



Go2-4G Industrial Grade 4G Cellular Router User Manual



Email: techsupport@go2sim.com

Web: www.go2sim.com

Telephone: 01634559846

WhatsApp: 07350396121



Content

1 Preparation before configuration.....	5
1.1 Features and model types	5
1.2 Using the correct SIM card for your router	5
1.3 Signal strength and antennas	6
2 Hardware specifications and installation	7
2.1 Overall Dimension, top and side panels	7
2.2 Router ports	1
2.3 SIM card installation	1
2.4 Antenna installation	2
2.5 Installation of terminal block	3
2.6 Grounding	5
2.7 Power Supply	5
2.8 LED lights and Checking Network Status	5
3 Software configuration	7
3.1 Overview	7
3.2 How to log into the Router	7
3.3 System Configuration	12
3.3.2 Setup wizard	12
3.3.1 System	16
3.3.2 Password	18
3.3.3 NTP	20
3.3.4 Backup/Restore	21
3.3.5 Upgrade	21
3.3.6 Reset (Restore to factory default settings)	22
3.3.7 Reboot	24
3.4 Router status	24
3.4.1 Status overview	24
3.4.2 Network status	27
3.4.3 Firewall status	29
3.4.4 Routes	30
3.4.5 System log	31
3.4.6 Kernel log	32
3.4.7 Realtime graphs	33
3.4.8 VPN	34
3.5 Services configuration	37
3.5.1 ICMP check (Ping Reboot)	37
3.5.2 VRRP	39
3.5.3 Failover (link backup)	40
3.5.3.1 Failover basic settings	40
3.5.4 DTU	41
3.5.4 SNMP	43
3.5.6 GPS	45
3.5.7 SMS	46

3.5.7	VPN.....	55
3.5.8.1	IPSEC.....	55
3.5.8.2	PPTP	58
3.5.8.3	L2TP.....	61
3.5.8.4	OpenVPN.....	63
3.5.8.5	GRE tunnel	65
3.5.9	DDNS.....	67
3.5.10	Connect Radio Module	69
3.6	Network Configuration.....	70
3.6.1	Operation Mode	
71 3.6.1.1	Set two LAN Ethernet Ports	71
3.6.2	Mobile configuration	
3.6.3	Cell mobile data limitation.....	73
3.6.4	LAN settings	74
3.6.5	Wired-WAN	77
3.6.6	WiFi Settings.....	79
3.6.6.1	Wifi General configuration	79
3.6.6.2	WiFi Advanced Configuration.....	80
3.6.6.3	WiFi Interface Configuration.....	81
3.6.6.4	WiFi AP client	83
3.6.7	Interfaces Overview.....	85
3.6.8	Firewall	86
3.6.8.1	General Settings	86
3.6.8.2	Port Forwarding	86
3.6.8.3	Traffic Rules.....	87
3.6.8.4	DMZ	91
3.6.8.5	Security.....	91
3.6.9	Static Routes	93
3.6.10	Switch	94
3.6.11	DHCP and DNS.....	95
3.6.12	Diagnostics	97
3.6.13	Loopback Interface.....	98
3.6.14	Dynamic Routing	98
3.6.15	QoS.....	100
3.6.16	Guest LAN (Guest WiFi).....	101



Go2-4G Series Routers

Go2-4G Routers are high spec industrial routers specifically designed for IOT/M2M applications, the Go2-4G runs on a purpose-built operating system based in OpenWRT. These are a small and ruggedised mobile routers capable of high-speed connections to mobile networks. The routers are ideal for integrating into machines or electrical/equipment cabinets. This allows you to connect to your external networks and remotely access and monitor your machines. Commonly used application are for: CCTV, BMS, EV Charging, Digital Signage, Wind and Solar power etc.

The main types of Go2-4G are categorized by the type of modem the router uses, and therefore the generation of mobile technology they can connect to. The hardware section (Chapter 2) of this manual is specific to Go2-4G routers with 4G and 3G modems. Chapter 3 (about the web interface) is applicable to 3G, 4G and the new 5G model also.

Go2-4G Routers are available in 3G, 4G LTE Cat4 and 4G LTE-A Cat6 versions. The Go2-4G 5G model is also now available, whilst there are differences in the hardware, the main functions and web interface are very similar for this model.

All routers are backwards compatible with previous generations of mobile technology. (i.e. Go2-4G 4G is 3G and 2G capable.)

Fixed or Private IP SIMS

If you also require a SIM which allows remote connection to your Go2-4G, feel free to contact us at **sales@go2sim.com** for more information on Fixed Public IP address SIM cards and SIMs with private IPs and secure VPN connections.



Chapter 1

1 Preparation before configuration

1.1 Features and model types

Main features for all models:

- ✓ SMS to control router online/offline, reboot, status, IO alarm, WiFi state.
- ✓ Automatic fallback to 3G / 2G.
- ✓ Small, Ruggedised construction. Easy integration into machines and cabinets.
- ✓ Mobile and WiFi antenna diversity.
- ✓ Supports port forwarding.
- ✓ Supports ping reboot function to reduce engineer site visits.
- ✓ WiFi for remote hotspot and mobile applications
- ✓ RS232 Serial Server via terminal block.
- ✓ Ethernet ports: 1x 100M LAN + 1x 100M LAN/WAN

Go2-4G Router type	Installed mobile module theoretical max values
4G Cat6	LTE-A up to 300 Mbps Down, 50Mbps Up
4G Cat4	LTE up to 150Mbps Down, 50Mbps Up
3G	HSPA+ Downlink 21 Mbps / Uplink 5.76 Mbps

Please note – For any mobile technology (3G, 4G or 5G) Theoretical max rates are industry standardised and will only be replicated in laboratory test settings. Real world speeds of any mobile phone or router in strong high-quality signal will be roughly 20-30% of the max theoretical values.

1.2 Using the correct SIM card for your router

Go2Sim routers are all 'unlocked' meaning any network SIM is compatible. You have free choice of any available network.

Take care to also install the correct type of SIM card to suit your Go2-4G router. There are multiple versions of the Go2-4G router (3G / 4G / 5G). Each is backwards compatible with older mobile technologies (i.e. 4G router is capable of connecting to 3G and 2G).



However, if a 3G only capable SIM is installed into the Go2-4G Router, the SIM does not allow a 4G connection. This applies to any mobile router.

If you need to remotely connect to your Go2-4G, it may need a publicly routable IP address, the most straight-forward method is using a Fixed Public IP SIM. Please contact us techsupport@go2sim.com for help with these SIMs.

1.3 Signal strength and antennas

Make sure the signal is good enough where you test or install the router for your application. Weak signal will affect the router's performance. If there is poor signal reaching the router inside, you may require an external antenna, feel free to contract us techsupport@go2sim for antenna options

If you find your signal strength is poor in the area both inside and outside, you will want to try a different mobile network.

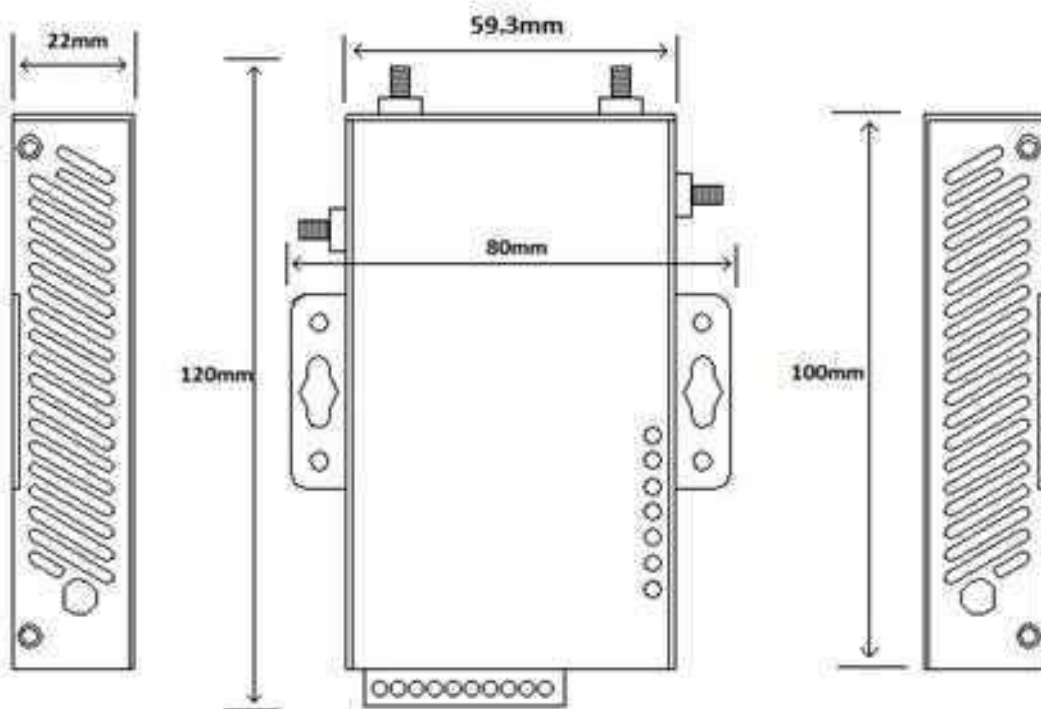
When using an external antenna, keep in mind there is significant signal loss down the length of coaxial cable from antenna to modem. Therefore it is recommended to use 5m max of cable if possible. If possible it is always better to move the router closer to the external antenna, and run a shorter coaxial but longer ethernet data cable.

Chapter 2

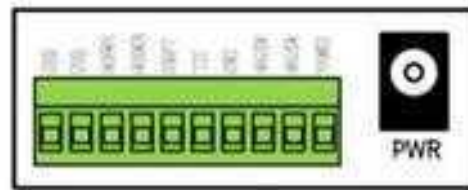
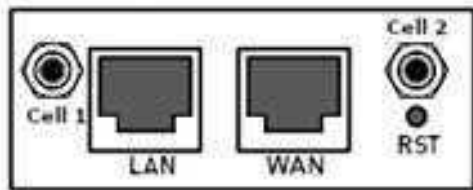
2 Hardware specifications and installation

This chapter describes the appearance and specifications of the hardware, including accessories and basic installation instructions.

2.1 Overall Dimension, top and side panels



2.2 Router ports



SIM: SIM/UIM card port.

LAN: LAN RJ45 Ethernet ports.

WAN: WAN RJ45 Ethernet ports.

RST: SYS reset button. (Factory reset options are found at **Section 3.3.6 Reset**)

PWR: DC power socket. DC7~30V (standard).

Terminal Block

VCC: DC wire positive pole. DC7~30V, - DC5~50V option is available for special order.

GND: DC wire ground

GND: Serial ground

RX: serial receiving

TX: serial transmission

RST: reset router

DIO0: digit I/O port 0

DIO1: digit I/O port 1

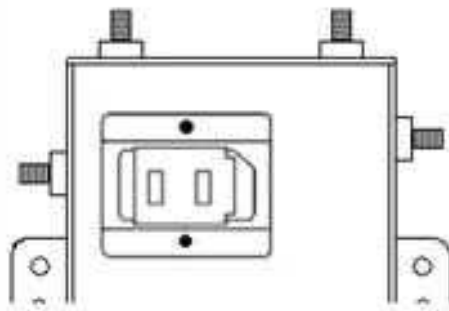
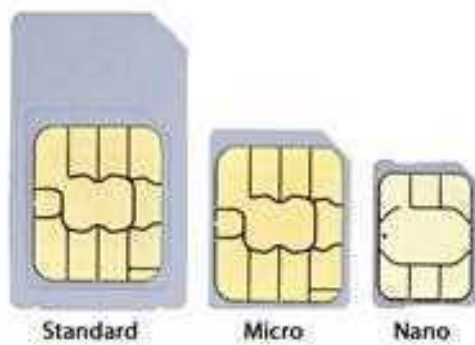
DIO2: digit I/O port 2

DIO3: digit I/O port 3

2.3 SIM card installation

The Go2-4G is compatible with SIM Size 2FF (standard SIM). It is possible to use Nano and Micro SIMs inserted into converter caddies.

SIM size examples



To install the SIM card:

- 1) Remove SIM cover panel on rear of router by removing the two screws.
- 2) Slide and lift the SIM holder, Insert SIM into holder and press and slide to lock SIM into place.
- 3) Fix the protector back into place and replace back the two screws.

Please Note

Please take care to ensure the SIM is inserted correctly. If the SIM is out of position when the SIM holder is slid back to position, the system will not detect the SIM card.

2.4 Antenna installation

Antenna Connection Table

Antenna Connector	Connector Type	Marks
Cell	SMA Female	For main cell antenna.
Aux / Cell Aux	SMA Female	For auxiliary cell antenna.
WiFi / WLAN / WiFi Aux	SMA Female	For WiFi antenna
GPS (Non-standard, Optional extra)	SMA Female	For GPS antenna

The Go2-4G has 2x Mobile Cell antenna connectors and 2x WiFi antenna connectors. The connectors on the router are SMA female.



As standard the Go2-4G comes with 4x stick antennas and 4x magnetically mountable antennas. These have SMA male connectors.

To install the antennas, place antenna connector on the router's connector and turn clockwise until tight. To remove antenna, turn anti-clockwise.

Please note

The mag-mount antennas will only function correctly when the base is placed on a flat metal surface at least 30cm x 30cm in size.

The 4G modem requires 2x antennas connected on Cell1 and Cell2 to allow max functionality and to pick up the strongest signal possible. Although some applications (usually running at lower data speeds) may function well with one antenna.

2.5 Installation of terminal block

As standard the Go2-4G router comes with a terminal block, this will be pre-installed already connected to the body of the router and does not need to be altered.

This enables the use of pluggable terminals, these can be used to give power to the unit, and to connect and transfer data also.

Terminal block specifications	Units
Spacing	3.81mm
Number of Pins	10
Suggested Wire gauge	14~24AWG

To install wires into the terminal block, make sure the router is not connected to power, and remove the terminal block from the router. Remove the terminal block by gently pulling it out of the router.

Use a small flat-headed screwdriver to open and close the individual terminals. Open by turning the screwhead anti-clockwise, insert the wire, then secure by turning the screwhead clockwise.

**Please note**

1. Take care to connect the power cable correctly. We suggest you double check before switching it on. Incorrect wiring can damage the equipment.
2. Power terminals: Pin 1 and Pin 2
3. Here: Pin 2 is “GND”, PIN 1 is power input “VCC” (DC7~30V).

PIN	Signal	Description	Note
1	VCC	+7-30V DC Input	Current: 12V/1A
2	GND	Ground	
3	TX	Transmit Data	
4	RX	Receive Data	
5	PGND	Ground	
6	RST	Reset	Reset Pin has the same function as the reset button at top of device.. To reset with pin, short both RST and GND terminals for 3 Seconds. This will restore the Router to factory default settings. This usually takes 2-4 minutes.
7	DIO0	General Purpose I/O	
8	DIO1	General Purpose I/O	
9	NC/DIO2	Not connect	Reserved for DIO2
10	NC/DIO3	Not connect	Reserved for DIO3

Note: When powering the router via the terminal block, the power cable should be wired with the



correct voltage polarity. Wrong wiring may damage the router. Pin 1 and Pin 2 are reserved for power, where Pin 2 is "GND" and PIN 1 is power input "Vin" (DC5~40V).

2.6 Grounding

To ensure a safe, stable, and reliable operation, the Go2-4G router should be grounded properly. If installed in a cabinet, the cabinet should be properly grounded also.

2.7 Power Supply

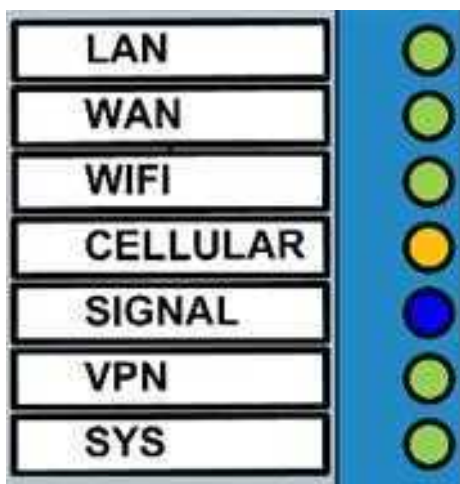
There are two options for powering the Go2-4G router:

- 1) The DC barrel connector into PWR.
- 2) Via a bare wire-connector into the terminal block.

In most cases, the standard power configuration is 12V/1A, one of these power supplies with a barrel connector is shipped with the router.

2.8 LED lights and Checking Network Status

LED Light order



Normal system lights on set-up

When the router is first powered on, the following light sequence is a good indication that the modem is set-up normally. 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 will start to flash and the Wi-Fi LED will come on.



When the router is reset, this sequence above is also a good indication that the modem has reset correctly as the Wi-Fi is enabled by default. **(For how to factory reset go to section 3.3.6)**

If a SIM card is inserted, and the antennas are receiving signal, the signal light will flash blue. Once the correct APN settings of the SIM are entered into the router, an internet connection will be established and the cell light will stop flashing and be solidly on.

If the router is receiving mobile signal, the signal light will flash blue. The faster the flash, the stronger the signal. (see table below for details). More details of signal strength is found in the web GUI. Status > Network.

- If LAN cable is connected and transmitting data, it will be flashing.
- If WiFi is enabled, the WiFi light will be solid on, and flickering if transmitting.
- If VPN tunnel is not connected, light is off. If VPN tunnel is connected, light is solid.
- If all lights are solid on and unchanging, most likely there is a system error. Try to factory reset the router.

LED	Colour	Indication Light	Description
SYS	Green	Solid on for 25 seconds	On for 25 seconds after power supply
		Flashing	System set-up normally
		Off, or solid on after 25 seconds	System set-up failure
LAN	Green	Flashing	Data transmission in Ethernet
		Off	No LAN cable connected, or error.
		Solid on	Ethernet is connected
VPN	Green	Solid on	IPSec VPN tunnel is set-up and connected
		Off	IPsec VPN tunnel set-up failure or inactivated
CELL	Orange	Flashing	Not connected to internet.
		Solid on	Internet access established.
WiFi	Green	Solid on	Enable
		Off	Disable
WAN	Green	Flashing	Transmitting data
		Off	No WAN cable connected, or error.
		Solid on	Ethernet is connected
Signal		Off	No signal, or signal checking system not ready



Blue	Flashing (2 seconds on, and 2 seconds off)	Signal bar is 1 (Low)
	Flashing (1 seconds on, and 1 seconds off)	Signal bar is 2 (Medium)
	Flashing (0.5 seconds on, and 0.5 seconds off)	Signal bar is 3 (High)

Chapter 3

3 Software configuration

1. *Overview*
2. *How to log into the Router*
3. *How to config web*

3.1 Overview

The Go2-4G routers have a built-in web Graphical User Interface (GUI) which allows configuration and management of the router. The web interface also has debugging tools, system logs and allows updates to the system. The Go2-4G is based in OpenWRT. project for embedded operating systems based on Linux.)

3.2 How to log into the Router

ONCE YOU HAVE LOGGED INTO THE ROUTER, IMMEDIATELY CHANGE YOUR PASSWORD FROM THE DEAFUALT PASSWORD TO SOMETHING SECURE AND MEMORABLE.

To access the web interface of the router, **connect an ethernet cable from the LAN port of the Go2-4G into your PC or Laptop.**

The factory default settings of the Go2-4G will have DHCP running on it's LAN port. Therefore, if= the PC/Laptop's network adapter is set to obtain an IP address automatically, communication with the router will be possible and you can reach the web interface.

Normally the network adapter on a Windows 10 machine will be set to obtain an IP address automatically. This means when the router and PC/laptop are connected with an ethernet cable, the router's web interface can be accessed straight away through a web browser (e.g. Chrome, IE, Edge, Firefox etc.) by inputting the router's default IP address 192.168.8.1 into the address bar.

3.2.1 Network Configuration of the Computer.

The router default IP parameters are as follows.

Default IP: 192.168.8.1, sub mask: 255.255.255.0.

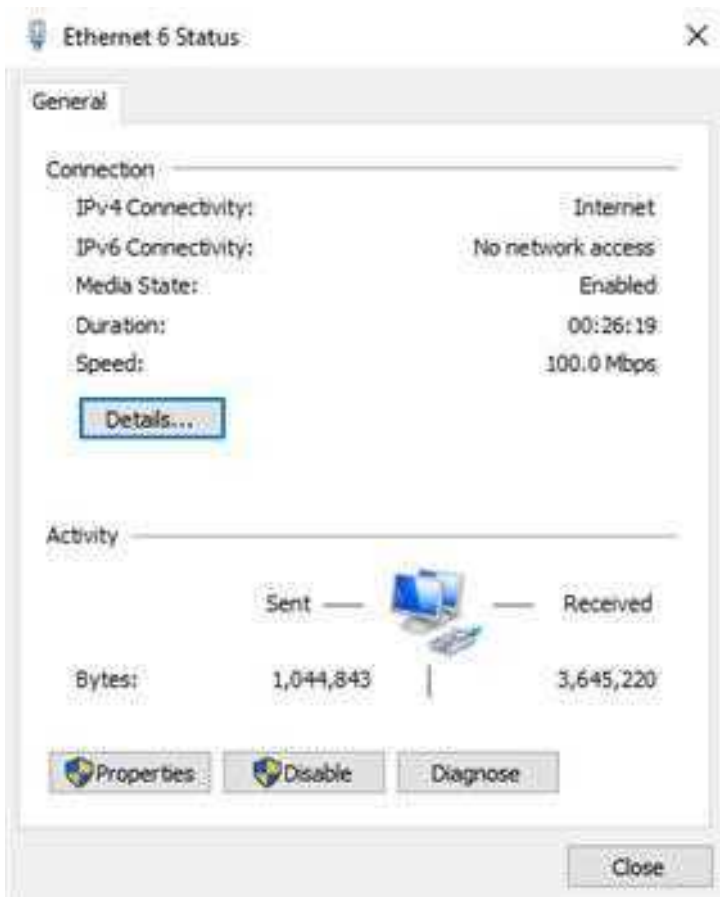
There are **two methods** to set the PC's IP address. For both, in Windows 10 go to:
Control Panel > Network and Sharing Centre.

Network and Sharing Centre

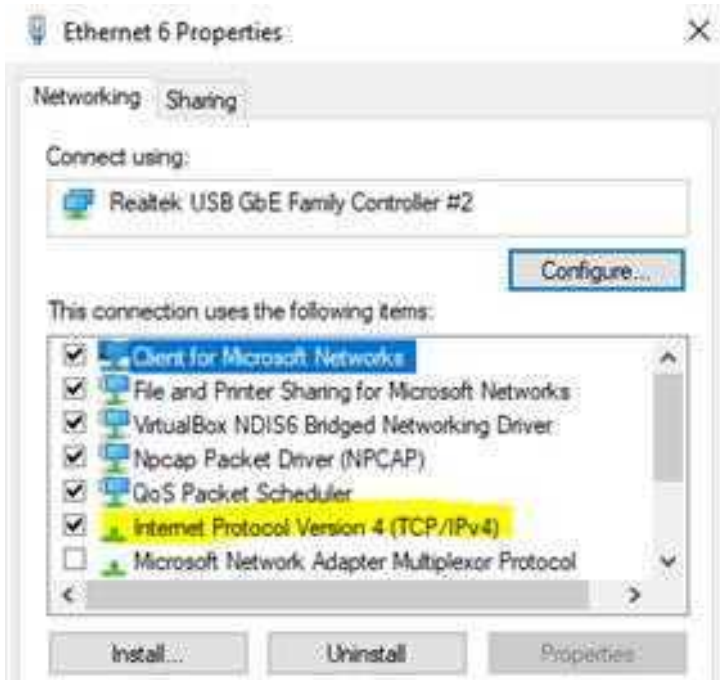


Find the router connection (usually called Cell_AP_XXXXXX), click onto the blue connections button (below 'Ethernet 6') This will open (in the picture here 'Ethernet 6 Status'). >Press Properties button.

***Connection* Status > Press Properties button.**



***Connection* Properties > double click Internet Protocol Version 4.**

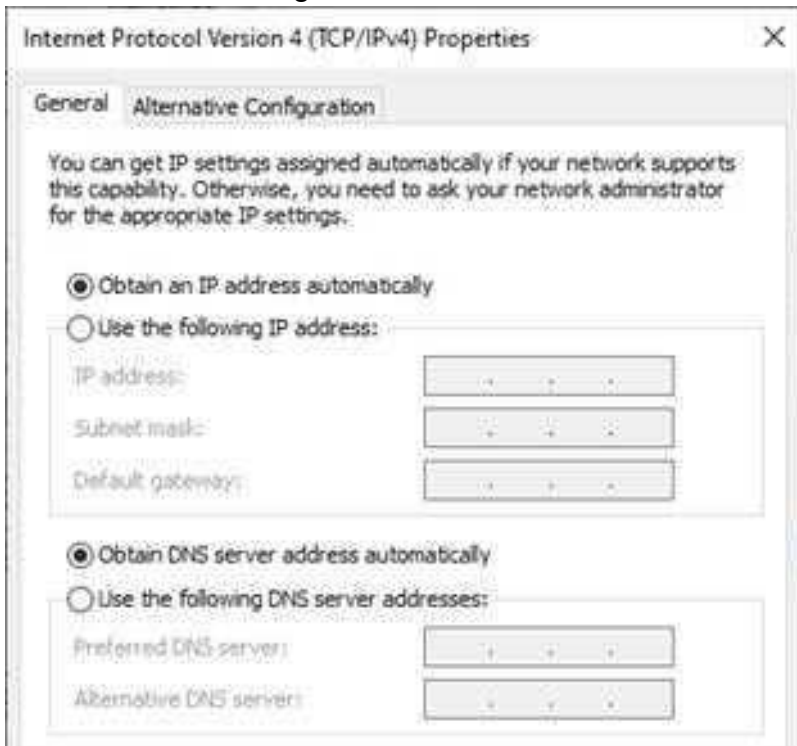


***Connection* Internet Protocol V4 Properties**

Two methods for setting the PC's IP address:

Method 1 – Automatically set IP

The settings below will obtain the IP address for the PC/Laptop automatically. When the router in it's factory default settings, it's DHCP server will give out an IP address and it will be reachable with the below settings.



Method 2 - Manually set IP

Set the PC IP as 192.168.8.xxx (xxx = 2~254), subnet mask: 255.255.255.0, default gateway: 192.168.8.1, primary DNS: 192.168.8.1.



Using either Method 1 or Method 2, you will now be connected to the router via IPv4 and you can access the web interface and log into the router.

3.2.2 Log into Router

3.2.3

- Open the Web Browser (Chrome, IE, Edge, Firefox, etc).
- **Please note it is best to access the router from a browser in 'private browsing / incognito mode'.**
- Type the IP address 192.168.8.1 into the address field and press Enter.
- Type default Username/Password - admin/admin, then press the **Login** button.





-
- You will now have access to the web interface and will initially land on the setup wizard.
 - **You should immediately change the password of the router to something secure and memorable.**

3.3 System Configuration

3.3.2 Setup wizard

On first login to the router, the Setup Wizard will be the landing page. It is not necessary to use the wizard, the settings can be changed by clicking into the tabs at the side of the page.

However, if you run through the wizard or not:

REMEMBER – IMMEDIATELY CHANGE YOUR PASSWORD FROM THE DEFAULT TO SOMETHING SECURE AND MEMORABLE. Especially if using a Fixed Public IP SIM card, as your router will be accessible on the internet.

Setup Wizard - Step 1 - General

- Prompt to change password, this is the most important task once you log in to a new router. Enter new password, and confirm again new password.
- Choose time zone
- Choose Hostname (you do not need to change from default).
- Choose language.

When ready, press 'Save and Next'. (Settings are applied immediately).

The screenshot shows the Go2SIM Setup Wizard interface. On the left is a sidebar menu with options: Status, System, Setup Wizard (highlighted), Password, NTP, Backup/Restore, Upgrade, Reboot, and Factory. The main content area is titled 'Step - General' and includes a progress bar at the top with steps: Step 1 - General, Step 2 - Mobile (active), Step 3 - LAN, and Step 4 - WLAN. Below the title, a note says 'First, lets change your router password from the default one.' The 'Password Settings' section has two input fields: 'New password' and 'Confirm new password'. The 'System Settings' section shows 'Current system time' as 'Mon May 17 06:20:50 EDT', a 'Sync with internet' button, and dropdown menus for 'Timezone' (set to UTC), 'Hostname' (set to 'Go2SIM'), and 'Language' (set to English). At the bottom right are 'Stop Wizard' and 'Save & Next' buttons.

Setup Wizard - Step 2 – Mobile (APN SETTINGS)

This is where the APN settings of the SIM are entered into the router. If using a standard SIM card (CGNAT dynamic IP), the router may auto-detect the SIM network and use a standard APN. In this case you will notice it is not necessary to manually enter the APN settings of the SIM into the router to get an internet connection. However, it is advised to always configure the SIM's correct APN settings manually, especially if using a fixed public IP SIM. If the router auto-detects an APN for a public IP SIM, the router will have an internet connection, but it may not have the SIM's associated fixed public IP address.

Please note – if you don't have the SIM's APN settings, these can be obtained from your SIM network or SIM provider.

Once these APN settings are saved; if the router has a SIM installed which matches the APN, the router has antennas attached on the cell connectors, and the router is in a location receiving signal from the SIM's network. The router will make an internet connection.

Please note - Changing the wrong settings here can make the router fail to make an internet connection. These settings can be obtained from the network or SIM provider. Only change the settings instructed below, unless you are an experienced engineer and require an advanced configuration.

- Enable – Tick to enable mobile network.
- Mobile connection – Leave as DHCP mode.



- APN – Enter APN Address of SIM.
- PIN code – Most SIMs don't have a PIN. Leave blank unless change required. **(Advanced)**
- Dialing number – Leave as *99# unless change required **(Advanced)**
- Authentication method – Most SIMs will require PAP.
- Username – Enter APN username of SIM. (sometimes this is just blank)
- Password – Enter APN password of SIM. (sometimes this is just blank)
- Network Type – Leave as automatic unless change required. **(Advanced)**
- MTU – Leave as 1500 unless change required **(Advanced)**.
- Online mode – Leave as Online mode unless change required **(Advanced)**.

When ready, press 'Save and Next'

The screenshot shows the 'Mobile Configuration' page in a web-based Setup Wizard. The left sidebar contains a navigation menu with options like Status, System, Setup Wizard (selected), Password, NAT, Backup/Restore, Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area has tabs for Step 1 - General, Step 2 - Mobile (selected), Step 3 - LAN, and Step 4 - WAN. The 'Mobile Configuration' section includes an 'Enable' checkbox (checked), a 'Mobile connection' dropdown (GPRS mode), and input fields for 'APN' (lgnet), 'PIN code', 'Dialing number' (*99#), 'Authentication method' (None), 'Network Type' (automatic), 'MTU' (1500), and 'Online mode' (keep alive). At the bottom right, there are two buttons: 'Step Wizard' and 'Save & Next'.

Setup Wizard - Step 3 – LAN

Here the LAN settings can be configured. It is not necessary to change the settings here. However, if you are connecting the router to devices on a different subnet (e.g. 192.168.1.X or 192.168.50.X) , you will either need to change the router's IP address to match, or your devices will need to change to be on the 192.168.8.X 255.255.255.0 subnet.

- IP address – set the IP address of the router (if changed from default, manual PC network adapter settings may need to be changed. See section 3.2 above).
- Netmask – default setting 255.255.255.0
- Enable DHCP – Tick if DHCP is required. (Unticking can cause loss of connection to router. You may need to manually configure your PC IP address, see section 3.2 above).

- Start – Start range of DHCP server addresses, default 100. (Change if conflicting with devices on LAN with static IPs)
- Limit – End range of DHCP server addresses, default 150. (Change if conflicting with devices on LAN with static IPs)
- Lease time – default 12h.

When ready, press ‘Save and Next’

The screenshot shows the 'Step 3 - LAN' configuration screen in the Go2SIM Setup Wizard. The left sidebar contains a navigation menu with options: Status, System, Setup Wizard (selected), Parameters, HTTP, 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 (active), and Step 4 - WiFi. Below the tabs, the title 'Step - LAN' is displayed, followed by a subtitle: '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.' The 'General Configuration' section includes the following fields: IP address (192.168.1.1), Netmask (255.255.255.0), Enable DHCP (checked), Start (100), Limit (150), and Lease time (12h). At the bottom right, there are two buttons: 'Step Wizard' and 'Save & Next'.

Setup Wizard - Step 4 – WiFi

Here WiFi settings can be configured.

Please note – If you are connected on WiFi, changing these settings may drop your connection. It is advised to change the default password of the WiFi (Key), and the SSID. Otherwise, the default settings are recommended, unless an advanced setup is required.

- Enable wireless – Tick to enable WiFi.
- SSID – Name of WiFi network
- Transmit Power – Default 20dBm
- Band – Default 2.4Ghz (802.11g+n)
- HT mode (802.11n) – Default disabled
- Channel – Default 11
- Encryption – Default is WPA2-PSK.
- Cipher – default is auto
- Key – This is the password to access WiFi network. Advised to change for security.
- Country Code – Select your country.

When ready, press ‘Finish’

The Wizard is now finished, and your router has a basic config installed. If using the router for remote monitoring at an un-manned location, one further feature we strongly advise enabling is the **ping reboot** function which is found at **Services > ICMP Check**. (Section 3.5.1 below)

Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi

Step 4 - Wireless

Now let's configure your wireless radio. (Note: If you are currently connecting via wireless and you change parameters, like SSID, encryption, etc., your connection will be dropped.)

WiFi Configuration

☒ Enable wireless

SSID:

Transmit Power:

Band:

HT mode (802.11n):

Channel:

Encryption:

Cipher:

Key:

Country Code:

3.3.1 System

General Settings

The screenshot shows the 'System' configuration page in the Go2SIM interface. 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 contains the text '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' (active), 'Logging', and 'Language'. Under 'General Settings', there are fields for 'Local Time' (Wed Jun 30 17:57:48 2021) with a 'Sync with browser' button, 'Hostname' (Cell_Router), 'Timezone' (UTC), and a 'Turn off LEDs' checkbox. At the bottom right are buttons for 'Save & Apply', 'Save', and 'Reset'.

Local Time

Displays system time. You can sync this time with browser by clicking button “Sync with browser”.

Hostname

This is the router’s name, the default name is Cell_Router.

Time zone

Select a suitable time zone. The default value is UTC

Logging settings

The screenshot shows the 'System' configuration page in the Go2SIM interface, specifically the 'Logging' tab. The sidebar menu is the same as in the previous screenshot. The main content area is titled 'System' and contains the text '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'. Under 'Logging', there are fields for 'System log buffer size' (64), 'External system log server' (0.0.0.0), 'External system log server port' (514), 'Log output level' (Debug), 'Cron Log Level' (Normal), and a 'Record Cell Status' checkbox. At the bottom right are buttons for 'Save & Apply', 'Save', and 'Reset'.

System log buffer size

The unit is KB, default value is 64 KB. If the actual log size exceeds the set value configured, the oldest log will be dropped (lost).

External system log server

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

External system log server port

This is the UDP port of 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

This is log level for process ‘Crond’.

Language

Language

The default language is “English”.

3.3.2 Password

PLEASE NOTE – IMMEDIATELY CHANGE THE PASSWORD FROM THE DEFAULT TO A SECURE MEMORABLE PASSWORD.

Status	Web Account	SSH Account	Guest Account
System	Web Account		
System	Changes the administrator username and password.		
Setup Wizard	Current username	<input type="text"/>	
Password	Current password	<input type="password"/>	
NTP	New username	<input type="text"/>	
Backup/Restore	Password	<input type="password"/>	
Upgrade	Confirmation	<input type="password"/>	
Reset			
Reboot			
Services			
Network			
Logout			
	<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>		



Web Account

Here it is possible to change the admin username and password for the router. To change the password, you will need to enter the current username in the current username field, also enter the current password, as well as the new password, with confirmation.

Click "eye button" to show the new password you entered.

- Current username. The username of web account is using.
- Current password. The password of web account is using.
- New username. The new username of the web account.
- Password. New password entered here.
- Confirmation. Repeat new password.

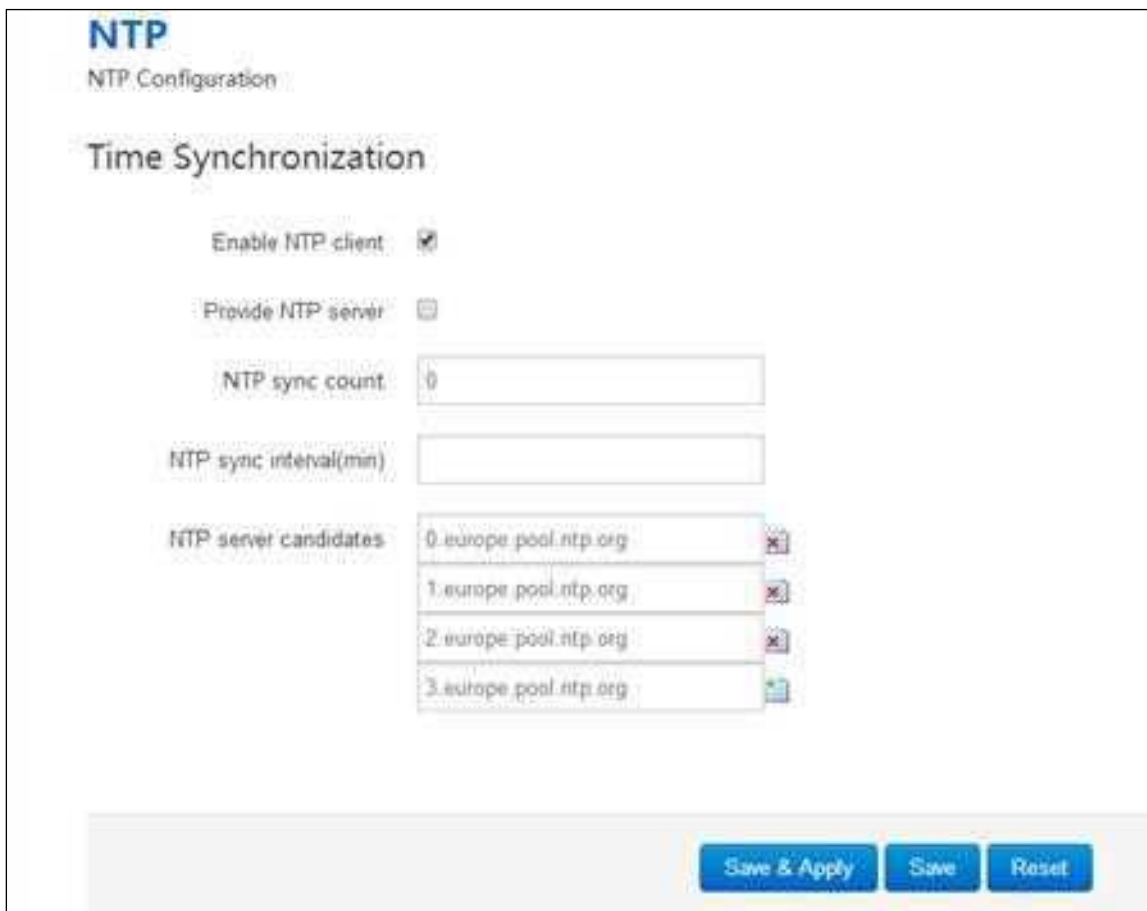
SSH Account

If using SSH the password can be changed here. As default SSH is disabled from WAN. Unless you are an advanced user and have a specific reason to use SSH, it is not recommended to allow SSH access. If allowing SSH access from WAN, you must change the password to something secure and memorable.

Guest Account

Here the guest account can be enabled, and a password can be set.

3.3.3 NTP



NTP
NTP Configuration

Time Synchronization





Enable NTP client ☒

Provide NTP server ☐

NTP sync count

NTP sync interval(min)

NTP server candidates

0.europe.pool.ntp.org	
1.europe.pool.ntp.org	
2.europe.pool.ntp.org	
3.europe.pool.ntp.org	

NTP is network timing protocol.

Enable NTP client

The default value is enabled. Router acts as a NTP client.

Provide NTP server

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

NTP sync count

NTP running counts after router connects to internet, 0 or empty means infinite.

NTP sync interval (min)

The interval time between NTP synchronization.

NTP server candidates

This is the NTP server list, entering multiple NTP servers is accepted. You can click the 

button to delete an entry, or click  button to add a new entry.

3.3.4 Backup/Restore

The screenshot shows the 'Configuration files operations' page. On the left is a sidebar menu with items: Status, System, System, Setup Wizard, Password, NTP, Backup/Restore (highlighted), Upgrade, Reset, Reboot, Services, Network, and Logout. The main content area is titled 'Configuration files operations' and contains two sections. The 'Backup' section says 'Download a tar archive of the current configuration files.' and has a 'Download' button. The 'Restore' section says 'To restore configuration files, you can upload a previously generated backup archive here.' and has a 'Restore backup configuration archive:' label, a 'Choose file' button, 'No file chosen' text, and an 'Upload...' button.

To backup the configuration file, click the 'Download' button. An archive file will be generated and be downloaded to your PC automatically.

To restore the configuration files, you can click the button "Choose File", then select an archived configuration file, and finally click button "Upload", then system will load this file and apply it, and then restart router.

3.3.5 Upgrade

The screenshot shows the 'System upgrade' page. It has a title 'System upgrade' and a description: 'Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to ret. firmware image).'. Below this are two checkboxes: 'Keep settings:' (checked) and 'Safe upgrade:' (checked). At the bottom, there is an 'Image:' label, a 'Choose File' button, the text 'no file selected', and an 'Upload image...' button.

Upload a system compatible firmware to replace the running firmware. The default value for "Keep settings" is checked, that means current configuration will be kept after system upgrade, otherwise router will be reset to the factory settings. We highly recommend unchecking "Keep settings" to

prevent conflicting parameters after the firmware upgrade.

Safe upgrade option is checked by default. Please always keep it checked to avoid broken firmware.

Click the button “[Choose File](#)” to select a compatible firmware, then click the button “[Upload image...](#)”. The router will do a basic check of the uploaded file. If it is an incompatible file, an error will be generated like the below:



System upgrade

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

Keep settings: ☒

Safe upgrade: ☒

Image: [Choose File](#) no file selected [Upload image...](#)

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 system will restart in 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: d49e4e53a837a6eca830ff8cod9c0c41
- Size: 10.25 MB (15.00 MB available)
- Configuration files will be kept.

[Cancel](#) [Proceed](#)

3.3.6 Reset (Restore to factory default settings)

There are three ways to perform a factory reset:

- 1) From within the web interface. **System > Reset**



Pressing the 'Reset' button as seen in the picture above, will reset the router to the factory default settings. After clicking the button, a confirmation button will appear. Press this and the system will reset.

- 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 router for approx. 10 seconds. Note: There is no immediate indication that the reset has been performed. Release the button and after about 10 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.

3.3.7 Reboot

Status

System

- System
- Setup Wizard
- Password
- NTP
- Backup/Restore
- Upgrade
- Reset
- Reboot**

Services

Network

Logout

Reboot Settings

Reboot At Time Settings

Reboot at time ☐

Time(H:M:S)

Reboot Timer Settings

Reboot when timeout ☐

Timer(min)

Reboot

Reboots the operating system immediately.

This function allows the Go2-4G to have a programmed reboot at a specified time of the day, this will occur every day. This is a useful feature for Go2-4Gs installed at remote un-manned sites. As all mobile devices will periodically lose connection to their local cell tower, and in some instances will fail to reconnect without a reboot. Setting the router to reboot once a day will ensure there is a chance to reconnect in this event.

Reboot at time: reboot router at a specific time.

Reboot when timeout: reboot router after the set timer times-out.







Click button “Reboot Now”, the system will restart in several seconds.

3.4 Router status

3.4.1 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	Cell_Router
Slt	860420156A00D094
Firmware Version	3.2.264
Kernel Version	3.18.29
Local Time	Mon May 1 / US: 11:55:23/1
Uptime	0h 16m 41s
Load Average	0.09, 0.05, 0.54
Port Status	<div>      </div> <div> LAN1 LAN2 LAN3 LAN4 WAN </div>
Mobile 1	
Cellular Status	Up
IP Address	10.176.239.44/255.255.255.248
DNS 1	82.132.254.2
DNS 2	82.132.254.3
Cell Modem	qwritel_EP00E (2CTC_0300)
IMEI/ESN	866186040362574
Sim Status	SM Ready
Strength	<div>  -18 / 31, dBm: -76 </div>
Selected Network	Automatic
Registered Network	Registered on Home network: "O2 - UK", 7.
Sub Network Type	FDD LTE
Location Area Code	9400
Cell ID	7A5407D
Band	1.199
RSRP	-107 dBm
RSRQ	-12 dB
SNR	14 dB



System Status

Field	Description
Hostname	Name of the device.
SN	Serial of the router.
Firmware Version	Firmware currently installed on the router. For latest firmware versions contact techsupport@go2sim.com
Kernel Version	Kernel version currently used by on the router. This is a program which connects the software to the router's hardware.
Local time	Current time of the device.
Uptime	Amount of time since the router has last been turned on / rebooted.
Load Average	Load average of the CPU in %. The three values are last: 1 minutes, 5 minutes, 15 minutes.
Port Status	Visualisation of connected ports. (Physical LAN is LAN4 in picture).

3.4.2 Network status

The Network status page consists of three tabs, these show detailed information of the cell mobile interface, WAN and LAN.

This section displays signal data values in -X dBm. These values require some explanation. The main acronyms are:

RSSI = Received Signal Strength Indicator
RSRP = Reference Signals Received Power
RSRQ = Reference Signal Received Quality
SINR = Signal-to-Interference-plus-Noise Ratio

Strength RSSI – Signal strength received from cell tower to modem. Indicated by negative dBm value, the closer to 0, the stronger the signal.

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

Cellular Status

Up

Cell Modem

quectel_EP06E (2C7C_0306)

IMEI/ESN

868180040382514

Sim Status

SIM Ready

Strength

18 / 31, dBm : -82

Selected Network

Automatic

Registered Network

Registered on Home network: '02 - UK', 7,

Sub Network Type

FDD LTE

Location Area Code

8420

Cell ID

7A84D7D

Band

1,100

RSRP

-107 dBm

RSRQ

-11 dB

SINR

16 dB

MSISDN/IMSI

7234107953990984

Connection Status

Port

Mobile-eth

IPv4 Addr

10.176.239.44/29

DNS 1

62.132.254.2

DNS 2

62.132.254.3

Gateway

10.176.239.45

WAN status page

Status

Overview

Network

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

System

Services

Network

Logout

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:

90:22:00:00:00:00

RX

0.00 B (0 Pkts.)

TX

34.61 KB (112 Pkts.)

IPv6 WAN Status

Not connected

Active Connections

444 / 1034 (2%)

LAN status page:

Status

Overview

Network

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

System

Services

Networks

Logout

Mobile

WAN

LAN

LAN Status

Status Overview

Uptime:	0h 5m 5s
Process:	state
Name:	br-lan
Type:	bridge
Mac Addr:	90:22:00:80:00:00
IPv4 Addr:	192.168.1.1/24
IPv6 Addr:	FE80::F00D:1001::1/64
RX	420.41 KB (3487 Pkts.)
TX	1.29 MB (3136 Pkts.)

LAN Ports

Port	MAC-Addr	RX	TX
wired-LAN	90:22:00:00:00:00	451.26 KB (3735 Pkts.)	1.29 MB (3147 Pkts.)
WiFi	90:22:00:00:00:00	0.00 B (0 Pkts.)	0.11 KB (62 Pkts.)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
88S-20150003MPW3L	192.168.1.174	00:00:00:00:00:00	50:00:00:00:00:00

3.4.3 Firewall status

The Firewall status page shows IPv4 and IPv6 rules and counters. Here you can reset counters

and restart firewall functionality.

Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Realtime Graphs
System
Services
Network
Logoff

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	1101	141.09 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	5213	1.48 MB	delegate_forward	all	—	+	+	0.0.0.0/0	0.0.0.0/0	—

Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1063	212.63 KB	delegate_output	all	—	+	+	0.0.0.0/0	0.0.0.0/0	—

3.4.4 Routes

The Routes page shows rules which are currently active on this router. The ARP table is displayed as well. The ARP table can be very useful to check if devices on your LAN are able to communicate with the router.

Overview

Network

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

System

Services

Network

Logview

Routes

The following rules are currently active on this system:

ARP

IPv4 Address	MAC Address	Interface
192.168.1.1/24	08:00:0E:47:71:37	eth0

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
eth0	0.0.0.0/0	10.64.64.64	0	main
eth0	10.64.64.64		0	main
eth	192.168.1.0/24		0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
eth	:::2001:1001::64		1024	main
eth0	:::2001::		256	local
eth	:::2001::		256	local
eth	:::2001::		256	local

3.4.5 System log

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

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

Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Zone ranges:	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Normal: [mem 0x00000000-0xc0000000]	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Movable zone start for each node	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Early memory node ranges	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] node 0: [mem 0x00000000-0xc0000000]	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] initmem: setup node 0 [mem 0x00000000-0xc0000000]	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] On node 0 totalpages: 10384	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] free_area_init_node: node 0, pgdat 00324180, node_mem_map 01000000	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] Normal zone: 128 pages used for memmap	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] Normal zone: 0 pages reserved	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] Normal zone: 10364 pages, LIFO batch:3	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Primary instruction cache 64KB, VIVT, 4-way, linesize 32 bytes	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Primary data cache 32KB, 4-way, FPBT, no aliases, linesize 32 bytes	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] pcpu-alloc: all 0-432768-432768 alloc=1*432768	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.000000] pcpu-alloc: [0] 0	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 10256	
Sat Aug 13 09:30:03 2016 kern.notice kernel: [0.000000] Kernel command line: console=ttyS0 57600 rootfstype=squashfs,jffs2	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] Dentry cache hash table entries: 5192 (order: 3, 32768 bytes)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] Writing ErrCtl register=0807e000	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] Readback ErrCtl register=0807e000	
Sat Aug 13 09:30:03 2016 kern.warn kernel: [0.000000] Memory: 01164K/5536K available (2626K kernel code, 140K rwdata, 106K ro	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPU=1, Nodes=1	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] NR_IRQS:256	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] CPG Clock: 540MHz	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.000000] SysTick: running - mull 214748, shift 32	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.010000] Calibrating delay loop... 365.84 BogoMIPS (pp=192016)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.010000] pvt_max: default: 32768 minimum: 305	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.010000] Mutex-cache hash table entries: 1024 (order: 0, 4096 bytes)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.060000] Moumpool-cache hash table entries: 1024 (order: 0, 4096 bytes)	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.050000] pinctrl core: simulated pinctrl subsystem	
Sat Aug 13 09:30:03 2016 kern.info kernel: [0.100000] NET: Registered protocol family 16	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] r2660 pinmux pinctrl try to register 73 pins	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] pinctrl core: registered pin 0 (i0) on r2660 pinmux	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] pinctrl core: registered pin 1 (i1) on r2660 pinmux	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] pinctrl core: registered pin 2 (i2) on r2660 pinmux	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] pinctrl core: registered pin 3 (i3) on r2660 pinmux	
Sat Aug 13 09:30:03 2016 kern.debug kernel: [0.110000] pinctrl core: registered pin 4 (i4) on r2660 pinmux	

3.4.6 Kernel log

This page shows the Kernel log from the system boot up. This log is not saved when router restarts. You can export the log by clicking the button “Export syslog”.

Status

Overview

Network

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

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
0.000000] Board has DDR2
0.000000] Analog PMU set to hw control
0.000000] Digital PMU set to fw control
0.000000] SoC Type: MediaTek MT7620A ver:2 eco:6
0.000000] bootconsole [early0] enabled
0.000000] CPU0 revision is: 00019650 (MIPS 24KEc)
0.000000] MIPS: machine is mt7620a_model_2
0.000000] Determined physical RAM map
0.000000] memory: 04000000 @ 00000000 (usable)
0.000000] Intrad not found or empty - disabling intrd
0.000000] Zone ranges:
0.000000] Normal [mem 0x00000000-0xd3ffff]
0.000000] Movable zone start for each node
0.000000] Early memory node ranges
0.000000] node 0 [mem 0x00000000-0xd3ffff]
0.000000] Initmem setup node 0 [mem 0x00000000-0xd3ffff]
0.000000] On node 0 totalpages: 16384
0.000000] free_area_init_node: node 0, pgdat 003241b0, 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 64kB, VIPT, 4-way, linesize 32 bytes
0.000000] Primary data cache 32kB, 4-way, PIPT, 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=ttyS0,57600 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)
0.000000] Writing ErrCtl register=0007e000
0.000000] Readback ErrCtl register=0007e000
0.000000] Memory: 61164K/65536K available (2626K kernel code, 140K rwdata, 556K rodata)
0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
0.000000] NR_IRQS:256
0.000000] CPU Clock: 580MHz
0.000000] systick: running - mull: 214748 - shift: 32

```

3.4.7 Realtime graphs

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



3.4.8 VPN

This page shows the status of the VPN connections, including: IPSec status, IPSec log, OpenVPN status, PPTP status and L2TP status.

IPSec Status page



Status

Overview

Network

Firewall

Routes

System Log

Kernel Log

Reboot Log

Realtime Graphs

VPN

System

Services

Network

Logout

IPsecIPsec LogOpenVPNSSH TunnelL2TP Tunnel

IPSec Status

Refresh

Status of IKE daemon (weakSwan 5.6.3, Linux 3.10.29, ipsec)
uptime: 2 minutes, since Dec 14 14:26:29 2015
main: state 122880, minlog 0, used 154640, key 9232
worker threads: 11 of 16 idle, 5/10/0 working, job queue: 0/0/0, scheduled: 4
loaded plugins: charon random nonce aes des sha1 sha2 md5 gcm pkcs1 gmp x509 libelliptic hmac stroke kernel-netlink
Listening IP addresses:
192.168.1.1
192.168.1.1
192.168.1.1
10.87.68.136
10.87.68.136
Connections:
IPSec_base: 10.87.68.136, 192.138.155.167, IKEv1
IPSec_base: local: [10.87.68.136] uses pre-shared key authentication
IPSec_base: remote: [192.138.155.167] uses pre-shared key authentication
IPSec_base: child: 192.168.1.0/24 === 0.0.0.0/0 TUNNEL
bypass: 192.168.1.0/24, 'None', 'None', IKEv1/2
bypass: 192.168.1.0/24, local: uses public key authentication
bypass: 192.168.1.0/24, remote: uses public key authentication
bypass: 192.168.1.0/24, child: 192.168.1.0/24 === 192.168.1.0/24 PASS
Suggested Connections:
bypass: 192.168.1.0/24, 192.168.1.0/24 === 192.168.1.0/24 PASS
Security Associations (1 up, 0 connecting):
IPSec_base[1]: ESTABLISHED 5 seconds ago, 10.87.68.136[10.87.68.136], 192.138.155.167[192.138.155.167]
IPSec_base[1]: IKEv1 SPIs: 7b64a6c6b57954, f78c450b1c526537, pre-shared key authentication in 23 hours
IPSec_base[1]: IKE proposal: AES_CBC, 128/HMAC, SHA2_256, 128PBF, HMAC, SHA2_256/MOQCP_3072
IPSec_base[1]: BISTALLED TUNNEL, reqid 1, ESP in UDP SPIs: ccb15262, c9d84763, 1
IPSec_base[1]: AES_CBC, 128/HMAC, SHA1_36, 8 bytes, 0 bytes, rekeying in 23 hours
IPSec_base[1]: 192.168.1.0/24 === 192.168.1.0/24

IPSec Log page

IPSec IPSec Log OpenVPN PPTP tunnel L2TP tunnel

IPSec Log

Export IPSec log

```
Dec 14 14:25:30 00[DMN] Starting IKE charon daemon (strongSwan 5.6.2, Linux 3.18.25, mips)
Dec 14 14:25:30 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Dec 14 14:25:30 00[CFG] loading aa certificates from '/etc/ipsec.d/accerts'
Dec 14 14:25:30 00[CFG] loading oasp signer certificates from '/etc/ipsec.d/oaspcerts'
Dec 14 14:25:30 00[CFG] loading attribute certificates from '/etc/ipsec.d/attrcerts'
Dec 14 14:25:30 00[CFG] loading crls from '/etc/ipsec.d/crls'
Dec 14 14:25:30 00[CFG] loading secrets from '/etc/ipsec.d/secrets'
Dec 14 14:25:30 00[CFG] loaded IKE secret for 10.87.58.158:182.138.159.167
Dec 14 14:25:30 00[DBG] loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel
Dec 14 14:25:30 00[JOB] spawning 16 worker threads
Dec 14 14:25:30 05[CFG] received stroke: add connection 'IPSec_base'
Dec 14 14:25:30 05[CFG] added configuration 'IPSec_base'
Dec 14 14:25:30 05[CFG] received stroke: initiate 'IPSec_base'
Dec 14 14:25:30 06[KE] <IPSec_base1> initiating Main Mode IKE_SA IPSec_base[1] to 182.138.159.167
Dec 14 14:25:30 06[ENC] <IPSec_base1> generating ID_PROT request 0 [ SA V V V V ]
Dec 14 14:25:30 06[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:30 08[CFG] received stroke: add connection 'bypass_182.168.1.0/24'
Dec 14 14:25:30 08[CFG] added configuration 'bypass_182.168.1.0/24'
Dec 14 14:25:30 10[CFG] received stroke: route 'bypass_182.168.1.0/24'
Dec 14 14:25:34 15[KE] <IPSec_base1> sending retransmit 1 of request message ID 0, seq 1
Dec 14 14:25:34 15[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:41 09[KE] <IPSec_base1> sending retransmit 2 of request message ID 0, seq 1
Dec 14 14:25:41 09[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:54 11[KE] <IPSec_base1> sending retransmit 3 of request message ID 0, seq 1
Dec 14 14:25:54 11[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:26:10 09[KE] <IPSec_base1> sending retransmit 4 of request message ID 0, seq 1
Dec 14 14:26:10 09[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:27:00 12[KE] <IPSec_base1> sending retransmit 5 of request message ID 0, seq 1
Dec 14 14:27:00 12[NET] <IPSec_base1> sending packet: from 10.87.58.158[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:27:00 12[NET] <IPSec_base1> received packet: from 182.138.159.167[500] to 10.87.58.158[500] (164 bytes)
Dec 14 14:27:00 13[ENC] <IPSec_base1> parsed ID_PROT response 0 [ SA V V V V ]
```

OpenVPN status page

IPSec IPSec Log OpenVPN PPTP tunnel L2TP tunnel

OpenVPN Status

Refresh

```
OpenVPN STATISTICS
Updated: Fri Dec 14 14:30:33 2018
TUN/TAP read bytes:0
TUN/TAP write bytes:0
TCP/UDP read bytes:8613
TCP/UDP write bytes:8527
Auth read bytes:928
pre-compress bytes:0
post-compress bytes:0
pre-decompress bytes:0
post-decompress bytes:0
END
```

PPTP Client Status page

IPSec	IPSec Log	OpenVPN	PPTP tunnel	L2TP tunnel
PPTP Status				
PPTP clients				
Username	Local IP	Remote IP	Remote WAN IP	
user	192.168.0.1	192.168.0.20	139.207.86.24	

L2TP Client Status page

IPSec	IPSec Log	OpenVPN	PPTP tunnel	L2TP tunnel
L2TP Status				
L2TP clients				
Username	Local IP	Remote IP		
user	192.168.0.2	192.168.0.20		

3.5 Services configuration

3.5.1 ICMP check (Ping Reboot)

In this section you can configure the ICMP check (Ping Reboot) function. This is a vital service which is recommended in most remote installations. ICMP check configures the router to ping a specific IP address or hostname at a set interval, if the IP address/hostname is unreachable for a set period, the router will reboot either the whole device or the module (modem). The IP address is usually set to a server which is guaranteed to be always online like google's DNS servers at 8.8.8.8.

The mobile networks will disconnect devices at certain times, ordinarily a 4G device will reconnect with no issue. However, there are occasions where a device will fail to reconnect to the local cell tower and the device will need to be rebooted to reconnect. If the router is in a remote location this will require an engineer to visit the site. The ICMP check will detect a disconnection from the internet when it fails to ping google at 8.8.8.8. The router will auto-reboot and this will avoid many engineer callouts.

We recommend using the pre-filled settings, just tick enable and save and apply to use this function.

ICMP Check

Enable: ☒

Host1 to ping: ipv4 or hostname

Host2 to ping:

Ping timeout: seconds (range [1 - 10])

Max retries: (range [3 - 1000])

Interval between ping: minutes (range [1 - 1440])

Reconnect: ☐

Action when failed:

Save & Apply

Save

Reset

- **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 timeout, then this ping has failed.
- **Max retries:** Denoted the number of retries which are attempted before the selected 'action when failed' field is triggered. If the ping is returned and therefore doesn't fail, the counter will be reset to 0.
- **Interval between ping:** 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 (modem), and "Restart router" will restart the whole system including radio module (modem).

3.5.2 VRRP

VRRP Configuration


VRRP LAN Configuration Settings


Enable

☒

Virtual ID

Virtual IP address






Priority

Advertisement interval

s

Password



Track interface

v

Track IP/Host

Track interval

s



Track Weight

Status

Save & Apply

Save

Reset

- **Enable:** Enable VRRP (Virtual Router Redundancy Protocol) for LAN.
- **Virtual ID:** Routers with same IDs will be grouped in the same VRRP cluster, range [1 - 255].
- **Virtual IP address:** Virtual IP addresses for LAN's VRRP cluster. The IP address entry can be deleted by clicking the button , or added by clicking the button .
- **Priority:** Router with highest priority in the same VRRP cluster will act as master. The possible options are numbers from 1 to 255.

3.5.3 Failover (link backup)

3.5.3.1 Failover basic settings

The screenshot shows the 'Failover Configuration' page with the 'Advanced' tab active. The 'Failover Settings' section includes an 'Enable' checkbox (checked), a 'Back To High priority' checkbox (checked), and a 'Current interface' dropdown set to 'primary'. The 'Primary Configuration' section includes a 'Primary' dropdown set to 'Wired_wan', and input fields for 'Host1 to ping', 'Host2 to ping', 'Ping timeout' (1), 'Max Retries' (10), and '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.
- **Host 1 to ping / Host 2 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 ping:** The time between twice ping. The unit is second.

3.5.4 DTU

- 1) This feature is for Go2-4G with DTU option only.
- 2) This feature conflicts with “Connect Radio module” and “GPS send to serial” features. Please disable the “DTU” feature when using either “Connect Radio Module” or “GPS send to serial” feature.

DTU Configuration

Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time

Enable

☐

Send DTU ID

☐

DTU ID

Send DTU ID on initial connection

☐

Forward delay

milliseconds (range[10,10000])

Terminate character(s)

Debug

Error

- **Enable:** Enable DTU feature.
- **Send DTU ID:** Send DTU ID at the front of packet.
- **DTU ID:** The default DTU ID is the SN of router, you can re-write it if necessary.
- **Forward delay:** This unit is in milliseconds. It is the time delay when sending data between the serial port and the network.
- **Terminate character:** split serial port data into different packages with terminate character. It can be a string, or hexadecimal which starts as 0x,such as 0x0a0d.
- **Debug:** Debug level for log output.

Serial Setting

Serial baudrate	115200 bps
Serial parity	None
Serial databits	8 bits
Serial stopbits	1 bits

- **serial baudrate:** supports 300/1200/2400/4800/9600/19200/38400/57600/115200bps
- **serial parity:** supports none/odd/even
- **serial databits:** supports 7 bits and 8 bits
- **serial stopbit:** supports 1 bits and 2 bits

Network Setting

Protocol	TCP
Service mode	Client
Enable Heartbeat	<input type="checkbox"/>
Heartbeat Interval	5
Heartbeat Content	


DTU center configuration

		Delete
CENTER1		
Center enable	<input checked="" type="checkbox"/>	
Center IP	192.168.1.171	
Center Port	5000	
	<input type="text"/> Add	

- **Protocol:** TCP and UDP are supported
- **Service mode:** Client and Server are supported.
- **Enable heartbeat:** The heartbeat is used for connection keep alive.
- **Heartbeat interval:** The time between two heartbeat packets.

- **Heartbeat content:** The content of heartbeat packet.
- **DTU center Configuration:** DTU center is the DTU server, you can input the center name and click button “Add” to add a new center here.
- **If the center is not needed, you can click button “Delete” to delete it, or set it to disabled.**

Please note - The maximum number of DTU centers is 32.

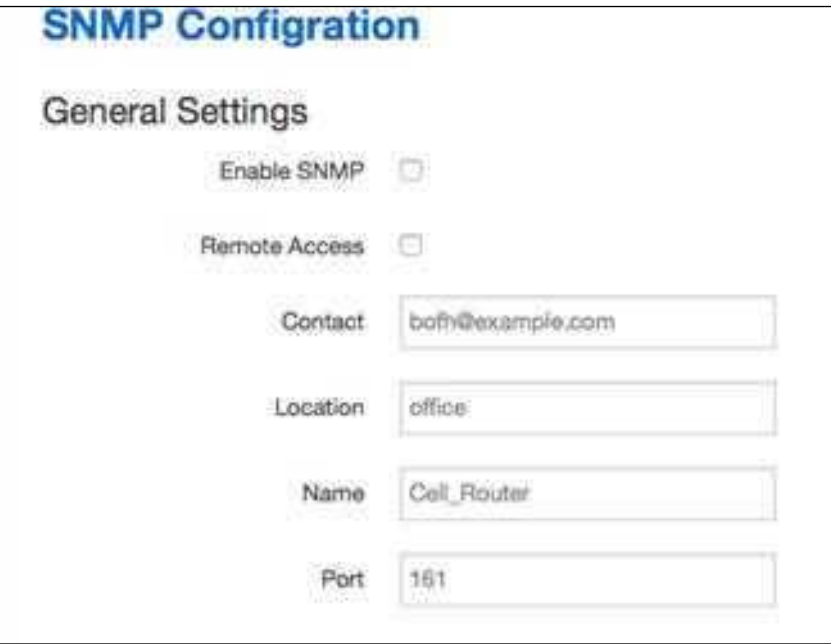


The image shows a 'Network Setting' form with four fields: 'Protocol' (a dropdown menu showing 'TCP'), 'Service mode' (a dropdown menu showing 'Server'), 'Server port' (an empty text input field), and 'Max connections' (a text input field containing '128').

When select Service mode as Server. There are 2 options.

- **Server port:** the port for client to connect.
- **Max connections:** the max amount of clients who can connect.

3.5.4 SNMP



The image shows an 'SNMP Configuration' form with a 'General Settings' section. It contains two checkboxes: 'Enable SNMP' and 'Remote Access', both of which are unchecked. Below these are four text input fields: 'Contact' (containing 'bofn@example.com'), 'Location' (containing 'office'), 'Name' (containing 'Cell_Router'), and 'Port' (containing '161').

- **Enable SNMP:** Enable 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 router's installation address.
- **Name:** Set the router's name in SNMP
- **Port:** SNMP service port, the default value is 161.



The image shows a web form titled "SNMP v1 and v2c Settings". It contains four input fields arranged in two pairs. The first pair is for "Get" operations: "Get Community" with the value "public" and "Get Host/Lan" with the value "0.0.0.0/0". The second pair is for "Set" operations: "Set Community" with the value "private" and "Set Host/Lan" with the value "0.0.0.0/0".

- **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 set as 0.0.0.0/0



The image shows a web form titled "SNMP v3 Settings". It contains six input fields. The first four are dropdown menus: "User" with "admin_user", "Security Mode" with "Private", "Authentication" with "MD5", and "Encryption" with "DES". The last two are password fields: "Authentication Password" and "Encryption Password", both masked with "*****" and having an eye icon to toggle visibility.

- **User:** SNMPv3 username
- **Security Mode:** three options: None, private and Authorized. If it is set to None, there is no password required. If it is set to Authorized, only Authentication method and password are required.
- **Authentication:** Authentication method, two options: MD5 and SHA.
- **Encryption:** Encryption method, DES and AES supported.

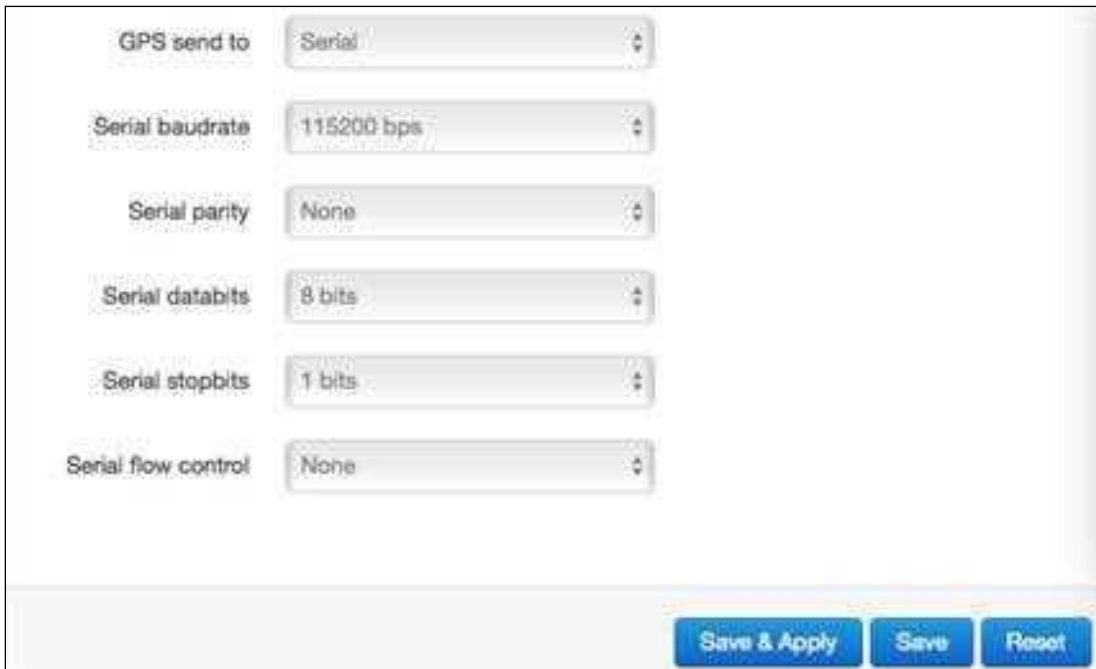
- **Authentication password:** SNMPv3 authentication password, at least 8 characters is required.
- **Encryption password:** SNMPv3 encryption password, at least 8 characters is required.

After all items is setup, click button “[Save & Apply](#)” to enable SNMP functionality.

3.5.6 GPS

The Go2-4G does not have GPS as standard. Units with GPS can be specially ordered.

- **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 SN to the data packet
- **Send interval:** Set the frequency of GPS data packets being sent
- **GPS Send to:** Choose “Serial” or “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 685 Router via a Serial Port, please choose “Serial”.
- If the GPS processor device is a remote server, 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.



The screenshot displays a configuration window for serial communication. It features six dropdown menus, each with a label to its left and a small up/down arrow to its right. The labels and their corresponding values are: 'GPS send to' (Serial), 'Serial baudrate' (115200 bps), 'Serial parity' (None), 'Serial databits' (8 bits), 'Serial stopbits' (1 bits), and 'Serial flow control' (None). At the bottom right of the window, there are three blue buttons: 'Save & Apply', 'Save', and 'Reset'.

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

- **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 ☒

Fix error for some network ☒

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_2 Set Command

DIO_2 Reset Command

DIO_3 Set Command

DIO_3 Reset Command

DIO Status Command

Wifi On Command

Wifi Off Command

Force Cellup Command

Operator List Command

Operator set 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 ☐

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 the 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 bigger or equal to Success Times Threshold, clear signal alarm.

Phone Number

The screenshot shows a web interface for configuring phone numbers. At the top, the title 'Phone Number' is in blue. Below it, 'Phone Number Configuration' is displayed. On the right, there is a 'Delete' button. On the left, under the label 'NUM1', there are three checkboxes: 'SMS Command', 'SMS Alarm', and 'DIO change'. Below these is a 'Phone Number' input field containing the digit '0'. At the bottom left, there is a 'New group name' input field and an 'Add' button. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

- **Add Phone number:** input a name and click button “Add” to add a new Phone number.
 - o **It is recommended to enter multiple possible formats to match your carrier’s network requirements.** (e.g. for UK enter 0044, +44 and 07 versions of number).
- **Delete Phone number:** click button “Delete”.
- **SMS command:** enable SMS command feature on this phone number.
- **SMS alarm:** this phone number can receive SMS Alarms.
- **DIO change:** DIO change alarm can be sent to this phone number.
- **DIO Mail**
Send email to receiver when DIO change.

Mail Configuration

Send email to specified address when DIO changed

Enable ☐

SMTP server

Port

SMTP Authentication ☒

Username

Password 

TLS

StartTLS

Check server certificate

TLS trust file: no file selected

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

11

DIO change

☐

Email address

New group name

Add

Delete

- DIO Default

DIO Configuration

DIO trap ☐

Set DIO to high for a period of time: s

DIO_0 default value

DIO_1 default value

DIO_2 default value

DIO_3 default value

DIO_0 Value

DIO_1 Value

DIO_2 Value

DIO_3 Value

DIO_0 Function

DIO_1 Function

DIO_2 Function

DIO_3 Function

DIO SMS configuration

send user defined SMS alarm when DIO changed

Enable user-defined DIO
SMS alarm ☒

SMS text for DIO0 changed
from low to high

SMS text for DIO0 changed
from high to low

SMS text for DIO1 changed
from low to high

SMS text for DIO1 changed
from high to low

SMS text for DIO2 changed
from low to high

SMS text for DIO2 changed
from high to low

SMS text for DIO3 changed
from low to high

SMS text for DIO3 changed
from high to low

3.5.7 VPN

3.5.8.1 IPSEC

IPSec

PPTP

L2TP

OpenVPN

GRE Tunnel

IPsec Configuration

Instance name	Enable	Exchange mode	Auth method	Operation level	
IPSec_base	Yes	IKEv1>Main	PSK Client	Main	<div>EditDelete</div>

New instance name:

Client

*

Add

Enable Route-based IPsec

☐

Save & Apply

Save

Reset

IPSec Instance: IPSec_base

[Switch to advanced configuration »](#)

Enable ☒

Exchange mode

Operation Level

Authentication method

Remote VPN endpoint

Local endpoint

Local IKE identifier

Remote IKE identifier

Preshared Keys 

Perfect Forward Secrecy

DPD action

DPD delay seconds

DPD timeout seconds

NAT Traversal

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 LAN bypass	<input checked="" type="checkbox"/>
Local subnet	<input type="text" value="192.168.1.0/24"/>
Remote subnet	<input type="text" value="0.0.0.0/0"/>
Local source ip	<input type="text"/>
Remote source ip	<input type="text"/>

- **Local subnet:** The local subnet which connects to the IPSEC VPN.
- **Remote subnet:** The remote subnet which connects to the IPSEC VPN.
- **Local source ip:** The internal source IP of local device to use in a tunnel, also known as virtual IP
- **Remote source ip:** The internal source IP of remote device to use in a tunnel, also known as virtual IP

Phase 1 Proposal

Enable: ☒

Encryption algorithm: 3DES ▼

Hash algorithm: HMAC_MD5 ▼

DH group: MODP1024/2 ▼

Life time: 86400 seconds

Phase 2 Proposal

Enable: ☐

Encryption algorithm: AES-128 ▼

PFS group: MODP1024/2 ▼

Authentication: HMAC_SHA1 ▼

Life time: 86400 seconds

Please Note:

All the 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	Edit Delete

New instance name: Role: [Add New](#)

PPTP NAT enable: ☒

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

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 NAT enable:** enable PPTP interface NAT.

PPTP Client configuration

PPTP Client Instance: Client

Main Settings

Enable ☐

Server

Username

Password



Remote LAN subnet

Remote LAN netmask

MTU

1500

Keep Alive

Use DNS servers advertised
by peer ☒

MPPE Encryption ☒

Debug ☐

Restart module when PPTP
connects failed ☒

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 ☐

PPTP Local IP

PPTP remote IP start

PPTP remote IP end

ARP Proxy ☐

MPPE Encryption ☒

Debug ☐

Username

admin

Password

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	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New instance name:

State

Client


Client

Server

L2TP Client configuration

L2TP Client Instance: Cli

Main Settings

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text" value="5"/>
Debug	<input type="checkbox"/>

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 ☐

L2TP Local IP

Remote IP range begin

Remote IP range end

Remote LAN IP

Remote LAN netmask

ARP Proxy ☐

Debug ☐

Username

Password

admin

 Add

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 go to overview page to restart openVPN instance manually after Save&Apply

	enabled	started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	No	start	full	1194	udp	Edit Delete
sample_server	No	No	start	full	1194	udp	Edit Delete
sample_client	No	No	start	full	1194	udp	Edit Delete

Create configuration for an effect Add

Save & Apply

Save

Reset

Please 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:

mtok ☒

disable_oc ☒

Additional Field

- cd
- chroot
- log
- log_append
- lxc
- echo
- vermap_user
- status_version
- rule
- up
- up_delay
- down
- route_up
- setenv
- ts_verify
- client_connect
- learn_address
- auth_user_pass_verify**

Additional Field

impropervpn-status sig

Add

3.5.8.5 GRE tunnel

IPSec | PPTP | L2TP | OpenVPN | **GRE Tunnel**

GRE Tunnel Configuration

Instance name	Enable	Peer IP addr	Remote network	Local tunnel IP	
GRE	No				<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New instance name:

GRE Tunnel

GRE Instance: Gre_tunnel

Enable ☐

TTL

MTU

Peer IP Address

Remote LAN subnet

Remote LAN netmask

Metric

Local Interface

Local Tunnel IP

Local Tunnel Mask

Keepalive

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.

3.5.9 DDNS

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

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	15349866a.iok.la No data	<input checked="" type="checkbox"/>	Never Verify	PID: 3229	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]

Hostname/Domain

Username

Password

- **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

The screenshot shows the 'Basic Settings' tab with the following fields:

- IP address source [IPv4]:** A dropdown menu with 'Network' selected.
- Network [IPv4]:** A dropdown menu with 'ifmobile' selected.
- DNS-Server:** A text input field containing 'mydns.lan'.
- PROXY-Server:** A text input field containing 'user:password@myproxy.lan:8080'.
- Log to syslog:** A dropdown menu with 'Notice' selected.
- Log to file:** A checkbox that is checked.

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.

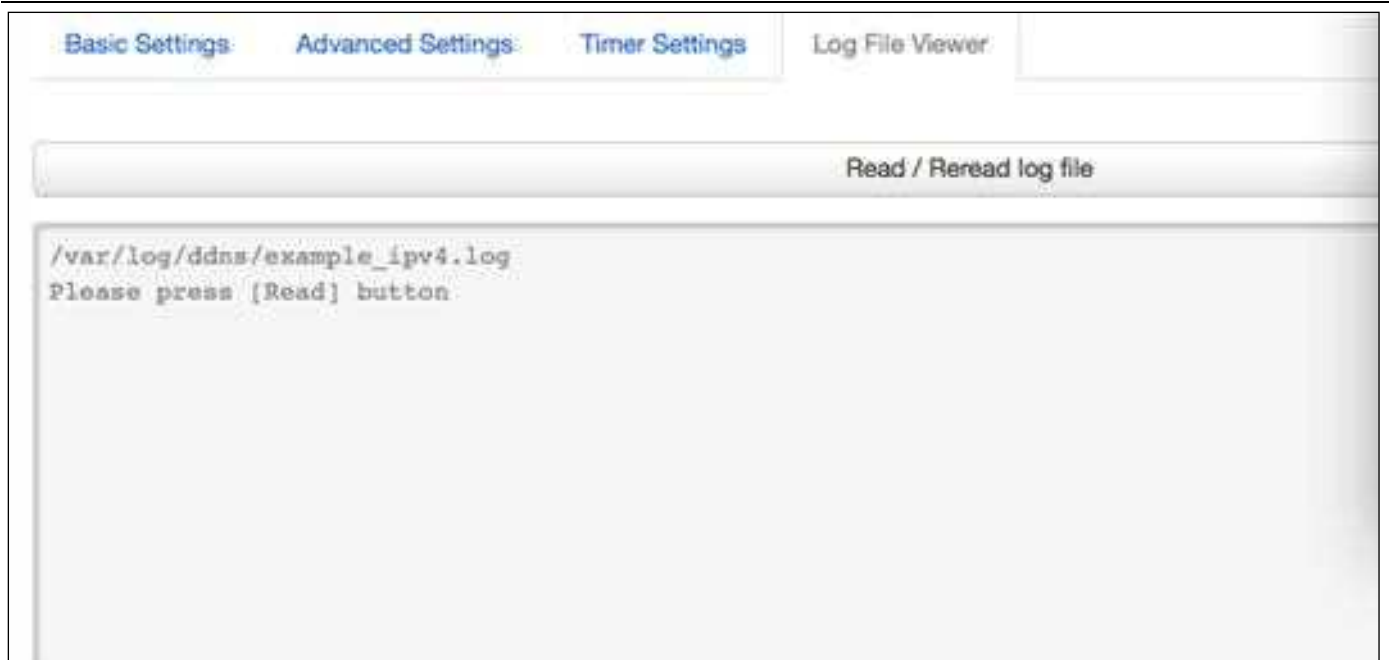
Log to syslog: Writes log messages to the syslog. Critical errors will always be written to the syslog.

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

The screenshot shows the 'Advanced Settings' tab with the following fields:

- Check Interval:** A text input field containing '10' and a dropdown menu with 'minutes' selected.
- Force Interval:** A text input field containing '72' and a dropdown menu with 'hours' selected.
- Error Retry Counter:** A text input field containing '0'.
- Error Retry Interval:** A text input field containing '60' and a dropdown menu with 'seconds' selected.

- **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 setting 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.

Please Notes

This feature is conflicts with DTU and "GPS sent to serial". Please make sure the other two features are disabled before enabling Connect Radio Module. Otherwise, the following error will occur.

Connect Radio Module Configuration

Exchange data between radio module and serial

Enable ☒

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

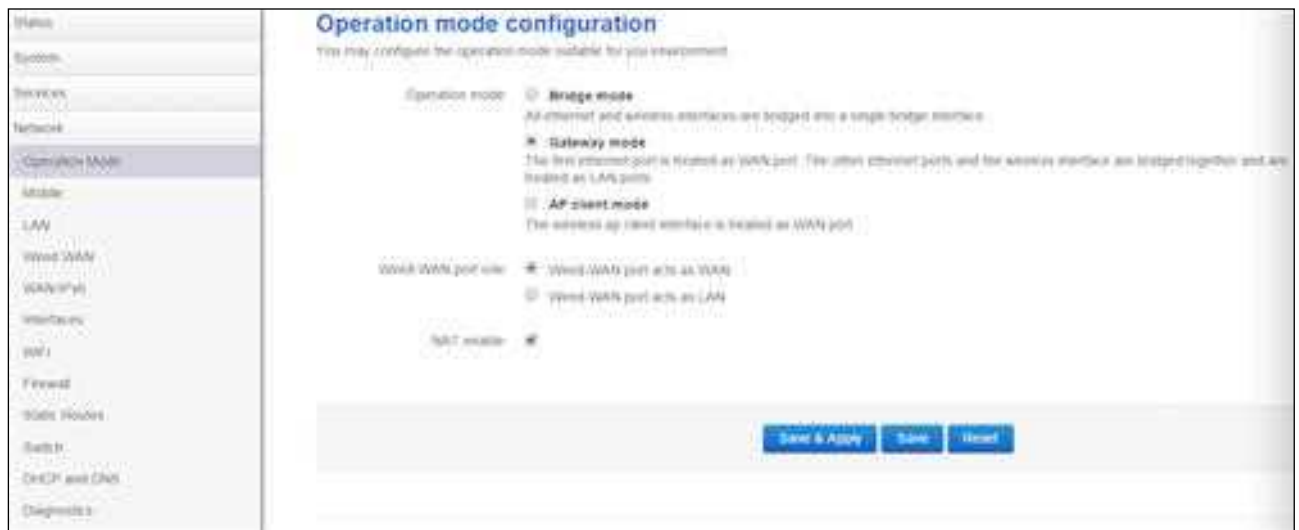
- **Connect Mode:** Serial only

Modem to Serial Settings

- **serial baudrate:** support 9600/19200/38400/57600/115200bps
- **serial parity:** support none/odd/even
- **serial databits:** support 7 bits and 8 bits
- **serial stopbit:** support 1 bits and 2 bits
- **Serial Flow Control:** support 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 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".

3.6.1.1 Set two LAN Ethernet Ports on Go2-4G

Check the "Wired-WAN port acts as LAN ". The router now has 2x LAN and no WAN port.

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.

For more detail on this function and information of the APN, please go to **section 3.3.2 Setup Wizard**.

Please Note:

The Cell Modem Type is marked on the back of the router.

Mobile Configuration

SIM 1

Enable ☒

Mobile connection

PIN code

Dialing number

APN

Authentication method

Dual APN support ☐

Network Type

MTU

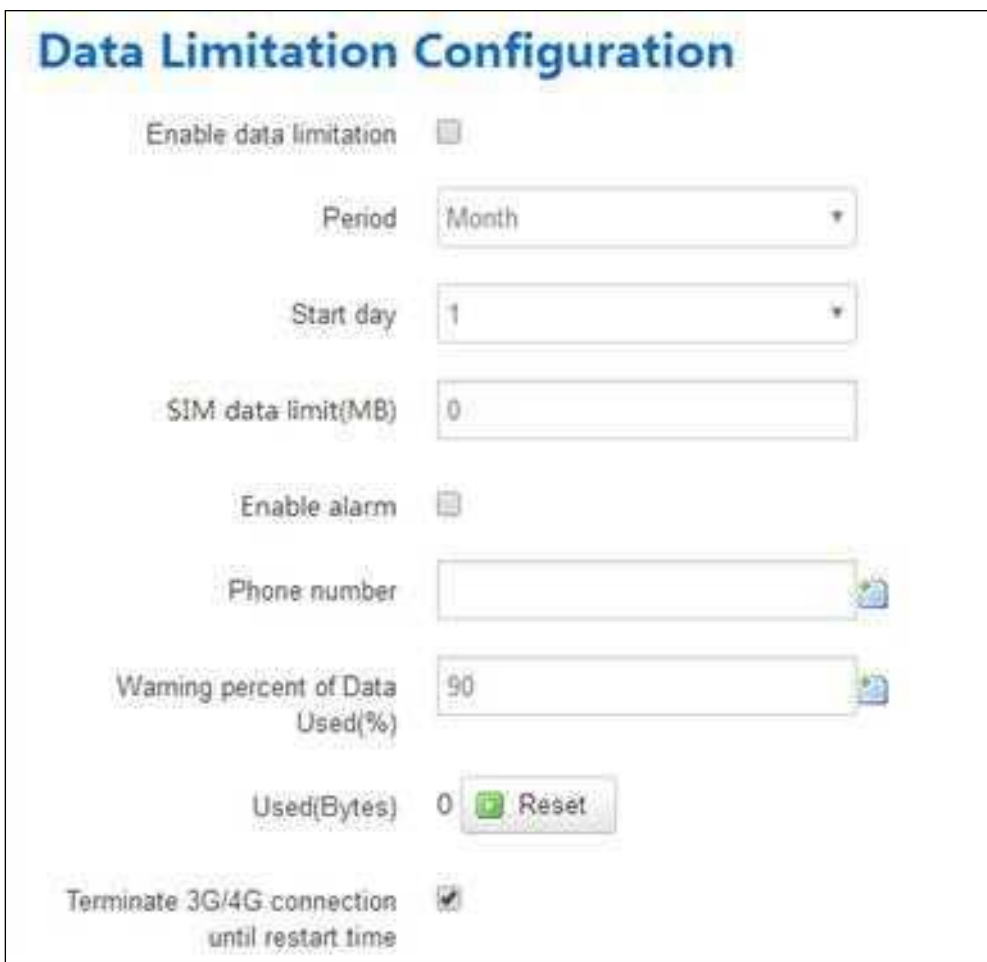
Online mode

Metric

- **Enable** – Tick to enable mobile network.
- **Mobile connection** – Select a suitable mode for the mobile connection. Default is DHCP mode.
- **APN** – Enter APN Address of SIM.
- **PIN code** – Most SIMs don't have a PIN. Leave blank unless change required. **(Advanced)**
- **Dialing number** – Leave as *99# unless change required **(Advanced)**
- **Authentication method** – Most SIMs will require PAP.
- **Username** – Enter APN username of SIM. (sometimes this is just blank)

- **Password** – Enter APN username of SIM. (sometimes this is just blank)
- **Network Type** – Leave as automatic unless change required. (**Advanced**)
- **MTU** – Leave as 1500 unless change required (**Advanced**).
- **Online mode** – Leave as Online mode unless change required (**Advanced**).

3.6.3 Cell mobile data limitation



The screenshot shows a web interface titled "Data Limitation Configuration". It contains several settings:

- Enable data limitation:** A checkbox that is currently unchecked.
- Period:** A dropdown menu set to "Month".
- Start day:** A dropdown menu set to "1".
- SIM data limit(MB):** A text input field containing "0".
- Enable alarm:** A checkbox that is currently unchecked.
- Phone number:** An empty text input field with a small icon to its right.
- Warning percent of Data Used(%):** A text input field containing "90" with a small icon to its right.
- Used(Bytes):** A text input field containing "0" next to a green "Reset" button.
- Terminate 3G/4G connection until restart time:** A checkbox that is currently checked.

- **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 disable the cell mobile network during this period.
- **Enable alarm:** enable 'data limitation' alarm.
- **Phone number:** the phone number receives data limitation alarm SMS.
- **Warning percent of data used:** if the used data arrives this setting, a data limitation alarm SMS will be sent.

- **Used(MB):** the data that has been consumed during this period.
- **Reset:** press this button to clear all used .
- **Terminate 3G/4G connection until restart time:** if the max data is exceed, the cell interface will be set to down. (This will cease the internet connection).

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 interface names separated by spaces. You can also use VLAN notation INTERFACE.VLANID (e.g. eth0.1).

Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Status


br-lan

Uptime: 0h 24m 3s
MAC-Address: 90:22:00:80:03:00
RX: 1.34 MB (13877 Pkts.)
TX: 4.46 MB (12981 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd35::10d:10d1:1/60

Protocol
Static address

Really switch protocol?
Switch protocol

IPv4 address
192.168.1.1

IPv4 netmask
255.255.255.0

IPv4 gateway

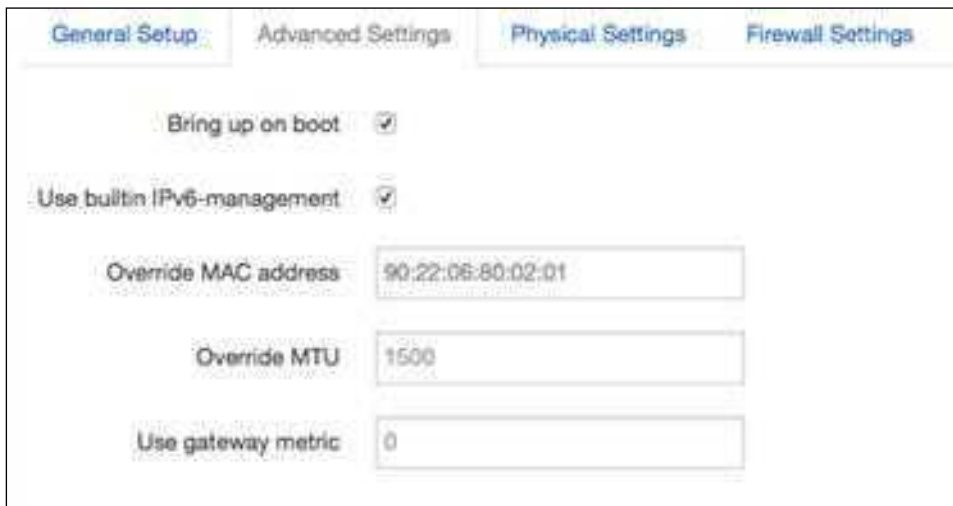
IPv4 broadcast

Use custom DNS servers

IPv6 assignment length
60

IPv6 assignment hint

- **Protocol:** Only a static address is supported for LAN
- **Use custom DNS servers:** multiple DNS server 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 ☒

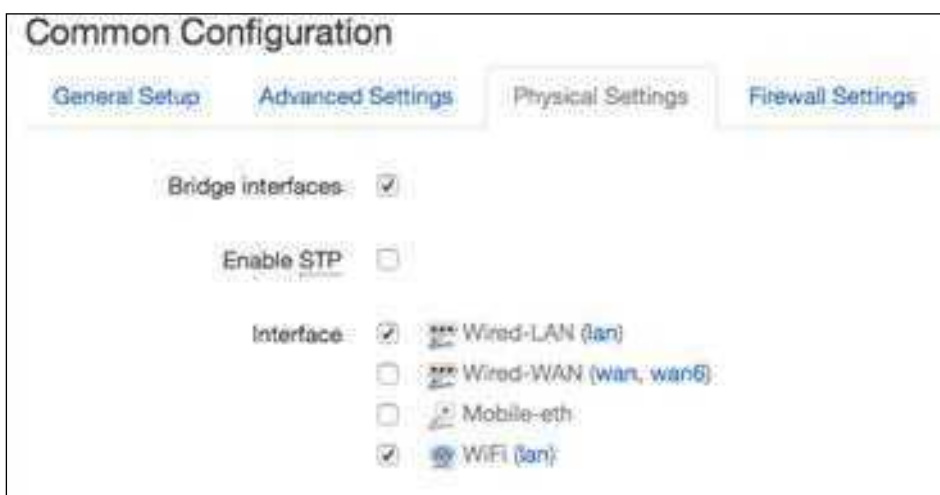
Use builtin IPv6-management ☒

Override MAC address

Override MTU

Use gateway metric

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

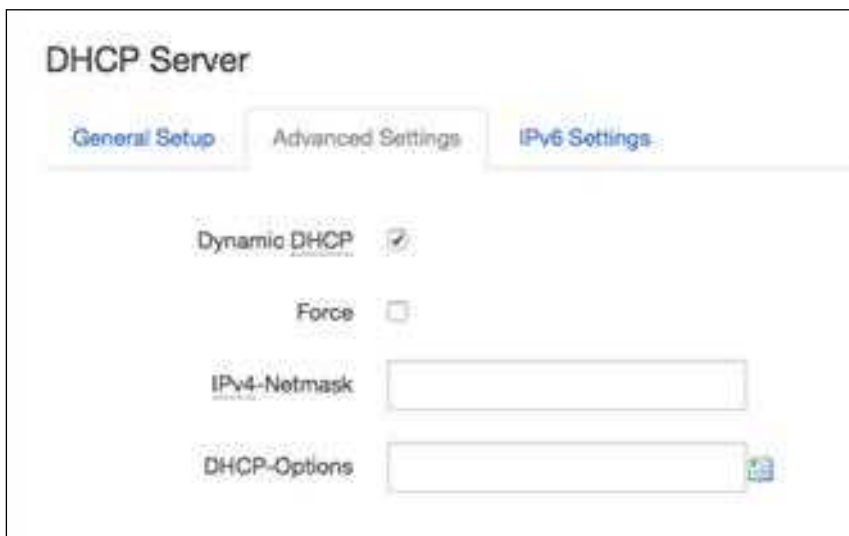
☒ WiFi (lan)

- **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.



The screenshot shows the 'DHCP Server' configuration page with the 'General Setup' tab selected. The 'Ignore interface' checkbox is unchecked. The 'Start' field is set to 100, the 'Limit' field is set to 150, and the 'Leasetime' field is set to 12h.

- **Ignore interface:** if it is unchecked, this will Disable DHCP on LAN.
- **Start:** Lowest leased address as offset from the network address.
- **Limit:** Maximum address number of the leased addresses.
- **Leasetime:** Expiry time of leased addresses, minimum is 2 minutes (2m). 12H means 12 hours.



The screenshot shows the 'DHCP Server' configuration page with the 'Advanced Settings' tab selected. The 'Dynamic DHCP' checkbox is checked. The 'Force' checkbox is unchecked. The 'IPv4-Netmask' and 'DHCP-Options' fields are empty.

- **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, 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: ☐

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

Common Configuration

General Setup | Advanced Settings | **Physical Settings** | Firewall Settings

Status: eth0.2

Uptime: 0h 0m 0s
MAC-Address: 90:22:06:C0:02:01
RX: 0.00 B (0 Pkts.)
TX: 332.81 KB (995 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP: Cell_Router

- **Protocol:** the default protocol is DHCP client. If you need to change it to a different protocol, (such as PPPoE), select the protocol from the drop-down menu, then click button "Switch protocol".

Common Configuration

General Setup

Status	eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:C0:02:01 RX: 0.00 B (0 Pkts.) TX: 346.66 KB (1036 Pkts.)
--------	--------	--

Protocol: PPPoE

Really switch protocol?

After clicking the button “Switch protocol”, the below is shown:

General Setup | **Advanced Settings** | Physical Settings | Firewall Settings

Status	pppoe-wan
--------	-----------

Protocol: PPPoE

PAP/CHAP username:

PAP/CHAP password:

Access Concentrator:

Service Name:

3.6.6 WiFi Settings

radio0: Master "Cell_AP_0002b2"

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | Bitrate: 43.3 Mbit/s

SSID: Cell_AP_0002b2 | Mode: Master
BSSID: 90:22:06:00:02:B2 | Encryption: None

Buttons: Wifi Restart, AP Client, Add, 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	192.168.1.106	-78 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 4, 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: 54%
Mode: Master | SSID: Cell_AP_0002b2
BSSID: 90:22:06:00:02:B2 | Encryption: None
Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm
Signal: -72 dBm | Noise: 0 dBm
Bitrate: 43.3 Mbit/s | Country: 00

Wireless network is enabled | Disable

Operating frequency: Mode: N | Channel: 11 (2462 MHz) | Width: 20 MHz

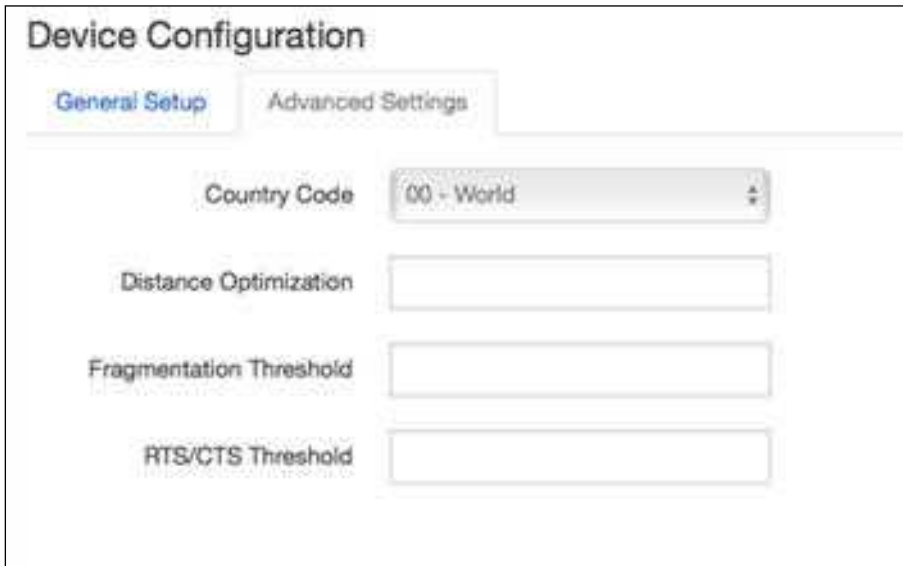
Transmit Power: 20 dBm (100 mW)

- **Status:** show 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 supported.
- **Width:** bandwidth options 20MHz and 40MHz.
- **Transmit Power:** from 0dBm to 20dBm supported.

3.6.6.2 WiFi Advanced Configuration



The screenshot shows the 'Device Configuration' window with the 'Advanced Settings' tab selected. It contains four configuration items:

Parameter	Value / Input Field
Country Code	00 - World (dropdown menu)
Distance Optimization	[Empty text input field]
Fragmentation Threshold	[Empty text input field]
RTS/CTS Threshold	[Empty text input field]

- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to farthest 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
Cell_AP_0002b2

Mode
Access Point

Network

☐ ifmobile:
☐ lan:
☐ 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: WPA-PSK

Cipher: auto

Key:

Enable WPS pushbutton, requires WPA(2)-PSK: ☒

Encryption options

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

Key: This is the password used to join the wireless network. If Encryption set to “No Encryption”, no password is needed.

Interface Configuration

General Setup Wireless Security MAC-Filter

MAC-Address Filter: Allow list

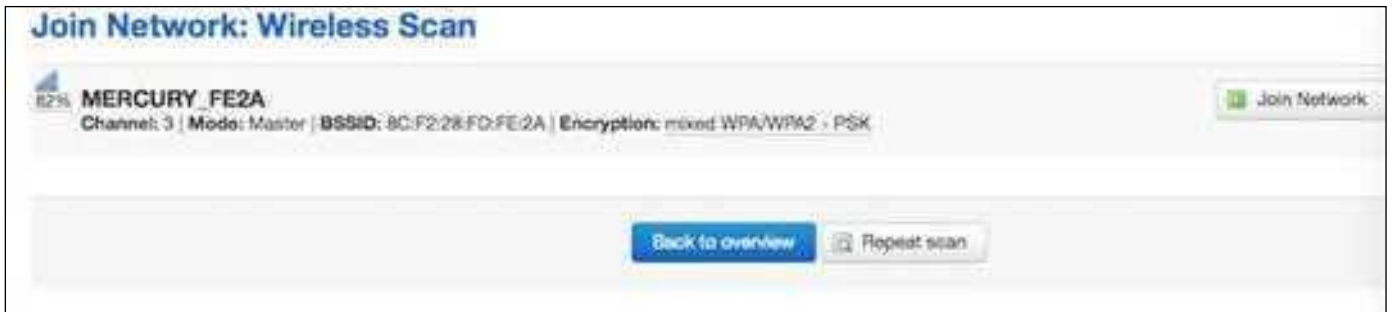
MAC-List:

00:1E:10:1F:00:00 (10.223.164	
68:A8:6D:48:77:5E (dentydeMi	
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 forwarded. Deny list: all packets can be forwarded except MAC address in the list.
- **MAC-List:** click button to delete MAC address from the list, click button to add a new MAC address into the list.

3.6.6.4 WiFi AP client

Step 1) click button “AP Client” on wireless overview page, then system will start to scan all WiFi signals available.



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



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. Leave as wwan unless it conflicts with another interface.

Step 4) Click Submit if everything is configured. The below is Wi-Fi configuration page. Don't change the Operating frequency, make sure the ESSID and BSSID is from the Wi-Fi you want to join.

Device Configuration

General Setup

Advanced Settings

Status:

0%

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

Operating frequency:

Mode	Channel	Width
N	3 (2422 MHz)	20 MHz

Transmit Power: 20 dBm (100 mW)

Interface Configuration

General Setup

Wireless Security

ESSID: MERCURY_FE2A

Mode: Client

BSSID: 8C:F2:28:FD:FE:2A

Network:

- ☐ ifmobile:
- ☐ lan:
- ☐ wan:
- ☐ wan6:
- ☒ wwan:
- ☐ create:

4 Step 5) Click button "Save & Apply" to start AP client.

Wireless Overview



Generic MAC80211 802.11bgn (radio0)
Channel: 3 (2.422 GHz) | Bitrate: 150 Mbit/s

Wifi Restart AP Client Add



SSID: Cell_AP_0002b2 | Mode: Master
BSSID: 90:22:06:00:02:B3 | Encryption: None

Disable Edit Remove



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:A8:8D:48:77:5E	?	-82 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	58.5 Mbit/s, MCS 8, 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 shows all interfaces status, including uptime, MAC-address, RX, TX and IP address.

Interfaces

Interface Overview

Network

Status

Actions

LAN



Uptime: 0h 50m 35s
MAC-Address: 90:22:06:00:02:01
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



MAC-Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Connect Stop Edit

WAN



Uptime: 0h 0m 0s
MAC-Address: 90:22:06:C9:02:01
RX: 0.00 B (0 Pkts.)
TX: 480.27 KB (1433 Pkts.)

Connect Stop Edit

WAN6



Uptime: 0h 0m 0s
MAC-Address: 90:22:06:C9:02:01
RX: 0.00 B (0 Pkts.)
TX: 480.27 KB (1433 Pkts.)

Connect Stop Edit

WWAN

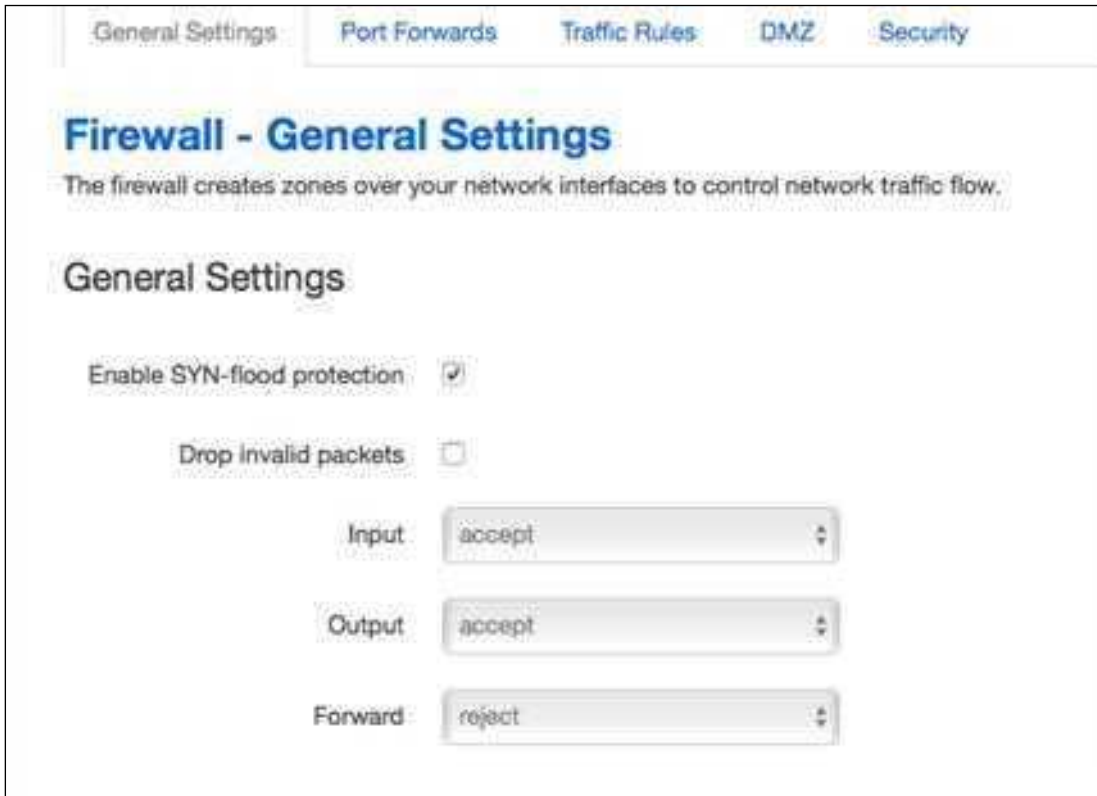
Client "MERCURY_FE2A"

Uptime: 0h 5m 46s
MAC-Address: 90:22:06:00:02:B2
RX: 243.14 KB (960 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



The screenshot shows the 'Firewall - General Settings' page. At the top, there are tabs for 'General Settings', 'Port Forwards', 'Traffic Rules', 'DMZ', and 'Security'. The 'General Settings' tab is active. Below the tabs, the title 'Firewall - General Settings' is displayed, followed by a description: 'The firewall creates zones over your network interfaces to control network traffic flow.' Under the 'General Settings' heading, there are three settings: 'Enable SYN-flood protection' with a checked checkbox, 'Drop invalid packets' with an unchecked checkbox, and three dropdown menus for 'Input', 'Output', and 'Forward'. The 'Input' and 'Output' dropdowns are set to 'accept', and the 'Forward' dropdown is set to 'reject'.

Setting	Value
Enable SYN-flood protection	<input checked="" type="checkbox"/>
Drop invalid packets	<input type="checkbox"/>
Input	accept
Output	accept
Forward	reject

3.6.8.2 Port Forwarding

This page includes the 'port forwards' list and how to add new port forward rules.

Please note – The router's default management port for the web interface is http port 80. Therefore, if you need to port forward 80 to a device on the LAN, you will need to change the http management port number. (e.g. if set to 81, you will need to enter into the web browser 192.168.8.1:81 to reach the router). This can be done at: Network > Firewall > Security. **(See section 3.6.8.5 below)**

TROUBLESHOOTING – The device on the LAN side (DVR/NVR, BMS system, Controller etc.) must be configured correctly to connect to the router. You will need to configure a static IP address on your device, this IP address needs to be in the same subnet as the Go2-4G and not conflicting with the DHCP server. **The device will also need its default gateway to be set as the router's IP address. (This is the most commonly missed setting).**

In most set-ups the external port will be the port contactable on the internet using the router's public IP, this will then send the request on to the device on the router's LAN side with the internal IP

address on the internal port.

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
New port forward	TCP+UDP	wan		lan		

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

- **Name:** port forward instance name. (This will auto-fill from the other parameters).
- **Protocol:** TCP+UDP, UDP or TCP.
- **External zone:** the recommend option is 'wan.' (wan will usually be traffic from the internet).
- **External port:** Specify the port on the external zone, which will be passed to the internal zone.
- **Internal zone:** the recommend 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-Receive	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	+ -	Edit Delete
Allow-Ping	IPv4-ICMP with type echo-request From any host in wan To any host in any zone	Accept forward	<input checked="" type="checkbox"/>	+ -	Edit Delete
Allow-IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+ -	Edit Delete
Allow-DHCPv6	IPv6-UDP From IP range fd8d::10 in wan with source port 547 To IP range fd8d::10 at port 545 on this device	Accept input	<input checked="" type="checkbox"/>	+ -	Edit Delete
Allow-MLD	IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0 From IP range fd8d::10 in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+ -	Edit Delete
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-advertisement From any host in wan To any router IP 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 echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	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

New input rule

TCP+UDP

[Add](#)

New forward rule:

Name

Source zone

Destination zone

New forward rule

lan

wan

[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
------	-------------	------------------	--------------	----------------

New SNAT rule	lan	wan	-- Please cho...	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

Name

Restrict to address family

Protocol

Match ICMP type

Source zone ☐ Any zone

☒ lan: lan:

☐ openvpn: (empty)

☐ vpnzone: (empty)

☐ wan: wan: wan6: mobile: wwan:

Source MAC address: any

Source address: any

Source port: any

Destination zone:

- ☐ Device (input)
- ☐ Any zone (forward)
- ☐ lan: lan:
- ☐ openvpn: (empty)
- ☐ vpnzone: (empty)
- ☒ wan: wan: wan6: ifmobile: wwlan:

Destination address: any

Destination port: any

Action: accept

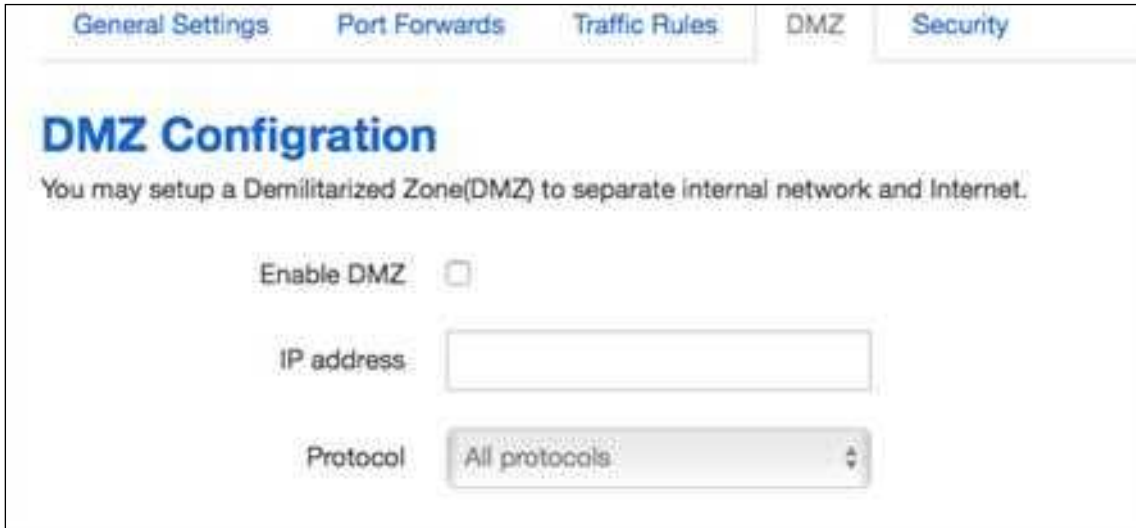
Extra arguments:

- **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:** This is the zone that the traffic comes from.
- **Source MAC address:** traffic rule checks if the incoming packet's source MAC address is matched.
- **Source address:** traffic rule checks if the incoming packet's source IP address is matched.
- **Source port:** traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Destination zone:** the zone that the traffic will go to.
- **Destination address:** traffic rule checks if the incoming packet's destination IP address is matched.
- **Destination port:** traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Action:** if traffic is matched, system will handle traffic according to the Action (accept, drop,

reject, don't track).

- **Extra argument:** passes additional argument to the 'iptables', use with care!

3.6.8.4 DMZ



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

- **IP Address:** Enter the IP address of the computer which you want to set as DMZ host
- **Protocol:** All protocols, TCP+UDP, TCP or UDP.

Please Note:

When the 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

Please Note

YOU MUST CHANGE THE DEFAULT PASSWORD OF THE WEB INTERFACE IMMEDIATELY.

The factory default settings of the router allows connections from WAN on HTTP and HTTPS. Therefore, if you give the router an internet connection with a publicly routable IP address, and you have not changed the default password, you are exposing the router to security threats on the internet.

As default the router does not allow connections from WAN on SSH. Do not change this to allow, unless you have changed the default password.

System Security Configuration

SSH access from WAN

Ping from WAN to LAN

Enable telnet ☐

HTTPS Access

HTTPS port

HTTPS access from WAN

Remote network

HTTP Access

HTTP port

HTTP access from WAN

Remote network

RFC1918 filter ☐

- **SSH access from WAN:** allow or deny users access the router from WAN. The default setting is deny for security reasons.
- **Ping from WAN to LAN:** allow or deny ping from remote side to internal LAN subnet.
- **Enable telnet:** enable telnet connect. The default setting is disabled for security reasons.
- **HTTPS port:** set HTTPS port, the default port is 443.
- **HTTPS access from WAN:** allow or deny access router web management page from remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** fill a remote IP address that can access router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, possible values are from 1 to 32.
- **HTTP port:** set HTTP port, the default port is 80. (if using port forwarding with port 80, you will need to change this to avoid conflicts).

- **HTTP access from WAN:** allow or deny access 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 router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, possible values are from 1 to 32.
- **RFC1918 filter:** reject requests from RFC1918 IPs to public server Ips.

3.6.9 Static Routes

The screenshot shows the 'Routes' configuration page in Go2Sim. It has a title 'Routes' and a subtitle 'Routes specify over which interface and gateway a certain host or network can be reached.' Below this, there are two sections: 'Static IPv4 Routes' and 'Static IPv6 Routes'. The 'Static IPv4 Routes' section contains a table with columns: Interface, Target, IPv4-Netmask, IPv4-Gateway, Metric, MTU, and Table. A single row is visible with the following values: Interface (empty), Target (192.168.8.8), IPv4-Netmask (255.255.255.0), IPv4-Gateway (192.168.1.101), Metric (1), MTU (1500), and Table (254). There is a '+ Add' button to the left of the table and a 'Delete' button to the right. The 'Static IPv6 Routes' section is currently empty, with a message '(This section contains no values yet)' and an '+ Add' button. At the bottom of the page, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

- **Interface:** You can choose the corresponding interface type.
- **Target:** the destination host IP or network.
- **IPv4-Netmask:** the destination IP mask.
- **IPv4-Gateway:** IP address of the next hop.
- **Metric:** used by router to make routing decisions.
- **MTU:** maximum transmission unit
- **Table:** the route table ID, the default value is 254, valid table ID 1-254.

Notice:

- o Gateway and LAN IP of this router must belong to the same network segment.
- o If the destination IP address is the one of a host, and then the Netmask must be 255.255.255.255.
- o If the destination IP address is 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

Please Note:

1. port 4 is Wired-WAN port, port 0, port 1, port 2, port 3 are LAN port.
2. "Untagged" means the Ethernet frame transmits from this port without VLAN tag.
3. "Tagged" means the Ethernet frame transmits from this port is with VLAN tag.
4. "Off" means this port does not belong to VLAN. For default setting, port 0 belongs to VLAN1, but 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](#) [Resolve and Hosts Files](#) [TFTP Settings](#) [Advanced Settings](#)

Domain required ☒

Authoritative ☒

Local server

Local domain

Log queries ☐

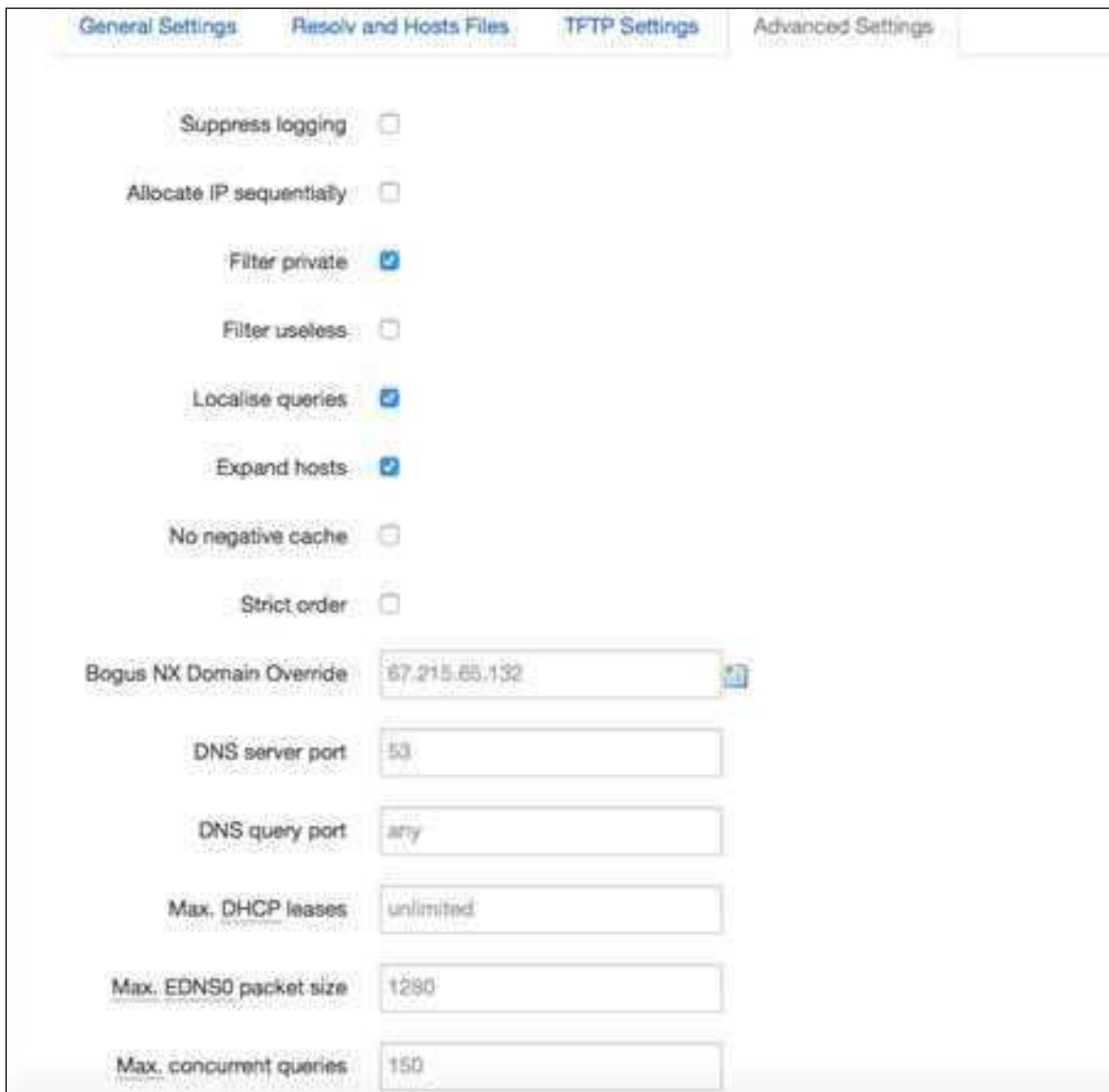
DNS forwardings

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 specification. 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



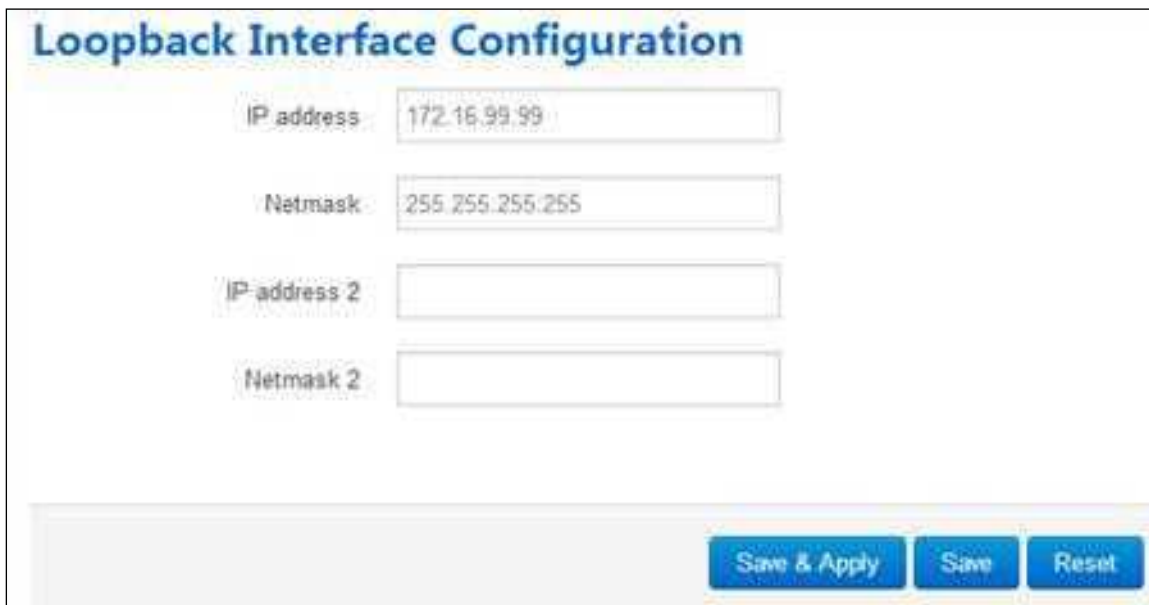
The screenshot shows the 'Diagnostics' section of the Go2Sim interface. Under the 'Network Utilities' heading, there are three columns. Each column has a text input field containing 'www.google.com'. Below the first input field are two buttons: 'IPv4: 1' and 'Ping'. Below the second input field is a 'Traceroute' button. Below the third input field is an 'Nslookup' button.

- **Ping** : This is a fundamental tool that 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.
 - o For example if I want to ping www.google.com, type the target domain name or IP address, then click button “Ping”. Wait couple of seconds, the result will be shown below.



This screenshot shows the same interface as the previous one, but with the results of a ping command displayed in a text area at the bottom. The text reads: 'PING www.google.com (93.46.8.89): 56 data bytes', followed by a separator line '--- www.google.com ping statistics ---' and the final result '5 packets transmitted, 0 packets received, 100% packet loss'.

3.6.13 Loopback Interface



Loopback Interface Configuration

IP address: 172.16.99.99

Netmask: 255.255.255.255

IP address 2:

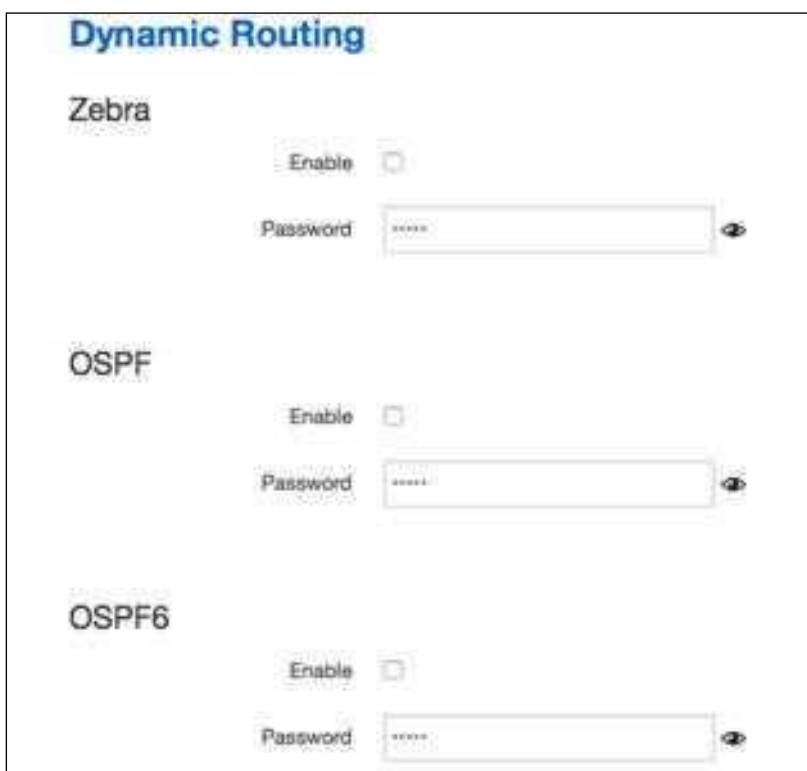
Netmask 2:

Save & Apply Save Reset

The default Loopback interface has IP address 127.0.0.1, you can change it here. The first IP address can be used in IPsec. The secondary can be used as management.

3.6.14 Dynamic Routing

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



Dynamic Routing

Zebra

Enable ☐

Password:

OSPF

Enable ☐

Password:

OSPF6

Enable ☐

Password:

RIP

Enable ☐

Password

RIPng

Enable ☐

Password

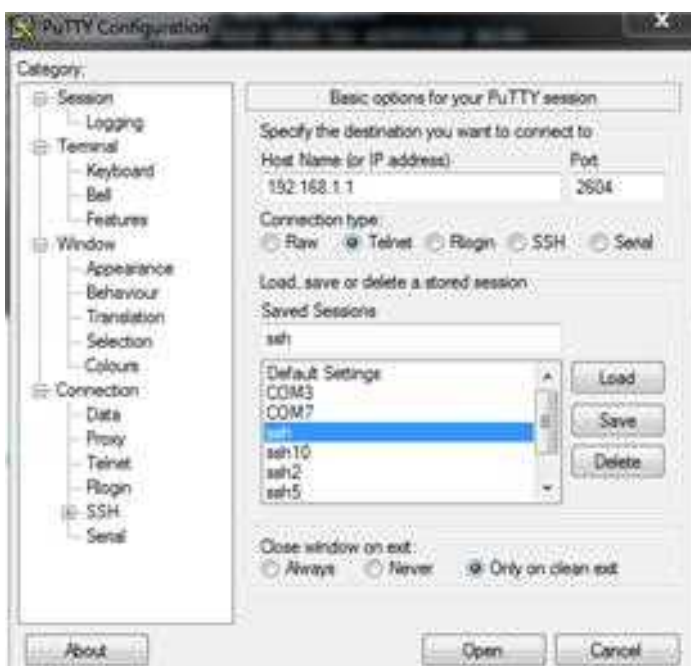
BGP

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.

Please Note: These services can be configured using the program PUTTY. For example, the router's LAN IP is 192.168.1.1. If we want to configure OSPF, we need to set OSPF to "Enable" firstly, 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 Kunihiko 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 prioritize network traffic selected by addresses, ports or services.

The image shows a web-based configuration interface for Quality of Service (QoS). At the top, it says "Quality of Service" in blue, followed by the text "With QoS you can prioritize network traffic selected by addresses, ports or services." Below this is a section titled "Interfaces". Under "Interfaces", there is a list of interfaces, with "WAN" selected. To the right of the "WAN" interface name is a "Delete" button. Below the interface name, there are several configuration options: "Enable" with a checked checkbox, "Classification group" with a dropdown menu showing "default", "Calculate overhead" with an unchecked checkbox, "Half-duplex" with an unchecked checkbox, "Download speed (kbit/s)" with a text input field containing "1024", and "Upload speed (kbit/s)" with a text input field containing "128". At the bottom of the interface list, there is an empty input field and an "Add" button.

- **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	Sort
priority	all	all	all	all	22,43		ssh, rsh	
normal	all	all	all	TCP	90,21,25,80,110,443,500,900		ftp, smtp, http, imap	
express	all	all	all	all	5199		ACL, iDRM, iCG	
normal	all	all	all	all	all			

Each classify 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.

3.6.16 Guest LAN (Guest WiFi)

guest WiFi is a specific WiFi which only can access internet but not local LAN.

Guest LAN(Guest Wi-Fi) Configuration

Enable ☐

LAN IP address

LAN mask

Wi-Fi ssid

Wi-Fi device name

- **Enable:** enable Guest Wi-Fi.
- **LAN IP address:** this LAN IP address must be different with the LAN interface IP address.
- **LAN mask:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in target.
- **Wi-Fi SSID:** the ssid of guest Wi-Fi.
- **Wi-Fi device name:** choose one Wi-Fi device to carry Guest Wi-Fi, the available device name is radio0 and radio1. Check Wi-Fi overview page for the device name. for example:

