



# Dual-SIM 4G LTE WiFi Router

CM210Q-W  
V1.1

18

### Copyright © COMSET 2018

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

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

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



Address: 37/ 125 Highbury Road, Burwood VIC 3125, Australia  
Web: <http://www.comset.com.au>  
Phone: +61 3 9001 9720  
Fax: +61 3 9888 7100

# Contents

## Contents

1.1 Product overview .....	4
1.2 Typical Application Diagram .....	4
1.3 Features.....	5
2 Hardware Installation .....	6
2.1 Panel:.....	6
2.2 LED Status.....	7
2.3 Powering up the CM210 router.....	10
3 Router Configuration .....	12
3.1 Configuration from a local network.....	12
3.2 Basic Configuration.....	13
3.3 WLAN Settings.....	19
3.4 Advanced Network Settings.....	21
3.5 VPN Tunnel.....	27
3.5.4.1 IPSec Group Setup.....	31
3.5.4.2 IPSec Basic Setup.....	33
3.5.4.3 IPSec Advanced Setup.....	34
3.6 Administration .....	35
3.7 Debugging Settings .....	46
3.8 “Reset” Button to Restore Factory Settings.....	48
3.9 Appendix (For advanced optional features only).....	48
3.9.1 GPS Settings.....	48

# 1

## Product Introduction

---

### 1.1 Product overview

The Comset Router CM210Q-W is an industrial grade 3G/4G/4GX LTE WiFi Modem Router with download speeds of up to 150 Mbps and upload speeds of up to 50 Mbps. It is one of the few routers on the Australian market that support band B28 (700MHz)\*.

The Comset Router CM210Q-W is designed to suit Australian conditions. It supports the latest LTE Advanced technology that performs fast and reliable data communication. It enables users to quickly create a secure and fast wireless network. It features built-in WiFi N300 with speeds of up to 300 Mbps, dual SIM card slots for backup redundancy, one Ethernet WAN port for fixed internet connection and two Ethernet LAN ports, as well as a GPIO with two digital input ports and one digital output port. Other features include VPN IPSEC, PPTP (Server and Client), L2TP and Open VPN to establish a secure connection over the 3G/4G network.

The durable and rugged design makes the CM210Q-W the router of choice for remote harsh environments. The compact design, easy integration and rich built-in features make it suitable for a wide range of industrial M2M applications, including industrial automation, building automation, smart metering, security, surveillance, transportation, health, mining and environmental monitoring.

*\* When it comes to mobile reception, low-frequencies are the Holy Grail. The B28 (700MHz) low-frequency radio bandwidth, also known as Telstra 4GX and Optus 4G Plus, can reach much longer distances than high-frequency bands and is better at penetrating solid obstacles like buildings, giving you much better indoor reception.*

### 1.2 Typical Application Diagram

The Comset CM210Q-W 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). A good example is the connection of ATM machines and POS systems back to a server over a secure 4G connection using a secure VPN IPSEC tunnel.

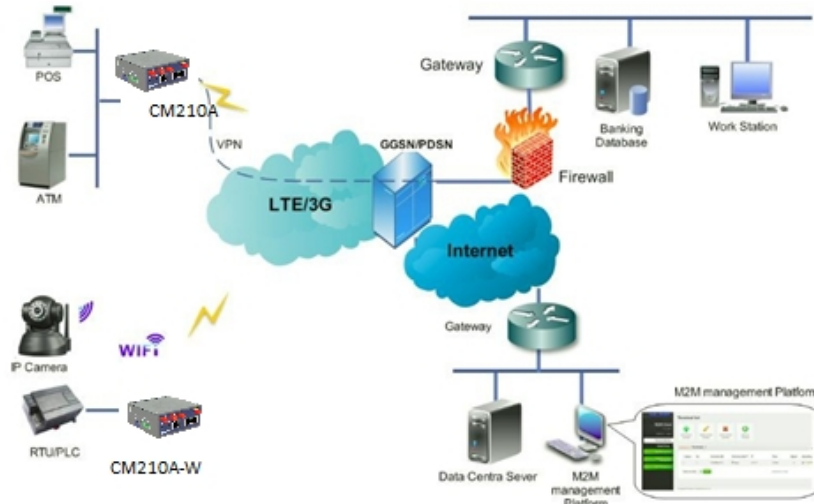


Figure 1-1 Network Topology

## 1.3 Features

The CM210Q-W supports the following:

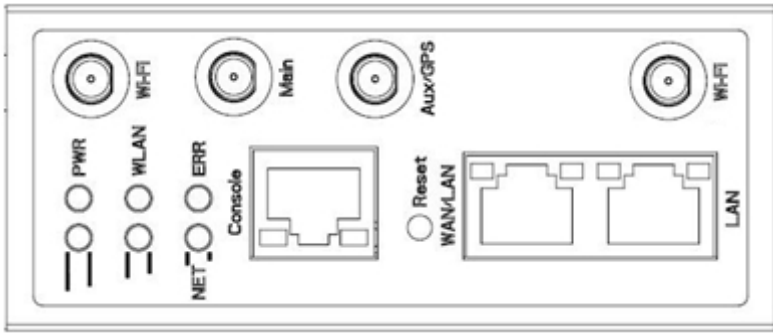
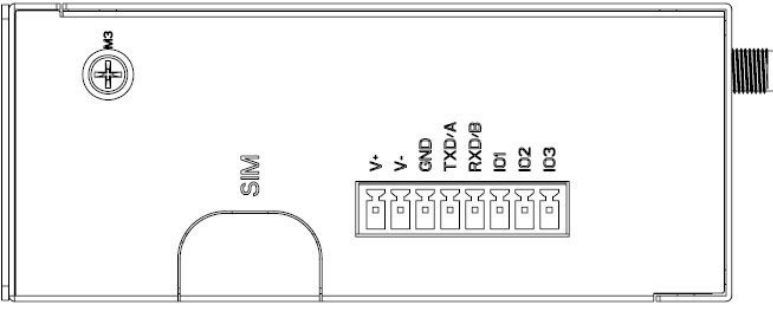
- LTE FDD B1/B2/B3/B4/B5/B7/B8/B28 and LTE TDD B40, with 3G fallback to DC-HSPA+/HSPA+/HSPA/WCDMA B1/B2/B5/B8
- IEEE802.11b/g/n N300 Wi-Fi AP function, extended support to Wi-Fi terminal, WDS bridging, WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, Authenticated encryption mode
- Virtual data and private network (APN/VPDN)
- RS-232 interface data transparent transmission and protocol conversion
- On-demand dialing, including time on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline
- Bandwidth limiter to limit Download and Upload speeds
- TCP/IP protocol stack, Telnet, HTTP, SNMP, PPP, PPPoE, network protocol
- VPN PPTP (Server and Client), L2TP, GRE, Open VPN, IPSec, HTTPs, SSH, advanced VPN function
- Configuration via a user-friendly interface using a web browser
- IPv6 protocol stack (optional)
- M2M terminal management platform (optional)
- WDT watchdog design, keep system stable

# 2 Hardware Installation

The images below might be slightly different from the actual product, but the specifications are the same.

## 2.1 Panel:

Table 2-1 CM210 Interface

COMSET	CM210
Front	
Top	



### NOTE

The Antenna interface and LED lights can be different depending on options such as extended WiFi and GPS.

Table 2-2 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, supports 1.8/3V/5V automatic detection.	
Main	3G/4G antenna, SMA connector, 50Ω.	
Aux/GPS	LTE MIMO antenna SMA connector, 50Ω.	GPS Optional
Wi-Fi	Two Wi-Fi antennas, SMA connector.	
LAN	10/100Base-TX, MDI/MDIX self-adaption.	
WAN/LAN	10/100Base-TX, MDI/MDIX self-adaption.	Default as LAN
Reset	Reset button,(press and hold for at least 5 seconds)	
PWR	Power connector.	5 ~ 32V DC
I/O	I/O-1 and I/O-2 are digital input. I/O-3 is digital output.	
Console	RJ45-DB9 cable for CLI configuration.	

## 2.2 LED Status

Table 2-3 Router LED indicator Status

silk-screen	status		Indication
Signal	Signal	Solid Light	LED1 indicates signal is weak (CSQ0~10). LED2 indicates signal is good (CSQ11~19). LED3 indicates signal is strong (CSQ20~31)
	Signal 1	Blinking	Dialing.
		Solid Light	Online.
PWR	Solid Light		System power operation.
WLAN	Solid light		WLAN enabled, but no data communication.
	Blinking quickly		Data is being transmitted.
	Dark		WLAN disabled.
ERR	Dark		System operation and LTE/3G online.
	Solid Light(Red)		System fail indicator. It indicates failure with SIM card/module.
LAN	Green	Solid light	Connected.

silk-screen	status		Indication
	Green	Blinking	
	Green	Blinking	Data in being transmitted.
	Green	Dark	Connection is lost.

**NOTE**

The LED indicators can be different depending on additional options such as extended Wi-Fi, GPS function or single/double SIM.

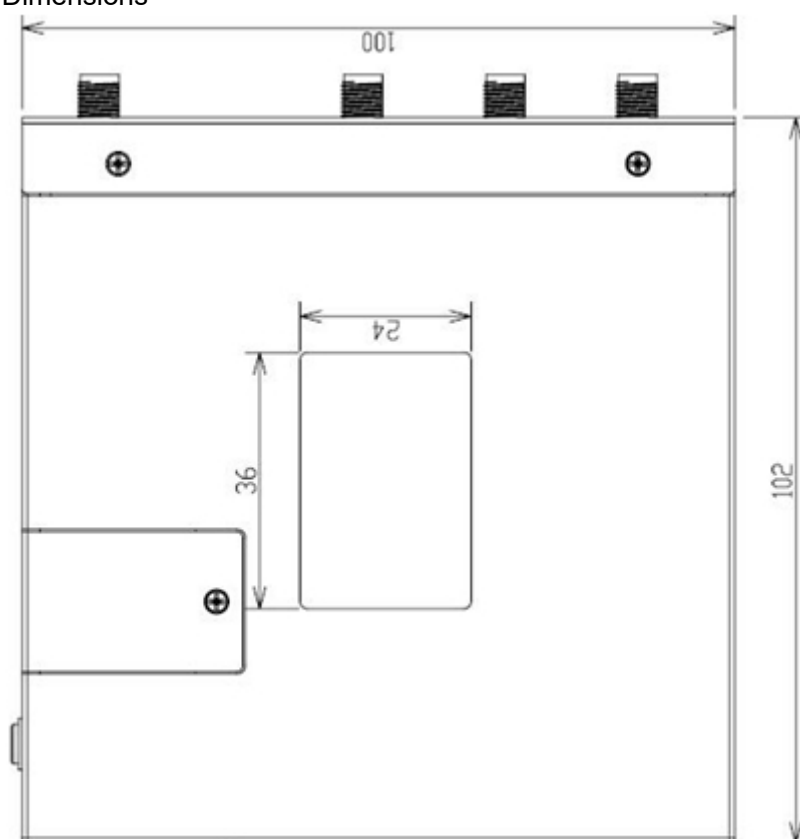
**Dimensions**

Figure 2-2 CM210 Series Router Dimensions

## 2.3 Powering up the CM210 router

### 2.3.1 SIM/UIM card installation

If you are configuring a dual-SIM router, you need to insert both SIMs prior to configuring the router.





Before connecting any cables, please disconnect the power source.

---

### 2.3.2 Ethernet Cable Connection

Use an Ethernet cable to connect the LAN port of the cellular Router to the LAN port of your PC or laptop computer.

### 2.3.3 Serial Port Connection

If you want to connect the router via a serial port to your laptop or any other device, you need to prepare a serial cable or a RJ45 cable. One end connects to the computer serial port, the other end connects to the console port of the router or the terminal block.

---



Before connecting the serial cable, please disconnect any power source.

---

### 2.3.4 Power Supply

The CM210 router supports a wide range of DC voltage between 5VDC and 32VDC.

### 2.3.5 Review

After inserting the SIM/UIM card(s) and connecting the Ethernet cable and antennas, please connect the power adaptor or the power cable.

---



Please connect the antennas prior to powering up the router, otherwise you may get a poor signal due to a mismatching impedance.

---

Notice:

- Step 1 Check the antennas' connection.
- Step 2 Check the SIM/UIM card is inserted.
- Step 3 Power up the industrial Router.

# 3 Router Configuration

The CM210Q-W can be configured via a web interface using a web browser such as Internet Explorer, Firefox or Google Chrome.

## 3.1 Configuration from a local network

To configure the CM210Q-W, please connect an Ethernet cable between the router and your PC computer. The IP address on your PC can be a static IP address, or you can select DHCP so that your computer can obtain a Dynamic IP address. The default IP address of the router is 192.168.1.1. The subnet mask is 255.255.255.0. Please follow the instructions below:

Step 1 Click “start > control panel”, find “Network Connections” icon and double click it. Select “Local Area Connection” corresponding to the network card on this page. Refer to the figure below.



Figure 3-3 Network Connection

Step 2 Select “Obtain an IP address automatically” or set up a fixed IP address in the range 192.168.1.xxx(XXX can be any number between 2 ~ 254)

Step 3 Run Internet Explorer, or any other web browser, and enter 192.168.1.1 in the address bar and press “enter”.

The username is “admin” and the password is “admin”.



Figure 3-4 User Interface

## 3.2 Basic Configuration

Below is a screenshot of the user interface of the CM210Q-W.

Status	System Status
Overview	Router Name: Comset_Router
LAN	Hardware Verion: C11-D20
Device List	Firmware Version: Router-4.2.2.3
Basic Network	Router Time: Tue, 05 Apr 2016 10:15:29 +1000 <a href="#">Clock Sync.</a>
WLAN	Uptime: 00:03:57
Advanced Network	Total / Free Memory: 60.08 MB / 47.32 MB (78.76%)
Firewall	Internet Status
VPN Tunnel	Connection Type: Cellular Network
Administration	MAC Address: 02:1E:10:1F:00:00
Debugging	Modem Type: LTE(Huawei ME90X)
Logout	Modem IMEI: 866582020035101
	Modem Status: Ready
	USIM Select: USIM 1 Running
	Cellular ISP: "Telstra"
	Cellular Network: "LTE"
	USIM Status: Ready
	CSQ: 30 ( 96% )
	IP Address: 10.96.113.200
	Subnet Mask: 255.255.255.240
	Gateway: 10.96.113.193
	DNS: 10.4.182.22:53, 10.4.81.105:53
	Connection Status: Connected
	Connection Uptime: 00:03:07

Figure 3-5 Router Status GUI

## 3.2.1 Cellular Network Configuration

Please follow the instructions below:

- Step 1 Select Basic Network> Cellular. Here you can enter the APN of your SIM card.  
If you have a dual-SIM router, you will need to enter the APN for both SIM1 and SIM2. Dual SIM mode can be “SIM 1 only”, “SIM 2 only”, “Backup” or “Failover”.

The screenshot displays the 'Cellular Settings' interface. On the left is a blue sidebar menu with options: Status, Basic Network (selected), WAN, Cellular, LAN, DDNS, Routing, WLAN, Advanced Network, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main content area is titled 'Cellular Settings' and includes the following fields:

- Cellular Network Type:** ME90X:LTE/HSPA+/WCDMA
- ICMP Check:** ☐
- Cellular Traffic Check:** ☐
- CIMI Send to:** [Empty field] : [Empty field]
- Dual Sim:** Failover (dropdown)
- Sim 1 Mode:** Auto (dropdown)
- Sim 1 PIN:** [Empty field]
- Sim 1 APN:** telstra.internet
- Sim 1 Auth:** Auto (dropdown)
- Sim 1 User:** [Empty field]
- Sim 1 Passwd:** [Empty field]
- Sim 2 Mode:** Auto (dropdown)
- Sim 2 PIN:** [Empty field]
- Sim 2 APN:** live.vodafone.com
- Sim 2 Auth:** Auto (dropdown)
- Sim 2 User:** [Empty field]
- Sim 2 Passwd:** [Empty field]

Figure 3-1 Dual SIM GUI

Table 3-1 Cellular Instructions

Item	Description
Enable	Enable SIM card dial.
ICMP check	To enable or disable “ICMP check” rules. Enable the ICMP check and setup a reachable IP address as a destination IP. When “ICMP check” fails, the router will switch SIM cards.
SIM Mode	Select the network type.
APN	APN, provided by your ISP. I.e. “telstra.internet” if using a Telstra SIM card.
Username	SIM card username is provided by your ISP. Usually leave blank.
Password	SIM card password is provided by your ISP. Usually leave blank.



**NOTE** ICMP Check and Cellular Traffic Check are different.

### 【ICMP Check】

If you enable ICMP, the router will automatically check whether the defined IP address is reachable every 60s. If the IP address is unreachable and the ICMP check fails the first time, it will check twice again at a 3s interval. If the ICMP check fails the third time, the router will implement the “fail action” as configured.

The Check IP is a public IP or a company server IP address.

ICMP Check	<input checked="" type="checkbox"/>
Check IP	8.8.8.8
Check IP (Optional)	4.4.4.4
Interval	60 (seconds)
Retries	3 (Times)
Fail Action	Reboot System ▼

### 【Cellular Traffic Check】

**【Check Mode】** there are three modes, Rx(Receive), Tx(Transmit) and Rx/Tx check modes.

**【Rx】** The router will check the 3G/LTE cellular traffic received. If no traffic is received within the defined check interval time, the router will implement the “fail action” selected, cellular reconnect or reboot.

Cellular Traffic Check	<input checked="" type="checkbox"/>
Check Mode	Rx ▼
Check Interval	10 (minutes) Range: 1 ~ 1440
Fail Action	Cellular Reconnect ▼
CIMI Send to	:

### 【SIM Mode】

**【Fail Over】** When SIM 1 fails, the router will switch to SIM 2. When SIM 2 fails, the router will switch back to SIM 1.

**【SIM1 Only】** Just SIM1 is available.

**【SIM2 Only】** Just SIM2 is available.

**【Backup】** SIM1 is the primary SIM. When SIM 1 fails, the router will switch to SIM 2 and stays on SIM 2 for a set period at the end of which it will switch back to SIM 1.

**Dual Sim** Failover

**Sim 1 Mode** Failover

**Sim 1 PIN**

**Sim 1 APN** telstra.internet

**Sim 1 Auth** Auto

**Sim 1 User**

**Sim 1 Passwd**

Step 2 To save your configuration, please click on the “save” button.

## 3.2.2 LAN Settings

Please follow the instructions below:

Step 1 Select “ Basic Network>LAN”

**LAN**

Router IP Address 1 192.168.1.1

Subnet Mask 1 255.255.255.0

Router IP Address 2 0.0.0.0

Subnet Mask 2 0.0.0.0

Router IP Address 3 0.0.0.0

Subnet Mask 3 0.0.0.0

Router IP Address 4 0.0.0.0

Subnet Mask 4 0.0.0.0

DHCP Server ☒

IP Pool 192.168.1.2 - 192.168.1.51 (50)

Lease 1440 (minutes)

Save Cancel

Figure 3-2 LAN Settings GUI

Table 3-2 LAN Settings Instructions

Item	Description
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service. When enabled, it will show the IP address range and lease option
IP Address Range	IP address range within the LAN
Lease	The valid time

Step 2 Please click “save” to save the configuration. The device will reboot.

### 3.2.3 Dynamic DNS Settings

Please follow the instructions below:

Step 1 Select “Basic Network>DDNS” to enter the DDNS settings page.

Figure 3-3 Dynamic DNS Settings

Table 3-3 DDNS Settings Instructions

Item	Description
IP address	The default is standard DDNS protocol. For a customised protocol, please contact Comset. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval for the DDNS client to obtain a new IP. We suggest 240s or above
Service provider	Select the DDNS service provider from the list.

Step 2 Please Click “Save” to finish.

## 3.2.4 Routing Settings

Please follow the instructions below:

Step 1 Select “Basic Network>Routing”.

**Current Routing Table**

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
120.157.94.45	*	255.255.255.255	0	usb0 (WAN)
120.157.94.44	*	255.255.255.252	0	usb0 (WAN)
192.168.1.0	*	255.255.255.0	0	br0 (LAN)
127.0.0.0	*	255.0.0.0	0	lo
default	120.157.94.45	0.0.0.0	0	usb0 (WAN)

**Static Routing Table**

Destination	Gateway	Subnet Mask	Metric	Interface	Description
192.168.8.0	192.168.9.201	255.255.255.0	0	VPN	

**Miscellaneous**

Mode: Gateway

RIPv1 & v2: Disabled

Efficient Multicast Forwarding: ☐

DHCP Routes: ☒

Spanning-Tree Protocol: ☐

Save Cancel

Figure 3-4 Routing Settings

Table 3-4 Routing Settings Instructions

Item	Description
Destination	Destination IP address.
Gateway	Next hop IP address which the router will reach.
Subnet Mask	Subnet mask for destination IP address.
Metric	Metrics are used to determine whether one particular route should be chosen over another.
Interface	Interface from router to gateway.
Description	Describes the routing function.

Step 2 Please Click “Save” to finish.



## 3.3 WLAN Settings

### 3.3.1 Basic Settings

Please follow the instructions below:

Step 1 Select “WLAN>Basic Settings”

The screenshot displays the 'Wireless (2.4 GHz / eth1)' configuration page. On the left, a blue sidebar menu lists various system functions, with 'WLAN' and its sub-item 'Basic Settings' highlighted. The main content area shows the following settings:

- Enable WLAN:** A checked checkbox.
- MAC Address:** A text field showing '34:4B:3D:35:BA:E8'.
- Wireless Mode:** A dropdown menu set to 'Access Point'.
- Wireless Network Mode:** A dropdown menu set to 'Auto'.
- SSID:** A text field containing 'Comset-WiFi'.
- Broadcast SSID:** A checked checkbox.
- Channel:** A dropdown menu set to '7 - 2.442 GHz', accompanied by a 'Scan' button.
- Security option:** A dropdown menu set to 'Disabled'.

At the bottom right of the main panel, there are 'Save' and 'Cancel' buttons.

Figure 3-5 WLAN Basic Settings GUI

Table 3-5 Basic Settings Instruction

Item	Description
Enable wireless	Enable or Disable WiFi
Wireless mode	Supports AP, AP+WDS, Bridge, Client, WDS
Wireless Network protocol	Supports Auto, IEEE 11b/g/n selectable
SSID	The default is router, but this can be changed.
Channel	The channel of wireless network. We suggest to keep the default.
Channel Width	20MHZ and 40MHZ alternative
Security	Supports various encryption methods

Step 2 Please click “Save” to finish.

### 3.3.2 Wireless Filter Settings

Please follow the instructions below:

Step 1 Select “WLAN > Wireless Filter”.

The screenshot shows the 'Wireless Client Filter' settings page. On the left is a navigation menu with options: Status, Basic Network, WLAN (selected), Basic Settings, MultiSSID, Wireless Filter, Advanced Wireless, Wireless Survey, Advanced Network, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main content area is titled 'Wireless Client Filter' and includes three radio button options: 'Disable filter' (which is selected), 'Permit only the following clients', and 'Block the following clients'. Below these options is a table with two columns: 'MAC Address' and 'Description'. The first row of the table contains the MAC address '00:00:00:00:00:00'. To the right of the table is an 'Add' button. At the bottom right of the page are 'Save' and 'Cancel' buttons.

Figure 3-6 Wireless Client Filter Settings GUI

The Wireless Filter allows you to permit only some clients and /or prohibit others from connecting to the WiFi network. This feature is invalid on a wired connection.

Table 3-6 "Wireless Client Filter" Settings Instructions

Item	Description
Disable Filter	Choose to disable.
Permit only the following clients	Allows only the listed MAC addresses to connect to the router via WiFi.
Block the following clients	Prevents the listed MAC addresses from connecting to the router via WiFi.

Step 2 Please click “save” to finish.

### 3.3.3 Wireless Survey

Please follow the instructions below:

Step 1 Select “WLAN> Wireless Survey” to check survey.

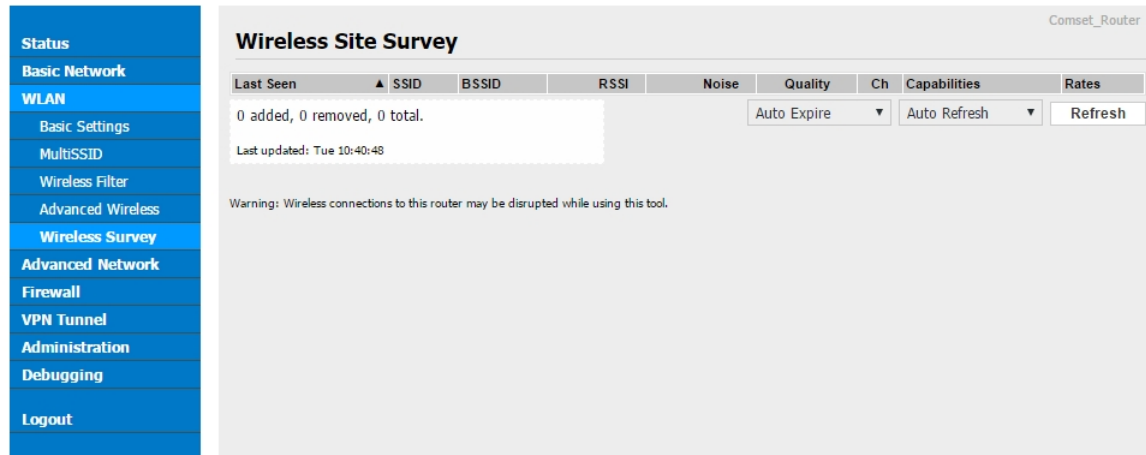


Figure 3-7 Wireless Survey Settings GUI

## 3.4 Advanced Network Settings

### 3.4.1 Port Forwarding

Please follow the instructions below:

Step 1 Select “Advanced Network > Port Forwarding”

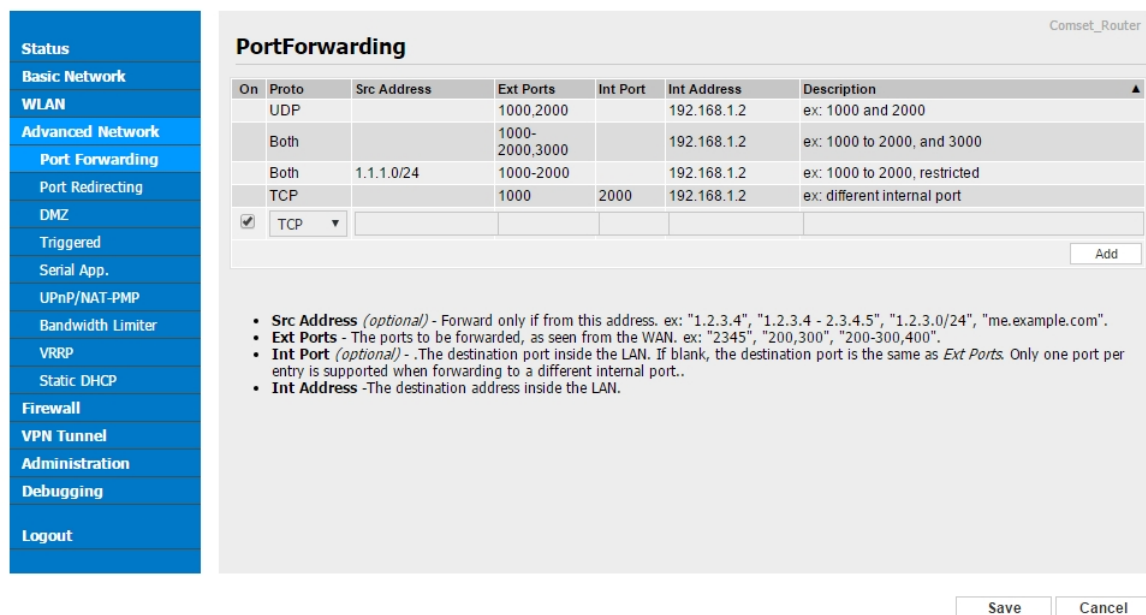


Figure 3-8 Port Forwarding GUI

Table 3-7 “Port Forwarding” Instructions

Item	Description
Protocol	Supports UDP, TCP, both UDP and TCP.
Src. Address	Source IP address. Forwards only if from this IP address.
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one port per entry is supported when forwarding to a different internal port.
Int. Address	Internal Address. The destination address inside the LAN.
Description	Rule brief description.

Step 2 Please click “save” to finish.

## 3.4.2 DMZ Settings

Please follow the instructions below:

Step 1 Select “Advanced Network> DMZ” to check or modify the relevant parameters.

Figure 3-9 DMZ GUI

Table 3-8 “DMZ” Instructions

Item	Description
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address is entered, it will allow access to all IP addresses. If defined IP addresses are entered, it will just allow access to the defined IP addresses.
Leave Remote Access	

Step 2 Please click “save” to finish

### 3.4.3 Triggered Port Forwarding Settings

Please follow the instructions below:

Step 1 Select “Advanced Network> Triggered” to check or modify the relevant parameters.

**Triggered Port Forwarding**

On	Protocol	Trigger Ports	Forwarded Ports	Description
<input checked="" type="checkbox"/>	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000

- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

Figure 3-10 Triggered GUI

Table 3-9 “Triggered” Instructions

Item	Description
Protocol	Supports UDP, TCP, both UDP and TCP.
Triggered Ports	Triggered Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

Step 2 Please click “save” to finish.

### 3.4.4 Firewall Settings

Please follow the instructions below:

Step 1 Select “Firewall>IP/URL Filtering” to check or modify the relevant parameter.

**IP/MAC/Port Filtering**

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NONE			Acc	

**Key Word Filtering**

On	Key Word	Description
<input checked="" type="checkbox"/>		

**URL Filtering**

On	URL	Description
<input checked="" type="checkbox"/>		

Save Cancel

Step 2 Select “Firewall>Domain Filtering” to check or modify the relevant parameter.

**Domain Filtering**

On ☐

Default Policy White List

On	Domain	Description
<input checked="" type="checkbox"/>		

Add

Save Cancel

Figure 3-11 Domain Filtering Settings GUI

Table 3-10 “Domain Filtering” Instructions

Item	Description
Applies To	White list.
Blocked Resources	Black list.

Step 2 Please click “save” to finish.

### 3.4.5 Serial App. Settings

Please follow the instructions below:

Step 1 Select “Advanced Network> Serial App” to check or modify the relevant parameters.

The screenshot displays the 'Serial to TCP/IP' configuration page. On the left, a blue sidebar lists navigation options: Status, Basic Network, WLAN, Advanced Network (selected), Port Forwarding, Port Redirecting, DMZ, Triggered, Serial App. (highlighted), UPnP/NAT-PMP, Bandwidth Limiter, VRRP, Static DHCP, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main configuration area has a title bar 'Serial to TCP/IP' and a 'Comset\_Router' label. It includes the following settings:

- Serial to TCP/IP Mode:** Client (dropdown)
- Server IP/Port:** 8.8.8.8 : 40002
- Socket Type:** TCP (dropdown)
- Socket Timeout:** 500 (milliseconds)
- Serial Timeout:** 500 (milliseconds)
- Paket Payload:** 1024 (bytes)
- Heart-Beat Content:** (empty text field)
- Heart-Beat Interval:** 2 (seconds)
- Baud Rate:** 115200 (dropdown)
- Parity Bit:** none (dropdown)
- Data Bit:** 8 (dropdown)
- Stop Bit:** 1 (dropdown)

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 3-12 Serial App Settings GUI

Table 3-11 “Serial App” Instructions

Item	Description
Serial to TC/IP mode	Supports Disable, Server and Client modes.
Server IP/Port	IP address and domain name are acceptable for Server IP.
Socket Type	Supports TCP/UDP protocol.
Socket Timeout	The router will wait for the set time to transmit data to the serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals the Packet payload, the serial port will transmit it immediately. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Sends heart beat to the defined server to keep the router online. It is handy to monitor the router from the server.
Heart beat Interval	Heart beat interval time.
Baud Rate	112100 as default.
Parity Bit	None as default.

Data Bit	8bit as default.
Stop Bit	1bit as default.

Step 2 Please click “save” to finish.

### 3.4.6 UPnp/NAT-PMP Settings

Please follow the instructions below:

Step 1 Please go to “Advanced Network> Upnp/NAT-PMP” to check or modify the relevant parameters.

**Forwarded Ports**

Ext Ports	Int Port	Internal Address	Protocol	Description
50310	50310	192.168.1.17	UDP	NAT-PMP 50310 udp
50310	50310	192.168.1.17	TCP	NAT-PMP 50310 tcp

[Delete All](#) [Refresh](#)

**Settings**

Enable UPnP ☒

Enable NAT-PMP ☒

Inactive Rules Cleaning ☒

Cleaning Interval  seconds

Cleaning Threshold  redirections

Secure Mode ☒ when enabled, UPnP clients are allowed to add mappings only to their IP)

Show In My Network Places ☐

[Save](#) [Cancel](#)

Figure 3-13 UPnp/NAT-PMP Settings GUI

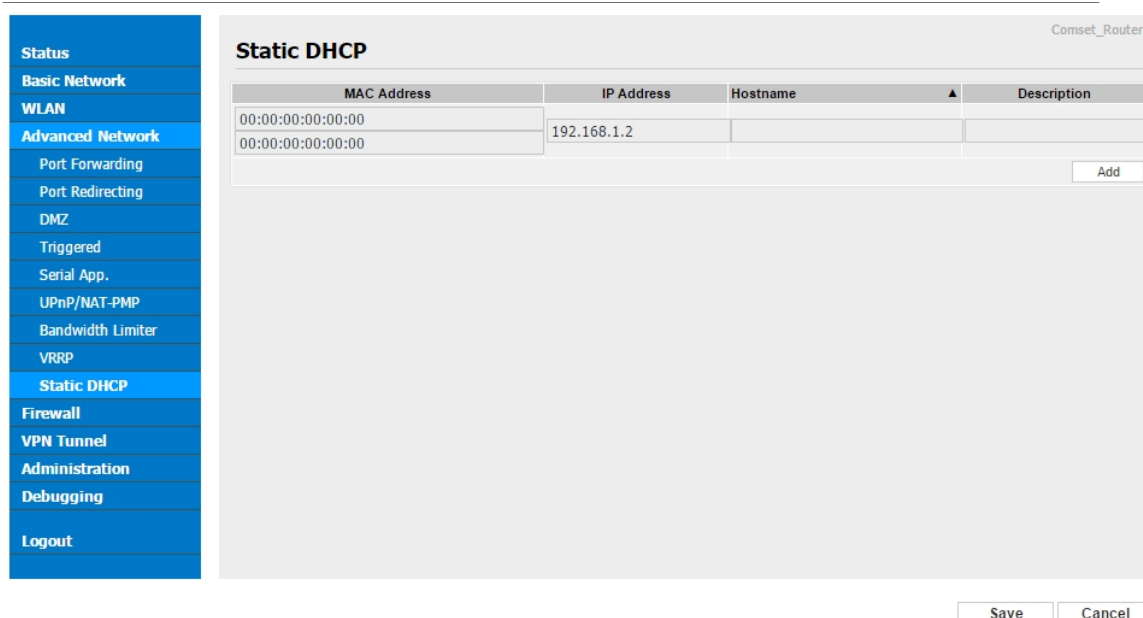
Step 2 Click “save” to finish.

### 3.4.7 Static DHCP Settings

Please follow the instructions below:

Step 1 Select “Advanced Network> Static DHCP” to check or modify the relevant parameters.





The Static DHCP Settings GUI shows a table with columns: MAC Address, IP Address, Hostname, and Description. The first row has MAC Address 00:00:00:00:00:00 and IP Address 192.168.1.2. There is an 'Add' button at the bottom right of the table. The left sidebar contains a menu with 'Static DHCP' highlighted. At the bottom right, there are 'Save' and 'Cancel' buttons.

MAC Address	IP Address	Hostname	Description
00:00:00:00:00:00	192.168.1.2		
00:00:00:00:00:00			

Save Cancel

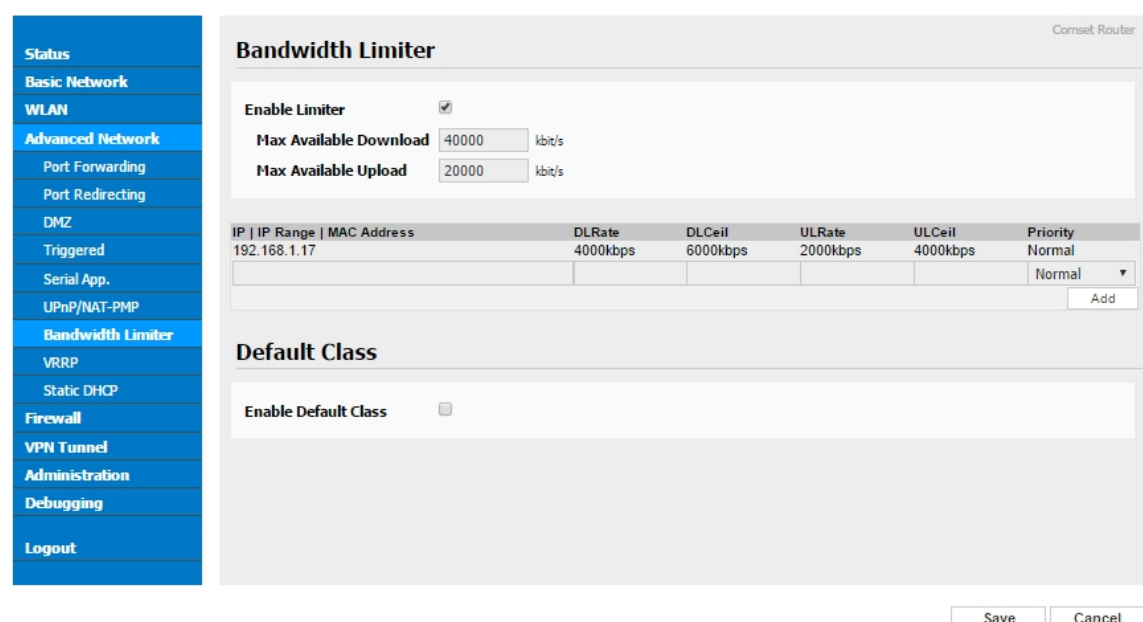
Figure 3-14 Static DHCP Settings GUI

Step 2 Click “save” to finish.

### 3.4.8 Bandwidth Limiter

Please follow the instructions below:

Step 1 Select “Advanced Network> Bandwidth Limiter” to check or modify the relevant parameters.



The Bandwidth Limiter Settings GUI shows the 'Enable Limiter' checkbox checked. Below it are input fields for 'Max Available Download' (40000 kbit/s) and 'Max Available Upload' (20000 kbit/s). A table lists bandwidth limits for IP 192.168.1.17 with columns: IP | IP Range | MAC Address, DLRate, DLCeil, ULRate, ULCeil, and Priority. The priority is set to Normal. There is an 'Add' button at the bottom right of the table. The 'Default Class' section has an 'Enable Default Class' checkbox which is unchecked. The left sidebar contains a menu with 'Bandwidth Limiter' highlighted. At the bottom right, there are 'Save' and 'Cancel' buttons.

IP   IP Range	MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority
192.168.1.17		4000kbps	6000kbps	2000kbps	4000kbps	Normal

Default Class

Enable Default Class

Save Cancel

Step 2 Click “save” to finish.

## 3.5 VPN Tunnel

### 3.5.1 GRE Settings

Please follow the instructions below:

Step 1 Select “VPN Tunnel> GRE” to check or modify the relevant parameters.

The screenshot shows the 'GRE Tunnel' and 'GRE Route' configuration pages. The 'GRE Tunnel' table has one row with 'On' checked, 'Idx' empty, and other fields empty. The 'GRE Route' table has one row with 'On' checked, 'Tunnel Index' set to 1, and other fields empty. The 'Save' and 'Cancel' buttons are at the bottom right.

Figure 3-15 GRE Settings GUI

Table 3-12 “GRE” Instructions

Item	Description
Idx	GRE tunnel number.
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router’s 3G/4G WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually a public IP address.
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.
Description	

Step 2 Click “save” to finish.

### 3.5.2 VPN Client Settings

Please follow the instructions below:

Step 1 Click “VPN Tunnel> VPN Client” to check or modify the relevant parameters.

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

VPN Client

IPSec

Administration

Debugging

Logout

Comset\_Router

### PPTP/L2TP Client

Enable VPN☐

VPN Mode

PPTP Client ▾

Server Address

124.104.36.211

Username:

a

Password:

•

Encryption

Auto ▾

Stateless MPPE connection☐

Accept DNS configuration

Disabled ▾

Redirect Internet traffic☐

Remote subnet / netmask

192.168.0.0

 / 

255.255.255.0

 -> As Firewall Rule ☒

Create NAT on tunnel☐

MTU

Default ▾

1450

MRU

Default ▾

1450

Local IP Address

192.168.100.1

Hostname:

Comset-Router

Custom Configuration

www.comset.com.au

29

Downloaded from [Arrow.com](http://Arrow.com)

Table 3-13 “VPN Client” Instructions

Item	Description
VPN Mode	VPN Mode for PPTP and L2TP.
Server Address	VPN Server IP address.
User name	As per user’s configuration.
Password	As per user’s configuration.
Encryption	As per user’s configuration.
Stateless MPPE	As per user’s configuration.
Accept DNS	As per user’s configuration.
Remote Subnet	As per user’s configuration.
Create NAT on Tunnel	As per user’s configuration.

Step 2 Click “save” to finish.

### 3.5.3 VPN Server Settings

Please follow the instructions below:

Step 1 Click “VPN Tunnel> VPN Server” to check or modify the relevant parameters.

**PPTP Server Configuration** [\(Click here to hide\)](#)

Enable ☒

Local IP Address/Netmask 192.168.1.1 / 255.255.255.0

Remote IP Address Range 172.19.0.1 - 172.19.0.6 (6)

Broadcast Relay Mode Disabled

Encryption MPPE-128

DNS Servers 0.0.0.0

WINS Servers 0.0.0.0

MTU 1450

MRU 1450

[Poptop](#)  
Custom configuration

**PPTP User List** [\(Click here to hide\)](#)

Username	Password

Add

Step 2 Click “save” to finish.

### 3.5.4 IPSec Settings

#### 3.5.4.1 IPsec Group Setup

Step 1 Select “IPsec> Group Setup” to check or modify the relevant parameters.

Table 3-14 “IPsec Group Setup” Instructions

Item	Description
IPsec Extensions	Supports Standard IPsec, GRE over IPsec, L2TP over IPsec.
Local Security Interface	Defines the IPsec security interface.

Local Subnet/Mask	IPSec local subnet and mask.
-------------------	------------------------------

Item	Description
Local Firewall	Forwarding-firewalling for Local subnet.
Remote IP/Domain	IPSec peer IP address/domain name.
Remote Subnet/Mask	IPSec remote subnet and mask.
Remote Firewall	Forwarding-firewalling for Remote subnet.

Step 2 Click “save” to finish.

### 3.5.4.2 IPSec Basic Setup

Step 1 Select “IPSec >Basic Setup” to check or modify the relevant parameters.

The screenshot displays the 'IPSEC' configuration interface for 'IPSEC 1'. The 'Basic Setup' tab is active, showing various parameters for Phase 1 and Phase 2 of the IKE process. The 'Keying Mode' is set to 'IKE with Preshared Key'. Both Phase 1 and Phase 2 are configured with 'Group 2 - modp1024' for the DH Group, '3DES (168-bit)' for Encryption, and 'MD5 HMAC (96-bit)' for Authentication. Phase 1 has a SA Life Time of 28800 seconds, while Phase 2 has a SA Life Time of 3600 seconds. A Preshared Key field is present at the bottom, currently showing masked characters. The left sidebar contains a menu with options like Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, GRE, OpenVPN Client, VPN Client, IPSec, Administration, Debugging, and Logout. The bottom right corner features 'Save' and 'Cancel' buttons.

Table 3-15 “IPSec Basic Setup” Instructions

Item	Description
Keying Mode	IKE pre-shared key.
Phase 1 DH Group	Select Group1, Group2, Group5 from the list. It must match the remote IPSec settings.
Phase 1 Encryption	Supports 3DES, AES-128, AES-192, AES-256.
Phase 1 Authentication	Supports HASH MD5 and SHA.
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime.

Item	Description
Phase 2 DH Group	Select Group1, Group2, Group5 from the list. It must match the remote IPsec settings.
Phase 2 Encryption	Supports 3DES, AES-128, AES-192, AES-256.
Phase 2 Authentication	Supports HASH MD5 and SHA.
Phase 2 SA Life Time	IPsec Phase 2 SA lifetime.
Pre-shared Key	Pre-shared Key.

Step 2 Click “save” to finish.

### 3.5.4.3 IPsec Advanced Setup

Step 1 Select “IPsec >Advanced Setup” to check or modify the relevant parameters.

Table 3-16 “ IPsec Advanced Setup” Instructions

Item	Description
Aggressive Mode	Default for main mode.
ID Payload Compress	Enable ID Payload compress.
DPD	To enable DPD service.
ICMP	ICMP Check for IPsec tunnel.
IPsec Custom	IPsec advanced settings such as left/right ID.



Item	Description
Options	

Step 2 Click “save” to finish.

## 3.6 Administration

### 3.6.1 Identification Settings

Please follow the instructions below:

Step 1 Select “Administrator> Identification” to enter the GUI, you may modify the Router name, Host name and Domain name as required.

The screenshot shows the 'Router Identification' configuration page. On the left is a blue sidebar menu with options: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, Administration (highlighted), Identification (selected), Time, Admin Access, Scheduler Reboot, SNMP, M2M Settings, DI/DO Setting, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The main content area has a title bar 'Router Identification' with 'Comset\_Router' on the right. Below the title bar are three text input fields: 'Router Name' with 'Comset\_Router', 'Hostname' with 'Comset-Router', and 'Domain Name' with 'vpn1'. At the bottom right of the main area are two buttons: 'Save' and 'Cancel'.

Figure 3-16 Router Identification GUI

Table 3-17 “Router Identification” Instructions

Item	Description
Router name	Default is router. Can be changed. Maximum 32 characters
Host name	Default is router. Can be changed. Maximum 32 characters
Domain name	Default is blank. Can be changed. Maximum 32 characters. This is the WAN domain. No need to configure in most applications.

Step 2 Click “save” to finish

## 3.6.2 Time Settings

Step 1 Select “Administrator> time” to check or modify the relevant parameters.

The screenshot shows the 'Time' configuration page of a Comset Router. On the left is a blue sidebar menu with the following items: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, Administration (highlighted), Identification, Time (highlighted), Admin Access, Scheduler Reboot, SNMP, M2M Settings, DI/DO Setting, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The main content area is titled 'Time' and contains the following settings:

- Router Time:** Tue, 05 Apr 2016 11:10:42 +1000. A 'Clock Sync.' button is next to it.
- Time Zone:** A dropdown menu showing 'UTC+10:00 Australia'.
- Auto Daylight Savings Time:** A checkbox that is checked.
- Auto Update Time:** A dropdown menu showing 'Every 1 Hour'.
- Trigger Connect On Demand:** A checkbox that is unchecked.
- NTP Time Server:** A dropdown menu showing 'Default'. Below it, the text '0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org' is displayed.

At the bottom right of the main content area, there are two buttons: 'Save' and 'Cancel'.

Figure 3-17 System Configurations GUI



If the time update fails, please try a different NTP Time Server.

Step 2 Click “save” to finish.

### 3.6.3 Admin Access Settings

Please follow the instructions below:

Step 1 Select “Administrator>Admin” to check and modify relevant parameters.

In this page, you can configure the basic web parameters. Please note the password is “password”.

The screenshot displays the 'WebAccess' configuration page of a Comset Router. On the left, a blue sidebar menu lists various system functions, with 'Admin Access' currently selected. The main configuration area is divided into several sections. The 'WebAccess' section includes 'Local Access' set to HTTP on port 80, 'Remote Access' set to HTTP on port 8080, 'Allow Wireless Access' checked, and 'Keepalive' unchecked. Below this is an 'Open Menus' section with checkboxes for Status, Basic Network, WLAN, Firewall, VPN Tunnel, Advanced Network, Administration, and Debugging. The bottom section, titled 'Password', contains two input fields for entering and confirming the password, both currently showing masked characters (dots).

Figure 3-18 Admin Settings GUI

Step 2 Click “save” to finish.

### 3.6.4 Schedule Reboot Settings

Please follow the instructions below:

Step 1 Select “Administrator>Schedule Reboot” to check and modify relevant parameters.

The screenshot displays the 'Scheduler Reboot' configuration page. On the left, a blue sidebar menu lists various system settings, with 'Scheduler Reboot' currently selected. The main content area, titled 'Scheduler Reboot', shows the following configuration: 'Enabled' is checked; 'Time' is set to 2:30 PM; and 'Days' are configured with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Everyday, all of which are checked. At the bottom right of the page, there are 'Save' and 'Cancel' buttons.

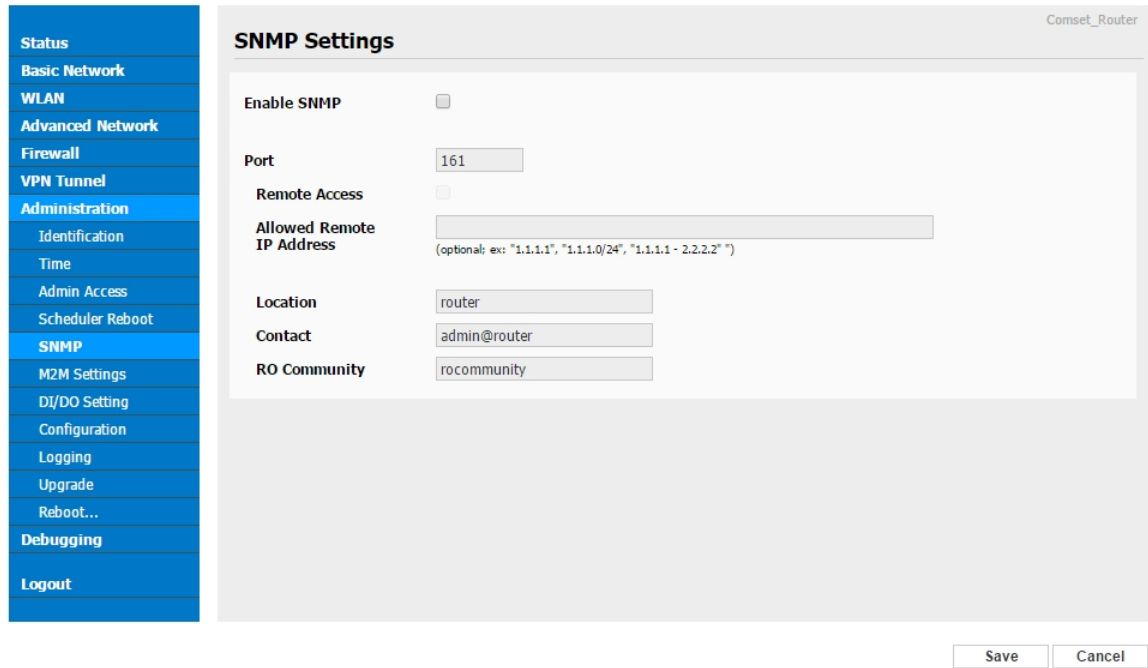
Figure 3-19 Schedule Reboot Settings GUI

Step 2 Click “Save” to finish.

### 3.6.5 SNMP Settings

Please follow the instructions below:

Step 1 Select “Administrator>SNMP” to check and modify relevant parameters.



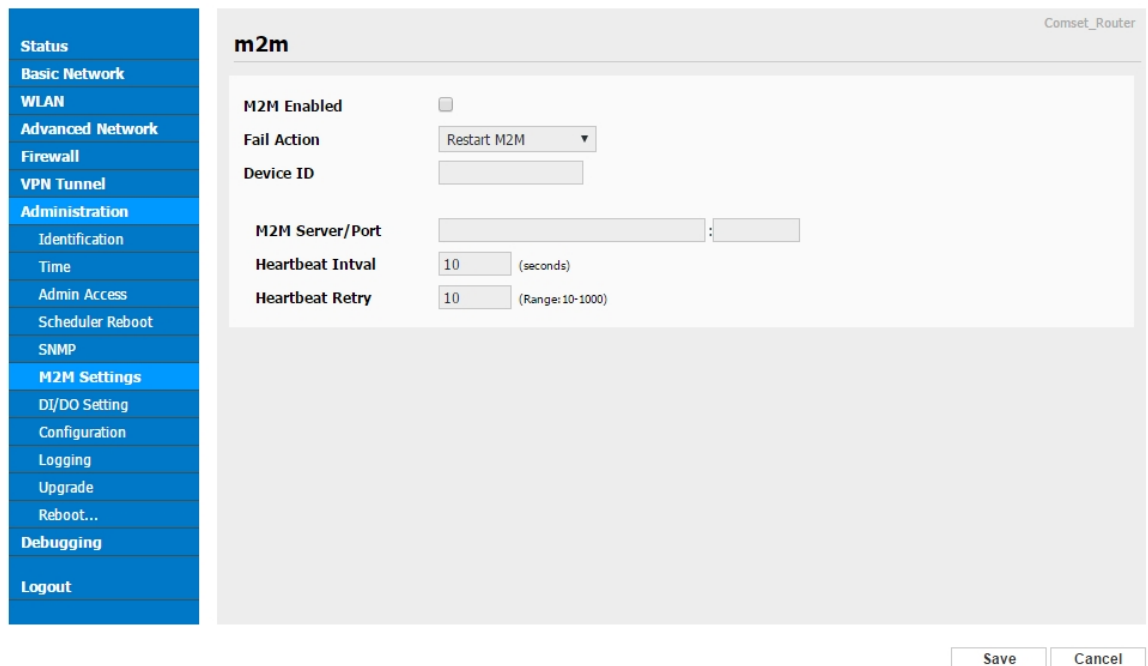
The image shows the 'SNMP Settings' configuration page in the Comset\_Router GUI. On the left is a blue sidebar menu with options: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, Administration (highlighted), Identification, Time, Admin Access, Scheduler Reboot, SNMP, M2M Settings, DI/DO Setting, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The main panel is titled 'SNMP Settings' and contains the following fields: 'Enable SNMP' (checkbox, unchecked), 'Port' (text box with '161'), 'Remote Access' (checkbox, unchecked), 'Allowed Remote IP Address' (text box with a placeholder and a note: '(optional: ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" )'), 'Location' (text box with 'router'), 'Contact' (text box with 'admin@router'), and 'RO Community' (text box with 'rocommunity'). At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-20 SNMP Settings GUI

Step 2 Click “Save” to finish.

### 3.6.6 M2M Access Settings

Step 1 Select “Administrator>M2M Access” to check and modify relevant parameters.



The image shows the 'm2m' configuration page in the Comset\_Router GUI. The left sidebar menu is the same as in Figure 3-20, with 'M2M Settings' highlighted. The main panel is titled 'm2m' and contains the following fields: 'M2M Enabled' (checkbox, unchecked), 'Fail Action' (dropdown menu showing 'Restart M2M'), 'Device ID' (text box), 'M2M Server/Port' (text box with a colon separator), 'Heartbeat Intval' (text box with '10' and '(seconds)' next to it), and 'Heartbeat Retry' (text box with '10' and '(Range: 10-1000)' next to it). At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-21 M2M Access Settings GUI

Step 2 Click “Save” to finish.

### 3.6.7 DI/DO Settings

Step 1 Select “Administrator>DI/DO Settings” to check and modify relevant parameters.

**DI Setting**

Enabled ☐ Port1 ☐ Port2 ☐

**DO Setting**

Enabled ☐

Alarm Source DI Control ☐ SMS Control ☐

Alarm Action

Power On Status

Keep On  (\*100ms)

Figure 3-22 DI/DO Settings GUI

#### 3.6.7.1 DI Configuration

**DI Configure**

Enable Port 1 ☒ Port 2 ☐

Port 1 Mode

Filtering  (\*100ms)

Counter Trigger

Counter Period  (\*100ms)

Counter Recover  (\*100ms)

Counter Active

Counter Start

SMS Alarm ☒

SMS Content  70 ASCII Char Max

SMS receiver num1

SMS receiver num2  backup receiver

Table 3-18 "DI" Instructions

Item	Description
Enable	Enable DI. Port1 is for I/O-1 and Port2 is for I/O-2. Both I/O-1 and I/O-2 are DI ports.
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: When I/O connects to "GND", the alarm is triggered. ON Mode: When I/O does not connect to "GND", the alarm is triggered. EVENT_COUNTER Mode: Enter EVENT_COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under ON and OFF modes, the CM210 detects the pulse signals and compares with first pulse shap and last pulse shape. If both are the same level, the CM210 will trigger alarm. Under EVENT_COUNTER mode, if the first pulse shape and the last pulse shape are not at the same level, the CM210 will trigger an alarm according to the Counter Action settings.
Counter Trigger	Available when the DI is under Event Counter mode input from 0 to 100. "0" means the alarm is not triggered. The alarm will be triggered when the counter reaches the set value. After the alarm is triggered, the DI will keep counting but will not trigger the alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check fails, GRE will get re-established.
Counter Recover	It will re-count after a counter trigger alarm. The value is 0~30000(*100ms). "0" means no counter.
	HI_TO_LO and LO_TO_HI is available when the DI is under Event Counter mode.
Counter Start	Available when the DI is under EVENT_COUNTER mode. The counting starts when you enable this feature.
SMS Alarm	The alarm SMS will send a text to a specified phone group. Each phone group contains up to 2 phones.
SMS Content	70 ASCII Char Max.
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Click “save” to finish.

### 3.6.7.1 DO Configuration

#### DO Configure

**Enable** ☐

**Alarm Source** DI Alarm ☒ SMS Control ☒ M2M Control ☐

**Alarm Action** Pulse

**Power On Status** ON

**Delay** 0  (\*100ms)

**Low** 10  (\*100ms)

**High** 10  (\*100ms)

**Output** 1

**SMS Trigger Content**  70 ASCII Char Max

**SMS Replay Content**  70 ASCII Char Max

**SMS Manager Num1**

**SMS Manager Num2**  backup receiver

Table 3-19 “DO” Instructions

Item	Description
Enable	DO is enabled.
Alarm Source	<p>Digital Output activates according to different alarm sources. You can select between DI Alarm, SMS Control and M2M Control. You can select one or more alarm sources.</p> <p>DI Alarm: The Digital Output gets triggered when there is an alarm from a Digital Input.</p> <p>SMS Control: The Digital Output gets triggered when receiving an SMS from a number in the phone book.</p> <p>M2M Control: Under development.</p>
Alarm Action	<p>The Digital Output initiates an alarm action. Select from “OFF”, “ON” and “Pulse”.</p> <p>OFF: Open from GND when triggered.</p> <p>ON: Short contact with GND when triggered.</p> <p>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.</p>



Power on Status	Specify the Digital Output status when the power is on. Select from "OFF" and "ON". OFF: Open from GND. ON: Short contact with GND.
Keep On	Available when the DO "Alarm On Action"/ "Alarm Off Action" status is ON. Input the DO "Keep On" status time. Input from 0 to 255 seconds. "0" means ON until the next action.
Delay	Available when you enable "Pulse" in "Alarm On Action"/ "Alarm Off Action". The first pulse will be generated after a "Delay" . Input from 0 to 30000ms. (0=generate pulse without delay)
Low	Available if Pulse is enabled in "Alarm On Action"/ "Alarm Off Action".
High	Available if Pulse is enabled in "Alarm On Action"/ "Alarm Off Action". In "Pulse Output" mode, the selected Digital Output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.
Output	Available if Pulse is enabled in "Alarm On Action"/ "Alarm Off Action". The number of pulses, input from 0 to 30000. (0 for continuous pulse output)
SMS Trigger Content	Available when you enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm On Action" by SMS (70 ASCII II char max).
SMS Reply Content	Input the SMS content, which will be sent after DO was triggered. (70 ASCII II char max).
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Click "save" to finish.

### 3.6.8 Configuration Settings

Step 1 Select “Administrator> Configuration” to configure the backup settings.

The screenshot displays the 'Backup Configuration' page in the router's web interface. On the left is a blue sidebar menu with options: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, Administration (highlighted), Identification, Time, Admin Access, Scheduler Reboot, SNMP, M2M Settings, DI/DO Setting, Configuration (highlighted), Logging, Upgrade, Reboot..., Debugging, and Logout. The main content area is titled 'Backup Configuration' and includes the following sections:

- Backup Configuration:** A text input field contains 'Router\_Router-4223\_m152150', followed by a '.cfg' label and a 'Backup' button. A 'Link' text is below the input field.
- Save As Default Configuration:** A 'Save' button.
- Restore Configuration:** A section with the text 'Select the configuration file to restore:'. It contains a 'Choose File' button, the text 'No file chosen', and a 'Restore' button.
- Restore Default Configuration:** A section with a 'Select...' dropdown menu and a 'Save' button.

At the bottom of the main content area, a status bar shows: 'Total / Free NVRAM: 32.00 kB / 9352 (28.54%)'.

Figure 3-23 Backup and Restore Configuration GUI



**CAUTION**

“Restore Default” would lose all configuration information, please be careful.

Step 2 After setting the backup and restore configuration, the system will reboot automatically.

### 3.6.9 System Log Settings

Step 1 Select “Administrator> Logging” to start the configuration. You can set the file path to save the log (Local or remote sever).

**Syslog** Comset\_Router

Log Internally ☒

Log To Remote System ☒

Host or IP Address / Port  :

Generate Marker

Limit  (messages per minute / 0 for unlimited)

Figure 3-24 System log Settings GUI

Step 2 Click “Save” to finish.

## 3.6.10 Firmware upgrade

Step 1 Select “Administrator>firmware upgrade” to open the upgrade firmware tab.

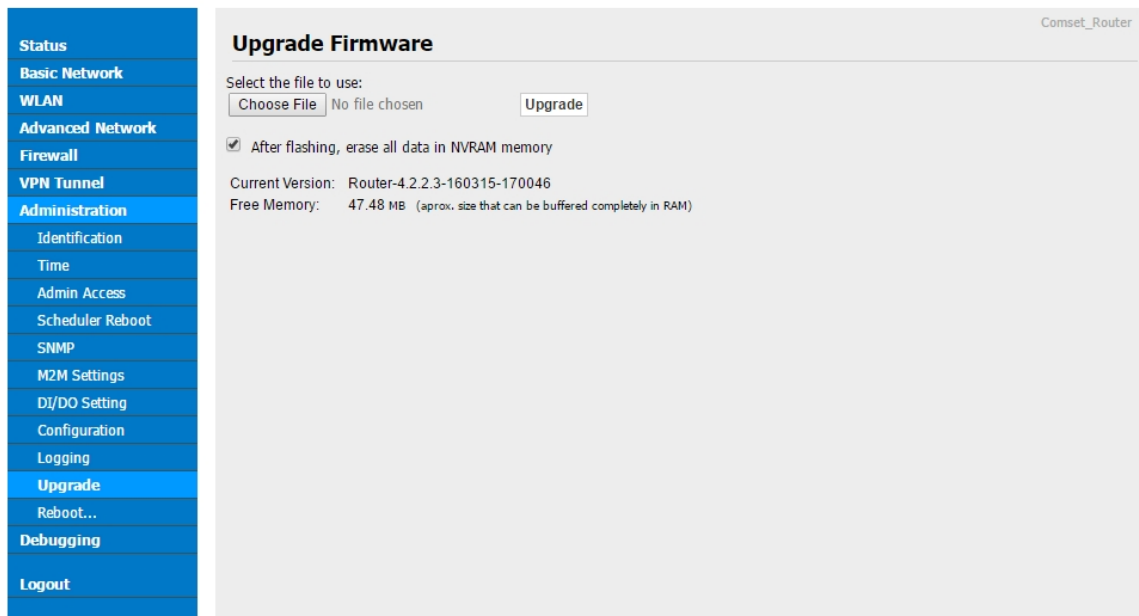


Figure 3-25 Firmware Upgrade GUI



### NOTE

Please do not disconnect the power when upgrading.

## 3.6.11 System Reboot

Step 1 Select “Administrator>Reboot” to restart the router. A pop-up window will prompt you to confirm “YES” or “NO” before the next step.

Step 2 If you choose “YES”, the system will restart. All configuration updates will be effective after the reboot.

## 3.7 Debugging Settings

### 3.7.1 Logs Settings

Step 1 Select “Debugging>Logs” to check and modify relevant parameters.

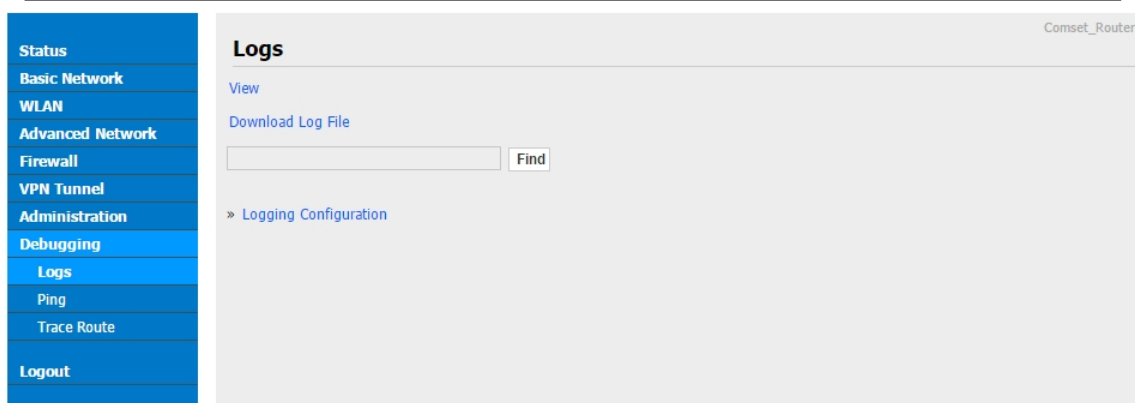


Figure 3-26 Logs GUI

### 3.7.2 Ping Settings

Step 1 Select “Debugging>Ping” to check and modify relevant parameters.

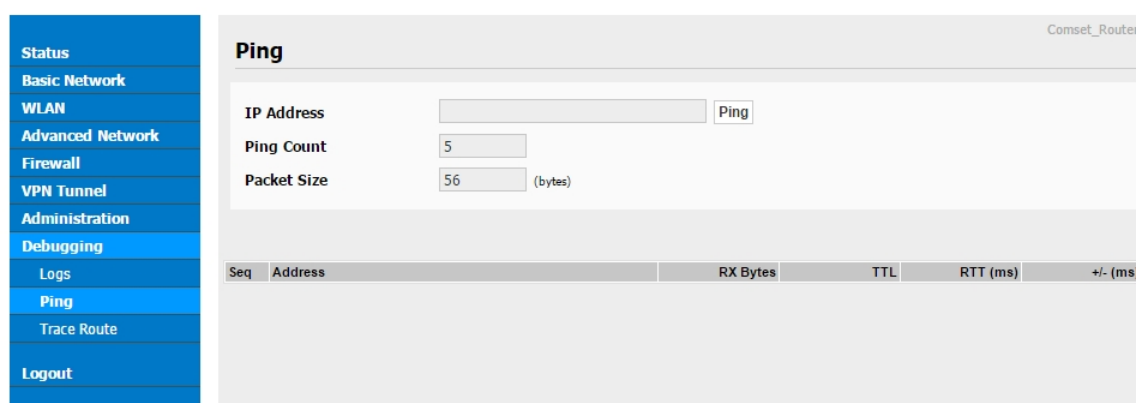


Figure 3-27 Ping GUI

### 3.7.3 Trace Settings

Step 1 Select “Debugging>Trace” to check and modify relevant parameters.

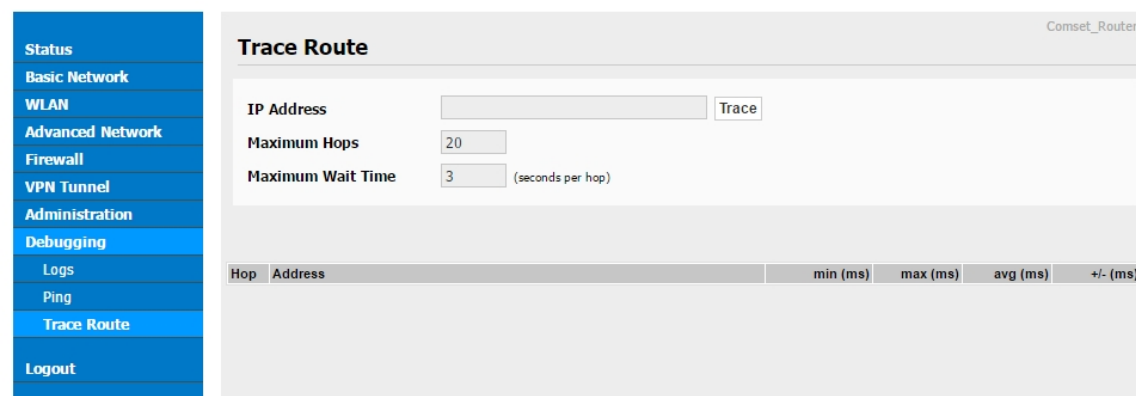


Figure 3-28 Trace GUI

## 3.8 “Reset” Button to Restore Factory Settings

If you can't access the GUI interface, you can perform a hardware reset. Press the “RST” button and keep holding for more than 8 seconds until the NET light stops blinking. The system will be restored to factory default settings.

Table 3-20 System Default Instructions

Item	Default settings
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin



### NOTE

After the reboot, the configuration will be deleted and restored to factory settings.

## 3.9 Appendix (For advanced optional features only)

### 3.9.1 GPS Settings

Step 1 Select “Advanced Network> GPS” to view or modify the relevant parameters.

The screenshot shows the 'GPS' configuration page. The left sidebar contains the following menu items: Status, Basic Network, WLAN, Advanced Network (selected), Port Forwarding, DMZ, Triggered, Firewall, GPS (selected), UPnP/NAT-PMP, Static DHCP, VPN Tunnel, Administration, Debugging, and Logout. The main configuration area is titled 'GPS' and includes the following settings:

- GPS Mode: Client (dropdown)
- Bind Port: 40001 (text input)
- Server IP/Port: 192.168.6.2 : 40002 (text input)
- Socket Type: UDP (dropdown)
- Socket Timeout: 500 (text input) (millisecond)
- Serial Timeout: 500 (text input) (millisecond)
- Paket Payload: 1024 (text input) (bytes)
- Heart-Beat Content: router\_00001 (text input)
- Heart-Beat Interval: 5 (text input) (seconds)
- Baud Rate: 9600 (dropdown)
- Parity Bit: none (dropdown)
- Data Bit: 8 (dropdown)
- Stop Bit: 1 (dropdown)

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 3-29 GPS Settings GUI

Table 3-21 “GPS” Instruction

Item	Description
Bind Port	Local port for GPS data.
Server IP and Port	GPS server IP address and port.
Socket type	GPS data protocol.
Socket Timeout	The timeout for socket connection. If the socket is not established, it will reconnect after the timeout.
Serial Timeout	The time is defined by the serial port buffer. After the time, the router will send GPS data to the server.
Packet Payload	The maximum packet for GPS data.
Heart-Beat Content	GPS heart beat packet.
Heart-Beat Interval	The heart beat packet interval.

Step 2 Click “save” to finish

**NOTE**

GPS data format is as below.

dtu.heartbeat.content,gps\_date, gps\_time, gps\_use, gps\_latitude, gps\_NS, gps\_longitude, gps\_EW, gps\_speed, gps\_degrees, gps\_FS, gps\_HDOP, gps\_MSL

e.g.

Router\_00001,083238,120313,12,2230.31563,N,11355.02863,E