

Industrial Grade 2G 3G 4G Cellular Router User Manual

H685 Series

E-Lins Technology Co., Limited

PHONE: +86-755-29230581

Email: sales@e-lins.com

WEB: <http://www.e-lins.com>

ADDRESS: Rm.33, Unit B, Floor 12, U chuangu, Xinniu Rd,
Minzhi, Longhua, Shenzhen, 518000, China

Content

1 Preparation job before configuration	4
1.1 Learn your router version and feature	4
1.2 Prepare SIM Card and working condition	6
1.3 Highly recommendation for the configuration	6
2 Hardware Installation	6
2.1 Overall Dimension	7
2.2 The Ports	7
2.3 Installment	9
2.4 SIM/UIM card installed	9
2.5 The installation of terminal blocks	9
2.6 Grounding	11
2.7 Power Supply	11
2.7.1 PoE Function (Option Feature)	11
2.8 LED and Check Network Status	12
3 Software configuration	13
3.1 Overview	14
3.2 How to log into the Router	14
3.3 Router status	17
3.3.1 Status overview	17
3.3.2 Network status	18
3.3.3 Firewall status	21
3.3.4 Routes	21
3.3.5 System log	22
3.3.6 Kernel log	23
3.3.7 Realtime graphs	23
3.4 System Configuration	25
3.4.1 Setup wizard	25
3.4.2 System	27
3.4.3 Password	29
3.4.4 NTP	30
3.4.5 Backup/Restore	33
3.4.6 Upgrade	34
3.4.7 Reset	35
3.4.8 Reboot	36
3.5 Services configuration	36
3.5.1 ICMP check	36
3.5.2 VRRP	38
3.5.3 Failover (link backup)	39
3.5.4 DTU	40
3.5.5 SNMP	42
3.5.6 GPS	44
3.5.7 SMS	45

3.5.8 VPN	错误!未定义书签。
3.5.8.1 IPSEC	65
3.5.8.2 PPTP	68
3.5.8.3 L2TP	71
3.5.8.4 OpenVPN	74
3.5.8.5 GRE tunnel	75
3.5.9 DDNS	52
3.5.10 Connect Radio Module	57
3.5.11 Modbus	57
3.6 Network Configuration	76
3.6.1 Operation Mode	77
3.6.1.1 Gets two LAN Ethernet Port for H685	77
3.6.2 Mobile configuration	78
3.6.3 Cell mobile data limitation	81
3.6.4 LAN settings	82
3.6.5 wired-WAN	85
3.6.6 WiFi Settings	86
3.6.6.1 Wifi General configuration	87
3.6.6.2 WiFi Advanced Configuration	87
3.6.6.3 WiFi Interface Configuration	88
3.6.6.4 WiFi AP client	90
3.6.7 Interfaces Overview	93
3.6.8 Firewall	94
3.6.8.1 General Settings	94
3.6.8.2 Port Forwards	94
3.6.8.3 traffic rules	95
3.6.8.4 DMZ	99
3.6.8.5 Security	100
3.6.9 Static Routes	101
3.6.10 Switch	102
3.6.11 DHCP and DNS	103
3.6.12 Diagnostics	105
3.6.13 Loopback Interface	106
3.6.14 Dynamic Routing	107
3.6.15 QoS	108
3.6.16 Guest LAN(Guest WiFi)	110

Chapter 1

1 Preparation job before configuration

1.1 Learn your router version and feature

- 1) H685 series contains different version and option feature. Please learn it before using it.
H685 series defines the model as follows,

H685 -x --- XXX (option features)

|

|

W: WiFi WLAN

G: GPS / GNSS

RS232/RS485: DTU feature (cellular to serial), RS232 or RS485 for choice

60V: DC input 5-60V supported, default is 5-40V

DIO: digital input and output feature, 2-4 ports

t: 4G LTE version. Support FDD LTE or TDD LTE or FDD+TDD LTE, back compatible to 3G and 2G

w: 3G WCDMA HSPA version, support HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM

p: 3G WCDMA HSPA+ version, support HSPA+/HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM

eva: 3G CDMA2000 EVDO version, support EVDO RevA/EVDO Rev0/CDMA1x

evb: 3G CDMA2000 EVDO version, support EVDO RevB/EVDO RevA/EVDO Rev0/CDMA1x

td: 3G TD-SCDMA version, support TD-HSUPA/TD-HSDPA/TD-SCDMA/EDGE/GPRS/GSM

e: 2G EDGE version, support EDGE/GPRS/GSM

g: 2G GPRS version, support GPRS/GSM

c: 2G CDMA version, support CDMA1x

Notes:

- 1) option feature can be select one or all
- 2) for LTE version, please confirm your LTE band and Network Carrier with order to avoid wrong selection

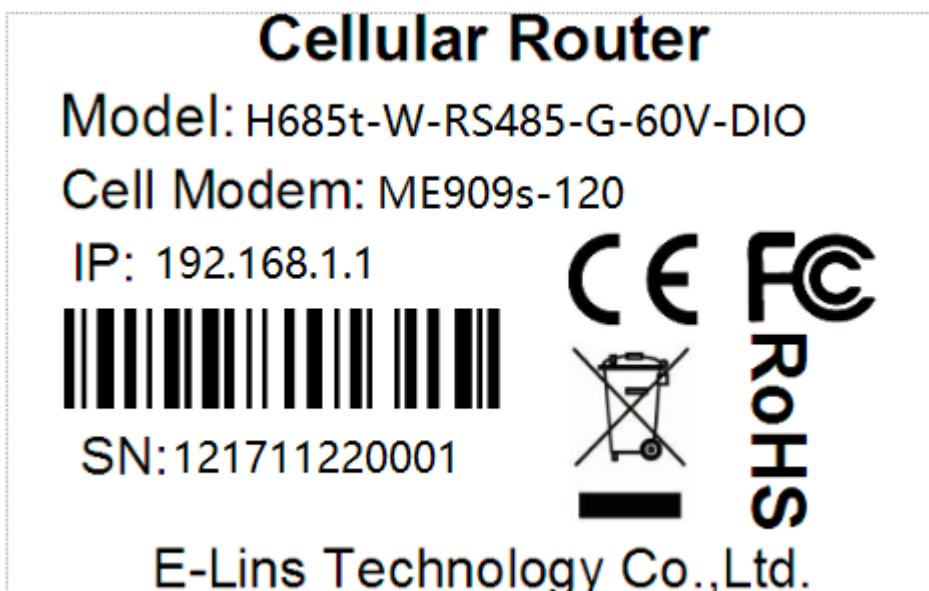
Notes: please be informed the following features are option. Please indicate with your

orders.

- 1) WiFi Feature
- 2) GPS feature
- 3) Serial to cellular feature, RS232 or RS485 can choose one
- 4) Voice/SMS control
- 5) DC5V~60V
- 6) BGP, OSPF, RIP, etc.
- 7) DIO (digital input and output feature)
- 8) RMS (Remote Management System)

2) Find the modem type info at the back cover of the router. This will be used while do configuration.

For example: the following label indicates the version, type and inside module modem. The module modem name is “ME909s-120”, remember this and will select this module name while do configuration.



1.2 Prepare SIM Card and working condition

1. H685 router has different version. Study your router version before installation.
2. For GSM/GPRS/EDGE/HSDPA/HSUPA/HSPA/HSPA+/4G LTE version, please get a SIM card with data business.
3. For CDMA2000 EVDO/CDMA1x version, please get a UIM card with data business or inform us before order if the network uses non-ruim (nam-flashing).
4. Make sure the sim card or uim card is with enough data business and balance.
5. Make sure the signal is good enough where you test or install the router. Weak signal will make the router no work. If you find your signal strength is not good, please contact us for high gain antenna.
6. Different countries and carriers use different network band and frequency. E-Lins packs units with free world-wide-use antenna. It can work, but the data speed or signal may not be good at your sites. Please buy dedicated high gain antenna from your local suppliers or contact E-Lins to OEM/ODM the antenna.

1.3 Highly recommendation for the configuration

The wireless cellular is unstable sometimes with some uncertain issue. In order to keep the router working in the best condition, it is highly recommended that the [Cell ICMP Check](#) feature is activated. Please refer to [chapter 3.5.1](#) to configure.

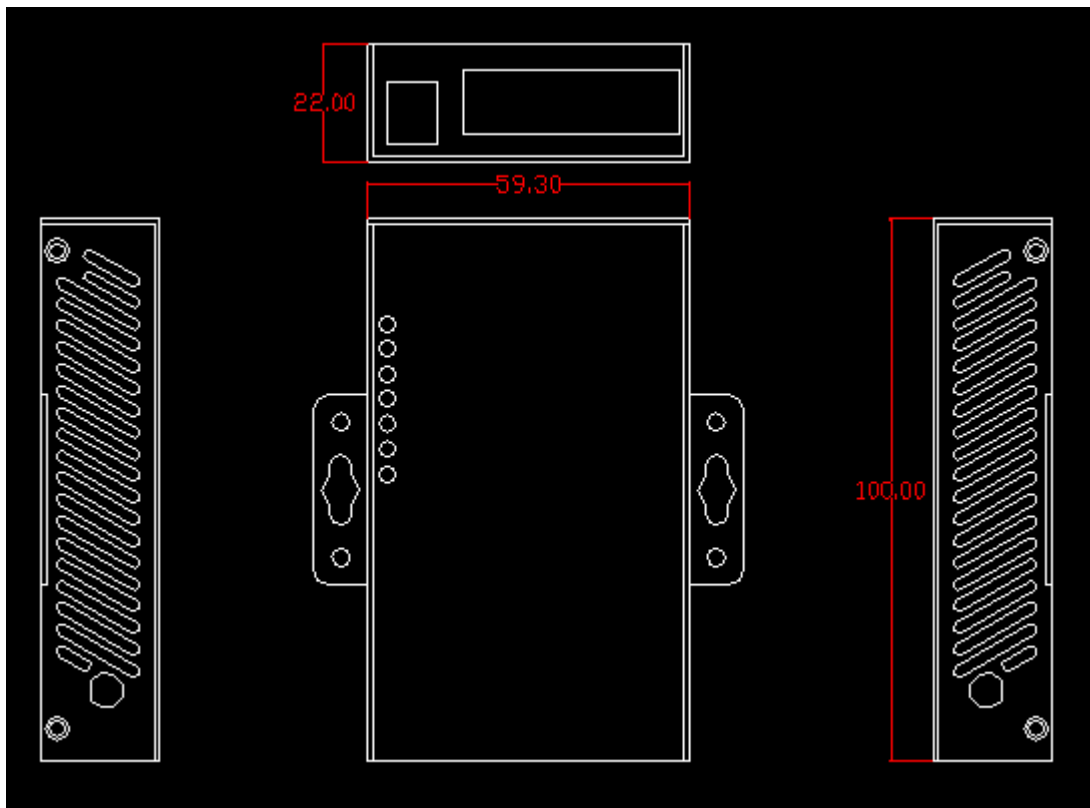
Chapter 2

2 Hardware Installation

This chapter mainly describes the appearance, model and function of H685 series and how to install and set the configurations.

1. *Overall Dimension*
2. *Accessories Description*
3. *Installment*

2.1 Overall Dimension



2.2 The Ports

Pictures:





LAN: LAN RJ45 Ethernet ports.

WAN: WAN RJ45 Ethernet ports.

RST: sys reset button

PWR: DC power socket. DC5~40V, DC5~50V option depends on the router version.

VCC: DC wire positive pole. DC5~40V, DC5~50V option depends on the router version

GND: DC wire ground

GND: Serial ground

RX: serial receiving

TX: serial transmission

RST: reset router

DIO0: digit I/O port 0

IDO1: digit I/O port 1

IDO2: digit I/O port 2

IDO3: digit I/O port 3

Antenna Connection Table

Antenna Connector	Marks
Cell1	for main cell antenna

Aux / Cell2	for auxiliary cell antenna
C3/W1	cellular antenna 3 or Wi-Fi antenna.
C4/G/W2	cellular antenna 4, or GPS antenna, or Wi-Fi 2 antenna
WiFi / W1/W2	for WiFi antenna

2.3 Installment

H685 series should be installed and configured properly before putting in service. The installation and configuration should be done or supervise by qualified engineer.

Attention:

Do not install H685 series or connect/disconnect its cable when it is power on.

2.4 SIM/UIM card installed

If your router has SIM/UIM card protector, please remove it, insert the sim card correctly, and fix the protector.

If your router has no SIM/UIM card protector, please insert the sim card correctly.

Attention: *SIM/UIM card does not reach the designated position, the equipment can not find a card, can't work normally, therefore inserted a try to check again for a SIM card is stuck fast.*

2.5 The installation of terminal blocks

This chapter is for version with terminal blocks only. Default, the H685 is with DB9 connector. Please use DB9 cable to connect H685 and the equipment directly.

The following is for version with terminal blocks only:

H685 uses pluggable terminals to connect the user's data and the power supply. Spacing: 3.81mm, 10 Pin; User data and power supply suggestion: 14~24AWG. Please refer to the table 2-4 for the interface definition of the power cable and connection sequence. Specific interface definition of the power cable and connection sequence you can read on the labels of H685 products. Using 14~24AWG cable and referring to H685 products labels or the bellowed interface definition and connection sequence, you need to use the oblate screw driver to fix the cable to the connecting jacks of the pluggable terminal. After successfully connection, you need to insert the terminal into the corresponding position in

the bottom of the H685 products.

Notes: Connection sequence should be accurate. Cable's insulating striping length is about 7mm. (For safety, insulating striping length should be too long). Please refer



to the picture.

Attention:

1. The power cable should be connected correctly. We "suggestion double check before switch it on .Wrong connections may destroy the equipment.
2. Power terminals: Pin 1 and Pin 2;
3. Here: Pin 2 is "GND", PIN 1 is power input "Vin"(DC5~40V, or DV5~50V).

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input, +5~50V option	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 with reset button. In the usage, it needs to be short connected to the GND. After giving the device a 1 sec low level, it will reboot.3 seconds, the device will restore factory settings
7	DIO0	General Purpose I/O	

8	DIO1	General Purpose I/O	
9	NC	Not connect	Reserved for DIO2
10	NC	Not connect	Reserved for DIO3
I/O Terminal on router		Serial port (RS485 or RS232)	
Port 3 (GND)		Pin 5	
Port 4 (RX)		Pin 2	
Port 5 (TX)		Pin 3	

Notes: If not through, can switch Port4 and port5.

2.6 Grounding

To ensure a safe, stable and reliable H685 series operation, Router cabinet should be grounded properly.

2.7 Power Supply

H685 series can be applied to complicated external environment and usually the power range is very large. So in order to fit the complicated application environment and improve the stability of the system, H685 series is designed with advanced power management technology. The DC power supply electronic to the device via the pluggable terminal PIN 2(GND) and PIN 1(Vin). Please refer to the above table for the detail definition of the terminal.

Normally, H685 series input powers supply is +5~+40V (if your H685 support 50V, the option is +5~+50V). In most cases, the standard configuration is 12V/1A.



Attention:

The H685 supports POE (Power over Ethernet) (This is option feature. Please confirm with your order). It supports 5-40VDC default, if the POE voltage is 48V, please order 5-60VDC version, otherwise it will defeat the hardware of H685.

2.7.1 PoE Function (Option Feature)

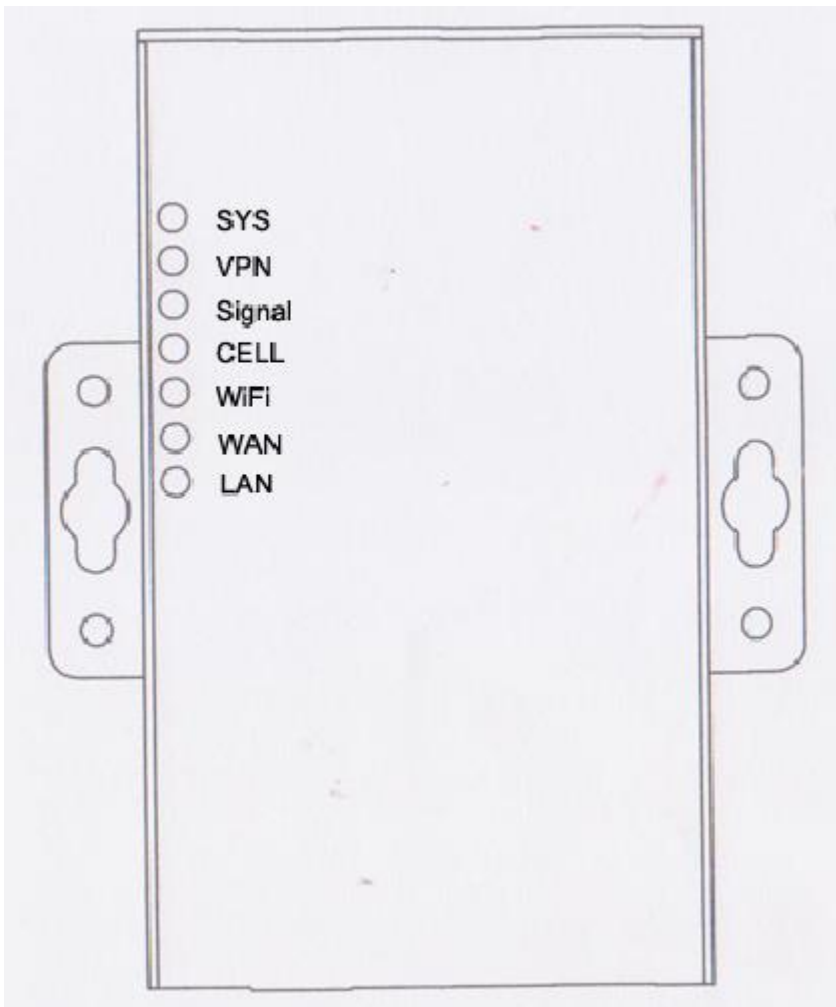
Both the LAN port and the WAN port support PoE, and the PoE switch uses an network

cable to connect to the router to supply power and transmit data.

The PoE is an optional function and is only used on models that support the PoE function.

2.8 LED and Check Network Status

Please connect the antenna after you successfully connect to the cable. And then insert the valid SIM/UIM card and provide the power to the H685 series via the cable. After provide the power to H685, if the SYS LED starts to blink in a few seconds, that means the system start-up is normal; if the CELL LED works, that means the network is online; if the VPN light works, that means VPN tunnel has been set up. Please refer to the below table for the situation of the indication lights.



LED	Indication Light	Description
SYS	On for 25 seconds	On for 25 seconds after power supply
	blink	System set-up normally

	Off or still on after 25 seconds	System set-up failure
LAN	blink	Data transmission in Ethernet
	Off	Ethernet connection abnormal
	On	Ethernet is connected
VPN	On	IPSec VPN tunnel set-up
	Off	IPsec VPN tunnel set-up failure or inactivated
CELL	On	Access to the Internet/Private Network
WiFi	On	Enable
	Off	Disable
WAN	blink	Data transmission in Ethernet
	Off	Ethernet connection abnormal
	On	Ethernet is connected
Signal	Off	No signal, or signal checking is not ready
	blink (2 seconds for on, and 2 seconds for off)	Signal bar is 1
	blink (1 seconds for on, and 1 seconds for off)	Signal bar is 2
	blink (0.5 seconds for on, and 0.5 seconds for off)	Signal bar is 3

Chapter 3

3 Software configuration

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

3.1 Overview

H685 series routers with built-in WEB interface configuration, management and debugging tools, user should configuration the parameters first; and it could be altered the parameters flexibility and software upgrades and simple testing. User can set up and manage the parameters of the router on its interface, detail step are bellow:

3.2 How to log into the Router

3.2.1 Network Configuration of the Computer.

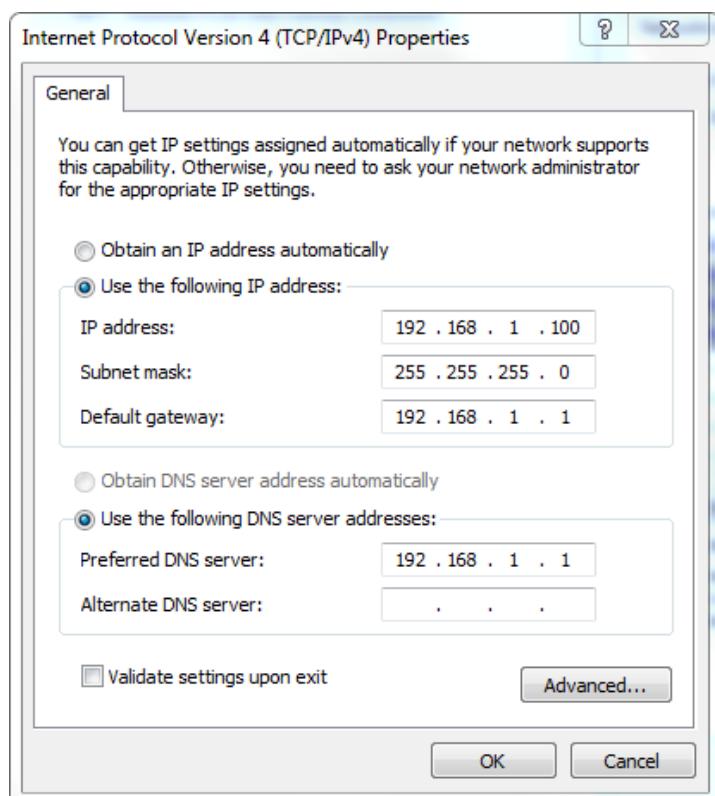
The router default parameters as follow

Default IP: 192.168.1.1, sub mask: 255.255.255.0.

There are two ways to set the PC's IP address.

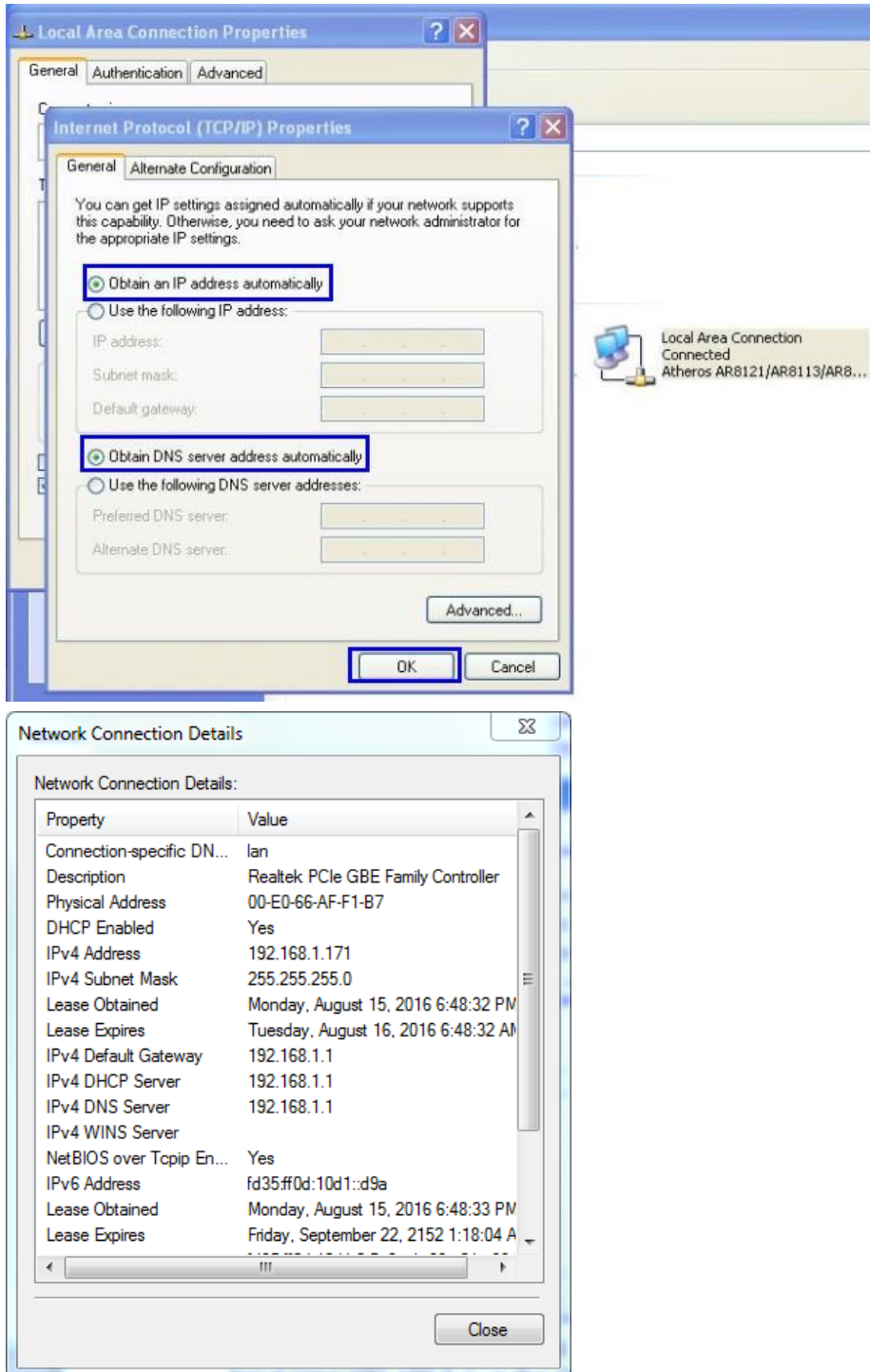
Way 1) Manual setting

Set the PC IP as 192.168.1.xxx (xxx = 2~254), subnet mask: 255.255.255.0, default gateway: 192.168.1.1, primary DNS: 192.168.1.1.



Way 2) DHCP

Choose "Obtain an IP address automatically" and "Obtain DNS server address automatically".



After IP setting, check it by ping. Click Windows start menu, run, execute "cmd" command. Input "ping 192.168.1.1" in the DOS window.

```
C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

This information means the connection is work.

```
Pinging 192.168.8.1 with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

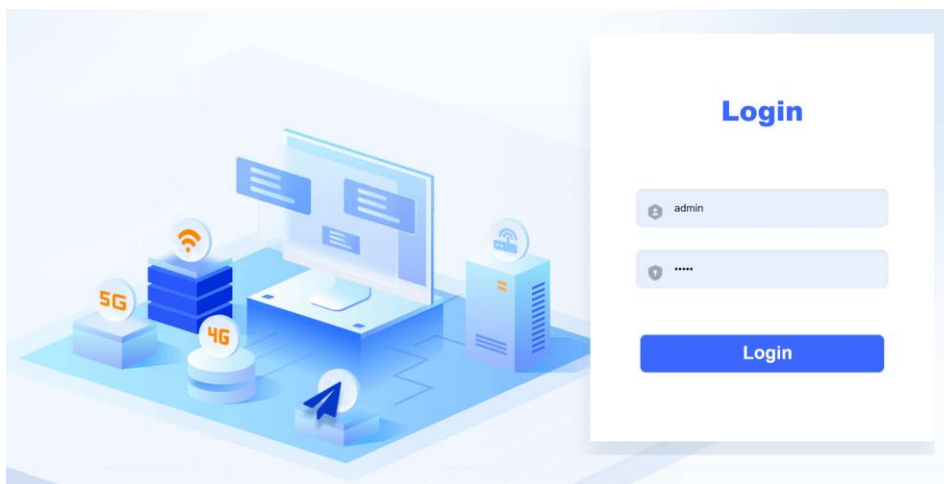
Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

This information means the connection is failure. If so, please check the network cable connection and IP address setting, and can refer to *Chapter 4.9*.

3.2.2 Log into Router

- Open the Web Browser, and type <http://192.168.1.1> into the address field and press Enter bottom in your computer keyboard.
- Type User Name “admin” and Password “admin” in the Login page, and then press the “Login” button.



- If you type into the correct User Name and Password, you will get the access into the Router’s status overview page.

Status

System

Hostname	Cell_Router
SN	860000253B002305
Firmware Version	3.2.319
Kernel Version	3.18.29
Local Time	Wed Nov 1 07:54:53 2023
Uptime	0h 6m 16s
Load Average	0.18, 0.40, 0.24
Port Status	 LAN1 LAN2 LAN3 LAN4 WAN

Mobile 1

Cellular Status	Up
IP Address	10.22.127.224/255.255.255.192
DNS 1	202.96.128.86
DNS 2	202.96.134.133
Cell Modem	forge4_SLM750 (05C6_F601)
IMEI/ESN	868159051832546
Sim Status	SIM Ready
Strength	31 / 31, dBm : -51

3.3 Router status

3.3.1 Status overview

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

Status

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

System

Services

VPN

Network

Logout

Status

⚙️ System

Hostname	Cell_Router
SN	860000253B002305
Firmware Version	3.2.319
Kernel Version	3.18.29
Local Time	Wed Nov 1 07:54:53 2023
Uptime	0h 6m 16s
Load Average	0.18, 0.40, 0.24
Port Status	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> LAN1</div> <div style="text-align: center;"> LAN2</div> <div style="text-align: center;"> LAN3</div> <div style="text-align: center;"> LAN4</div> <div style="text-align: center;"> WAN</div> </div>

📶 Mobile 1

Cellular Status	Up
IP Address	10.22.127.224/255.255.255.192
DNS 1	202.96.128.86
DNS 2	202.96.134.133
Cell Modem	forge4_SLM750 (05C6_F601)
IMEI/ESN	868159051832546
Sim Status	SIM Ready
Strength	📶 31 / 31, dBm : -51

3.3.2 Network status

Network status pages show detail information of cell mobile interface, WAN and LAN.

Cell mobile interface page:

Status ▾

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

System ▾

Services ▾

VPN ▾

Network ▾

Logout ▾

Mobile

WAN

LAN

Mobile Status

Mobile 1

Cellular Status	Up
Cell Modem	forge4_SLM750 (05C6_F601)
IMEI/ESN	868159051832546
Sim Status	SIM Ready
Strength	📶 31 / 31, dBm : -51
Selected Network	Automatic
Registered Network	Registered on Home network: "CHN-CT",7
Sub Network Type	FDD LTE
Location Area Code	30560
Cell ID	31
ICCID	89860321247558334500
RSRP	-61 dBm
RSRQ	-5 dB
SINR	25.8 dB
MSISDN/IMSI	undefined / 460115059440179

Connection Status

Port	Mobile-eth
IPv4 Addr	10.22.127.224/26
DNS 1	202.96.128.86
DNS 2	202.96.134.133
Gateway	10.22.127.225
Uptime	0h 7m 33s

WAN status page:

Mobile **WAN** LAN

WAN Status

Status Overview

IPv4 WAN Status	Port	Wired-WAN
	Protocol:	dhcp
	Address:	0.0.0.0
	Netmask:	255.255.255.255
	Gateway:	0.0.0.0
	Connection:	down
	Mac Addr:	90:22:08:C1:75:BC
	RX	0.00 B (0 Pkts.)
	TX	63.00 KB (200 Pkts.)
IPv6 WAN Status	Not connected	
Active Connections	56 / 16384 (0%)	

LAN status page:

Mobile WAN **LAN**

LAN Status

Status Overview

Uptime:	0h 9m 59s
Protocol:	static
Name:	br-lan
type:	bridge
Mac Addr:	90:22:08:81:75:BC
IPv4 Addr:	192.168.1.1/24
IPv6 Addr:	DD25:87DE:78EC::1/60
RX	115.55 KB (1306 Pkts.)
TX	442.54 KB (1377 Pkts.)

LAN Ports

Port	MAC-Addr	RX	TX
Wired-LAN	90:22:08:01:75:BC	136.26 KB (1503 Pkts.)	440.53 KB (1355 Pkts.)
WiFi	90:22:08:01:75:BC	0.00 B (0 Pkts.)	13.27 KB (120 Pkts.)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

3.3.3 Firewall status

Firewall status page shows IPv4 and IPv6 rules and counters. The final user can reset counters and restart firewall functionality here.

Firewall Status

IPv4 Firewall | IPv6 Firewall

Actions

- Reset Counters
- DestinationDestination

Table: Filter

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1519	167.58 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	0	0.00 B	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	1664	566.85 KB	delegate_output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain delegate_forward (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for forwarding */

3.3.4 Routes

Routes page shows rules which are currently active on this router. And ARP table is displayed as well.

IPV4-Address	MAC-Address	Interface
192.168.1.100	00:e0:4c:68:9f:f3	br-lan

Network	Target	IPV4-Gateway	Metric	Table
lan	192.168.1.0/24	192.168.1.1	0	144
ifmobile	0.0.0.0/0	10.22.127.225	11	main
ifmobile	10.22.127.192/26		11	main
ifmobile	10.22.127.225		11	main
lan	192.168.1.0/24		0	main

Network	Target	Source	Metric	Table
lan	dd25:87de:78ec::/64		1024	main
wan	:::2:1:2		0	local
(eth0)	:::0:::8		256	local
lan	:::0:::8		256	local

3.3.5 System log

This page shows system log from system boot up. System log is not saved when router restarts. It can be exported by click button "Export syslog".

System Log
Last System Log

Status

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

- System
- Services
- VPN
- Network
- Logout

System Log

Export syslog

```

Tue Oct 31 11:15:08 2023 kern.notice kernel: [ 0.000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r49294) ) #4255 Tue Oct 31 18:46:44 CST 2023
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Board has DDR2
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Analog PMU set to hw control
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Digital PMU set to hw control
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] SoC Type: MediaTek MT7620A ver:2 eco:6
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] bootconsole [early0] enabled
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] CPU0 revision is: 00019650 (MIPS 24KEc)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] MIPS: machine is mt7620a_model_2
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Determined physical RAM map:
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] memory: 04000000 @ 00000000 (usable)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Inifrd not found or empty - disabling inifrd
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Zone ranges:
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Normal [mem 0x00000000-0x03ffff]
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Movable zone start for each node
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Early memory node ranges
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] node 0: [mem 0x00000000-0x03ffff]
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Inifmem setup node 0 [mem 0x00000000-0x03ffff]
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] On node 0 totalpages: 16384
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] free_area_init_node: node 0, pgdat 803241b0, node_mem_map 81000000
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] Normal zone: 128 pages used for memmap
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] Normal zone: 0 pages reserved
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] Normal zone: 16384 pages, LIFO batch:3
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Primary instruction cache 64KB, VIPT, 4-way, linesize 32 bytes.
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Primary data cache 32KB, 4-way, PIPT, no aliases, linesize 32 bytes
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
Tue Oct 31 11:15:08 2023 kern.debug kernel: [ 0.000000] pcpu-alloc: [0] 0
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 16256
Tue Oct 31 11:15:08 2023 kern.notice kernel: [ 0.000000] Kernel command line: console=ttyS1,57600 rootfstype=squashfs,jffs2
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Writing ErrCtl register=0007fd91
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] Readback ErrCtl register=0007fd91
Tue Oct 31 11:15:08 2023 kern.warn kernel: [ 0.000000] Memory: 61164K/65536K available (2629K kernel code, 138K rwdata, 556K rodata, 188K init, 186K bss, 4372K reserved)
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Tue Oct 31 11:15:08 2023 kern.info kernel: [ 0.000000] NR IRQS:256
                    
```

3.3.6 Kernel log

This page shows Kernel log from system boot up. This log is not saved when router restarts. It can be exported by click button “Export syslog”.

The screenshot shows the 'Kernel Log' section of a web interface. It features a sidebar on the left with various system management options. The main area displays a list of kernel boot logs, including system information, hardware details, and memory management. An 'Export log' button is visible at the top of the log content.

```
[ 0.000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r49294) ) #4255 Tue Oct 31 18:46:44 CST 2023
[ 0.000000] Board has DDR2
[ 0.000000] Analog PMU set to hw control
[ 0.000000] Digital PMU set to hw 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] Initrd not found or empty - disabling initrd
[ 0.000000] Zone ranges:
[ 0.000000]  Normal  [mem 0x00000000-0x03ffffff]
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000]  node 0: [mem 0x00000000-0x03ffffff]
[ 0.000000] Initmem setup node 0 [mem 0x00000000-0x03ffffff]
[ 0.000000] On node 0 totalpages: 16384
[ 0.000000] free_area_init_node: node 0, pgdat 803241b0, 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=ttyS1,57600 rootfstype=squashfs,jffs2
[ 0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)
[ 0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
[ 0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
[ 0.000000] Writing ErrCtl register=0007fd91
[ 0.000000] Readback ErrCtl register=0007fd91
[ 0.000000] Memory: 61164K/65536K available (2629K kernel code, 138K rwdata, 556K rodata, 188K init, 186K bss, 4372K reserved)
[ 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 - mult: 214748, shift: 32
```

3.3.7 Reboot Log

Shows device and cell module reboot event since last upgrade firmware or reset to factory default.

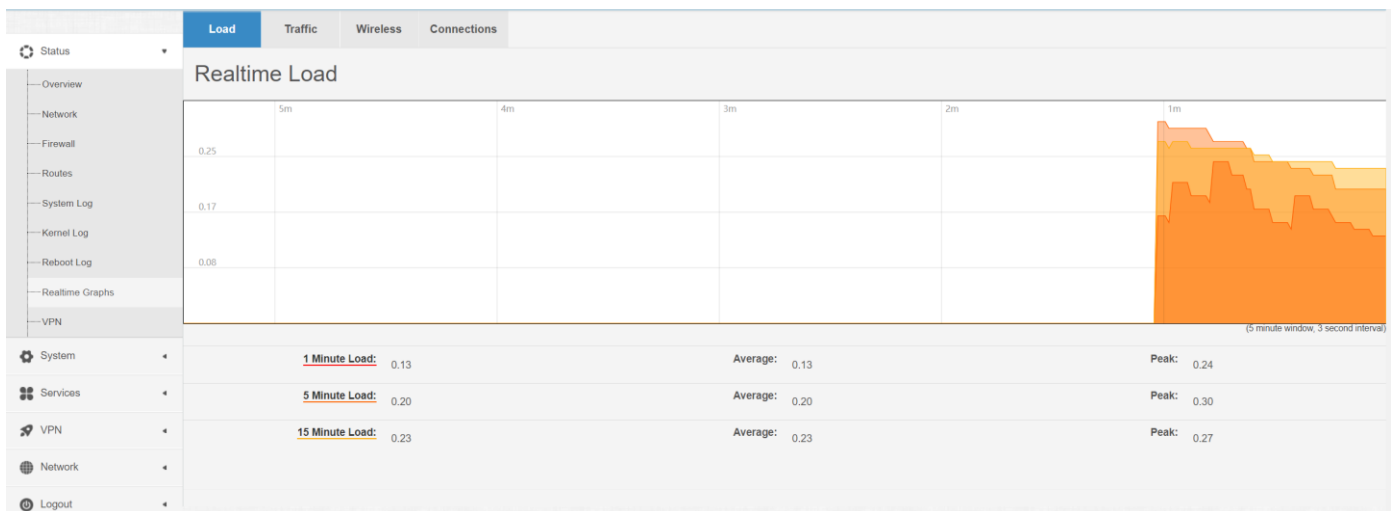
Reboot Log

Clear log

Sat Nov 4 02:14:00 AEDT 2023 : Reboot cell module
 Sat Nov 4 02:14:01 AEDT 2023 : Router reboots from web
 Sat Nov 4 02:14:40 AEDT 2023 : Router boots up
 Sat Nov 4 02:14:51 AEDT 2023 : Reboot cell module
 Sat Nov 4 02:15:00 AEDT 2023 : Reboot cell module
 Sat Nov 4 02:16:00 AEDT 2023 : Reboot cell module
 Sat Nov 4 02:17:00 AEDT 2023 : Reboot cell module

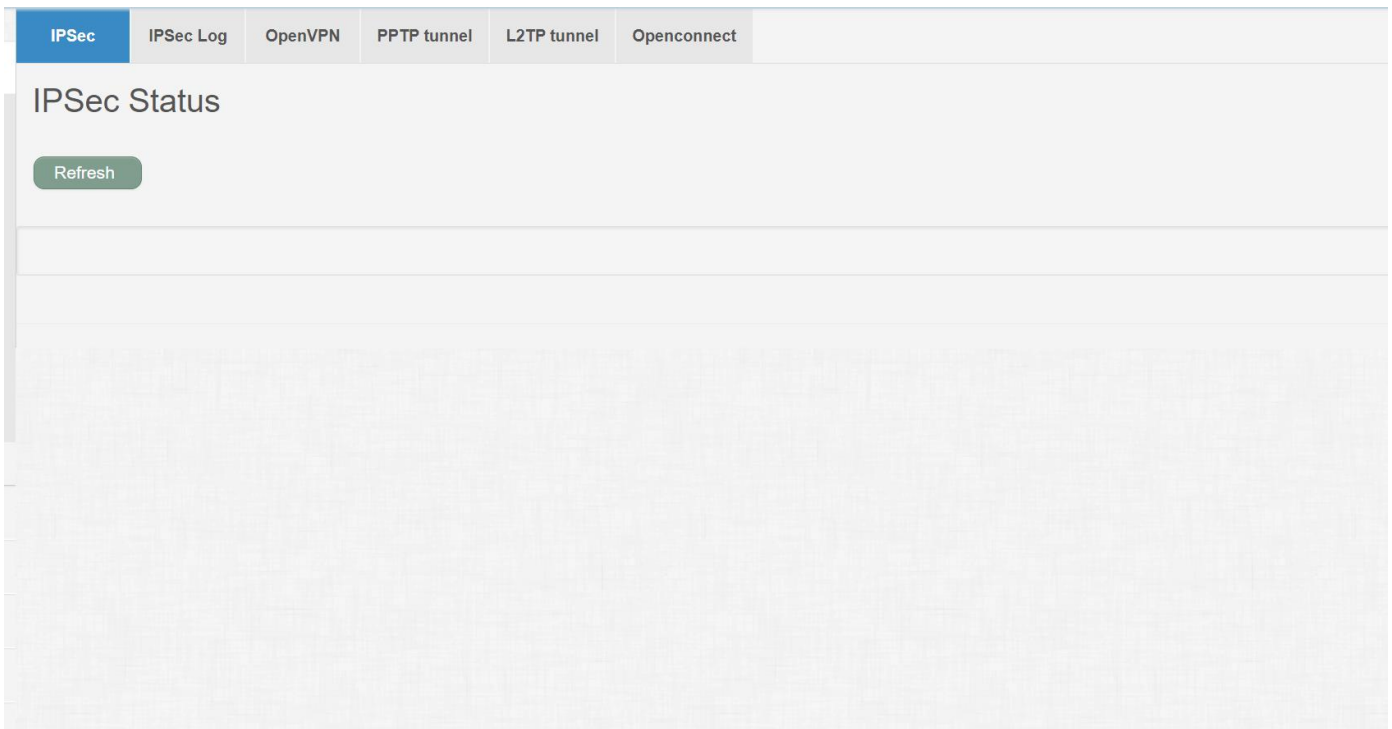
3.3.8 Realtime Graphs

Realtime Graphs page shows real time system load, interfaces traffic, etc..



3.3.9 VPN Status

VPN Status, include IPSec status, IPSec logs, OpenVPN status, PPTP and L2TP clients when device works as PPTP/L2TP server. And also Openconnect status.



3.4 System Configuration

3.4.1 Setup wizard

When login in router at the first time, setup wizard pages show.

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

Step - General

First, let's change your router password from the default one.

Password Settings

New password

Confirm new password

System Settings

Current system time Wed Nov 1 08:19:51 2023 [Sync with browser](#)

Timezone

Hostname

Language

[Skip Wizard](#) [Save & Next](#)

Note: pressing button “Save & Next” will save configuration and jump to the next page. All configurations will be applied after click button “Finish” at the final step (Step-WiFi).

3.4.2 System

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

- General Settings** | Logging | Language
- Local Time**: Wed Nov 1 08:21:17 2023 [Sync with browser](#)
- Hostname**: Cell_Router
- Timezone**: UTC
- Turn off LEDs**:

[Save](#)

General Settings

- **Local Time:** It displays device time, and the final user can Sync this time with browser by clicking button “Sync with browser”.
- **Hostname:** It is the router’s name, the default name is Cell_Router.
- **Time zone:** Select a suitable time zone. The default value is UTC
- **Turn off LEDs:** set all LEDs to off except LAN,WAN LED.

Logging settings

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings **Logging** Language

System log buffer size	<input type="text" value="64"/>
External system log server	<input type="text" value="0.0.0.0"/>
External system log server port	<input type="text" value="514"/>
Log output level	<input type="text" value="Debug"/> ▾
Cron Log Level	<input type="text" value="Normal"/> ▾
Record Cell Status	<input type="checkbox"/>

Save

- **System log buffer size:** The unit is KB, default value is 64 KB. If the real log size is bigger than the value configured, the oldest log will be dropped.
- **External system log server:** The IP address of external log server. The final user can setup a Linux machine with syslogd run as log server.
- **External system log server port:** The UDP port of external log server.
- **Log output level:** Log level, the default is debug with highest level, Emergency is the lowest level.
- **Cron log level:** It is log level for process Crond.
- **Record Cell Status:** print cell status information in system log periodically.

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

The screenshot shows the 'System Properties' configuration page with the 'Language' tab selected. The 'Language' dropdown menu is set to 'English'. A 'Save' button is located at the bottom right of the configuration area.

- **Language:** The default language is “Auto”. The final user can choose English or Chinese.

3.4.3 Password

Web Account only can be used on web GUI Login.

The screenshot shows the 'Web Account' configuration page. It has three tabs: 'Web Account', 'SSH Account', and 'Guest Account'. The 'Web Account' tab is active. Below the tabs, there are five input fields: 'Current username', 'Current password', 'New username', 'New password', and 'Repeat new password'. Each password field has an eye icon for visibility. A 'Save' button is at the bottom.

- **Current username:** must input to change username or password.
- **Current password:** must input to change username or password.
- **New username:** only needed when changing username.
- **New password:** only needed when changing password.
- **Repeat new password:** only needed when changing password.

SSH Account only can be used on SSH login.




Web Account **SSH Account** Guest Account

SSH Account

Changes SSH username and password..

To change password you must enter: Current username, Current password, New password and Repeat new password.

To change Username you must enter: Current username, Current password, New username.

Current username	<input type="text"/>
Current password	<input type="password"/> 
New username	<input type="text"/>
New password	<input type="password"/> 
Repeat new password	<input type="password"/> 

Save

Guest Account page to enable guest user and change guest password, guest account cannot change any configuration.


Web Account SSH Account **Guest Account**

Guest Password


Changes the guest password

Enable guest

Password

Repeat password

Save



3.4.4 Certificates

Cert file and key file for HTTPS access, the default cert and key file is self-signed file.

Web GUI SSH

Web GUI

HTTPS Certificate

Cert file	Uploaded File (606.00 B)	
Key file	Uploaded File (609.00 B)	

Save

Enable/disable SSH password authentication, or SSH-Key access.

Web GUI SSH

SSH Access

Dropbear Instance

Password authentication	<input checked="" type="checkbox"/>
-------------------------	-------------------------------------

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

Save

3.4.5 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

Save

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 server candidates:** It is NTP server list, multiple NTP server is accepted. The final user can click the button  to delete an entry, or click button  to add a new entry.

3.4.6 Backup/Restore

Configuration files operations

The screenshot displays a web interface for configuration file operations, divided into four main sections:

- Export Config:** A section with a dark green header. It contains a label "Download backup configuration archive:" followed by a green "Download" button.
- Import Config:** A section with a light blue header. It contains a label "Restore backup configuration archive:", a file selection input with "Choose File" and "No file chosen" text, and a green "Upload..." button.
- Backup Config:** A section with a dark green header. It contains a label "Backup time:", a label "Restore after factory reset:" with an unchecked checkbox, and a label "Backup configuration to flash:" followed by a green "Backup" button.
- Restore Config:** A section with a light blue header. It contains a label "Restore configuration from flash:" followed by a green "Restore" button.

It is used for configuration files backup and restore.

Export Config, click button "Download", an archive file will be generated and be downloaded to your PC automatically.

Import Config, click 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.

Backup Config, save current config in flash, after factory reset, the configuration is still in flash. If "Restore after factory reset" is enabled, after reset router will use the configuration in flash as current configuration.

Restore Config, restore configuration from flash to cover current configuration.

3.4.6 Upgrade

System upgrade

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

Keep settings:	<input checked="" type="checkbox"/>
Safe upgrade:	<input checked="" type="checkbox"/>
Image:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload image..."/>

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 factory setting. But we highly recommend uncheck “Keep settings”, otherwise it may bring uncertain parameters conflicting after updating.

Click button “Choose File” to select a compatible firmware then click button “Upload image...”. Router will do a basic checking for the uploaded file. If it is not compatible file, an error will be generated like this:

System upgrade

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

Keep settings:	<input checked="" type="checkbox"/>
Safe upgrade:	<input checked="" type="checkbox"/>
Image:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload image..."/>

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

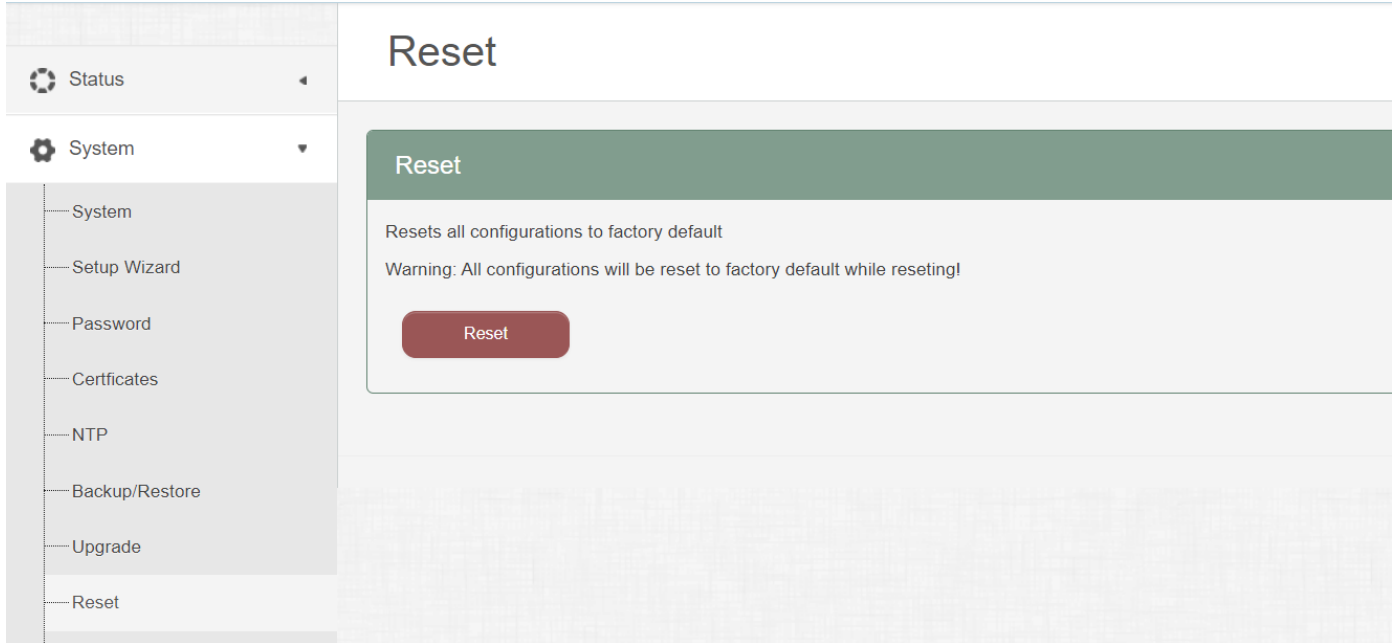
If the firmware file is OK, it will go to the verify page, then click button “Proceed”, and system will restart soon.

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: 93069f91cfeb8b355cfe10507d4d2021
- Size: 14.31 MB (15.00 MB available)
- Configuration files will be kept.
- Firmware checksum is OK.

3.4.7 Reset



Reset all configurations to factory default, after click button “Reset”, there is pop dialog to ask it’s really to reset, click button “cancel” will do nothing, click button “OK” will reset all configuration to default and restart system.

3.4.8 Reboot

Reboot Settings

Reboot At Time Settings

Reboot at time

Time(H:M:S)

Reboot Timer Settings

Reboot when timeout

Timer(min)

Reboot Now

Save

Click button “Reboot”, the system will restart in several seconds.
You can also set up a schedule to reboot.

3.5 Services configuration

3.5.1 ICMP check

For router working with best stability, we highly suggest activate and use this feature.
With this feature, the Router will automatically detect its working status and fix the problem.

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

ICMP Check

☰ Cell Interface Ping

Enable	<input type="checkbox"/>
Host1 to ping	<input type="text" value="www.google.com"/> <small>ipv4 or hostname</small>
Host2 to ping	<input type="text" value="8.8.8.8"/>
Ping packet size	<input type="text" value="1"/> <small>bytes. (range [1 - 1000])</small>
IPV6	<input type="checkbox"/>
Ping timeout	<input type="text" value="4"/> <small>seconds (range [1 - 10])</small>
Max retries	<input type="text" value="10"/> <small>(range [3 - 1000])</small>
Interval between ping	<input type="text" value="2"/> <small>minutes (range [1 - 1440])</small>
Reconnect	<input type="checkbox"/>
Start ping after cell up	<input checked="" type="checkbox"/>
Action when failed	<input type="text" value="Restart module"/>

- **Enable:** Enable ICMP check feature
- **Host1 to ping / Host2 to ping:** The domain name or IP address for checking the network connection.
- **Ping timeout:** If ping packet is sent, the response packet is not received before timeout, then this ping is failed.
- **Max retries:** If the ping is failed, the failed counter will add one. If the failed counter is bigger or equal to the Max retries, then system will say the ICMP check is failed, an action configured in item "Action when failed" will be triggered. If the ping is succeeding, failed counter will be reset to 0 at any time.
- **Interval between ping:** The time between twice ping. The unit is minute.
- **Reconnect:** If ping failed, reconnect cell network immediately.
- **Start ping after cell up:** don't ping host until cell network is up .
- **Action when failed:** there are "Restart module" and "Restart router". "Restart module" will fix the problem from radio module, and "Restart router" will fix the problem from the whole system including radio module.

3.5.2 VRRP

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

VRRP Configuration

VRRP LAN Configuration Settings

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

- **Enable:** Enable VRRP(Virtual Router Redundancy Protocol) for LAN.
- **IP address:** Virtual IP address(es) for LAN's VRRP cluster. IP address entry can be deleted by click button , or added by click button .
- **Virtual ID:** Routers with same IDs will be grouped in the same VRRP cluster. The legal number is from 1 to 255.
- **Priority:** Router with highest priority in the same VRRP cluster will act as master. The legal number is from 1 to 255.

3.5.3 Failover (link backup)

	Failover	Advanced																						
<ul style="list-style-type: none"> Status System Services <ul style="list-style-type: none"> ICMP Check VRRP Failover DTU SNMP Modbus GPS SMS DDNS Connect Radio Module NMS Captive Portal WEB Filter VPN Network Logout 	<h2>Failover Configuration</h2> <div style="background-color: #4f7942; color: white; padding: 5px;"> <h3>Failover Settings</h3> </div> <table border="1"> <tr> <td>Enable</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Back To High priority</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Current interface</td> <td>primary</td> </tr> </table> <div style="background-color: #4f81bd; color: white; padding: 5px;"> <h3>Primary Configuration</h3> </div> <table border="1"> <tr> <td>Primary</td> <td>Wired_wan</td> </tr> <tr> <td>Host1 to ping</td> <td></td> </tr> <tr> <td>Host2 to ping</td> <td></td> </tr> <tr> <td>IPV6</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Ping timeout</td> <td>1</td> </tr> <tr> <td>Max Retries</td> <td>10</td> </tr> <tr> <td>Interval between ping</td> <td>30</td> </tr> <tr> <td>NAT</td> <td>Default</td> </tr> </table>		Enable	<input type="checkbox"/>	Back To High priority	<input checked="" type="checkbox"/>	Current interface	primary	Primary	Wired_wan	Host1 to ping		Host2 to ping		IPV6	<input type="checkbox"/>	Ping timeout	1	Max Retries	10	Interval between ping	30	NAT	Default
Enable	<input type="checkbox"/>																							
Back To High priority	<input checked="" type="checkbox"/>																							
Current interface	primary																							
Primary	Wired_wan																							
Host1 to ping																								
Host2 to ping																								
IPV6	<input type="checkbox"/>																							
Ping timeout	1																							
Max Retries	10																							
Interval between ping	30																							
NAT	Default																							

- **Enable:** Enable failover feature
- **Back to high priority:** If back to high priority is checked, when the high priority interface is available, using the high priority interface as WAN port.
If back to high priority is unchecked, even if the high priority interface is available, router will keep current interface as WAN port, it won't switch to high priority interface.
Primary/Secondary/Third: interface which can be treat as WAN port. There are 4 options, Wired-WAN, Wi-Fi client, Cell mobile, and None.
- **Host 1 to ping / Host 2 to ping:** It is external IP address or domain name for checking the connection is available.
- **Ping timeout:** If ping packet is sent, the response packet is not received before timeout, then this ping is failed.
- **Max retries:** If the ping is failed, the failed counter will add one. If the failed counter is bigger or

equal to the Max retries, then system will say this interface is unavailable.
If the ping is succeeding, failed counter will be reset to 0 at anytime.

- **Interval between ping:** The time between twice ping. The unit is second.

3.5.4 DTU

Notes:

- 1) This feature is for H685 with DTU option only.
- 2) This feature is conflict with “Connect Radio module” and “GPS send to serial”. Please disable the “DTU” feature if use “Connect Radio Module” or “GPS send to serial” feature.

The screenshot displays the 'DTU Configuration' page. On the left is a sidebar menu with items: Status, System, Services, ICMP Check, VRRP, Failover, DTU (highlighted), SNMP, Modbus, GPS, SMS, DDNS, Connect Radio Module, NMS, and Captive Portal. The main area has tabs for 'DTU' and 'DTU Log'. Below the title 'DTU Configuration' is a note: 'Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time'. The 'General Settings' section contains the following configuration items:

- Enable:** A checkbox that is currently unchecked.
- Send DTU ID:** A checkbox that is currently unchecked.
- DTU ID:** A text input field containing the value '860000253B002305'.
- Send DTU ID on initial connection:** A checkbox that is currently unchecked.
- Forward delay:** A text input field containing '200', with a unit label 'milliseconds (range[10,10000])'.
- Terminate character(s):** An empty text input field.
- Debug:** A dropdown menu currently set to '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, the final user can re-write it if necessary.
- **Forward delay:** The unit is millisecond. It is delay time that forward data between serial port and network.

Serial Setting

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

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

Network Setting

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


- **Protocol:** TCP and UDP is supported
- **Service mode:** Client and Server is supported.
- **Enable heartbeat:** The heartbeat is used for connection keep alive.
- **Heartbeat interval:** The time between two heartbeat packet.
- **Heartbeat content:** The content of heartbeat packet.
- **DTU center Configuration:** DTU center is the DTU server, the final user can input the center name and click button “Add” to add a new center here.
- **If the center is not needed, the final user can click button “Delete” to delete it, or set it to disabled.**

Notes:

The maximum number of DTU center is 32.


3.5.5 SNMP



- **Enable SNMP:** Enable SNMP feature
- **Remote Access:** Allow remote access SNMP. If it is unchecked, only LAN subnet can access SNMP.
- **Contact:** Set the contact information here
- **Location:** set router's installation address.
- **Name:** Set the router's in SNMP
- **Port:** SNMP service port, the default value is 161.

 **SNMP v1 and v2c Settings**

Get Community	<input type="text" value="public"/>
Get Host/Lan	<input type="text" value="0.0.0.0/0"/>
Set Community	<input type="text" value="private"/>
Set Host/Lan	<input type="text" value="0.0.0.0/0"/>
SNMPv1 only	<input type="checkbox"/>

- **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 we set all as 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 we set all as 0.0.0.0./0

 **SNMP v3 Settings**

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

- **User:** SNMPv3 username
- **Security Mode:** three options: None, private and Authorized. If it is set to None, there is no password required. If it is set to Authorized, only Authentication method and password 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

- **Enable:** please check it once you need use GPS feature.
- **Only GPRMC:** if check it, only send GPRMC data info (Longitude Latitude altitude)
- **Prefix SN No.:** if check it, add the router SN to the data packet
- **Send interval:** configure the frequency time of updated GPS data packet sending
- **GPS Send to:** Choose “Serial” or “TCP/IP” method. The router only receives the GPS signal, will not process it. It will just send the received GPS signal to your GPS processor devices or servers.

If the GPS processor device is connected to the H685 Router via Serial Port, please choose “Serial”.

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

➤ **GPS to TCP/UDP Settings**

- **Server IP:** fill in the correct destination server IP or domain name
- **Server port:** fill in the correct destination server port

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

- **serial baudrate:** 9600/19200/38400/57600/115200bps for choice
- **serial parity:** none/odd/even for choice
- **serial databits:** 7/8 for choice
- **serial stopbits:** 1/2 for choice
- **serial flow control:** none/hardware/software for choice

3.5.7 SMS

➤ **SMS Command**

	SMS Command	SMS Alarm	Phone Number	SMS	SMS Gateway	DIO Mail	DIO Default	DIO sms																										
<ul style="list-style-type: none"> Status System Services <ul style="list-style-type: none"> ICMP Check VRRP Failover DTU SNMP Modbus GPS SMS DDNS Connect Radio Module NMS Captive Portal WEB Filter VPN Network Logout 	<h2>SMS Command</h2> <div style="background-color: #4f7942; color: white; padding: 5px; margin-bottom: 10px;">SMS Command</div> <table border="1"> <tr> <td>Enable</td> <td><input type="checkbox"/></td> </tr> <tr> <td>SMS ACK</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Fix error for some network</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Password access</td> <td><input type="checkbox"/></td> </tr> <tr> <td>SMSC</td> <td><input type="text"/></td> </tr> <tr> <td>Reboot Router Command</td> <td><input type="text" value="reboot"/></td> </tr> <tr> <td>Get Cell Status Command</td> <td><input type="text" value="cellstatus"/></td> </tr> <tr> <td>Set Cell link-up Command</td> <td><input type="text" value="cellup"/></td> </tr> <tr> <td>Set Cell link-down Command</td> <td><input type="text" value="celldown"/></td> </tr> <tr> <td>DIO_0 Set Command</td> <td><input type="text" value="dio01"/> Set DIO0</td> </tr> <tr> <td>DIO_0 Reset Command</td> <td><input type="text" value="dio00"/> Reset DIO0</td> </tr> <tr> <td>DIO_1 Set Command</td> <td><input type="text" value="dio11"/> Set DIO1</td> </tr> <tr> <td>DIO_1 Reset Command</td> <td><input type="text" value="dio10"/> Reset DIO1</td> </tr> </table>								Enable	<input type="checkbox"/>	SMS ACK	<input type="checkbox"/>	Fix error for some network	<input type="checkbox"/>	Password access	<input type="checkbox"/>	SMSC	<input type="text"/>	Reboot Router Command	<input type="text" value="reboot"/>	Get Cell Status Command	<input type="text" value="cellstatus"/>	Set Cell link-up Command	<input type="text" value="cellup"/>	Set Cell link-down Command	<input type="text" value="celldown"/>	DIO_0 Set Command	<input type="text" value="dio01"/> Set DIO0	DIO_0 Reset Command	<input type="text" value="dio00"/> Reset DIO0	DIO_1 Set Command	<input type="text" value="dio11"/> Set DIO1	DIO_1 Reset Command	<input type="text" value="dio10"/> Reset DIO1
Enable	<input type="checkbox"/>																																	
SMS ACK	<input type="checkbox"/>																																	
Fix error for some network	<input type="checkbox"/>																																	
Password access	<input type="checkbox"/>																																	
SMSC	<input type="text"/>																																	
Reboot Router Command	<input type="text" value="reboot"/>																																	
Get Cell Status Command	<input type="text" value="cellstatus"/>																																	
Set Cell link-up Command	<input type="text" value="cellup"/>																																	
Set Cell link-down Command	<input type="text" value="celldown"/>																																	
DIO_0 Set Command	<input type="text" value="dio01"/> Set DIO0																																	
DIO_0 Reset Command	<input type="text" value="dio00"/> Reset DIO0																																	
DIO_1 Set Command	<input type="text" value="dio11"/> Set DIO1																																	
DIO_1 Reset Command	<input type="text" value="dio10"/> Reset DIO1																																	

- **Enable:** check it to enable SMS command feature.
- **SMS ACK:** If checked, the router will send command feedback to sender's phone number. If unchecked, the router will not send command feedback to sender's 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 checking" operation, default is "cellstatus". For example, if we send "cellstatus" to router, router will feedback the status to sender such as "Router SN: 086412090002 cell_link_up", which indicated the router SN number and Cell Working Status.
- **Set cell link-up Command:** input the command for "router cell link up" operation, default is "cellup". If router gets this command, the Router Cell will be online.
- **Set cell link-down Command:** input the command for "router cell link down" operation, default is "celldown". If router gets this command, the Router Cell will be offline.
- **DIO_0 Set Command:** input the command for I/O port 0. For SMS feature, please keep the parameter default.
- **DIO_0 Reset Command:** input the command for I/O port 0. For SMS feature, please keep the parameter default.

- **DIO_1 Set Command:** input the command for I/O port 1. For SMS feature, please keep the parameter default.
- **DIO_1 Reset Command:** input the command for I/O port 1. For SMS feature, please keep the parameter default.
- **DIO Status Command:** input the command for I/O port status. For SMS feature, please keep the parameter default.
- **Wifi on Command:** input the command for turning on Wifi. For SMS feature, please keep the parameter default.
- **Wifi off Command:** input the command for turning off Wifi. For SMS feature, please keep the parameter default.

➤ **SMS alarm**

SMS Command	SMS Alarm	Phone Number	SMS	SMS Gateway	DIO Mail	DIO Default	DIO sms
<h2>SMS Alarm</h2>							
General Settings							
SMS Alarm		<input type="checkbox"/>					
RSSI Alarm Settings							
Signal Alarm							
Enable Signal Quality Alarm		<input type="checkbox"/>					
Singal Quality Threshold		<input type="text" value="1"/>					
Failed Times Threshold		<input type="text" value="5"/>					
Success Times Threshold		<input type="text" value="2"/> ▼					
<input type="button" value="Save"/>							

- **SMS Alarm:** enable SMS alarm feature
- **Enable Signal Quality Alarm:** enable Signal Quality Alarm feature
- **Signal Quality Threshold:** When signal alarm is generated, if realtime signal strength is lower than Singal Quality Threshold, reset success counter to 0. If realtime signal strength is bigger than this threshold, success counter will add one.
When signal alarm is not generated, if realtime signal strength is lower than Singal

Quality Threshold, failed counter will add one. If realtime signal strength is bigger than this threshold, reset failed counter to 0.

- **Failed Times Threshold:** if failed counter is more than this threshold, a signal alarm will be generated.
- **Success Times Threshold:** if an signal alarm is generated, and the success counter is bigger or equal to Success Times Threshold, clear signal alarm.

➤ Phone Number

SMS Command	SMS Alarm	Phone Number	SMS	SMS Gateway	DIO Mail	DIO Default	DIO sms
-------------	-----------	---------------------	-----	-------------	----------	-------------	---------

Phone Number

☰ Phone Number Configuration

NUM1 Delete

SMS Command

SMS Alarm

DIO change

Phone Number

New group name Add

Save

- **Add Phone number:** input a name and click button “Add” to add a new Phone 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 Alarm.
- **DIO change:** this phone number can receive DIO voltage changing event.

➤ SMS

SMS log, all received and sent SMS are in the list.

SMS Log



Clear SMS log

➤ SMS Gateway

Read or Send SMS via URL.

- **Send SMS:** For example, URL to send SMS:

http://192.168.1.1/cgi-bin/sms_send?username=user2&password=abc123&text=test%20get%20to%20send%20message&number=0123456789

Username: it is the username configured in SMS Gateway page.

Password: it is the password configured in SMS Gateway page.

Text: it is SMS content.

Number: it is the SMS receiver phone number.

- **SMS sending response status:**

http://192.168.1.1/cgi-bin/sms_response?username=user2&password=abc123

- **Read SMS:**

http://192.168.1.1/cgi-bin/sms_list?username=user2&password=abc123.

➤ DIO Mail

SMS Command	SMS Alarm	Phone Number	SMS	SMS Gateway	DIO Mail	DIO Default	DIO sms
-------------	-----------	--------------	-----	-------------	----------	-------------	---------

Mail Configuration

Send email to specified address when DIO changed

☰ Account Settings

Enable	<input type="checkbox"/>
SMTP server	<input type="text"/>
Port	<input type="text" value="25"/>
Username/Account	<input type="text"/>
SMTP Authentication	<input checked="" type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password"/>
TLS	<input type="text" value="On"/>
StartTLS	<input type="text" value="Off"/>
Check server certificate	<input type="text" value="Off"/>

- **Enable:** enable DIO change notice via email.
- **SMTP server:** the sender SMTP server.
- **Username/Account:** the sender email address.
- **SMTP Authentication:** if the sender need username/password to login SMTP server, then enable it.
- **TLS:** Enable or disable TLS (also known as SSL) for secured connections.
- **StartTLS:** Choose the TLS variant: start TLS from within the session ('on', default), or tunnel the session through TLS ('off').
- **Check server certificate:** Check server certificate.
- **TLS trust file:** Activate server certificate verification using a list of trusted Certification Authorities (CAs).
- **Mail format:** the mail title and content are user-defined or use device default.
- **DIO_X name:** DIO_X name in mail.
- **Receiver Configuration:** config receiver email addresses.

➤ DIO Default

SMS Command

SMS Alarm

Phone Number

SMS

SMS Gateway

DIO Mail

DIO Default

DIO sms

DIO Configuration

☰ DIO Settings

DIO trap	<input type="checkbox"/>
Set DIO to high for a period of time	<input type="text" value="0"/> s
DIO_0 direction	Output ▼
DIO_1 direction	Output ▼
DIO_2 direction	Output ▼
DIO_3 direction	Output ▼
DIO_0 default value	Low ▼
DIO_1 default value	Low ▼
DIO_2 default value	Low ▼

- **DIO trap**: send SNMP trap when DIO changed from 1 to 0, or 0 to 1.
- **Use SNMPv1**: the trap is SNMPv1 or SNMPv2.
- **Set DIO to high for a period of time**: If the value is bigger than 0, when DIO is set to high, it will go to low automatically after the value seconds. value 0 means disable.
- **DIO_X direction**: set DIO_X direction: Input or output.
- **DIO_X default value**: when DIO_X direction is out, set the default value to 1(High) or Low(0).
- **DIO_X Value**: DIO_X current is high(1) or low(0).
- **DIO_X Input Function**: DIO value set high to turn on functionality, set low to turn off it.
- **DIO_X Output Function**: toggle DIO status to other functionality, such as if cell is up, turn on DIO. Cell is down, turn off DIO.

➤ DIO SMS

SMS Command

SMS Alarm

Phone Number

SMS

SMS Gateway

DIO Mail

DIO Default

DIO sms

DIO SMS configuration

send user defined SMS alarm when DIO changed

DIO SMS Settings

Enable self-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

- **Enable self-defined DIO SMS alarm:** use self-defined DIO sms contact when DIO changed is enabled.
- **SMS text for DIOX changed from low to high:** Max. length is 64 characters.
- **SMS text for DIOX changed from high to low:** Max. length is 64 characters.

3.5.8 DDNS

DDNS allows that router can be reached with a fixed domain name while have 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	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	-----	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
myddns_ipv6	yourhost.example.com no data	<input type="checkbox"/>	never Disabled	-----	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

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] 3322.org

Hostname/Domain yourhost.example.com

Username your_username

Password

Use HTTP Secure

- **Enabled:** enable this instance.
- **IP address version:** IPv4 and IPv6 supported
- **DDNS Service provider:** select a suitable provider.
- **Hostname/Domain:** the Domain name that you can access router.

Dynamic DNS

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

Details for: **example_ipv4**

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

IP address source [IPv4]	Network
Network [IPv4]	ifmobile
DNS-Server	mydns.lan
Log to syslog	Notice
Log to file	<input checked="" type="checkbox"/>

Back to Overview Save

- **IP address source:** Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider. The recommend option is network.
- **Network:** Defines the network to read systems IPv4-Address from.
- **DNS-server:** OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'. IP address and domain name is required.
- **Log to syslog:** Writes log messages to syslog. Critical Errors will always be written to syslog.
- **Log to file:** Writes detailed messages to log file. File will be truncated automatically.

Dynamic DNS

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

☰
Details for: **example_ipv4**

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
Check Interval		<input style="width: 80px;" type="text" value="10"/>	<input style="width: 100px;" type="text" value="minutes"/> ▼
Force Interval		<input style="width: 80px;" type="text" value="72"/>	<input style="width: 100px;" type="text" value="hours"/> ▼
Error Retry Counter		<input style="width: 150px;" type="text" value="0"/>	
Error Retry Interval		<input style="width: 80px;" type="text" value="60"/>	<input style="width: 100px;" type="text" value="seconds"/> ▼

- **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 given number of retries. The default setting of '0' will retry infinite.

Dynamic DNS

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

☰
Details for: **example_ipv4**

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
<div style="border: 1px solid #ccc; padding: 10px; min-height: 150px;"> <pre style="font-family: monospace; font-size: 0.9em; margin: 0;">/var/log/ddns/example_ipv4.log Please press [Read] button</pre> </div>			

Read the log file of DDNS.

Notes:

If use DDNS server no-ip.com, please check the " Use HTTP Secure" and put "8.8.8.8" for the DNS-Server referring to following picture.

Dynamic DNS

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

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]

3322.org

Hostname/Domain

yourhost.example.com

Username

your_username

Password

.....

Use HTTP Secure



Path to CA-Certificate

/etc/ssl/certs

Back to Overview

Save

Details for: **example_ipv4**

Basic Settings

Advanced Settings

Timer Settings

Log File Viewer

IP address source [IPv4]

Network

Network [IPv4]

ifmobile

DNS-Server

8.8.8.8

Log to syslog

Notice

Log to file

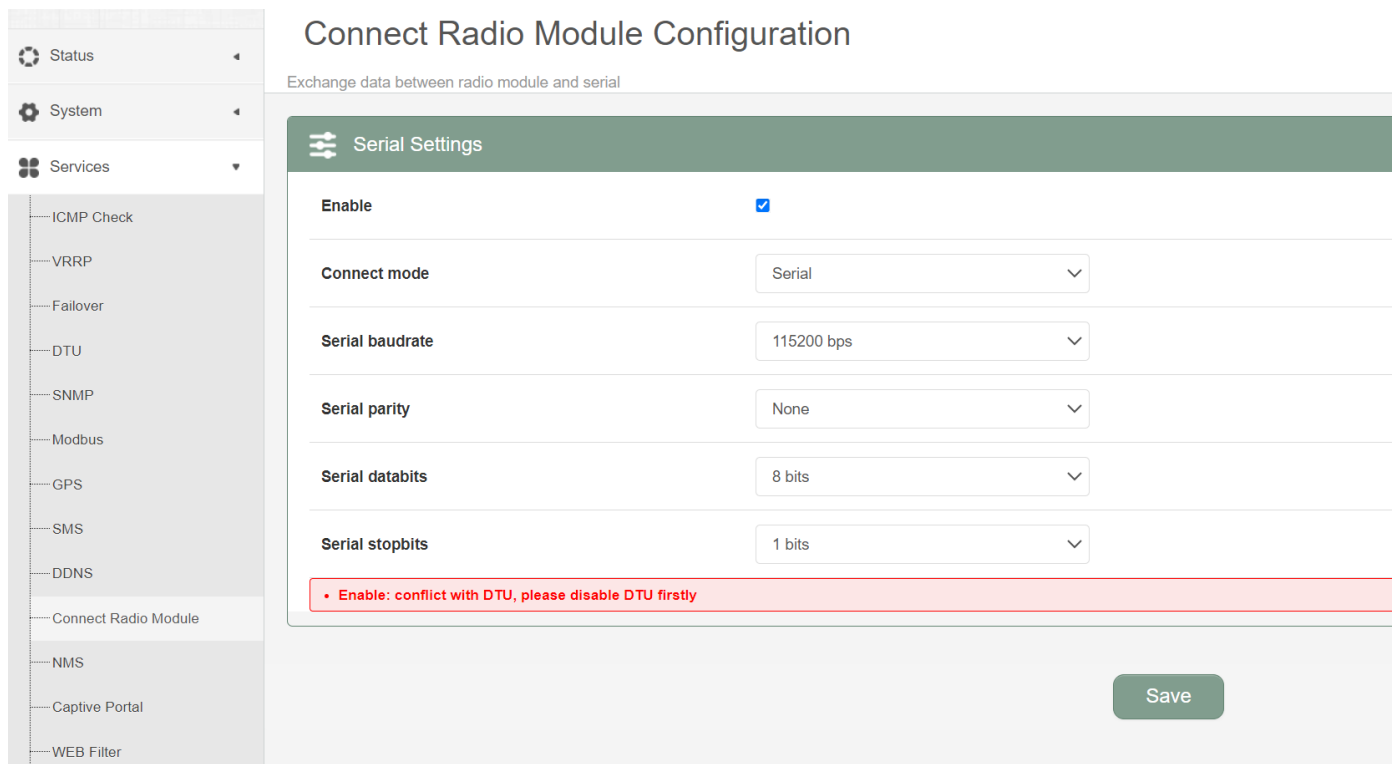


3.5.9 Connect Radio Module

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

Notes:

This feature is conflict with DTU and “GPS sent to serial”. Please make sure the other two features are disabled before enable Connect Radio Module. Otherwise this error will occur.



- **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

3.5.10 Modbus

Modbus is conflict with DTU, since both functions are using RS232 or RS485 interface of router.

Status

System

Services

- ICMP Check
- VRRP
- Failover
- DTU
- SNMP
- Modbus
- GPS
- SMS
- DDNS
- Connect Radio Module
- NMS
- Captive Portal
- WEB Filter

VPN

Network

Logout

Modbus

Modbus Log

Modbus Configuration

Notes: Modbus and DTU cannot be used at the same time

☰
Modbus

Modbus TCP to RTU Enable	<input type="checkbox"/>
Debug	<input type="text" value="2"/>
Ignore Byte Count	<input type="checkbox"/>
Serial baudrate	<input type="text" value="115200 bps"/>
Serial parity	<input type="text" value="None"/>
Serial databits	<input type="text" value="8 bits"/>
Serial stopbits	<input type="text" value="1 bits"/>
TCP server address	<input type="text" value="0.0.0.0"/>
TCP port	<input type="text" value="502"/>
Max connections	<input type="text" value="32"/>
Retries	<input type="text" value="3"/>
Pause interval	<input type="text" value="100"/>

- **Modbus TCP to RTU Enable:** Enable Modbus gateway between TCP and RTU.
- **Modbus TCP Server(Slave) Enable:** Router act as Modbus Slave also.
- **Local DIO Slave ID:** the Modbus Slave ID assigns to router.
- **Local DIO Slave Address:** the Address assigns to router DIO.
- **DIO 0:** DIO 0 acts as Input or output.
- **DIO 1:** DIO 1 acts as Input or output.
- **DIO 2:** DIO 2 acts as Input or output.
- **DIO 3:** DIO 3 acts as Input or output.
- **Debug:** from 1 to 7, default is 2. 7 means all logs.
- **Ignore Byte Count:** ignore byteCount field in modbus package.
- **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.
- **TCP server address:** Binding IP address on modbus TCP, the default value 0.0.0.0 means any router IPs.
- **TCP port:** TCP server port number.
- **Max connections:** Maximum number of simultaneous TCP connections.

- **Retries:** Maximum number of request retries. 0 - without retries.
- **Pause interval:** Pause between requests in milliseconds.
- **Response wait:** Response wait time in milliseconds.
- **Connect timeout:** Connection timeout value in seconds. 0 - no timeout.

3.5.11 NMS

Network Management System: upload device status to NMS and sync configurations with NMS.

NMS

NMS Settings

Enable

Local Interface

Device ID

URL

Password

Get config interval minutes

Send status interval minutes

NMS Version

Status

Save

- **Local Interface:** Local interface or IP Addr. for NMS access.
- **Device ID:** device ID in NMS.
- **URL:** NMS URL to communicate with devices.
- **Password:** password for NMS communication.
- **Get config interval:** interval to get config from NMS.
- **Send status interval:** interval to send device status to NMS, set 0 to disable it.

3.5.12 Captive Portal

➤ Remote Auth

Use remote Radius server to authenticate hotspot.

Remote Auth

Local Auth

Remote Hotspot Configuration

General Settings

Enable

AP IP addr

Radius server 1

Radius server 2

Authentication port

Radius account port

Radius secret

Radius NAS ID

Location ID

Location name

UAM port	<input type="text" value="3990"/>
UAM UI port	<input type="text" value="4990"/>
UAM secret	<input type="text"/>
Login URL	<input type="text"/>
DNS 1	<input type="text" value="8.8.8.8"/>
DNS 2	<input type="text" value="8.8.4.4"/>
Wi-Fi SSID	<input type="text" value="Cell_AP_018aa5"/>
Debug	<input type="checkbox"/>

Allow access list without authentication

Enabled	Address	Allow subdomains	
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>

- **Enable:** Enable Captive portal.
- **AP IP addr:** The IP address of the router on the hotspot network..
- **Radius server:** IP address of radius server.
- **Authentication port:** The UDP port number to use for radius authentication requests.
- **Radius account port:** The UDP port number to use for radius accounting requests.
- **Radius secret:** Radius shared secret for both servers.
- **Radius NAS ID:** Radius NAS-Identifier.
- **Location ID:** "WISPr Location ID. Should be in the format: isocc=(ISO_Country_Code),cc=(E.164_Country_Code),ac=(E.164_Area_Code),network=(ssid/ZONE).
- **Location name:** WISPr Location Name. Should be in the format: HOTSPOT_OPERATOR_NAME,LOCATION.
- **UAM port:** TCP port to listen to for authentication requests.
- **UAM UI port:.**
- **UAM secret:** Shared between device and authentication web server.
- **Login URL:** URL of web server handling authentication.
- **DNS:** Domain Name server.
- **Wi-Fi SSID:** the Wi-Fi SSID provides network service.

➤ **Local Auth**

Remote Auth Local Auth

Local Hotspot Configuration

Hotspot authenticate client via password.

General Settings

Enable	<input type="checkbox"/>
AP IP addr	<input type="text"/>
Enable password	<input type="checkbox"/>
Session Timeout	<input type="text" value="0"/> second(s)
DNS 1	<input type="text" value="8.8.8.8"/>
DNS 2	<input type="text"/>
Wi-Fi SSID	<input type="text"/>
Redirect URL	<input type="text"/>
Web Filter	<input type="checkbox"/>

Account Settings

Username	Password
----------	----------

This section contains no values yet

Add

Logo Picture

Enable

Background Picture

Enable

Login button

Enable

- **AP IP addr:** The IP address of the router on the hotspot network, such as 192.168.5.254/24.
- **Enable password:** only password needed to access hotspot.
- **Session Timeout:** Session remains time in seconds. Set it to 0 the session never

E-Lins Technology Co. Limited

Tel: +86-755-29230581 E-mail: sales@e-lins.com www.e-lins.com

timeout.

- **DNS:** Domain Name server.
- **Redirect URL:** Redirect to URL after logon successful.
- **Web Filter:** Enable web filter.
- **URLs:** URL list for block/allow.
- **Account Settings:** set username/password to access hotspot.
- **Logo Picture:** upload picture as portal web UI logo.
- **Background Picture:** upload picture as portal web UI bakground.
- **Login button:** set portal web UI login button.

3.5.13 WEB Filter

Proxy Web Filter

Support HTTP filtering only.

Configuration Log File Viewer

Enable

Listen address

Listen port

Allowed clients

Filter mode

URLs


Save

- **Listen address:** Specifies the LAN IP address proxy is listening on for requests.
- **Listen port:** Specifies the HTTP port proxy is listening on for requests.
- **Allowed clients:** List of IP addresses or ranges which are allowed to use the proxy server.
- **Filter mode:** Black list or White list.
- **URLs:** URL list for block/allow.

Proxy Web Filter

Web Filter

Web Filter

 Support HTTP and HTTPS filtering.


Enable	<input type="checkbox"/>
Filter Method	Keyword Web Filter
Filter mode	Black list
URLs	<input type="text"/>


Save





- **Filter method:** Keyword Web Filter, the specified string in URLs is allowed or denied. DNS Web Filter, the specified URLs will be allowed to be resolved or not to be resolved.
- **Filter mode:** Black list or White list.
- **URLs:** URL list for block/allow.

3.6 VPN Configuration

3.6.1 IPSEC

 General Settings

Enable	<input type="checkbox"/>
Exchange mode	<input type="text" value="IKEv1-Main"/>
Operation Level	<input type="text" value="Main"/>
Authentication method	<input type="text" value="PSK Server"/>
Remote VPN endpoint	<input type="text" value="-- Please choose --"/>
Local endpoint	<input type="text" value="-- Please choose --"/>
Local IKE identifier	<input type="text"/>
Remote IKE identifier	<input type="text"/>
Connection type	<input type="text" value="Tunnel"/>
Preshared Keys	<input type="text"/> 

DPD action	None	▼
DPD delay	30	seconds
DPD timeout	150	seconds
NAT Traversal	Enable	▼
Local source IP	<input type="text"/>	
Remote source IP	<input type="text"/>	
Additional phase1	<input type="text"/> 	
Additional phase2	<input type="text"/> 	
<hr/>		
Local LAN bypass	<input type="checkbox"/>	
Local subnet	192.168.1.0/24 	
Remote subnet	192.168.10.0/24 	

- **Enable:** enable IPSEC feature
- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main mode are supported.
- **Operation Level:** Main or Backup, Backup Means when Main IPsec is down, device will try to bring Backup IPsec up; when Main IPsec is up, set Backup IPsec down.
- **Authentication method:** PSK, Xauth or x.509 Client and Server. Client is the machine which start the IPSEC connection.
- **Remote VPN endpoint:** domain name or IP address of the remote endpoint. It can be visited from internet.
- **Local endpoint:** domain name or IP address of the device interface, device will establish IPsec tunnel with this interface.
- **Local IKE identifier:** local IKE ID, the default is empty.
- **Remote IKE identifier:** Remote IKE ID, the default is empty.
- **Connection type:** Tunnel, Transport, Transport proxy and Passthrough.
- **Preshared Keys:** it is known as PSK, the length is 16 to 32.
- **CA file:** CA certificate file.
- **Cert file:** certificate file.
- **private key file:** private key file.
-
- **Remote subnet:** the subnet of remote which connects to IPSEC VPN.
- **DPD action:** controls the use of the Dead Peer Detection protocol where DPD messages are periodically sent in order to check the liveness of the IPsec peer.
- **DPD delay:** defines the period time interval with which DPD messages exchanges are

sent to the peer.

- **DPD timeout:** defines the timeout interval, after which all connections to a peer are deleted in case of inactivity. It must be bigger than DPD delay.
- **Local source IP:** the internal source IP to use in a tunnel for local peer, also know as virtual IP.
- **Remote source IP:** the internal source IP to use in a tunnel for the remote peer.
- **DNS:** Comma separated list of DNS server addresses to exchange as configuration attributes.
- **Remote auth:** Authentication method to require from the remote (right) side.
- **Additional phase1:** Additional phase 1 proposal, such as: aes128-sha1-modp1024.
- **Additional phase2:** Additional phase 2 proposal, such as: aes128-sha1-modp1536
- **NAT Traversal:** the subnet of remote which connects to IPSEC VPN.
- **Local subnet:** the subnet of local which connects to IPSEC VPN.
- **Remote subnet:** the subnet of remote which connects to IPSEC VPN.

Phase 1 Proposal

Enable	<input checked="" type="checkbox"/>
Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds

Phase 2 Proposal

Enable	<input checked="" type="checkbox"/>
Encryption algorithm	AES 128
PFS group	MODP1024/2
Authentication	HMAC_SHA1
Life time	3600 seconds

Notes:

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

3.6.2 IPsec Track

IPsec Track

IPsec Track

Enable

Host1 to ping ipv4 or hostname

Host2 to ping

the source interface for tracking ▾

Ping timeout seconds (range [1 - 10])

Max retries (range [3 - 1000])

Interval between ping seconds (range [1 - 1440])

Action ▾

3.6.3 PPTP

Point-to-Point Tunneling Protocol

PPTP Configuration

Name	Type	Enable	
	Server	No	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New instance name: Role: ▾


▾

PPTP NAT enable

This page is a list of configured PPTP instance and their state. The final user can click button “Edit” to modify it, or click button “Delete” to delete an instance.

➤ **PPTP Client configuration**

PPTP Client Instance: Aaaa

General 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"/>
Local tunnel IP	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text"/>
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>
Refuse PAP	<input type="checkbox"/>
Refuse EAP	<input type="checkbox"/>
Refuse CHAP	<input type="checkbox"/>
Refuse MS-CHAP	<input type="checkbox"/>
MPPE Encryption	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>
Restart module when PPTP connects failed	<input checked="" type="checkbox"/>

- **Enable:** enable this instance.
- **Server:** domain name or IP address of PPTP server.
- **Username:** server authentication user name.
- **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.
- **Refuse PAP:** With this option, will not agree to authenticate itself to the peer using PAP.
- **Refuse EAP:** With this option, will not agree to authenticate itself to the peer using EAP.
- **Refuse CHAP:** With this option, will not agree to authenticate itself to the peer using CHAP.
- **MPPE Encryption:** Require the use of MPPE (Microsoft Point to Point Encryption). This option disables all other compression types. This option enables both 40-bit and 128-bit encryption. In order for MPPE to successfully come up, you must have authenticated with either MS-CHAP or MS-CHAPv2. This option is presently only supported under Linux, and only if your kernel has been configured to include MPPE support.
- **Debug:** Enabled debug will print detail log in system log.

➤ PPTP Server Configuration

☰
General Settings

Enable	<input type="checkbox"/>
PPTP Local IP	<input type="text" value="192.168.0.1"/>
PPTP remote IP start	<input type="text" value="192.168.0.20"/>
PPTP remote IP end	<input type="text" value="192.168.0.30"/>
ARP Proxy	<input type="checkbox"/>
MPPE Encryption	<input checked="" type="checkbox"/>
IPCP-accept-remote	<input type="checkbox"/>
Debug	<input type="checkbox"/>

Username	Password	Address	Subnet	
<input type="text" value="youruser"/>	<input type="password" value="*****"/> 👁	<input type="text" value=""/>	<input type="text" value=""/>	<input type="button" value="Delete"/>

- **PPTP Local IP:** indicate server's IP address.
- **PPTP Remote IP start:** the remote IP address leases start

- **Pptp remote IP end:** the remote IP address lease end.
- **ARP Proxy:** if the remote IP has the same subnet with LAN, tick it for connecting each other.
- **MPPE Encryption:** Require the use of MPPE (Microsoft Point to Point Encryption). This option disables all other compression types. This option enables both 40-bit and 128-bit encryption. In order for MPPE to successfully come up, you must have authenticated with either MS-CHAP or MS-CHAPv2. This option is presently only supported under Linux, and only if your kernel has been configured to include MPPE support.
- **IPCP-accept-remote:** will accept the peer's idea of its (remote) IP address, even if the remote IP address was specified in an option.
- **Debug:** for PPTP server debug, the log can be monitored in system log.
- **Username:** server authentication username
- **Password:** server authentication password.
- **Address:** PPTP client IP assigned.
- **Subnet:** the subnet of PPTP client LAN.

3.6.4 L2TP

This page is a list of configured L2TP instance and their state. The final user can click button “Edit” to modify it, or click button “Delete” to delete an instance.

Layer 2 Tunneling Protocol

L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	<button>Edit</button> <button>Delete</button>


New instance name: Role: Client
Client
Server

L2TP NAT enable

➤ L2TP Client configuration

L2TP Client Instance: Bbbb

General 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"/>
Local tunnel IP	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text" value="5"/>
Checkup Interval	<input type="text" value="5"/>

Refuse PAP	<input type="checkbox"/>
Refuse EAP	<input type="checkbox"/>
Refuse CHAP	<input type="checkbox"/>
Refuse MS-CHAP	<input type="checkbox"/>
Debug	<input type="checkbox"/>

- **Enable:** enable this L2TP instance.
- **Server:** domain name or IP address of L2TP server.
- **Username:** server authentication user name.
- **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.

- **Refuse PAP:** With this option, will not agree to authenticate itself to the peer using PAP.
- **Refuse EAP:** With this option, will not agree to authenticate itself to the peer using EAP.
- **Refuse CHAP:** With this option, will not agree to authenticate itself to the peer using CHAP.
- **Refuse MS-CHAP:** With this option, will not agree to authenticate itself to the peer using MS-CHAP.
- **Debug:** Enabled debug will print detail log in system log.

➤ L2TP Server configuration

☰ General Settings

Enable	<input type="checkbox"/>
L2TP Local IP	<input type="text" value="192.168.0.1"/>
Remote IP range begin	<input type="text" value="192.168.0.20"/>
Remote IP range end	<input type="text" value="192.168.0.30"/>
DNS	<input type="text"/>
IPCP-accept-remote	<input type="checkbox"/>
Length bit	<input type="checkbox"/>
IPSec saref	<input type="checkbox"/>
ARP Proxy	<input type="checkbox"/>
Debug	<input type="checkbox"/>

Username	Password	Address	Subnet	
<input type="text" value="user"/>	<input type="password" value="****"/>	<input type="text" value="*"/>	<input type="text"/>	<input type="button" value="Delete"/>

- **Local IP:** indicate server's IP address.
- **Remote IP range begin:** the remote IP address leases start
- **Remote IP range end:** the remote IP address lease end.
- **DNS:** DNS sending to clients.
- **ARP Proxy:** if the remote IP has the same subnet with LAN, tick it for connecting each other.
- **Length bit:** If ticked, the length bit present in the L2TP packet payload will be used.
- **IPSec saref:** Use IPsec Security Association trackinging.

- **Debug:** Enabled debug will print detail log in system log.
- **Username:** server authentication username
- **Password:** server authentication password.
- **Address:** L2TP client IP assigned.
- **Subnet:** the subnet of L2TP client LAN.

3.6.5 OpenVPN

This page is a list of configured OpenVPN instance and their state. You can click button “Edit” to modify it, or click button “Delete” to delete an instance.

And you can click button “Start” or “Stop” to start or stop a specific instance.

OpenVPN

OpenVPN instances

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

New instance name: Client configuration for an ether ▼ Add

Note: for OpenVPN detail configuration page, you can put mouse on the title on item to get more help information.

If the item you needed is not show in the main page, please check the “Additional Field” dropdown list at bottom of page.

Overview » Instance "sample_server"

« Switch to basic configuration

Configuration category: **Service** | Networking | VPN | Cryptography

Service

enabled

verb

mlock

disable_occ

-- Additional Field --

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

-- Additional Field --

3.6.6 GRE tunnel

GRE Tunnel Configuration

GRE Instances

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

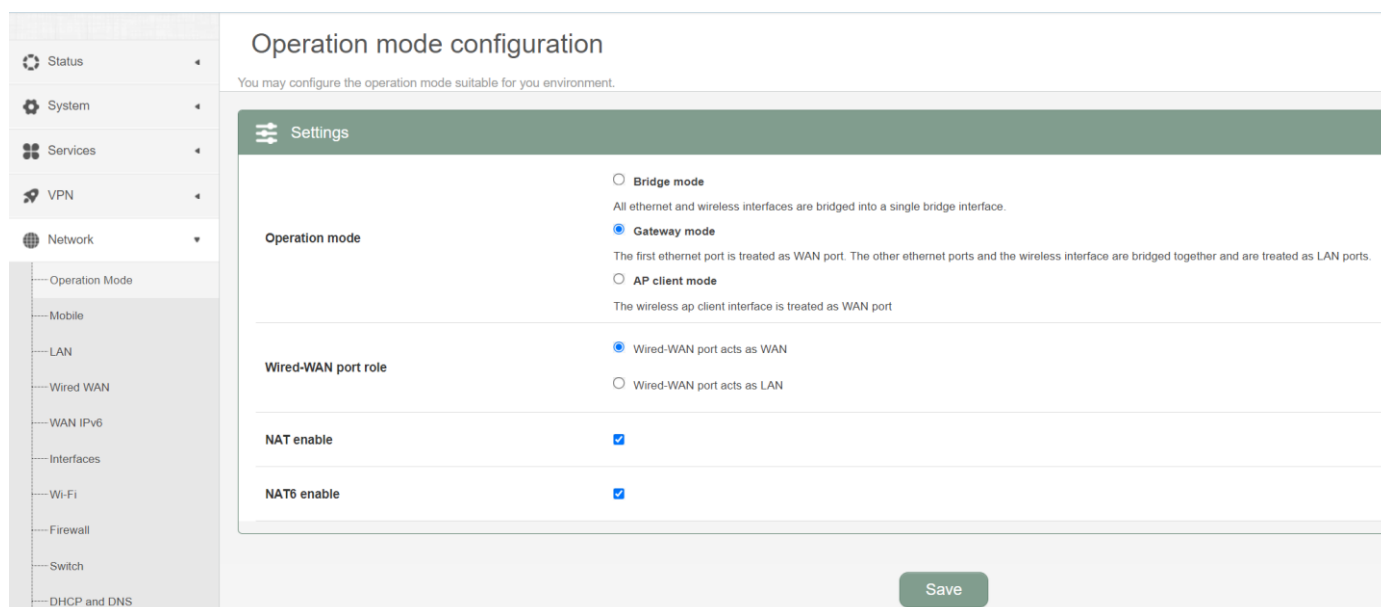
GRE Instance: Gre_tunnel

Enable	<input type="checkbox"/>
TTL	<input type="text" value="255"/>
MTU	<input type="text" value="1500"/>
Peer IP Address	<input type="text"/>
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
Metric	<input type="text" value="0"/>
Local Interface	<input type="text" value="All"/>
Local Tunnel IP	<input type="text"/>
Local Tunnel Mask	<input type="text"/>
Keepalive	<input type="text" value="None"/>

- **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, such as 192.168.100.0
- **Remote LAN Netmask:** remote LAN subnet mask, such as 255.255.255.0
- **Metric:** The metric of GRE tunnel interface.
- **Local interface:** Binding GRE tunnel to this interface.
- **Local Tunnel IP:** Virtual IP address. cannot be in same subnet as LAN network.
- **Local Tunnel Mask:** Virtual IP mask.
- **Keepalive:** Send and receive GRE tunnel keepalive message.

3.7 Network Configuration

3.7.1 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 WAN port. The other Ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- **AP Client:** The wireless apcli interface is treated as WAN port and the wireless AP interface and the Ethernet ports are LAN ports.

➤ NAT Enabled

Network Address Translation. Default is *Enabling*

➤ Ethernet wan port role:

Wired-WAN port acts as WAN

The Ethernet wan port is used as for WAN. Default is *Checked*

Wired-WAN port acts as LAN

The Ethernet wan port is used as for lan port to get 2 LAN Ethernet ports. If is WAN RJ45 Ethernet port is used for WAN, please do not check this feature.

Normally and default we select “Gateway mode”, and keep all other parameters as default.

3.7.1.1 Gets two LAN Ethernet Port for H685

Check the " Wired-WAN port acts as LAN ".

Notes:

- 1) If checked the " Wired-WAN port acts as LAN ", the H685 does not have WAN RJ45 port.

2) Please do not use any features for WAN RJ45 if check the " Wired-WAN port acts as LAN "

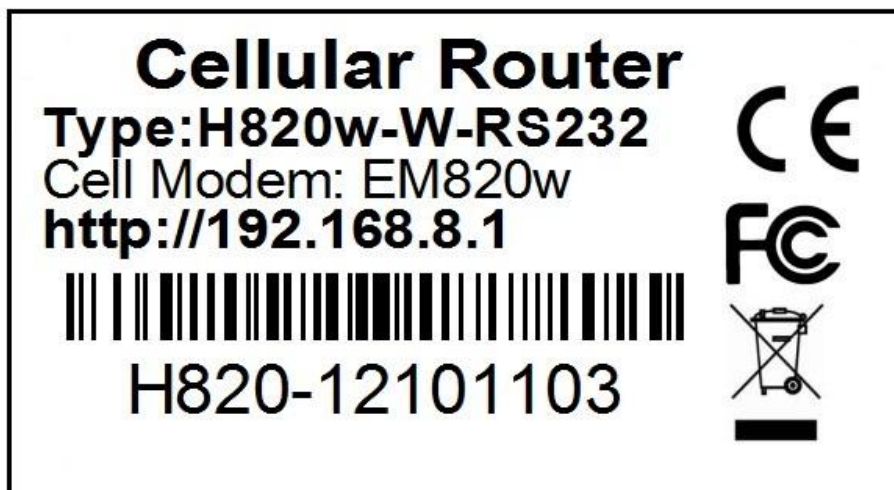
3.7.2 Mobile configuration

System supports different cell modems. Default, the router is with right Cell Modem name before shipment. If you replace with other different Cell Modem, if it is supported, the router will automatically detect the Cell Modem.

Notes:

the Cell Modem Type was marked on the back of the router.

For example, it shows the following picture. H685 is the router series name, H685w-W-RS232 is the part number name. And the EM820w Cell Modem is the Cell Modem name.



The screenshot displays the 'Mobile Configuration' page for 'SIM 1'. The interface includes a sidebar with navigation options like Status, System, Services, VPN, Network, and Logout. The main content area is titled 'Mobile Settings' and contains the following configuration items:

- Enable:** Checked (checkbox).
- Mobile connection:** DHCP mode (dropdown).
- IPv4v6:** IPv4 only (dropdown).
- IP Passthrough:** Unchecked (checkbox).
- PIN code:** (text input field).
- PUK:** (text input field).
- Dialing number:** *99# (text input field).
- APN:** ctnet (text input field).
- Authentication method:** None (dropdown).
- Dual APN support:** Unchecked (checkbox).
- Network Type:** automatic (dropdown).
- MTU:** 1500 (text input field).
- Online mode:** Keep Alive (dropdown).
- Metric:** 0 (text input field).
- IPv4 netmask:** (dropdown).
- Default route:** Checked (checkbox).

- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for mobile to connect, for the cell modem only supports 3G, the default mode is *pppd* mode, otherwise the default value is DHCP mode;
- **APN:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier;
- **PIN number:** If necessary, fill in the related parameters. Most of sim card has no PIN code, and then keep it as blank;
- **Dialing number:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier;
- **Authentication method:** Three options (None, PAP, CHAP). Please confirm your carrier provide the types of authentication. Normally select *None*. If not work, try to use *PAP* or *CHAP*;
- **Username:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier.

Notes: If your SIM card has no user name, please input out default value, otherwise the router may not dialup. Note: if the authentication method is None, this parameter will not be displayed.

- **Password:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier.

Notes: If your SIM card has no user name, please input out default value, otherwise the router may not dialup.

Note: if the authentication method is None, this parameter will not be displayed.

- **Network Type:** Select the type. Different Cell Modem supports different types. The default value is *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the max size of packet transmitted on network. The default value is 1500. Please configure it to optimize your own network.
- **Online Mode**
 - Keep Alive:** means always online. The router will keep online whatever there is data for transmission or not.
 - On Demand:** The router will dialup when there is data for transmission.
Idle time (minutes): fill in the time. For example, fill in 5, the router will offline after 5 minutes if there is no data for transmission.
 - Scheduled:** router dialup or offline with schedule. One group is supported.

3.7.3 Cell mobile data limitation

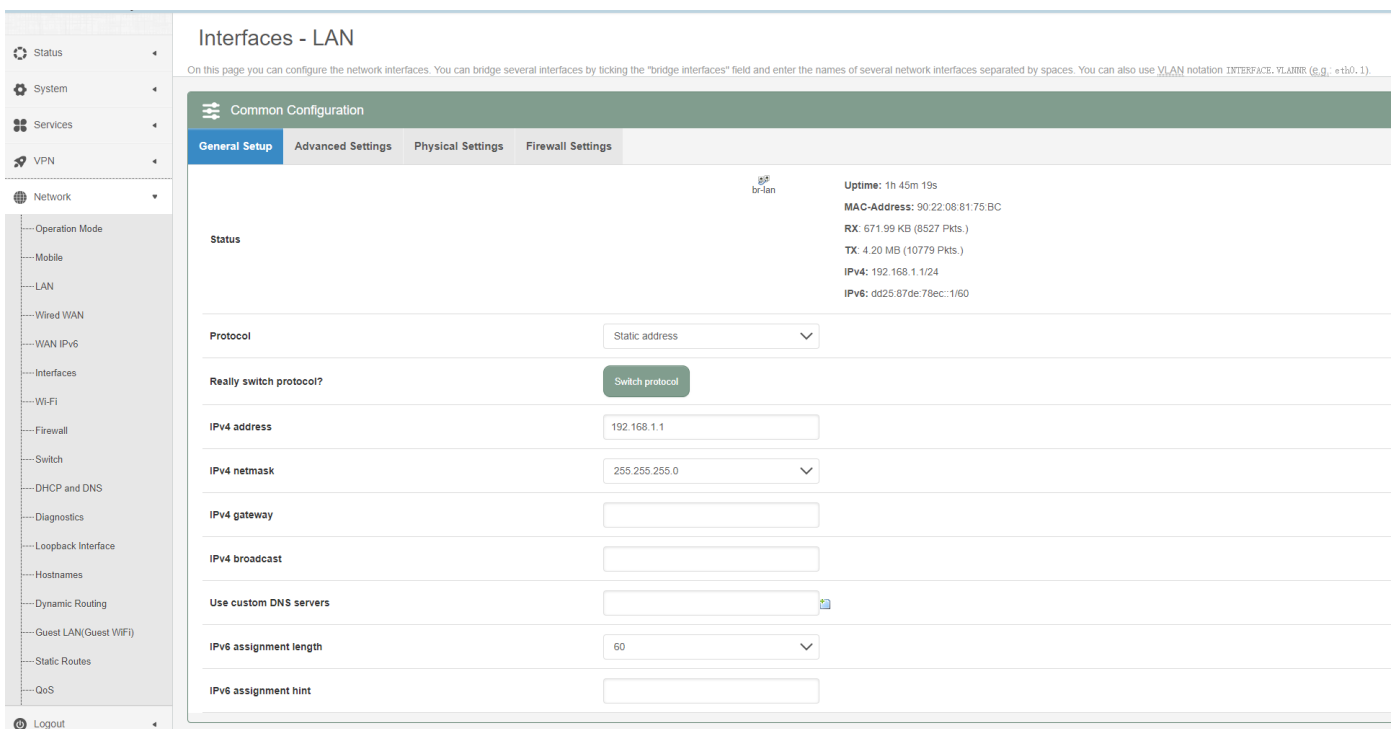
General Operator Selection **Data Limitation**

Data Limitation Configuration

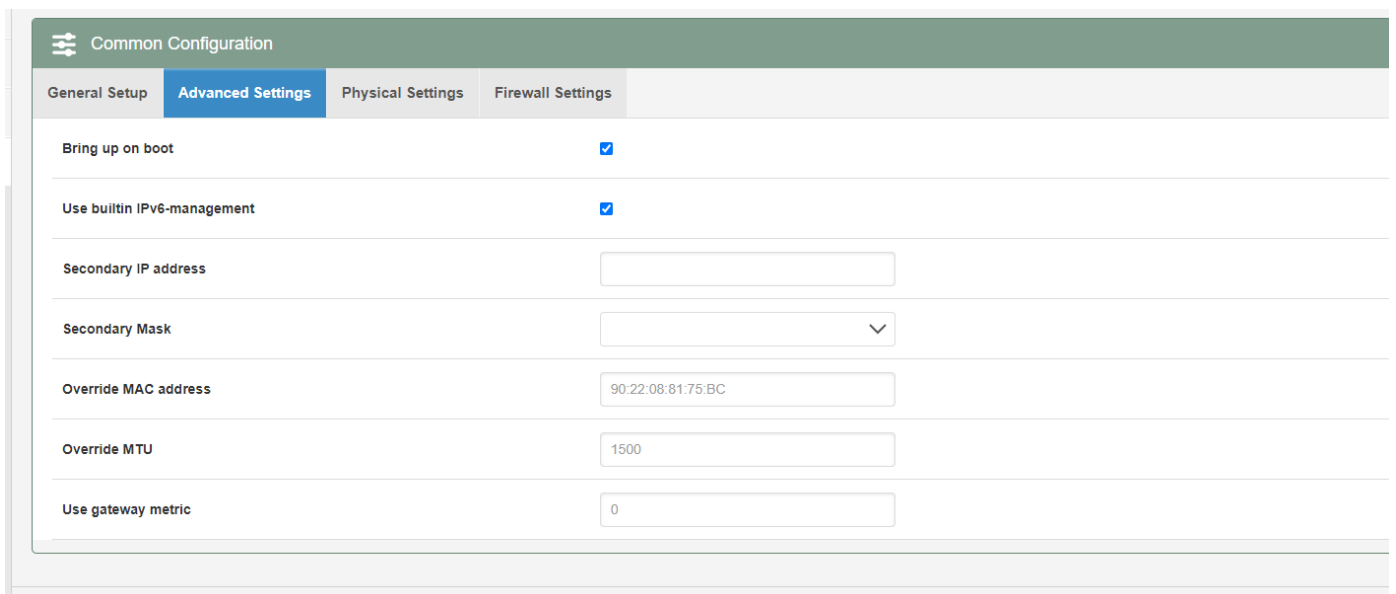
Enable data limitation	<input type="checkbox"/>
Period	Month
Start day	1
SIM data limit(MB)	0
Enable alarm	<input type="checkbox"/>
Phone number	<input type="text"/>
Warning percent of Data Used(%)	90
Used(Bytes)	0 <input type="button" value="Reset"/>
Terminate 3G/4G connection until restart time	<input checked="" type="checkbox"/>

- **Enable data limitation:**
- **Period:** support period are Month, Week and Day.
- **Start day:** the beginning day of period.
- **SIM data limit(MB):** the maximum data can be used during this period. If it exceeds, router will disable 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 has been consumed during this period.

3.7.4 LAN settings

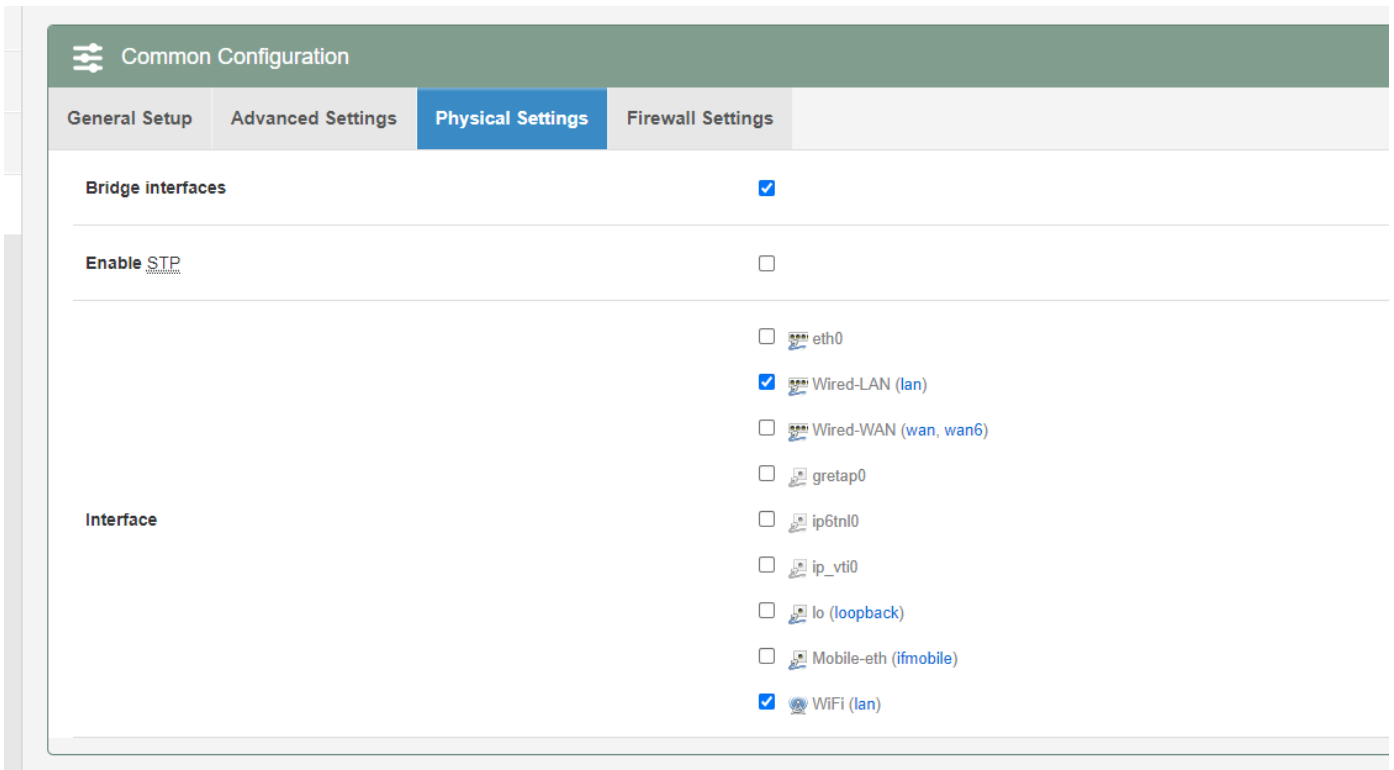


- **Protocol:** only static address is supported for LAN
- **Use custom DNS servers:** multiple DNS server supported.
- **IPv6 assignment length:** Assign a part of given length of every public IPv6-prefix to LAN interface
- **IPv6 assignment hint:** Assign prefix parts using this hexadecimal subprefix ID for LAN interface.

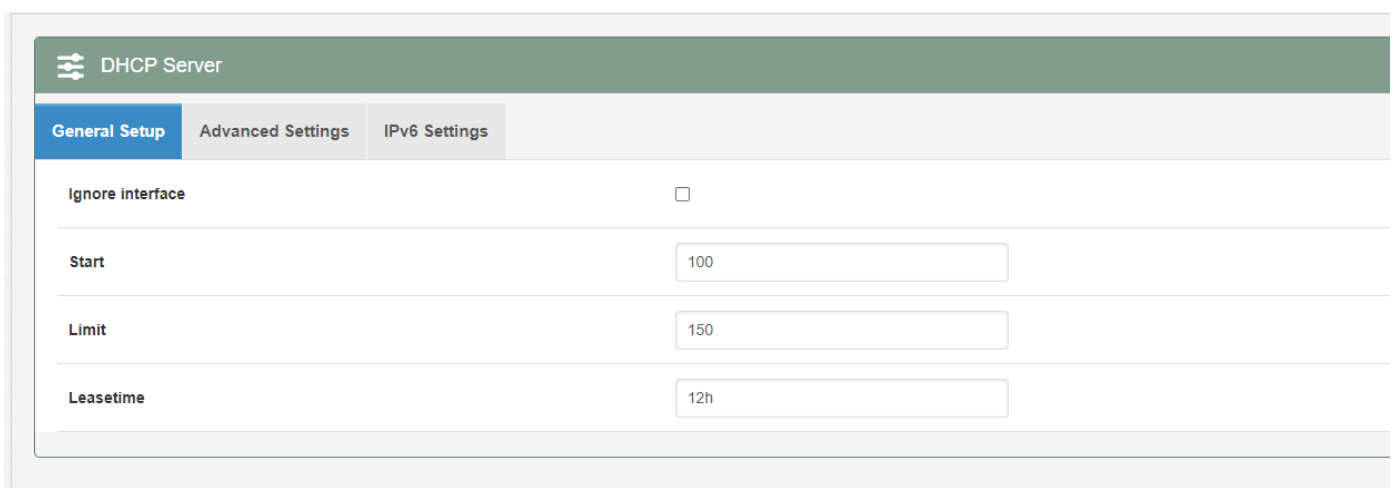


- **Bring up on boot:** if checked, LAN interface will be set to up when system bootup. If unchecked, LAN interface will be down. Don't set it to unchecked if don't have special purpose.

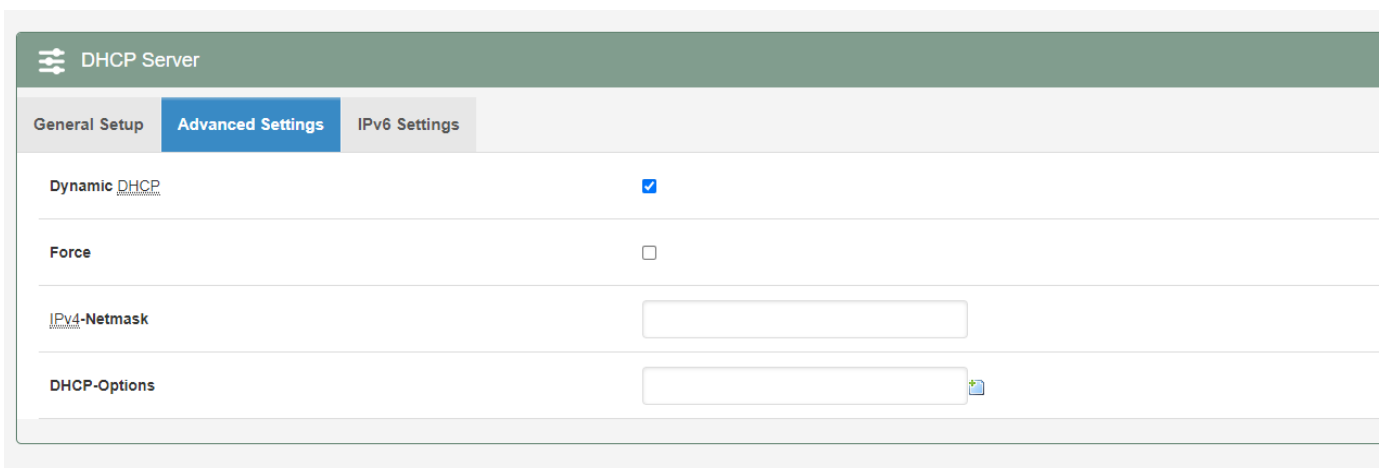
- **Use builtin IPv6-management:** the default is checked. If IPv6 is not needed, it can be set to unchecked.
- **Override MAC address:** override LAN MAC address.
- **Override MTU:** Maximum Transmission Unit.
- **Use gateway metric:** the LAN subnet's metric to gateway.



- **Bridge interfaces:** LAN bridges wired-LAN and WiFi in a same LAN subnet.
- **Enable STP:** enable Spanning Tree Protocol on LAN. The default value is unchecked.



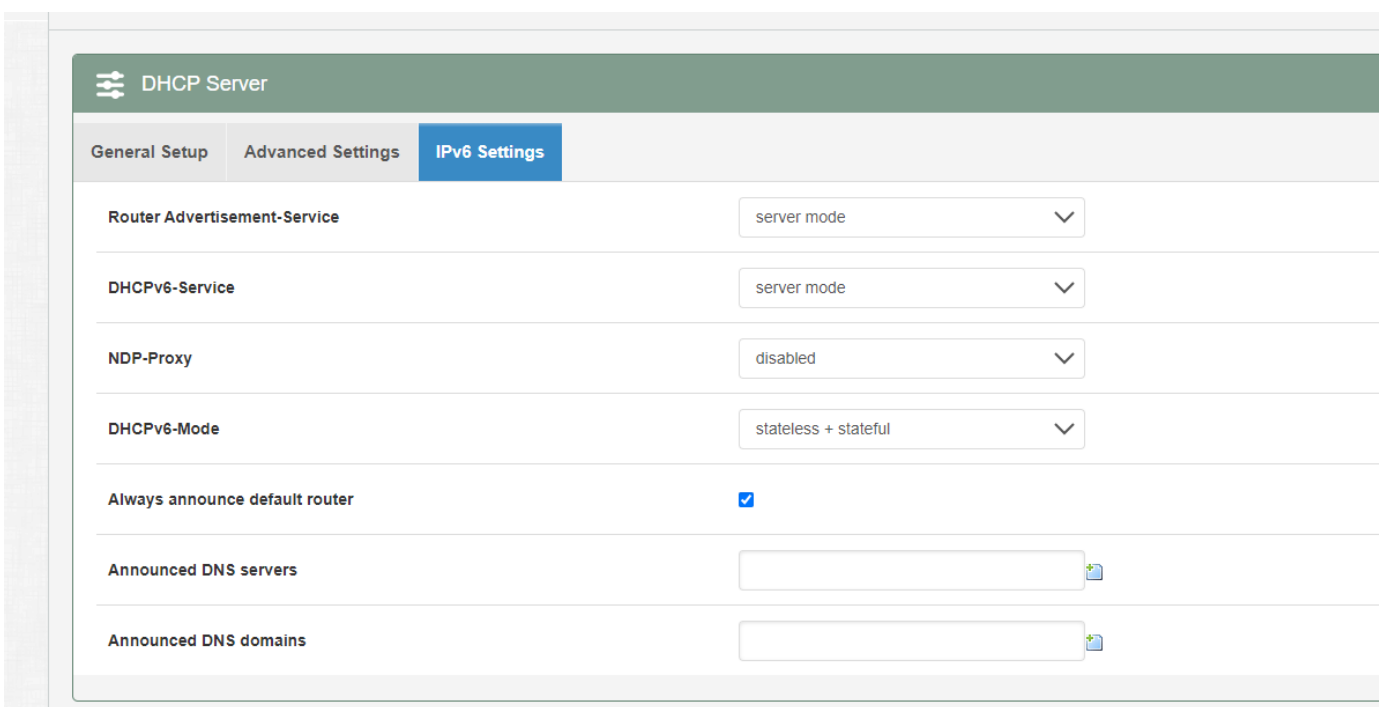
- **Ignore interface:** if it is unchecked, Disable DHCP on LAN.
- **Start:** Lowest leased address as offset from the network address.
- **Limit:** Maximum number of leased addresses.
- **Leasetime:** Expiry time of leased addresses, minimum is 2 minutes(2m). 12H means 12 hours.



The screenshot shows the 'DHCP Server' configuration page with the 'Advanced Settings' tab selected. The settings are as follows:

Setting	Value
Dynamic DHCP	<input checked="" type="checkbox"/>
Force	<input type="checkbox"/>
IPv4-Netmask	<input type="text"/>
DHCP-Options	<input type="text"/>

- **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 '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients.

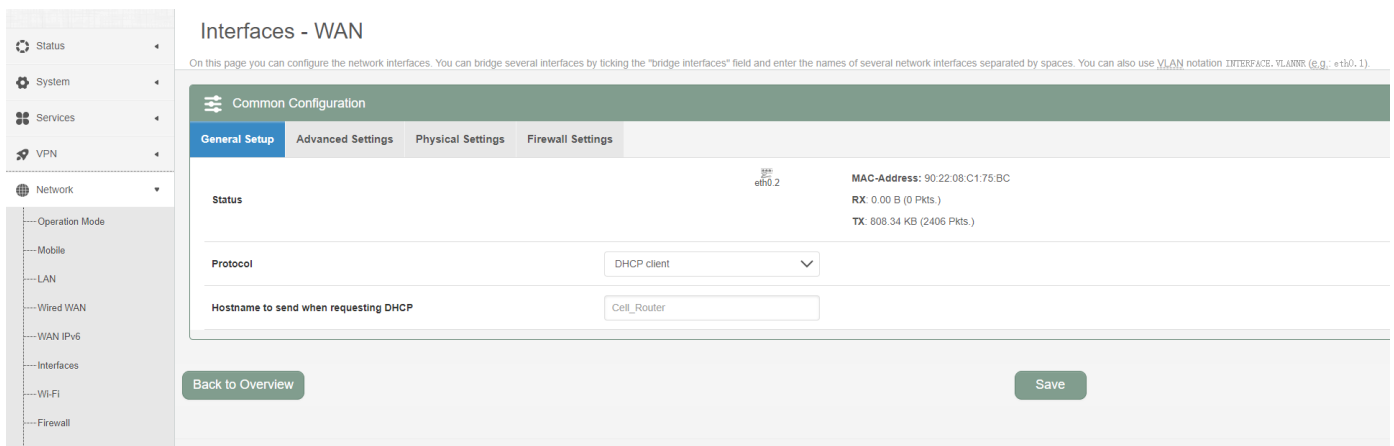


The screenshot shows the 'DHCP Server' configuration page with the 'IPv6 Settings' tab selected. The settings are as follows:

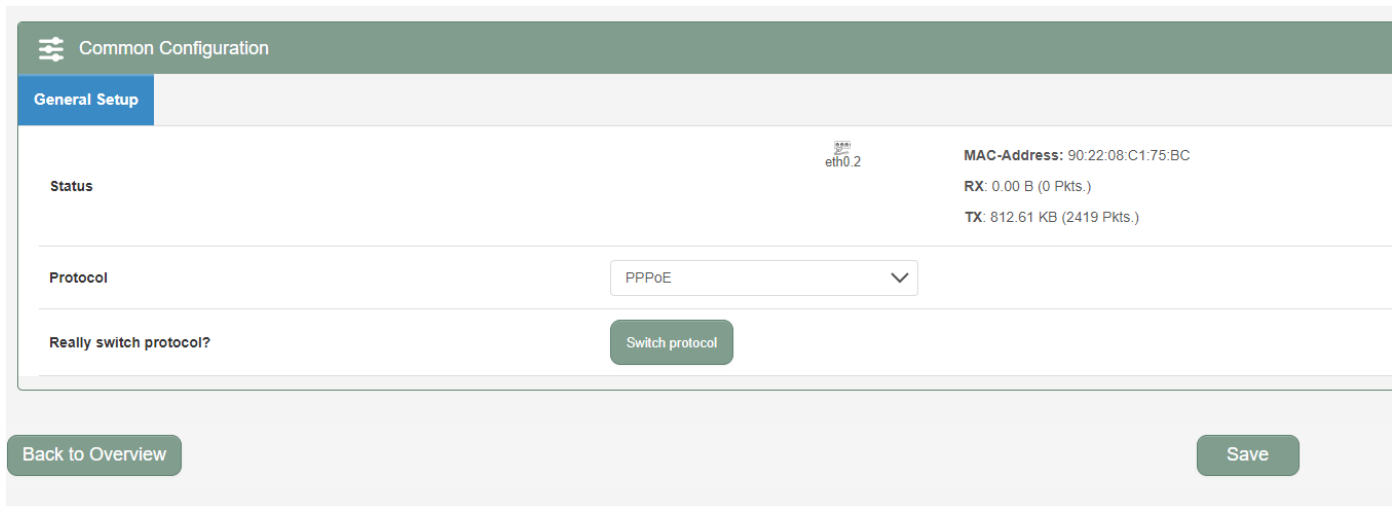
Setting	Value
Router Advertisement-Service	server mode
DHCPv6-Service	server mode
NDP-Proxy	disabled
DHCPv6-Mode	stateless + stateful
Always announce default router	<input checked="" type="checkbox"/>
Announced DNS servers	<input type="text"/>
Announced DNS domains	<input type="text"/>

- **Router Advertisement-Service:** four options: disabled, server mode, relay mode and hybrid mode.
- **DHCPv6-Service:** has same options with Router Advertisement-Service.
- **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.

3.7.5 wired-WAN



- **Protocol:** the default protocol is DHCP client. If it should be changed to other protocol, such as PPPoE, select protocol PPPoE, then click button “Switch protocol”.



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

Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status

pppoe-wan
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol

PPPoE

PAP/CHAP username

PAP/CHAP password

Access Concentrator

auto

Service Name

auto

Back to Overview

Save

Note: for different protocol, the Advanced Settings is different, please put mouse on title to get help information, the recommend web browser is Google Chrome.

3.7.6 WiFi Settings

- Status
- System
- Services
- VPN
- Network
 - Operation Mode
 - Mobile
 - LAN
 - Wired WAN
 - WAN IPv6
 - Interfaces
 - Wi-Fi
 - Firewall

radio0: Master "Cell_AP_0175bc"

Wi-Fi Overview

Devices Overview

Generic MAC80211 802.11bgn (radio0)

Channel: 11 (2.462 GHz) | Bitrate: 120 Mbit/s

SSID: Cell_AP_0175bc | Mode: Master

BSSID: 90:22:08:01:75:BC | Encryption: WPA2 PSK (CCMP)

WiFi Restart
AP Client
Add

Disable
Edit
Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cell_AP_0175bc	72:E1:DF:0B:DA:36	?	-66 dBm	0 dBm	6.0 Mbit/s, MCS 0, 20MHz	120.0 Mbit/s, MCS 11, 40MHz

- **Wifi Restart:** turn off Wifi firstly, and then turn on.
- **AP Client:** Scan all frequency to get Wifi network information.
- **Add:** add a new Wireless network.
- **Disable:** set a wireless network to down.
- **Edit:** modify detail information of wireless network.
- **Remove:** delete a wireless network.
- **Associated Stations:** it is a list of connected wireless stations.

3.7.6.1 Wifi General configuration

- **Status:** show the WiFi signal strength, mode, SSID and so on.
- **Operating frequency Mode:** supports 802.11b/g/n. the Legacy means 802.11b/g. “N” means 802.11n.
- **Channel:** channel 1-11 supported.
- **Width:** 20MHz and 40MHz.
- **Transmit Power:** from 0dBm to 20dBm supported.

3.7.6.2 WiFi Advanced Configuration




- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to farthest network member in meters.

- **Fragmentation Threshold:**
- **RTS/CTS Threshold:**

3.7.6.3 WiFi Interface Configuration

Interface Configuration

- General Setup**
- Wireless Security
- MAC-Filter

ESSID	<input type="text" value="Cell_AP_0175bc"/>
Mode	<input type="text" value="Access Point"/>
Network	<input type="checkbox"/> ifmobile:  <input checked="" type="checkbox"/> lan:  <input type="checkbox"/> wan6:  <input type="checkbox"/> create: <input type="text"/>
Hide Extended Service Set Identifier	<input type="checkbox"/>
WMM Mode	<input checked="" type="checkbox"/>

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

☰ Interface Configuration

General Setup	Wireless Security	MAC-Filter
ESSID	<input style="width: 100%;" type="text" value="Cell_AP_0175bc"/>	
Mode	<div style="border: 1px solid #ccc; padding: 2px;"> Access Point ▼ </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Access Point Client Ad-Hoc 802.11s Pseudo Ad-Hoc (ahdemo) Monitor Access Point (WDS) Client (WDS) </div>	
Network	<input type="checkbox"/> create: <input style="width: 50px;" type="text"/>	
Hide Extended Service Set Identifier	<input type="checkbox"/>	
WMM Mode	<input checked="" type="checkbox"/>	



- **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	<input style="width: 100%;" type="text" value="WPA2-PSK"/>	
Cipher	<input style="width: 100%;" type="text" value="auto"/>	
Key	<input style="width: 100%;" type="password" value="....."/> 👁	
Enable WPS pushbutton, requires WPA(2)-PSK	<input type="checkbox"/>	

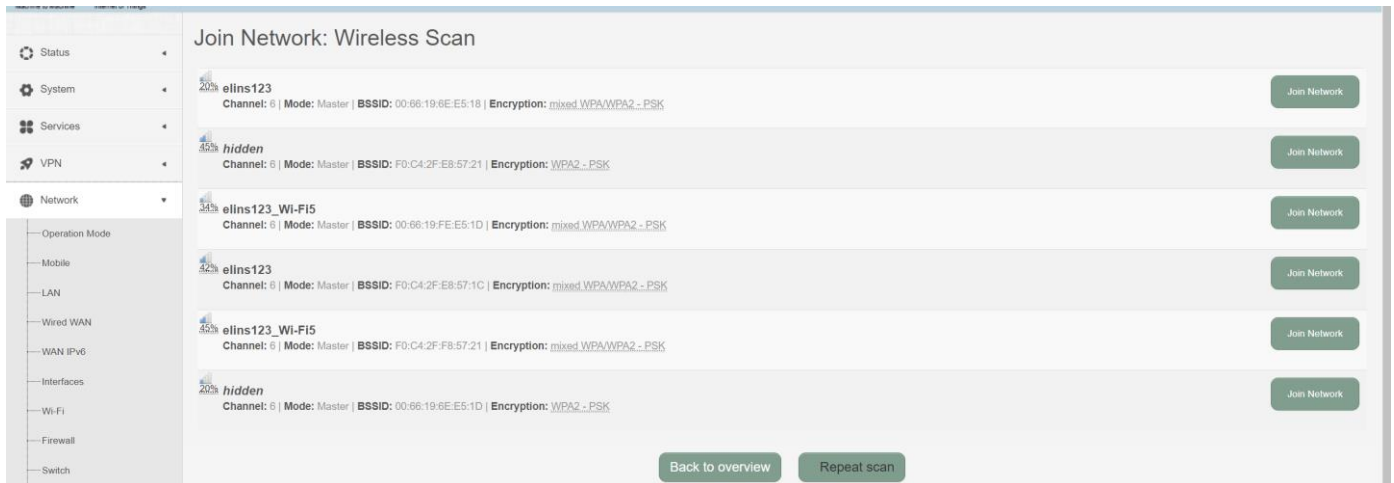
- **Encryption:**

- **Key:** it is the password to Join wireless network. If Encryption set to “No Encryption”, no password is needed.

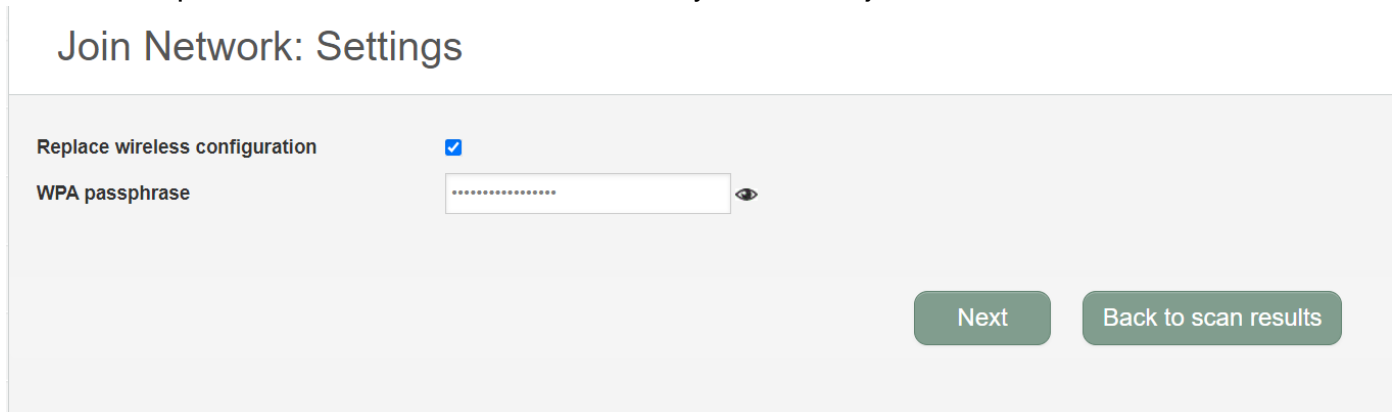
- **MAC-Address Filter:** MAC address access policy. Disabled: disable MAC-address filter functionality. Allow list: only the MAC address in the list is allowed to forward. Deny list: all packet is allowed to forward except MAC address in the list.
- **MAC-List:** click button  to delete MAC address from list, click button  to add a new MAC address into list.

3.7.6.4 WiFi AP client

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



- **Step 2)** If the WiFi you want to join in the list, click button “Join Network” accordingly. If it is not, click “Repeat Scan” until to 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. If it conflicts with other interface, please change it. Otherwise don't change it.
- **Step 4)** Click Submit if everything is configured. The below is Wi-Fi configuration page. Don't change Operating frequency, make sure the ESSID and BSSID is from the Wi-Fi you want to join.

Wi-Fi Network: Client "elins123" (radio0.network1)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined Wi-Fi r like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup | Advanced Settings

Status

0% **Mode:** Client | **SSID:** elins123

BSSID: 00:66:19:6E:E5:18 | **Encryption:** -

Channel: 11 (2.462 GHz) | **Tx-Power:** 0 dBm

Signal: 0 dBm | **Noise:** 0 dBm

Bitrate: 0.0 Mbit/s | **Country:** 00

Wi-Fi network is enabled

Operating frequency

Mode	Channel	Width
11g/n mixed	6 (2437 MHz)	40 MHz

Transmit Power 20 dBm (100 mW)

Interface Configuration

General Setup | Wireless Security

ESSID elins123

Mode Client

BSSID 00:66:19:6E:E5:18

Network

ifmobile:

lan:

wan6:

wwan:

create:

- **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:A8:6D:48:77:5E	?	-62 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	58.5 Mbit/s, MCS 6, 20MHz
MERCURY_FE2A	8C:F2:28:FD:FE:2A	192.168.1.1	-50 dBm	0 dBm	135.0 Mbit/s, MCS 7, 40MHz	150.0 Mbit/s, MCS 7, 40MHz

3.7.7 Interfaces Overview

Interfaces overview shows all interfaces status, including uptime, MAC-address, RX, TX and IP address.

Network	Status	Actions
LOOPBACK lo	Uptime: 2h 13m 51s MAC-Address: 00:00:00:00:00:00 RX: 175.86 KB (2070 Pkts.) TX: 175.86 KB (2070 Pkts.) IPv6: ::1::28	Connect Stop Edit
LAN br-lan	Uptime: 0h 1m 19s MAC-Address: 90:22:08:01:75:8C RX: 32.05 KB (342 Pkts.) TX: 281.26 KB (428 Pkts.) IPv4: 192.168.1.1/24 IPv6: 6025:879c:78ec::1/60	Connect Stop Edit
EMODULE usb0	Uptime: 2h 13m 18s MAC-Address: 02:50:F4:00:00:00 RX: 13.52 MB (11564 Pkts.) TX: 609.97 KB (788 Pkts.) IPv6: 10.22.127.224/25	Connect Stop Edit Delete
WAN pppoe-wan	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit
WAN2 eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:08:01:75:8C RX: 0.00 B (0 Pkts.) TX: 2.62 KB (36 Pkts.)	Connect Stop Edit
WWAN Client "elins123"	Uptime: 0h 0m 0s MAC-Address: 90:22:08:01:75:8C RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete

3.7.8 Firewall

3.7.8.1 General Settings

The screenshot shows the 'Firewall - General Settings' page. The left sidebar contains a navigation menu with 'Firewall' selected. The main content area has tabs for 'General Settings', 'Port Forwards', 'Traffic Rules', 'Source NAT', 'DMZ', 'Security', 'MAC Filter', and 'Custom Rules'. The 'General Settings' tab is active, showing a list of configuration options:

- Enable firewall:**
- Enable SYN-flood protection:**
- Drop invalid packets:**
- Enable SIP ALG:** Please reboot router after Save & Apply
- Input:** accept
- Output:** accept
- Forward:** reject

At the bottom, there is a 'Restart Firewall:' button with a 'Restart' sub-button and a 'Save' button.

3.7.8.2 Port Forwards

This page includes port forwards list and add new port forwards rule functionality.

The screenshot shows the 'Firewall - Port Forwards' page. The left sidebar is the same as in the previous screenshot, with 'Firewall' selected. The main content area has tabs for 'General Settings', 'Port Forwards', 'Traffic Rules', 'Source NAT', 'DMZ', 'Security', 'MAC Filter', and 'Custom Rules'. The 'Port Forwards' tab is active, showing a list of port forwards and a form to add a new one.

The 'Port Forwards' section contains a table with the following structure:

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

Below the table is a 'New port forward:' form with the following fields:

- Name:** New port forward
- Protocol:** TCP+UDP
- External port:** (empty)
- Internal IP address:** (empty)
- Internal port:** (empty)

There are 'Add' and 'Save' buttons at the bottom of the form.

- **Name:** port forward instance name.

- **Protocol:** TCP+UDP, UDP and TCP can be chosen.
- **External zone:** the recommend option is wan.
- **External port:** match incoming traffic directed at the given destination port on this host.
- **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.

3.7.8.3 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 content the follow functionalities.

Traffic rules list:

Firewall - Traffic Rules						
Traffic Rules						
Name	Match	Action	Enable	Sort		
DTU server	Any TCP/UDP From any host in wan To any router IP at port 5000 on this device	Accept input	<input type="checkbox"/>	↑ ↓	Edit	Delete
Allow-All-LAN-Ports	Any traffic From any host in wan To any host, ports 1-65535 in lan	Accept forward	<input type="checkbox"/>	↑ ↓	Edit	Delete
Allow-DHCP-Renew	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-WAN	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	<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 fe80::/10 in wan with source port 547 To IP range fe80::/10 at port 546 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 fe80::/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-solicitation, router-advertisement, 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

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

New forward rule

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	lan ▾	wan ▾	<input type="button" value="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	
<i>This section contains no values yet</i>					
New source NAT:					
	Name	Source zone	Destination zone	To source IP	To source port
	<input type="text" value="New SNAT rule"/>	lan ▾	wan ▾	-- Please cho ▾	<input type="text" value="Do not rewrite"/>
	<input type="button" value="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 - DTU server

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

Rule is disabled

Enable

Name

DTU server

Restrict to address family

IPv4 and IPv6

Protocol

TCP+UDP

Match ICMP type

any

Source zone

- Any zone
- l2tpzone: (empty)
- lan: lan:
- openvpn: (empty)
- pptpzone: (empty)
- vpnzone: (empty)
- wan: wan: wan6: ifmobile: wwan:

Source MAC address	any
Source address	any
Source port	any
Destination zone	<input checked="" type="radio"/> Device (input) <input type="radio"/> Any zone (forward) <input type="radio"/> l2tpzone: (empty) <input type="radio"/> lan: lan: <input type="radio"/> openvpn: (empty) <input type="radio"/> pptpzone: (empty) <input type="radio"/> vpnzone: (empty) <input type="radio"/> wan: wan: wan6: ifmobile: wwan:
Destination address	any
Destination port	5000
Action	accept
Extra arguments	

- **Name:** traffic rule entry name
- **Restrict to address family:** IPv4+IPv6, IPv4 and IPv6 can be selected. Specified the matched IP address family
- **Protocol:** specified the protocol matched in this rule. "Any" means any protocol is matched.
- **Source zone:** it is the zone that the traffic comes from.
- **Source MAC address:** traffic rule check if the incoming packet's source MAC address is matched.
- **Source address:** traffic rule check if the incoming packet's source IP address is matched.
- **Source port:** traffic rule check if the incoming packet's TCP/UDP port is matched.
- **Destination zone:** the zone that the traffic will go to.
- **Destination address:** traffic rule check if the incoming packet's destination IP address is

matched.

- **Destination port:** traffic rule check if the incoming packet's TCP/UDP port is matched.
- **Action:** if traffic is matched, system will handle traffic according to the Action(accept, drop, reject, don't track).
- **Extra argument:** passes additional argument to iptable, use with care!

3.7.8.4 DMZ

DMZ Configuration

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

DMZ

Enable DMZ

Source zone wan

IP address

Protocol All protocols

Save

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

- **Source zone:** Usually use wan as source zone, if VPN created and need to DMZ on VPN interface, then choose vpnzone instead.
- **IP Address:** Please Enter the IP address of the computer which you want to set as DMZ host
- **Protocol:** All protocols, TCP+UDP,TCP,UDP.

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

3.7.8.5 Security

General Settings	Port Forwards	Traffic Rules	Source NAT	DMZ	Security	MAC Filter	Custom Rules
------------------	---------------	---------------	------------	-----	----------	------------	--------------

System Security Configuration

☰ Basic Settings

SSH enable	<input checked="" type="checkbox"/>
SSH port	<input type="text" value="22"/>
SSH access from WAN	<input type="text" value="Allow"/> ▼
Ping from WAN to LAN	<input type="text" value="Deny"/> ▼
Enable telnet	<input type="checkbox"/>

☰ HTTPS Access

HTTPS port	<input type="text" value="443"/>
HTTPS access from WAN	<input type="text" value="Allow"/> ▼
Remote network	<input type="text" value="Subnet"/> ▼
IP address	<input type="text" value="192.168.1.1"/>
Netmask	<input type="text" value="24"/>

☰ HTTP Access

HTTP enable	<input checked="" type="checkbox"/>
HTTP port	<input type="text" value="80"/>
HTTP access from WAN	<input type="text" value="Allow"/> ▼
Remote network	<input type="text" value="Any IP address"/> ▼
RFC1918 filter	<input type="checkbox"/>

- **SSH access from WAN:** allow or deny users access H685/H685 router from remote side.
- **Ping from WAN to LAN:** allow or deny ping from remote side to internal LAN subnet.
- **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, the illegal value is from 1 to 32.

3.7.9 Static Routes

- **Interface:** You can choose the corresponding interface type.
- **Target:** the destination host IP or network.

Gateway: IP address of the next router.

Notice:

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

3.7.10 Switch

Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0" (mt7620)

Enable VLAN functionality

VLANs on "switch0" (mt7620)

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	Port 5	CPU	Port 7	
1	untagged	untagged	untagged	untagged	off	off	tagged	off	Delete
2	off	off	off	off	untagged	off	tagged	off	Delete

Add

Save

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.

3.7.11 DHCP and DNS

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

General Settings | Resolv and Hosts Files | TFTP Settings | Advanced Settings

Domain required

Authoritative

Local server

Local domain

Log queries



DNS forwardings

Rebind protection

Allow localhost

Domain whitelist

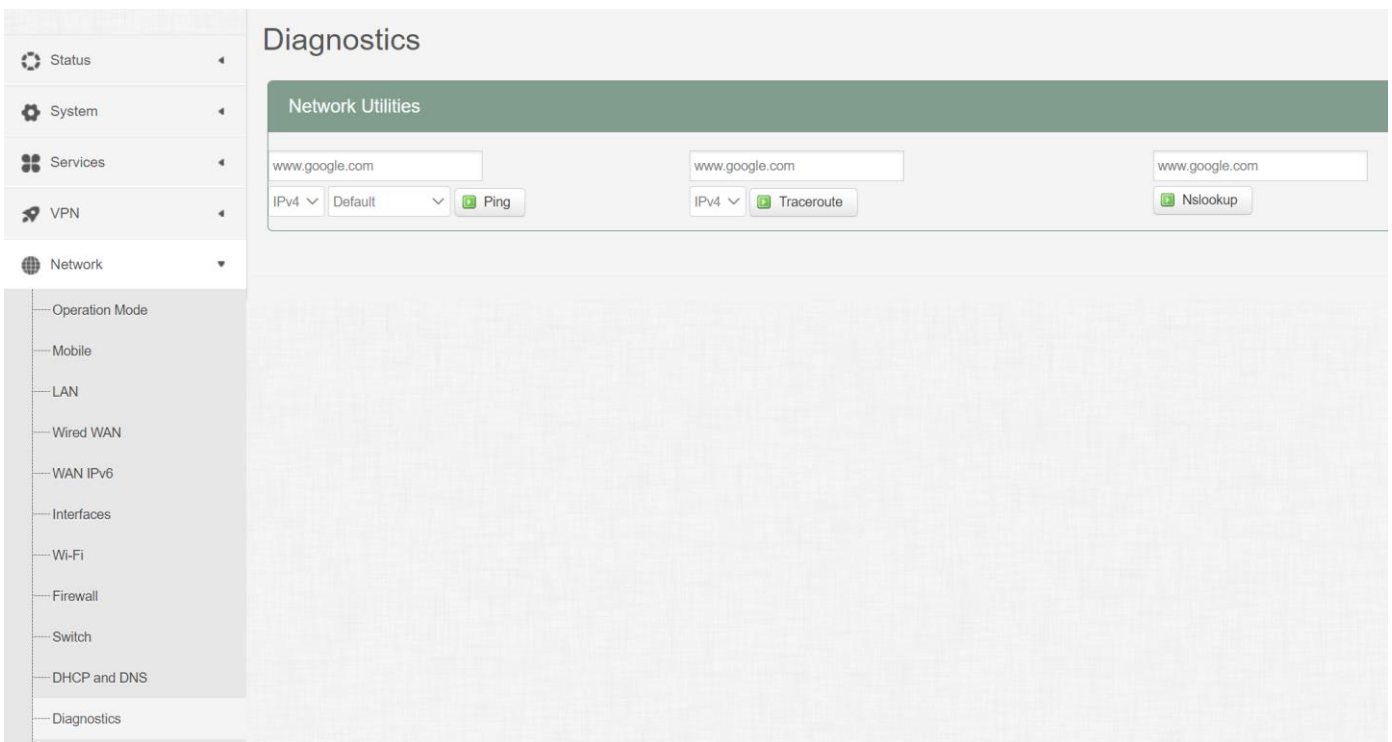
- **Domain required:** don't forward DNS-requests without DNS-Name.
- **Authoritative:** This is the only DHCP on the local network.
- **Local server:** Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only.
- **Local domain:** Local 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		<input type="checkbox"/>	
Allocate IP sequentially		<input type="checkbox"/>	
Filter private		<input checked="" type="checkbox"/>	
Filter useless		<input type="checkbox"/>	
Localise queries		<input checked="" type="checkbox"/>	
Expand hosts		<input checked="" type="checkbox"/>	
No negative cache		<input type="checkbox"/>	
Strict order		<input type="checkbox"/>	
Bogus NX Domain Override		<input type="text" value="67.215.65.132"/>	
DHCP Relay		<input type="text"/>	
DNS server port		<input type="text" value="53"/>	
DNS query port		<input type="text" value="any"/>	
Max. DHCP leases		<input type="text" value="unlimited"/>	
Max. EDNS0 packet size		<input type="text" value="1280"/>	
Max. concurrent queries		<input type="text" value="150"/>	

- **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 not 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.

3.7.12 Diagnostics



- **Ping** : it is a 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.
- 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.

Diagnostics

Network Utilities

www.google.com www.google.com www.google.com

IPv4 ▾ Default ▾ IPv4 ▾

```
PING www.google.com (96.44.137.28): 56 data bytes  
  
--- www.google.com ping statistics ---  
5 packets transmitted, 0 packets received, 100% packet loss
```

3.7.13 Loopback Interface

Loopback Interface Configuration

Loopback Settings

IP address	<input type="text" value="127.0.0.1"/>
Netmask	<input type="text" value="255.0.0.0"/>
IP address 2	<input type="text"/>
Netmask 2	<input type="text"/>

- Status
- System
- Services
- VPN
- Network
 - Operation Mode
 - Mobile
 - LAN
 - Wired WAN
 - WAN IPv6
 - Interfaces
 - Wi-Fi
 - Firewall
 - Switch
 - DHCP and DNS
 - Diagnostics
 - Loopback Interface

The default Loopback interface has IP address 127.0.0.1, the final user can change it here.

3.7.14 Dynamic Routing

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

- Status
- System
- Services
- VPN
- Network
 - Operation Mode
 - Mobile
 - LAN
 - Wired WAN
 - WAN IPv6
 - Interfaces
 - Wi-Fi
 - Firewall
 - Switch
 - DHCP and DNS
 - Diagnostics
 - Loopback Interface
 - Hostnames
 - Dynamic Routing
 - Guest LAN(Guest WiFi)

Dynamic Routing

Zebra

Enable

Password

Enable password

OSPF

Enable

Password

Enable password

OSPF6

Enable

Password

Enable password

RIP

Enable

Password

Enable password

RIPng

Enable

Password

Enable password

BGP

Enable

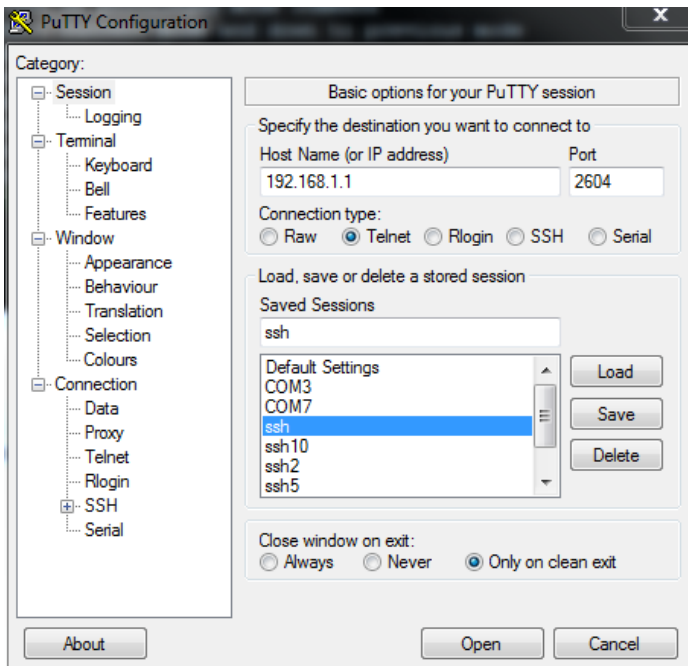
Password

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.

Note: How to configure these services? For example, the router's LAN IP is 192.168.10.1. 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 Kunihiro Ishiguro, et al.

User Access Verification

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

3.7.15 QoS

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

Quality of Service

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

☰ Interfaces

Delete

WAN

Enable	<input type="checkbox"/>
Device	default ▼
Classification group	default ▼
Calculate overhead	<input type="checkbox"/>
Half-duplex	<input type="checkbox"/>
Download speed (kbit/s)	1024
Upload speed (kbit/s)	128

Add

- **Enable:** enable QoS on this interface.
- **Classification group:** Specify classgroup 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 ▼	22,53 ▼		ssh, dns	↑ ↓	Delete
normal ▼	all ▼	all ▼	all ▼	TCP ▼	20,21,25,80,110,443,993,995 ▼		ftp, smtp, http(s), imap	↑ ↓	Delete
express ▼	all ▼	all ▼	all ▼	all ▼	5190 ▼		AOL, iChat, ICQ	↑ ↓	Delete

Add
Save


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:** Packets matching this protocol belong to the bucket defined in target.
- **Ports:** Packets matching this, belong to the bucket defined in target. If more than 1 port required, they must be separated by comma.
- **Number of bytes:** Packets matching this, belong to the bucket defined in target.

3.7.16 Guest LAN(Guest WiFi)


Guest WiFi is a specific WiFi which only can accesses internet bot not local LAN.

Guest LAN(Guest Wi-Fi) Configuration


 Guest LAN Settings

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:

Wi-Fi Overview

	Qualcomm Atheros QCA9880 802.11bgnac (radio0) Channel: 149 (5.745 GHz) Bitrate: ? Mbit/s	 Wifi Restart	 AP Client	 Add
0% 	SSID: SPEEDROUTE H820Q 5GHz Mode: Master BSSID: 04:F0:21:1A:D8:35 Encryption: WPA2 PSK (CCMP)	 Disable	 Edit	 Remove
	Generic MAC80211 802.11bgn (radio1) Channel: 5 (? GHz) Bitrate: ? Mbit/s	 Wifi Restart	 AP Client	 Add
0% 	SSID: Cell_AP_007622 Mode: Client BSSID: 90:22:06:00:76:22 Encryption: -	 Disable	 Edit	 Remove