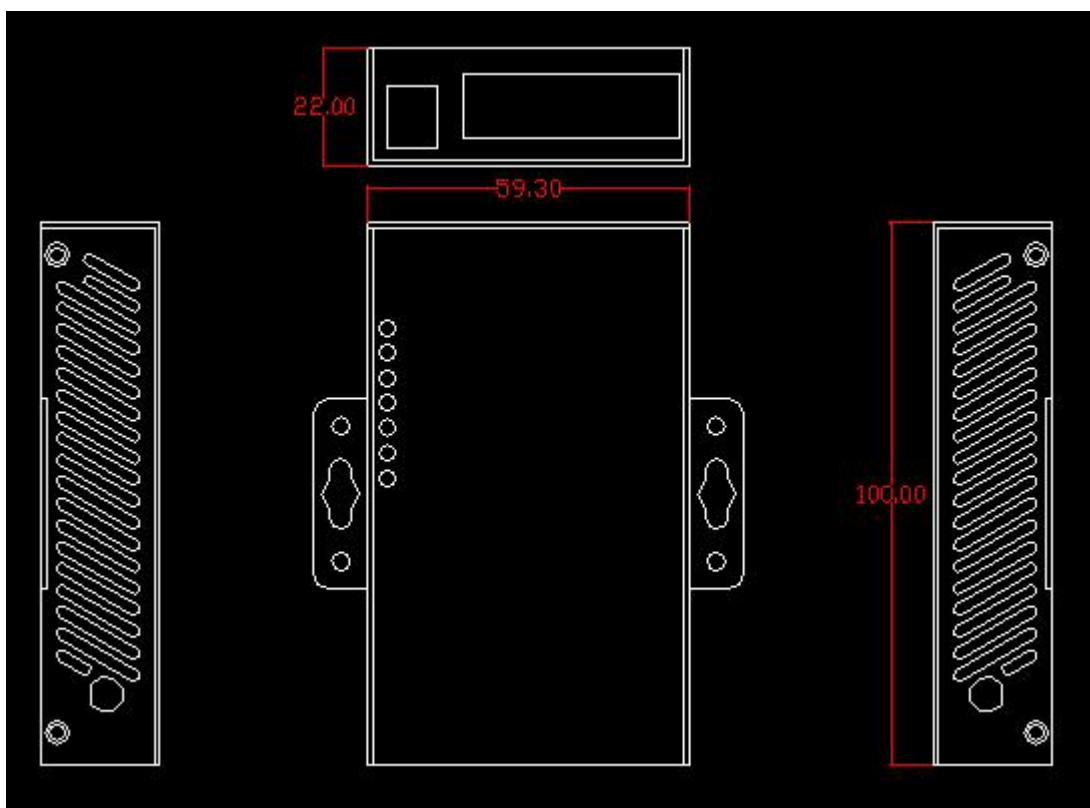
- LTE FDD B1/B2/B3/B4/B5/B7/B8/B28 and LTE TDD B40 with 3G fallback to DC-HSPA+/HSPA+/HSPA/WCDMA B1/B2/B5/B8
- IEEE802.11b/g/n N300 Wi-Fi AP function, WDS bridging, WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, Authenticated encryption mode
- RS232 interface data transparent transmission and protocol 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

Chapter 2

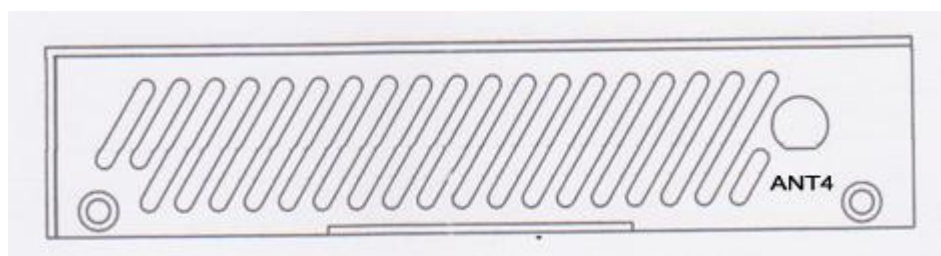
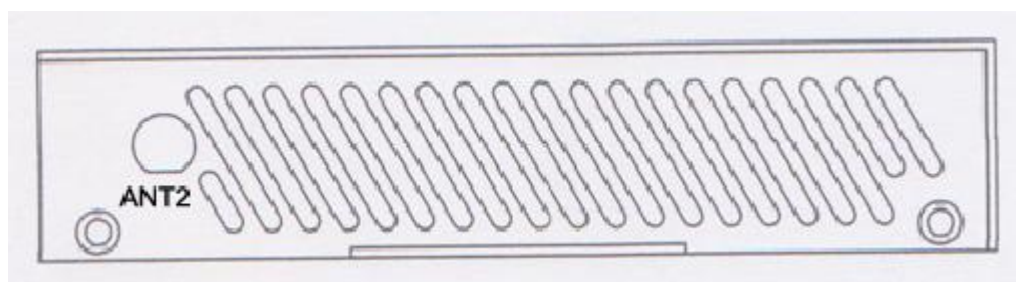
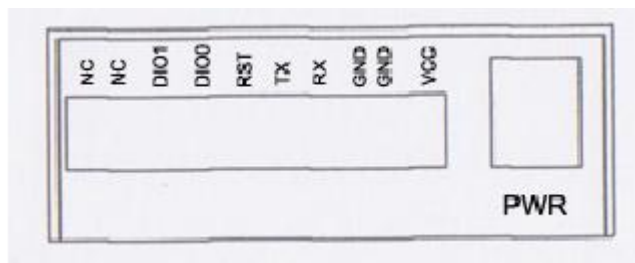
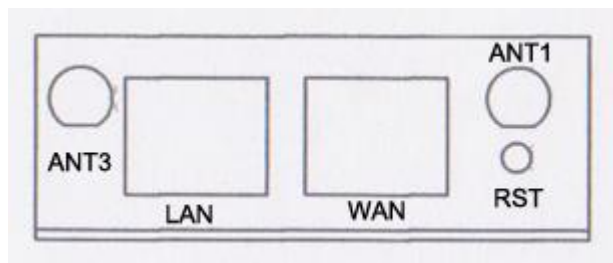
2 Hardware Installation

1. *Overall Dimensions*
2. *Accessories*
3. *Installation*

2.1 Overall Dimensions



2.2 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: Not connected

WPS: WPS button

Antenna Connections Table

Antenna Connector	Marks
Cell	for main cell antenna
Aux	for auxiliary cell antenna
WiFi 1	for WiFi-1 antenna
WiFi 2	For WiFi-2 antenna
GPS	for GPS antenna (optional)

2.3 Powering up the CM685V-4

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

2.4 SIM/UIM card

If your router has a SIM/UIM card cover, please remove it and have the SIM card properly inserted.

2.5 Terminal block

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



Attention:

1. If you are not using the AC adapter supplied with the router, and if you wish to power up the unit using the terminal block, the power cable should be wired with the correct voltage polarity. Wrong wiring will destroy the equipment. Pin 1 and Pin 2 are reserved for power, where Pin 2 is "GND" and PIN 1 is power input "Vin"(DC5~40V).

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input, +5~50V optional	Current: 12V/1A
2	GND	Ground	
3	GND	Ground	
4	RX	Receive Data	
5	TX	Transmit Data	
6	RST	Reset	The Reset Pin has the same function as the reset button. Simply short the RST pin with the GND Pin and hold for 3 sec and the device will restore to factory settings. If you hold for 1 sec, the router will reboot.
7	DIO0	General Purpose I/O	
8	DIO1	General Purpose I/O	
9	NC	Not connected	
10	NC	Not connected	
I/O Terminal on router		Serial port (RS485 or RS232)	

Pin 3 (GND)	Pin 5
Pin 4 (RX)	Pin 2
Pin 5 (TX)	Pin 3

Note: If you do not get a serial connection, try to switch Pin 4 and Pin 5.

2.6 Grounding

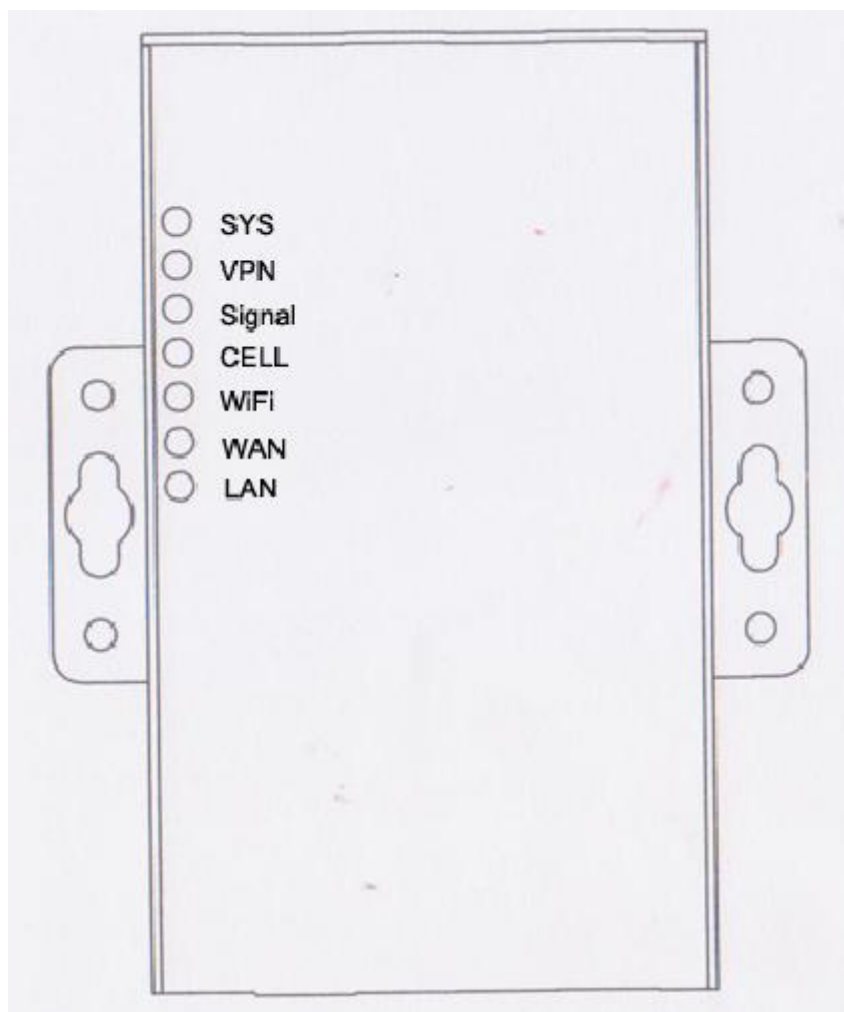
To ensure a safe operation, the cabinet where the router is installed should be grounded properly.

2.7 Power Supply

The CM685V-4 supports a wide range of DC voltage between 5 VDC and 40 VDC. The router is supplied with a 12 VDC power adapter.

2.8 LED Description

Please refer to the following table for LED description.



LED	Indication Light	Description
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
LAN	Blink	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
VPN	On	VPN tunnel set-up
	Off	VPN tunnel not set-up or VPN failure
CELL	On	Cell connection is 'UP' and now you have access to the Internet

WIFI	On	WiFi enabled
	Off	WiFi disabled
WAN	Blink	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
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

Chapter 3

3 Software configuration

1. Overview
2. How to log into the router
3. How to configure the router

3.1 Overview

The CM685V-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

3.2.1 Network Configuration

The router's default parameters are:

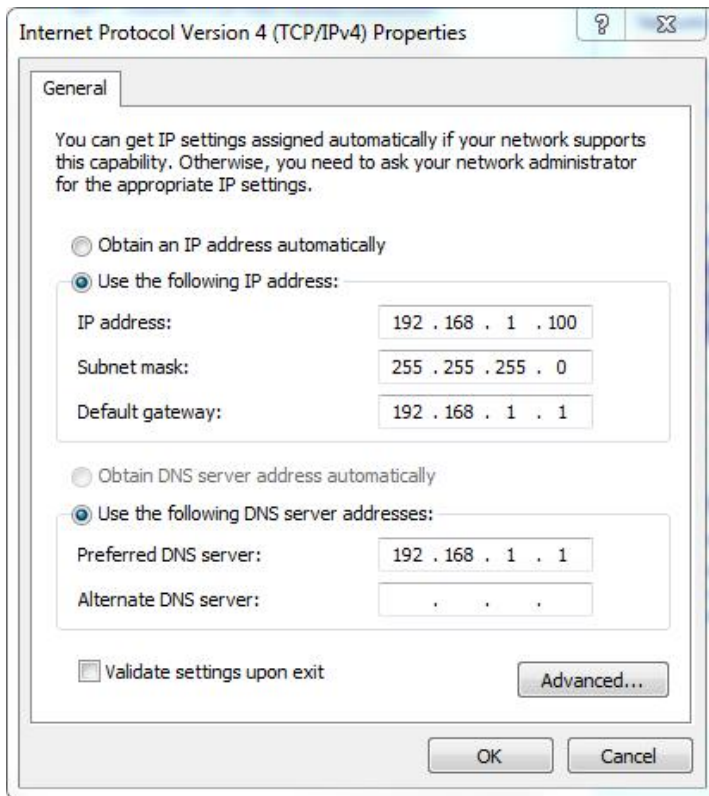
Default IP: 192.168.1.1

Subnet mask: 255.255.255.0

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

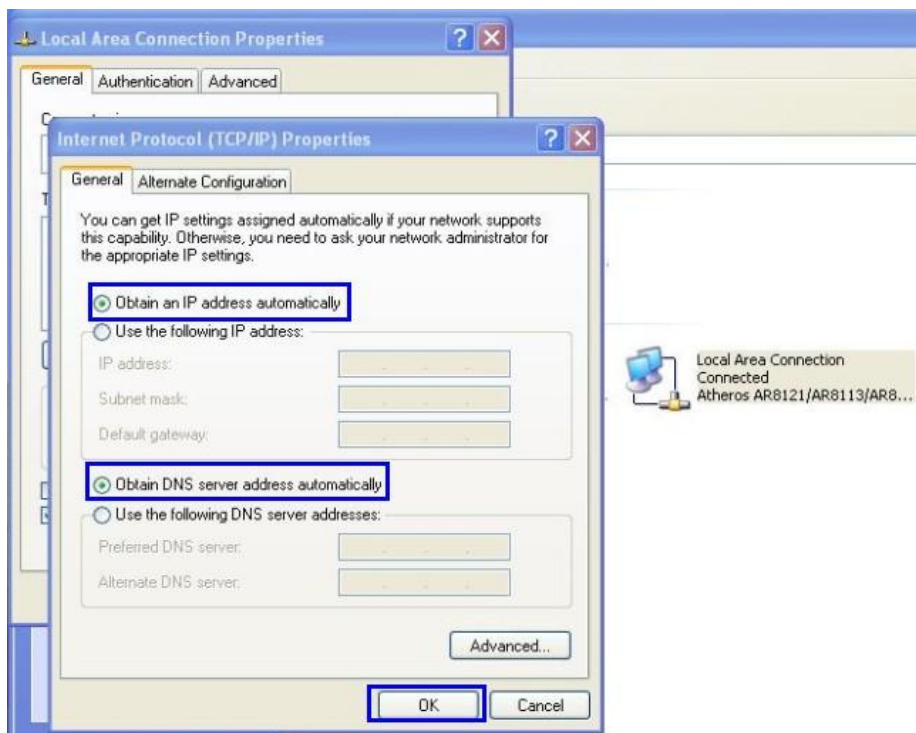
1) Manual settings

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.



2) DHCP settings

Choose “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Then click the ‘OK’ button.



3.2.2 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 User Name and Password are “admin”. Then click on the “Login” button.

Authorization Required

Please enter your username and password.

Username

admin

Password

Login Reset

To configure the router, you can skip the following section “Router status” and go straight to System> Setup wizard which is covered in section 3.4.1

3.3 Router status

3.3.1 Status overview

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

Status

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log
- Reboot Log
- Realtime Graphs
- VPN
- System
- Services
- Network
- Logout

Status

System

Hostname	CM685V_W
SN	860000000015153A
Firmware Version	3.2.31
Kernel Version	3.18.29
Local Time	Wed Oct 12 14:09:27 2016
Uptime	0h 15m 55s
Load Average	0.15, 0.36, 0.34

Mobile 1

Cellular Status	Up
IP Address	10.96.89.89/255.255.255.252
DNS 1	10.4.149.70
DNS 2	10.4.130.164
Cell Modem	HUAWEI-ME906s-158 (12D1_15C3)

3.3.2 Network status

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

Cell mobile interface page:

Status

Overview

Network

Firewall

Routes

System Log

Kernel Log

Reboot Log

Realtime Graphs

VPN

System

Services

Network

Logout


Mobile

WAN

LAN

Mobile Status

Mobile 1

Celluar Status	Up
Cell Modem	HUAWEI-ME906s-158 (12D1_15C3)
IMEI/ESN	866582020057832
Sim Status	SIM Ready
Strength	 23 / 31
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra", 7,
Sub Network Type	LTE
Location Area Code	304B
Cell ID	0817FC0D

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

Overview

Network

Firewall

Routes

System Log

Kernel Log

Reboot Log

Realtime Graphs

VPN

System

Services

Network

Mobile

WAN

LAN

WAN Status

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

Mobile

WAN

LAN

LAN Status

Status Overview

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.)

LAN Ports

Port	MAC-Addr	RX	TX
Wired-LAN	90:22:06:00:03:6F	691.42 KB (5329 Pkts.)	584.10 KB (3915 Pkts.)
WiFi	90:22:06:00:03:6F	0.00 B (0 Pkts.)	109.41 KB (854 Pkts.)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
lenovo-PC	192.168.1.165	f0:76:1c:62:f2:e5	11h 52m 3s

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

3.3.3 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

Firewall Status

IPv4 Firewall
IPv6 Firewall

Actions

- Reset Counters
- Restart Firewall

Table: Filter

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	1600	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)										
--	--	--	--	--	--	--	--	--	--	--

3.3.4 Routes

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

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

Routes

The following rules are currently active on this system:

ARP

IPv4-Address	MAC-Address	Interface
10.56.89.30	4c:54:00:45:e5:d5	usb0
192.168.1.165	10:76:1c:62:12:ab	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
imobile	0.0.0.0/0	10.56.89.90	0	main
imobile	10.56.89.38/30		0	main
imobile	10.56.89.30		0	main
lan	192.168.1.0/24		0	main

3.3.5 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”.

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

3.3.6 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

Kernel Log

[Export log](#)

```
[ 0 000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014 04 f49294)) #933 Wed Sep 28 21:07:09 CST 2016
[ 0 000000] SoC Type: Ralink RT5350 Id:1 rev:3
[ 0 000000] bootconsole [early0] enabled
[ 0 000000] CPU0 revision is: 0001964c (MIPS 24KEc)
[ 0 000000] MIPS: machine is rt5350_model
[ 0 000000] Determined physical RAM map:
[ 0 000000] memory: 04000000 @ 00000000 (usable)
[ 0 000000] initrd not found or empty - disabling initrd
[ 0 000000] Zone ranges:
[ 0 000000] Normal [mem 0x00000000-0x03ffff]
[ 0 000000] Movable zone start for each node
[ 0 000000] Early memory node ranges
[ 0 000000] node 0: [mem 0x00000000-0x03ffff]
[ 0 000000] Initmem setup node 0 [mem 0x00000000-0x03ffff]
[ 0 000000] On node 0 totalpages: 16384
[ 0 000000] free_area_init_node: node 0, pgdat 80300190, node_mem_map 81000000
[ 0 000000] Normal zone: 128 pages used for memmap
[ 0 000000] Normal zone: 0 pages reserved
[ 0 000000] Normal zone: 16384 pages, LIFO batch:3
[ 0 000000] Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes.
[ 0 000000] Primary data cache 16kB, 4-way, VIPT, no aliases, linesize 32 bytes
[ 0 000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[ 0 000000] pcpu-alloc: [0] 0
[ 0 000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 16256
[ 0 000000] Kernel command line: console=ttyS1,57600 rootfstype=squashfs,jffs2
[ 0 000000] PID hash table entries: 256 (order: -2, 1024 bytes)
[ 0 000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
[ 0 000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
```

3.3.7 Realtime graphs

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

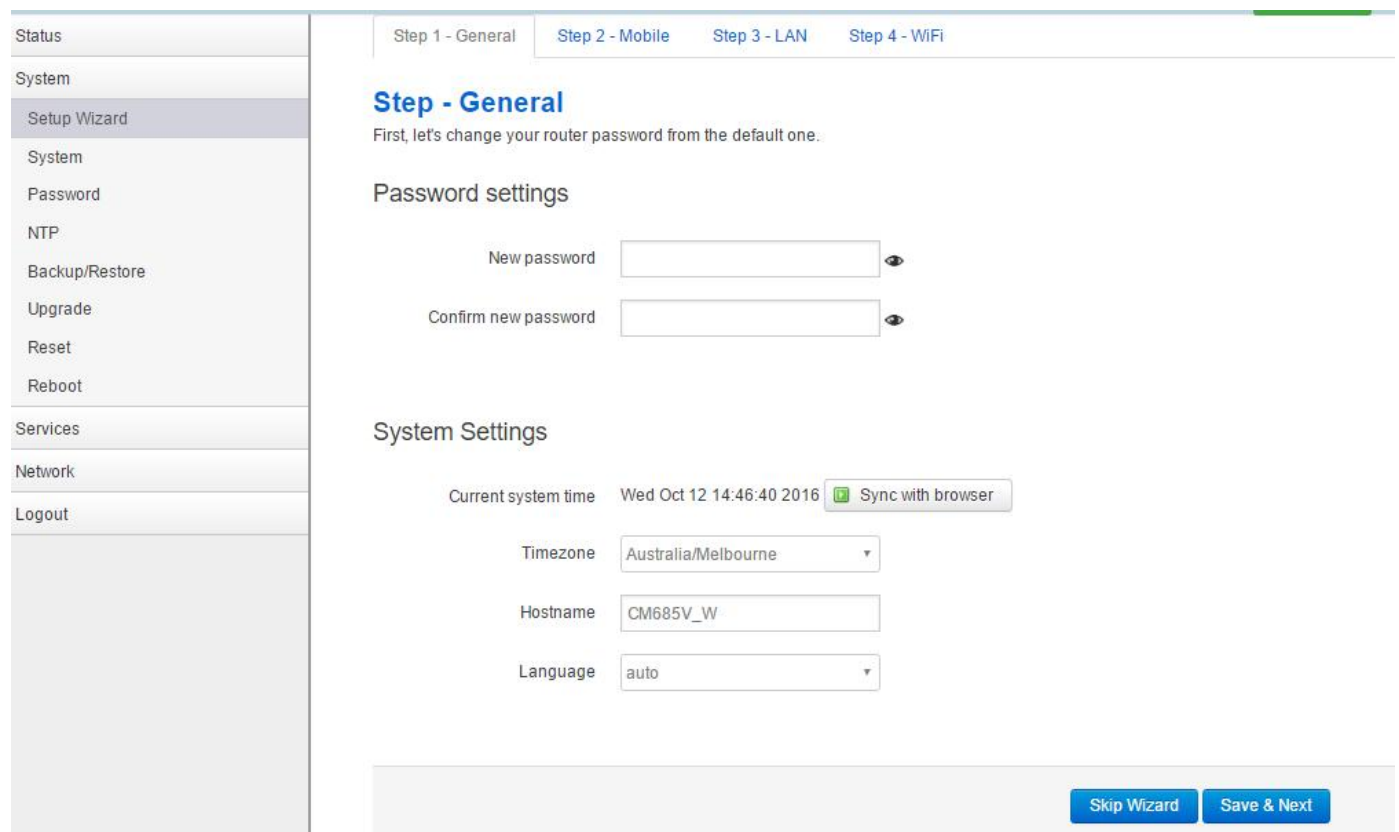


3.4 System Configuration

3.4.1 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



The screenshot shows the 'Step 1 - General' configuration page. On the left is a sidebar menu with options: Status, System, Setup Wizard (highlighted), System, Password, NTP, Backup/Restore, Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area has a progress bar at the top with four steps: Step 1 - General, Step 2 - Mobile, Step 3 - LAN, and Step 4 - WiFi. Below the progress bar, the title 'Step - General' is followed by the instruction: 'First, let's change your router password from the default one.' The 'Password settings' section contains two input fields: 'New password' and 'Confirm new password', each with a toggle icon. The 'System Settings' section displays the 'Current system time' as 'Wed Oct 12 14:46:40 2016' with a 'Sync with browser' button. Below this are three dropdown menus: 'Timezone' (set to 'Australia/Melbourne'), 'Hostname' (set to 'CM685V_W'), and 'Language' (set to 'auto'). At the bottom right, there are two buttons: 'Skip Wizard' and 'Save & Next'.

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

Status

System

Setup Wizard

System

Password

NTP

Backup/Restore

Upgrade

Reset

Reboot

Services

Network

Logout

Step 1 - General

Step 2 - Mobile

Step 3 - LAN

Step 4 - WiFi

Mobile Configuration

Mobile Configuration

SIM 1

Enable

☒

Mobile connection

DHCP mode

APN

telstra.internet

PIN code

Dialing number

*99#

Authentication method

None

Network Type

automatic

Demand

0

MTU

1500

Skip Wizard

Save & Next

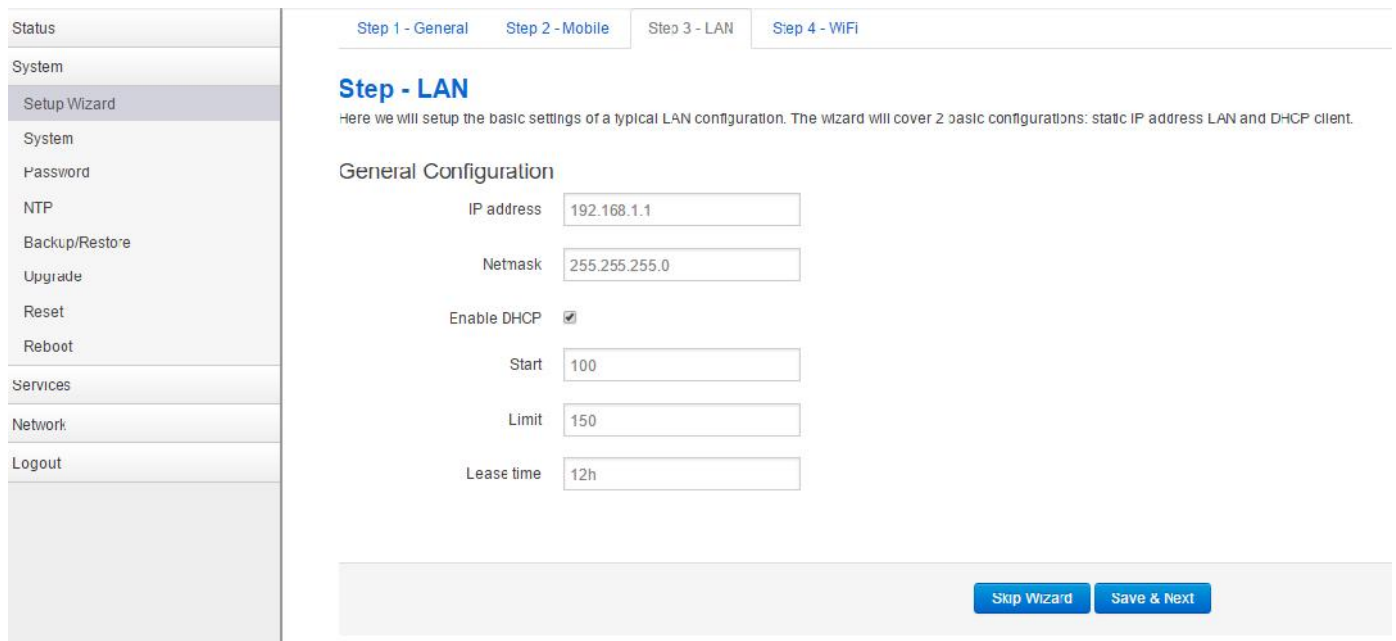
- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for the mobile connection. The default value is 'DHCP mode';
- **APN:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider;
- **PIN code:** Most SIM cards don't have a PIN code, in 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 user name, 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”



The screenshot shows the 'Step 3 - LAN' configuration screen. On the left is a sidebar menu with options: Status, System, Setup Wizard (selected), System, Password, NTP, Backup/Restore, Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area has tabs for Step 1 - General, Step 2 - Mobile, Step 3 - LAN, and Step 4 - WiFi. Below the tabs, the title 'Step - LAN' is followed by a description: '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.' Under 'General Configuration', there are input fields for IP address (192.168.1.1), Netmask (255.255.255.0), a checked 'Enable DHCP' checkbox, and fields for Start (100), Limit (150), and Lease time (12h). At the bottom right are 'Stop Wizard' and 'Save & Next' buttons.

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

Status

System

Setup Wizard

System

Password

NTP

Backup/Restore

Upgrade

Reset

Reboot

Services

Network

Logout

Step 1 - General

Step 2 - Mobile

Step 3 - LAN

Step 4 - WiFi

Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, en reconnect with a new set of parameters.)

WiFi Configuration

Enable wireless

☒

SSID

Cell_AP_00036f

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

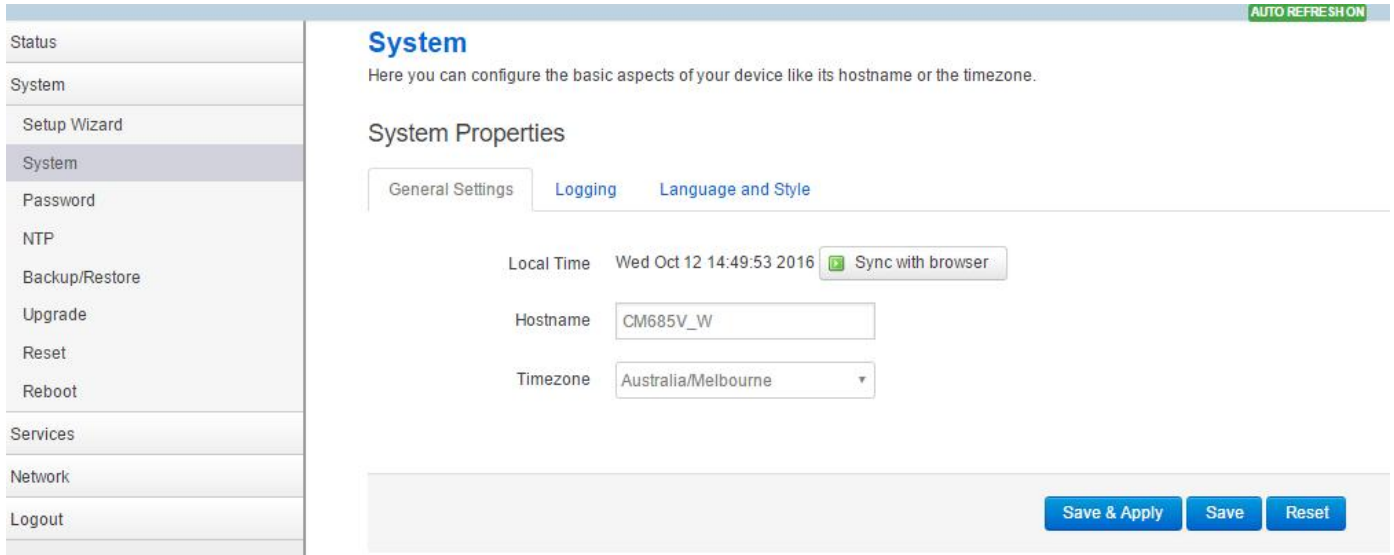
00 - World

Skip Wizard

Finish

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).

3.4.2 System



The screenshot shows the 'System' configuration page of the Comset CM685V-4. On the left is a sidebar menu with options: Status, System (selected), Setup Wizard, Password, NTP, Backup/Restore, Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area is titled 'System' and includes a sub-header 'System Properties'. Below this are three tabs: 'General Settings' (active), 'Logging', and 'Language and Style'. Under 'General Settings', there are three fields: 'Local Time' showing 'Wed Oct 12 14:49:53 2016' with a 'Sync with browser' button, 'Hostname' with a text box containing 'CM685V_W', and 'Timezone' with a dropdown menu set to 'Australia/Melbourne'. At the bottom right are three buttons: 'Save & Apply', 'Save', and 'Reset'. An 'AUTO REFRESH ON' indicator is visible in the top right corner of the main content area.

General Settings

➤ Local Time

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

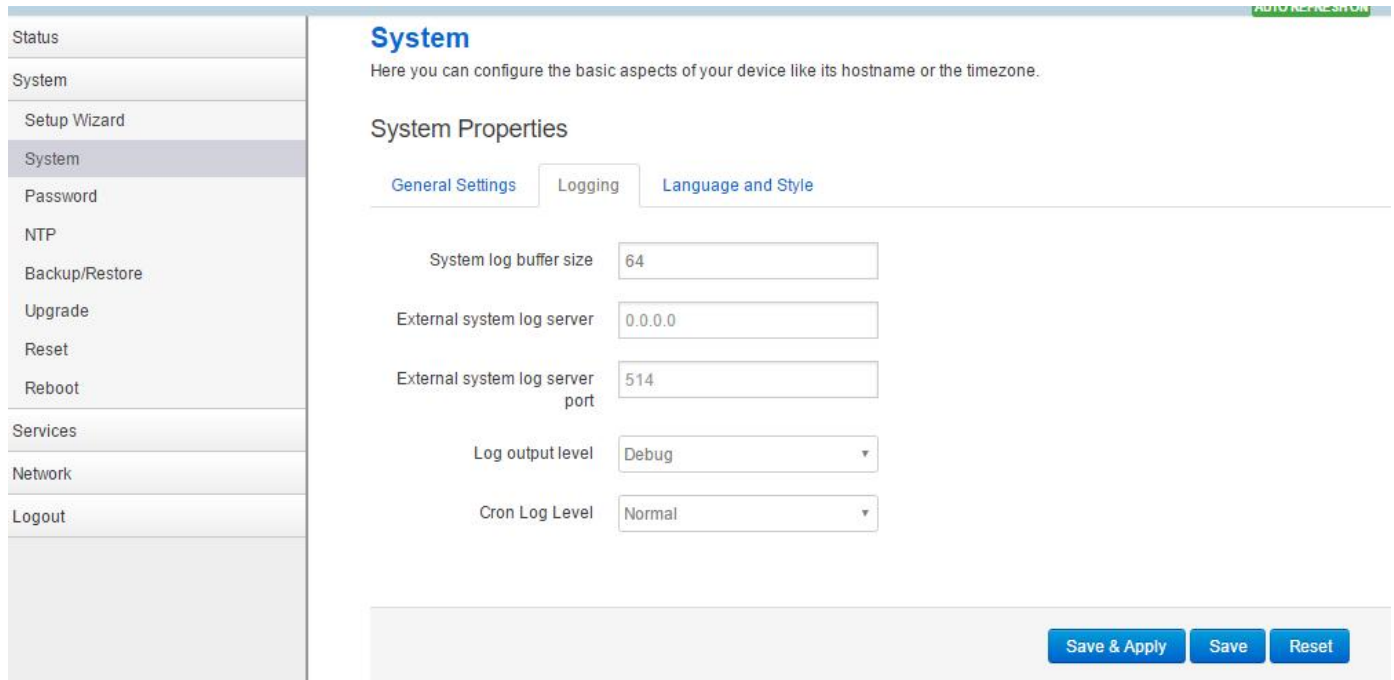
➤ Hostname

It is the router’s name. The default name is “CM685V_W”

➤ Time zone

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

Logging



The screenshot shows the 'System' configuration page with the 'Logging' tab selected. The left sidebar contains a menu with options: Status, System, Setup Wizard, System (highlighted), Password, NTP, Backup/Restore, Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area is titled 'System' and includes a subtitle: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is the 'System Properties' section with three tabs: 'General Settings', 'Logging' (active), and 'Language and Style'. The 'Logging' tab contains the following fields:

- System log buffer size:** A text input field with the value '64'.
- External system log server:** A text input field with the value '0.0.0.0'.
- External system log server port:** A text input field with the value '514'.
- Log output level:** A dropdown menu with 'Debug' selected.
- Cron Log Level:** A dropdown menu with 'Normal' selected.

At the bottom right of the form are three buttons: 'Save & Apply', 'Save', and 'Reset'.

➤ 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



The screenshot shows a 'Language' label next to a dropdown menu. The dropdown menu is currently set to 'English'.

The default language is "English".

3.4.3 Password

Router Password

Changes the administrator password for accessing the device

Password



Confirmation















Save & Apply

Save

Reset

Here you can change the administrator's password for accessing the device. Click the "eye button" to show the new password you entered.

3.4.4 NTP

Status	<h4>NTP</h4> <p>NTP Configuration</p> <h5>Time Synchronization</h5> <p>Enable NTP client <input checked="" type="checkbox"/></p> <p>Provide NTP server <input type="checkbox"/></p> <p>NTP server candidates</p> <table border="1"> <tr><td>0.au.pool.ntp.org</td><td></td></tr> <tr><td>1.au.pool.ntp.org</td><td></td></tr> <tr><td>2.au.pool.ntp.org</td><td></td></tr> <tr><td>3.au.pool.ntp.org</td><td></td></tr> </table>	0.au.pool.ntp.org		1.au.pool.ntp.org		2.au.pool.ntp.org		3.au.pool.ntp.org	
0.au.pool.ntp.org									
1.au.pool.ntp.org									
2.au.pool.ntp.org									
3.au.pool.ntp.org									
System									
Setup Wizard									
System									
Password									
NTP									
Backup/Restore									
Upgrade									
Reset									
Reboot									
Services									
Network									
Logout									

Save & Apply Save Reset

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.

3.4.5 Backup/Restore

Status	<h3>Configuration files operations</h3> <h4>Backup</h4> <p>Download a tar archive of the current configuration files.</p> <p>Download backup configuration archive : <input type="button" value="Download"/></p> <h4>Restore</h4> <p>To restore configuration files, you can upload a previously generated backup archive here.</p> <p>Restore backup configuration archive : <input type="button" value="Choose File"/> No file chosen <input data-bbox="1204 985 1348 1019" type="button" value="Upload..."/></p>
System	
Setup Wizard	
System	
Password	
NTP	
Backup/Restore	
Upgrade	
Reset	
Reboot	
Services	
Network	
Logout	

- 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.

3.4.6 Upgrade

Status	<h3>System upgrade</h3> <p>Upload a sysupgrade-compatible image here to replace the running firmware. (Check “Keep settings” to retain the current configuration (requires an compatible firmware image))</p> <p>Keep settings: <input type="checkbox"/></p> <p>Image: <input type="button" value="Choose File"/> No file chosen <input data-bbox="869 1758 1013 1792" type="button" value="Upload image..."/></p>
System	
Setup Wizard	
System	
Password	
NTP	
Backup/Restore	
Upgrade	
Reset	

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 an 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

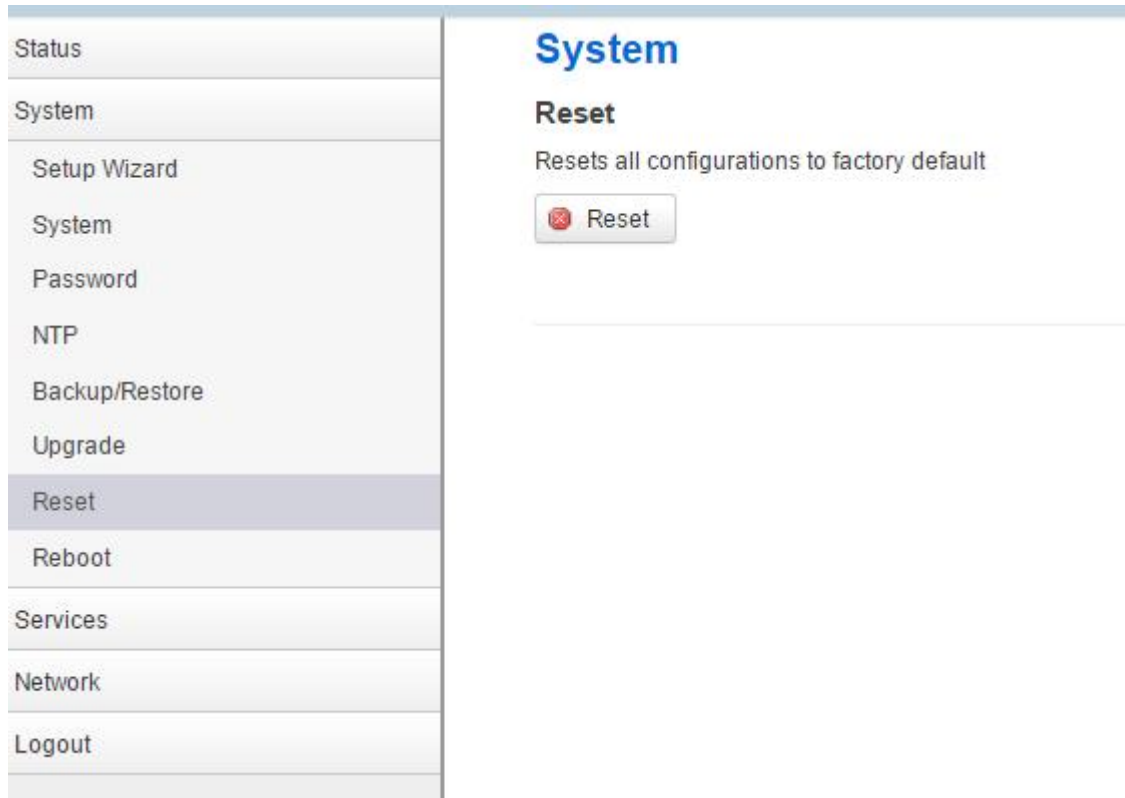
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the upgrade procedure.

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

Cancel

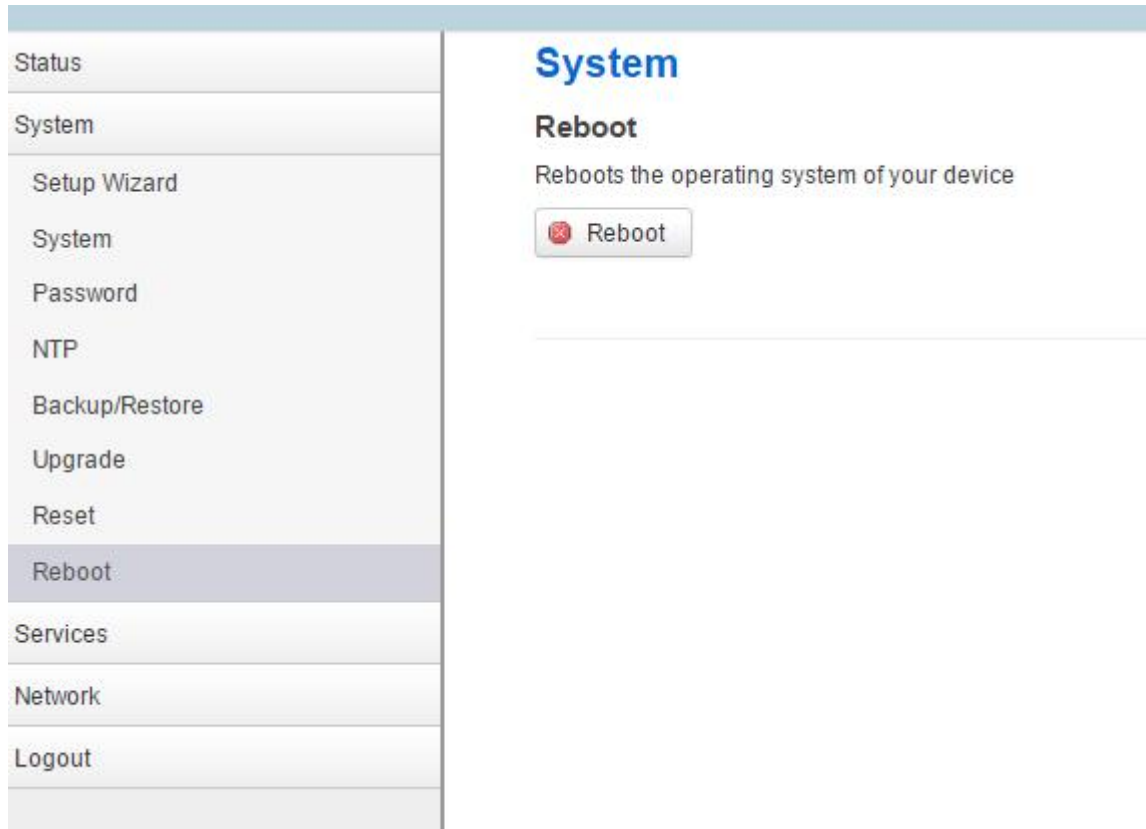
Proceed

3.4.7 Reset



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

3.4.8 Reboot



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

3.5 Services configuration


3.5.1 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	<h2>ICMP Check</h2> <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>Action when failed <input type="text" value="Restart module"/></p> <p>Save & Apply Save Reset</p>
System	
Services	
ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	
Connect Radio Module	
Network	
Logout	

- **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.

3.5.2 VRRP

Status	<h3>VRRP Configuration</h3> <h4>VRRP LAN Configuration Settings</h4> <p>Enable <input type="checkbox"/></p> <p>IP address <input type="text" value="192.168.1.253"/> </p> <p>Virtual ID <input type="text" value="1"/></p> <p>Priority <input type="text" value="100"/></p> <div style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>
System	
Services	
ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	

- **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.

3.5.3 Failover (link backup)

Status	<h2>Failover Configuration</h2> <h3>Failover Settings</h3> <p>Enable <input type="checkbox"/></p> <p>Back To High priority <input checked="" type="checkbox"/></p> <h3>Primary Configuration</h3> <p>Primary <input type="text" value="Wired_wan"/></p> <p>Host1 to ping <input type="text"/></p> <p>Host2 to ping <input type="text"/></p> <p>Ping timeout <input type="text" value="1"/></p> <p>Max Retries <input type="text" value="10"/></p> <p>Interval between ping <input type="text" value="30"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	
Connect Radio Module	
Network	
Logout	

Secondary Configuration

Secondary	Wired_wan ▼
Host1 to ping	<input type="text"/>
Host2 to ping	<input type="text"/>
Ping timeout	1
Max Retries	10
Interval between ping	30

Third Configuration

Third	None ▼
Host1 to ping	<input type="text"/>
Host2 to ping	<input type="text"/>
Ping timeout	1
Max Retries	10
Interval between ping	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.

3.5.4 DTU

Notes:

- 1) This feature is for the CM685V-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.

Status	<h3>DTU Configuration</h3> <p>Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time</p> <p>Enable <input type="checkbox"/></p> <p>Send DTU ID <input type="checkbox"/></p> <p>DTU ID <input type="text" value="860000000015153A"/></p> <p>Forward delay <input type="text" value="200"/> milliseconds (range[1,10000])</p> <h3>Serial Setting</h3> <p>Serial baudrate <input type="text" value="115200 bps"/></p> <p>Serial parity <input type="text" value="None"/></p> <p>Serial databits <input type="text" value="8 bits"/></p> <p>Serial stopbits <input type="text" value="1 bits"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	
Connect Radio Module	
Network	
Logout	



Comset
your m2m specialist

Network Setting

Protocol

Service mode

Enable Heartbeat ☐

Heartbeat Interval

Heartbeat Content

DTU center configuration

CENTER1

Center enable ☒

Center IP

Center Port

New center name:

Add

Delete

Save & Apply

Save

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.

3.5.5 SNMP

SNMP Configuration

General Settings

Enable SNMP ☐

Remote Access ☐

Contact

Location

Name

Port

- **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 v1 and v2c Settings

Get Community

Get Host/Lan


Set Community

Set Host/Lan

- **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 v3 Settings

User	<input type="text" value="admin_user"/>
Security Mode	<input type="text" value="Private"/>
Authentication	<input type="text" value="MD5"/>
Encryption	<input type="text" value="DES"/>
Authentication Password	<input type="password" value="....."/> 
Encryption Password	<input type="password" value="....."/> 

- **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.

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

3.5.6 GPS (optional)

Status	<h4>GPS Configuration</h4> <p>Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time</p> <p>Enable <input type="checkbox"/></p> <p>Prefix SN No. <input type="checkbox"/></p> <p>Only GPRMC <input type="checkbox"/></p> <p>Send interval <input type="text" value="10"/></p> <p>GPS send to <input type="text" value="TCP"/></p> <p>Server IP <input type="text" value="192.168.1.100"/></p> <p>Server port <input type="text" value="6000"/></p> <p>Save & Apply Save Reset</p>
System	
Services	
ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	
Connect Radio Module	
Network	
Logout	

- **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 CM685V-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.

GPS send to	Serial
Serial baudrate	115200 bps
Serial parity	None
Serial databits	8 bits
Serial stopbits	1 bits
Serial flow control	None

[Save & Apply](#)[Save](#)[Reset](#)

- **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

3.5.7 SMS

➤ SMS Command

SMS Command

Enable ☐

SMS ACK ☐

Reboot Router Command

Get Cell Status Command

Set Cell link-up Command

Set Cell link-down Command

DIO_0 Set Command

DIO_0 Reset Command

DIO_1 Set Command

DIO_1 Reset Command

DIO Status Command

Wifi On Command

Wifi Off Command

- **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

SMS Alarm ☐

RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm ☐

Singal Quality Threshold

Failed Times Threshold

Success Times Threshold

- **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.

➤ Phone Number

Phone Number

Phone Number Configuration

NUM1 Delete

SMS Command ☐

SMS Alarm ☐

Phone Number

Add

Save & Apply Save Reset

- **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.

➤ SMS

Send SMS

Receiver Phone Number

Message

Submit Reset

- **Receiver Phone Number:** The phone number that receives SMS messages.
- **Message:** Message content.
- **Submit:** Click the button “Submit” to send the message immediately.

3.5.8 VPN

3.5.8.1 IPSEC

IPsec

IPsec Configuration

Enable ☐

Exchange mode

Authentication method

Remote VPN endpoint

Preshared Keys

Local subnet

Remote subnet

- **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.

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

Note:

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

3.5.8.2 PPTP

Point-to-Point Tunneling Protocol

PPTP Configuration

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

Name	Type	Enable
	Server	No

Role:


Client
Client
Server

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.

➤ **PPTP Client configuration**

PPTP Client Instance: Aaaa

Main Settings

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text"/>
Use default gateway	<input checked="" type="checkbox"/>
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>

- **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 Server Configuration

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" value="*****"/> 

 Add



- **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.

3.5.8.3 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.

Layer 2 Tuneling Pprotocol

L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	 Edit  Delete

New instance name:
 Role: Client
 Add New

Client
 Server

➤ L2TP Client configuration


L2TP Client Instance: Bbbbb

Main Settings

Enable ☐

Server

Username

Password 

MTU

Keep Alive

Checkup Interval


- **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 Server configuration

L2TP Server Instance: L2tpd_server

Main Settings

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

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

- **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.










3.5.8.4 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

Client configuration for an ethernet
 Add

Save & Apply
Save
Reset

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 ☐

verb

3

mlock ☐

disable_ocr ☐

-- 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
-- Additional Field --

Add

3.5.8.5 GRE tunnel

GRE Tunnel

GRE Tunnel Configuration

Enable ☐

TTL

MTU

Peer IP Address

Remote Network IP

Remote Netmask

Local Tunnel IP

Local Tunnel Mask

Local Gateway

- **Enable:** Enable GRE tunnel feature.
- **TTL:** Time-to-live.
- **MTU:** Maximum Transmission Unit.
- **Peer IP address:** Remote WAN IP address.
- **Remote Network IP:** Remote LAN subnet address.
- **Remote Netmask:** Remote LAN subnet mask.
- **Local Tunnel IP:** Virtual IP address. This cannot be in the same subnet as the LAN network.
- **Local Tunnel Mask:** Virtual IP mask.
- **Local Gateway:** Local gateway

3.5.9 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
Fail over
SNMP
DTU
CPS
SMS
VPN
DDNS
Connect Radio Module
Network
Logout

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Overview

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'

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

[Add](#)

[Save & Apply](#)
[Save](#)
[Reset](#)

Details for: example_ipv4

Basic Settings
Advanced Settings
Timer Settings
Log File Viewer

Enabled ☒

IP address version
☒ IPv4-Address
☐ IPv6-Address

DDNS Service provider [IPv4]

dyndns.org

Hostname/Domain

comsetsupport.dvrdns.org

Username

techsupport

Password

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

- **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.

[Basic Settings](#)
[Advanced Settings](#)
[Timer Settings](#)
[Log File Viewer](#)

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file ☒

- **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](#)

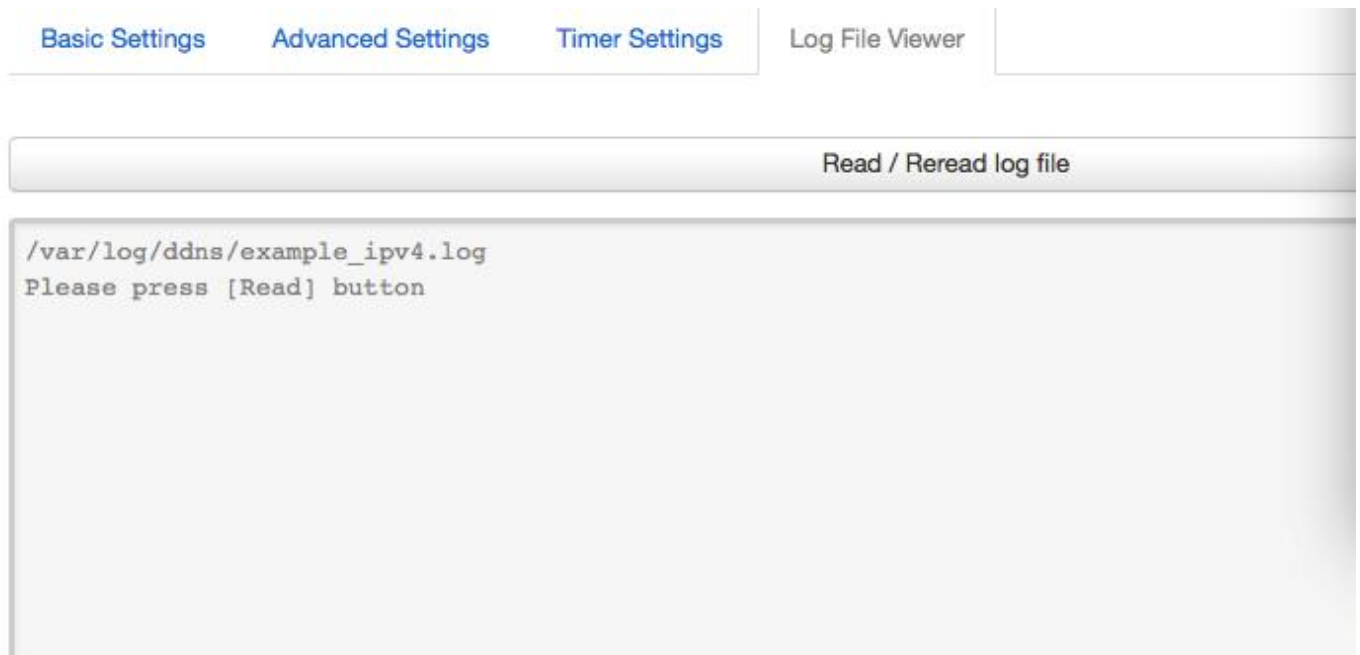
Check Interval

Force Interval

Error Retry Counter

Error Retry Interval

- **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.



Read the log file of DDNS.

3.5.10 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 Radio Module Configuration

Exchange data between radio module and serial

Enable ☒

Connect mode

Serial baudrate

Serial parity

Serial databits

Serial stopbits

• Enable: conflict with DTU, please disable DTU firstly

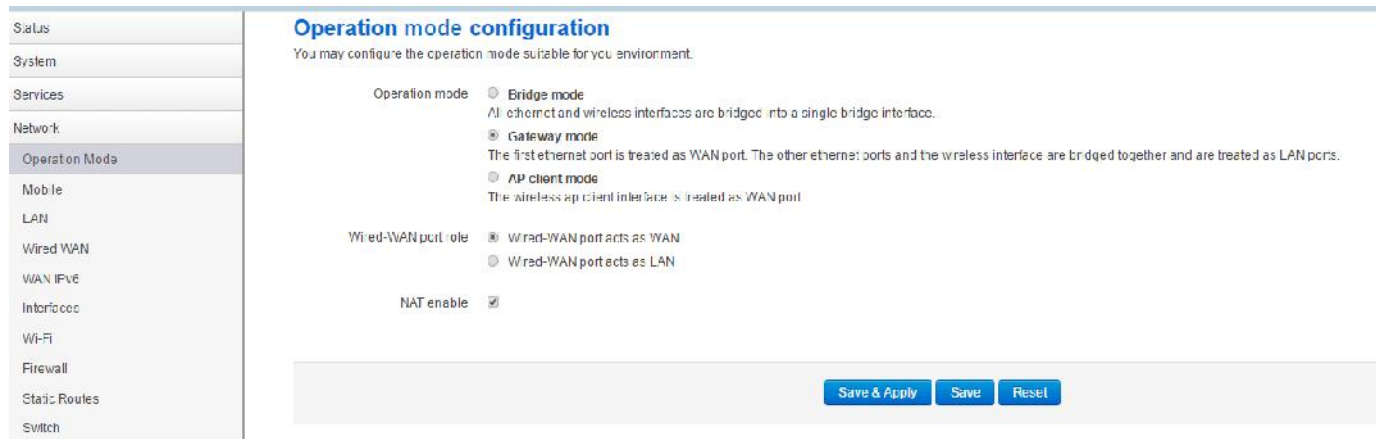
- **Connect Mode:** Serial only

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

3.6 Network Configuration

3.6.1 Operation Mode

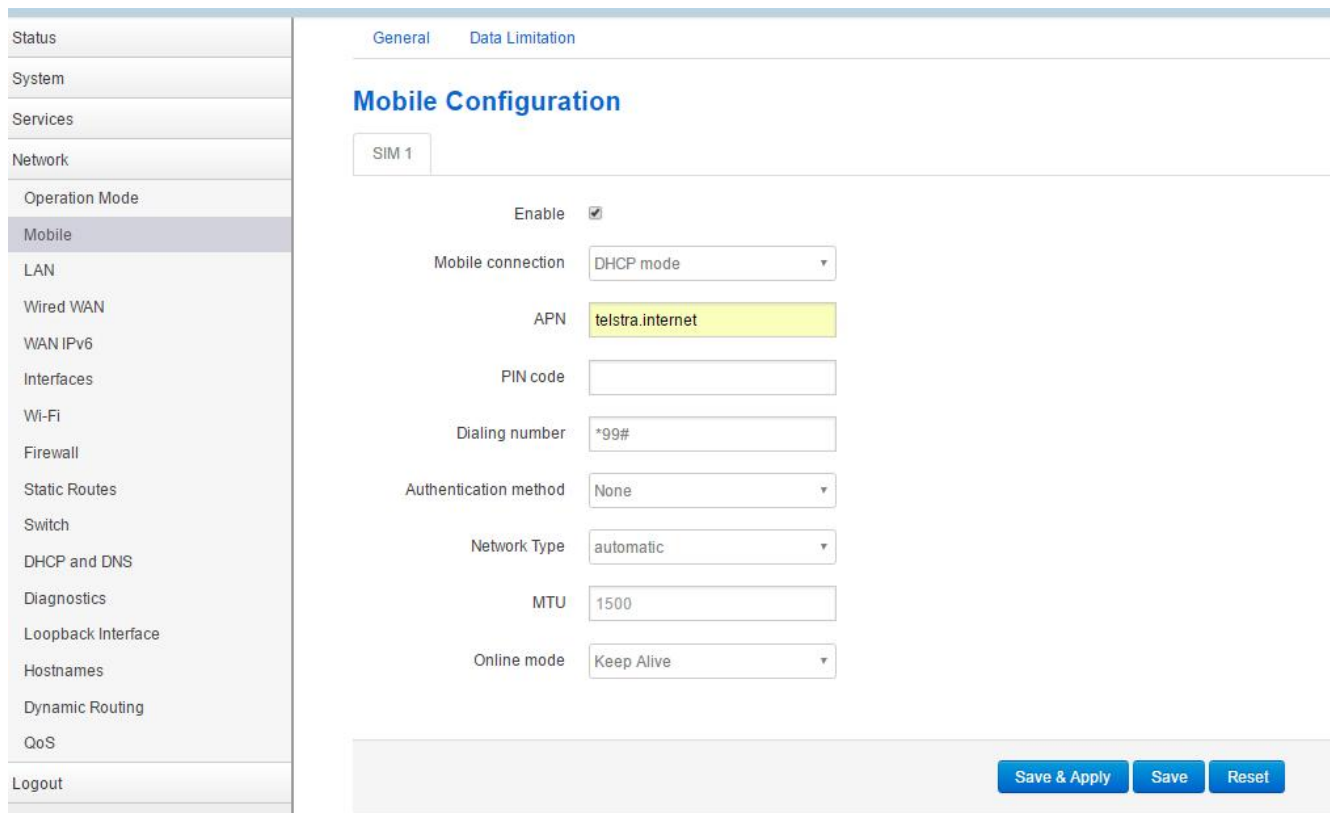


- **Operation mode**
 - **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
 - **Gateway:** The first Ethernet port is treated as a WAN port. The second Ethernet port and the wireless interface are bridged together and are treated as LAN ports.
 - **AP Client:** The wireless apcli 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”.

3.6.2 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.



The screenshot shows the 'Mobile Configuration' page in a web browser. On the left is a sidebar menu with options: Status, System, Services, Network, Operation Mode, Mobile (selected), LAN, Wired WAN, WAN IPv6, Interfaces, Wi-Fi, Firewall, Static Routes, Switch, DHCP and DNS, Diagnostics, Loopback Interface, Hostnames, Dynamic Routing, QoS, and Logout. The main content area has tabs for 'General' and 'Data Limitation'. Under 'General', there's a 'SIM 1' tab. The configuration fields are as follows:

- Enable:** A checkbox that is checked.
- Mobile connection:** A dropdown menu set to 'DHCP mode'.
- APN:** A text field containing 'telstra.internet'.
- PIN code:** An empty text field.
- Dialing number:** A text field containing '*99#'.
- Authentication method:** A dropdown menu set to 'None'.
- Network Type:** A dropdown menu set to 'automatic'.
- MTU:** A text field containing '1500'.
- Online mode:** A dropdown menu set to 'Keep Alive'.

At the bottom right of the configuration area are three buttons: 'Save & Apply', 'Save', and 'Reset'.

- **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.

3.6.3 Cell mobile data limitation

Status	General	Data Limitation
System		
Services		
Network		
Operation Mode		
Mobile		
LAN		
Wired WAN		
WAN IPv6		
Interfaces		
Wi-Fi		
Firewall		
Static Routes		
Switch		
DHCP and DNS		

Data Limitation Configuration

Enable data limitation ☐

Period

Start day

SIM data limit(MB)

Enable alarm ☐

Phone number

Warning percent of Data Used %

Used(Bytes) 6474236

- **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.

3.6.4 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: 1.33 MB (7506 Pkts.)
TX: 1.10 MB (5224 Fkts.)
IPv4: 192.168.1.1/24
IPv6: fcef:1a1b:e9dc::1/60

Protocol Static address

Really switch protocol? ☒ 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 ☒

Use builtin IPv6-management ☒

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


DHCPv6-Service

NDP-Proxy

DHCPv6-Mode

Always announce default router ☐

Announced DNS servers 

Announced DNS domains 


- **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.

3.6.5 Wired-WAN

Interfaces - WAN

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

Common Configuration


General Setup	Advanced Settings	Physical Settings	Firewall Settings
<p>Status  Uptime: 0h 0m 0s MAC-Address: 90:22:06:00:00:00 RX: 0.00 B (0 Pkts.) TX: 131.81 KB (399 Pkts.)</p>			
<p>Protocol <input type="text" value="DHCP client"/></p>			
<p>Hostname to send when requesting DHCP <input type="text" value="CM685V_W"/></p>			

- **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.

3.6.6 WiFi Settings

Wi-Fi Overview



Generic MAC80211 802.11bgn (radio0)
 Channel: 11 (2.462 GHz) | Bitrate: 65 Mbit/s

Wifi Restart
 AP Client
 Add

85%
 SSID: Cell_AP_00036f | Mode: Master
 BSSID: 00:22:06:00:03:6F | Encryption: WPA2 PSK (COMP)

Disable
 Edit
 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.

3.6.6.1 Wifi General configuration

Device Configuration

General Setup

Advanced Settings

Status



Mode: Master | SSID: Cell_AP_00036f

BS SID: 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

	Mode	Channel	Width
Operating frequency	11g/n mixed ▼	11 (2462 MHz) ▼	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.

3.6.6.2 WiFi Advanced Configuration

Device Configuration

General Setup

Advanced Settings

Country Code

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**

3.6.6.3 WiFi Interface Configuration

Interface Configuration

General Setup

Wireless Security

MAC-Filter

ESSID

Mode

Network ☐ ifmobile: 

☒ lan: 

☐ wan: 

☐ wan6: 

☐ create:

Hide Extended Service Set Identifier ☐

WMM Mode ☒

- **ESSID:** Extended Service Set Identifier. It is the broadcast name.
- **Mode:** Supported options.

✓ Access Point
Client
Ad-Hoc
802.11s
Pseudo Ad-Hoc (ahdemo)
Monitor
Access Point (WDS)
Client (WDS)

- **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

Encryption WPA2-PSK

Cipher auto

Key

Enable WPS pushbutton,
requires WPA(2)-PSK

● Encryption:

- No Encryption
- WEP Open System
- WEP Shared Key
- / WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK Mixed Mode
- WPA-EAP
- WPA2-EAP

- **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



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	+

- **MAC-Address Filter:** MAC Address Access Policy. Disabled: disable MAC-address filter

functionality. Allow list: only the MAC address in the list is allowed to forward. Deny list: all packet is allowed to forward 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.

3.6.6.4 WiFi AP client

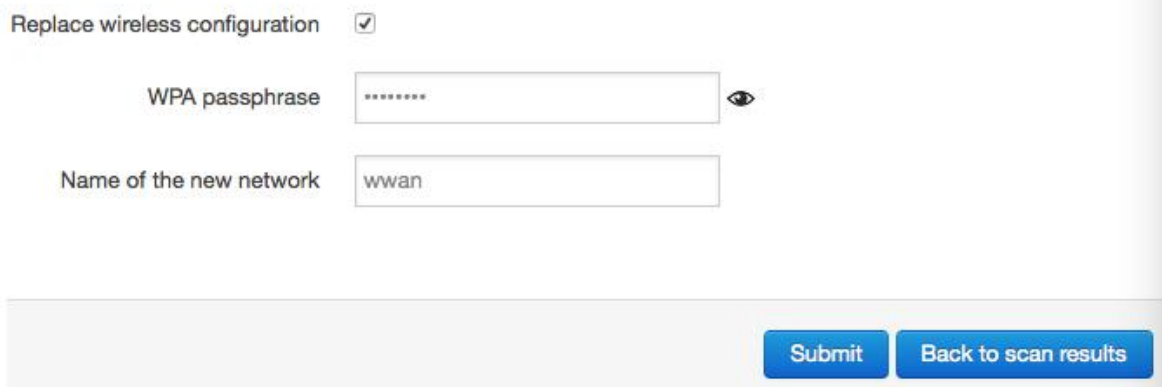
- **Steps 1)** Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.

Join Network: Wireless Scan



- **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



- **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

General Setup

Advanced Settings

Status



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

Wireless network is enabled

☒ Disable

	Mode	Channel	Width
Operating frequency	N	3 (2422 MHz)	20 MHz
Transmit Power	20 dBm (100 mW)		

Interface Configuration

General Setup

Wireless Security

ESSID

Mode

BSSID

Network

☐ ifmobile: 

☐ lan: 

☐ wan: 

☐ wan6: 

☒ wwan: 

☐ create:

- **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

3.6.7 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

3.6.8 Firewall

3.6.8.1 General Settings

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

3.6.8.2 Port Forwards

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

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

Name	Match	Forward to	Enable	Sort
------	-------	------------	--------	------

This section contains no values yet

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
<input type="text" value="New port forward"/>	<input type="text" value="TCP+UDP"/>	<input type="text" value="wan"/>	<input type="text"/>	<input type="text" value="lan"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Save & Apply

Save

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.





























3.6.8.3 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</i> at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	 	 Edit  Delete
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"/>	 	 Edit  Delete
Allow-IGMP	IPv4-IGMP From <i>any host in wan</i> To <i>any router IP</i> on this device	Accept input	<input checked="" type="checkbox"/>	 	 Edit  Delete
Allow-DHCPv6	IPv6-UDP From IP range <i>fe80::/10</i> in <i>wan</i> with source port 547 To IP range <i>fe80::/10</i> at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	 	 Edit  Delete
Allow-MLD	IPv6-ICMP with types <i>130/0, 131/0, 132/0, 143/0</i> From IP range <i>fe80::/10</i> in <i>wan</i> To <i>any router IP</i> on this device	Accept input	<input checked="" type="checkbox"/>	 	 Edit  Delete
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</i> on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	 	 Edit  Delete
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"/>	 	 Edit  Delete

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

Open ports on router:

Name	Protocol	External port	
<input type="text" value="New input rule"/>	<div>TCP+UDP</div>	<input type="text"/>	 Add

New forward rule:

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	<div>lan</div>	<div>wan</div>	 Add and edit...

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
------	-------	--------	--------	------

This section contains no values yet

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="-- Please cho"/>	<input type="text" value="Do not rewrite"/>	Add and edit...

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 sou

Rule is enabled

Disable

Nameforwardtest









Restrict to address familyIPv4 and IPv6

ProtocolTCP+UDP

Match ICMP typeany

Source zone

- ☐ Any zone
- ☒ lan: lan: [lan icon] [wan icon]
- ☐ openvpn: (empty)
- ☐ vpnzone: (empty)
- ☐ wan: wan: [wan icon] wan6: [wan6 icon] ifmobile: [ifmobile icon] wwan: [wwan icon]

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

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 iptable.

3.6.8.4 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

All protocols

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.

3.6.8.5 Security

General Settings Port Forwards Traffic Rules DMZ Security

System security configuration

SSH access from WAN Allow

Ping from WAN to LAN Deny

HTTPS Remote Access

HTTPS access from WAN Allow

Remote network Subnet

IP address 192.168.1.1

Netmask 24

HTTP Remote Access

HTTP access from WAN Allow

Remote network Any IP address

- **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.

3.6.9 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		255.255.255.255		0	1500	Delete

Add

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
-----------	--------	--------------	--------	-----

This section contains no values yet

Add

Save & Apply

Save

Reset

- **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.

3.6.10 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

Add

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.

3.6.11 DHCP and DNS

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

Domain required ☒

Authoritative ☒

Local server

Local domain

Log queries ☐

DNS forwardings

Rebind protection ☒

Allow localhost ☒

Domain whitelist

- **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 forwardings:** 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.

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Suppress logging ☐

Allocate IP sequentially ☐

Filter private ☒

Filter useless ☐

Localise queries ☒

Expand hosts ☒

No negative cache ☐

Strict order ☐

Bogus NX Domain Override

DNS server port

DNS query port

Max. DHCP leases

Max. EDNS0 packet size

Max. concurrent queries

- **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 resolvfile.
- **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.

3.6.12 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"/>
IPv4 Ping	Traceroute	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"/>
IPv4 Ping	Traceroute	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
```

3.6.13 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.

3.6.14 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="password" value="****"/> 

OSPF

Enable	<input type="checkbox"/>
Password	<input type="password" value="****"/> 

OSPF6

Enable	<input type="checkbox"/>
Password	<input type="password" value="****"/> 

RIP

Enable ☐

Password 

RIPng

Enable ☐

Password 

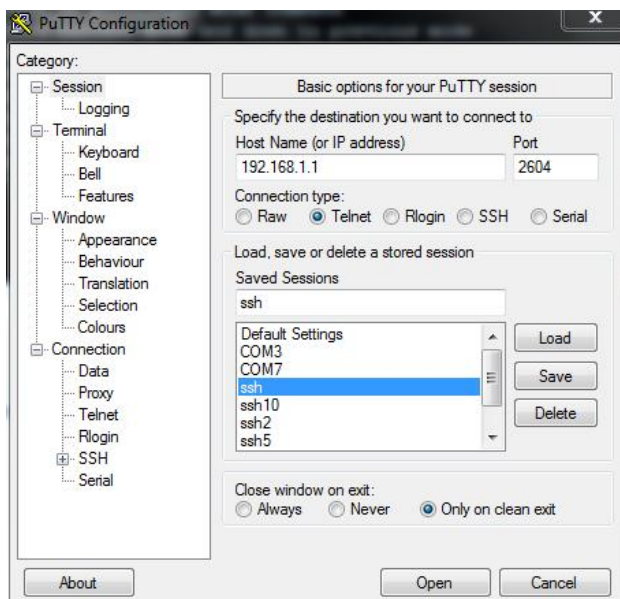
BGP

Enable ☐

Password 

- **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:



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

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

3.6.15 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

WAN

Delete

Enable ☒

Classification group

default

Calculate overhead ☐

Half-duplex ☐

Download speed (kbit/s)

1024

Upload speed (kbit/s)

128

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 ▼	all ▼	all ▼	all ▼	all ▼	22,53 ▼		ssh, dns
normal ▼	all ▼	all ▼	all ▼	TCP ▼	20,21,25,80,110,443,993,995 ▼		ftp, smtp, http(s), imap
express ▼	all ▼	all ▼	all ▼	all ▼	5190 ▼		AOL, iChat, ICQ

 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.