

# Industrial Grade TR 1803-3G/ TR1804-4G

## 2G 3G 4G Cellular Router

### User Manual

#### Content

1 Preparation job before configuration	3
1.1 Learn your router version and feature	3
1.2 Prepare SIM Card and working condition	4
1.3 Highly recommendation for the configuration	4
2 Hardware Installation	5
2.1 Overall Dimension	5
2.2 The Ports	5
2.3 Installment	6
2.4 SIM/UIM card installed	7
2.5 The installation of terminal blocks	7
2.6 Grounding	8
2.7 Power Supply	9
2.8 LED and Check Network Status	9
3 Software configuration	10
3.1 Overview	10
3.2 How to log into the Router	10
3.3 Router status	13
3.3.1 Status overview	13
3.3.2 Network status	14
3.3.3 Firewall status	15
3.3.4 Routes	16
3.3.5 System log	17
3.3.6 Kernel log	17
3.3.7 Realtime graphs	18
3.4 System Configuration	19
3.4.1 Setup wizard	19
3.4.2 System	20
3.4.3 Password	21
3.4.4 NTP	21
3.4.5 Backup/Restore	22
3.4.6 Upgrade	22
3.4.7 Reset	23
3.4.8 Reboot	24
3.5 Services configuration	24
3.5.1 ICMP check	24
3.5.2 VRRP	25
3.5.3 Failover (link backup)	26

---

3.5.4 DTU .....	26
3.5.5 SNMP .....	29
3.5.6 GPS .....	31
3.5.7 SMS .....	32
3.5.8 VPN .....	36
3.5.8.1 IPSEC .....	36
3.5.8.2 PPTP .....	37
3.5.8.3 L2TP .....	39
3.5.8.4 OpenVPN .....	41
3.5.8.5 GRE tunnel .....	43
3.5.9 DDNS .....	43
3.5.10 Connect Radio Module .....	47
3.6 Network Configuration .....	48
3.6.1 Operation Mode .....	49
3.6.2 Mobile configuration .....	49
3.6.3 Cell mobile data limitation .....	51
3.6.4 LAN settings .....	52
3.6.5 wired-WAN .....	55
3.6.6 WiFi Settings .....	56
3.6.6.1 Wifi General configuration .....	57
3.6.6.2 WiFi Advanced Configuration .....	57
3.6.6.3 WiFi Interface Configuration .....	58
3.6.6.4 WiFi AP client .....	59
3.6.7 Interfaces Overview .....	62
3.6.8 Firewall .....	63
3.6.8.1 General Settings .....	63
3.6.8.2 Port Forwards .....	63
3.6.8.3 traffic rules .....	64
3.6.8.4 DMZ .....	67
3.6.8.5 Security .....	68
3.6.9 Static Routes .....	69
3.6.10 Switch .....	69
3.6.11 DHCP and DNS .....	70
3.6.12 Diagnostics .....	72
3.6.13 Loopback Interface .....	72
3.6.14 Dynamic Routing .....	72
3.6.15 QoS .....	74

# Chapter 1

## 1 Preparation job before configuration

### 1.1 Learn your router version and feature

- 1) TR1803/TR1804 contains different version and option feature. Please learn it before using it. TR1803/TR1804 series defines the model as follows,

#### TR1803/TR1804

**W:** WiFi WLAN

**G:** GPS

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

**50V:** DC input 5~50V support, default is 5~40V

**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

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

#### 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~50V

6) BGP, OSPF, RIP, etc.

7) 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 “TR1803-3G/TR1804-4G”, remember this and will select this module name while do configuration.



## 1.2 Prepare SIM Card and working condition

1. TR1803 /TR1804 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. Make sure the sim card or uim card is with enough data business and balance.
4. 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.

## 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.

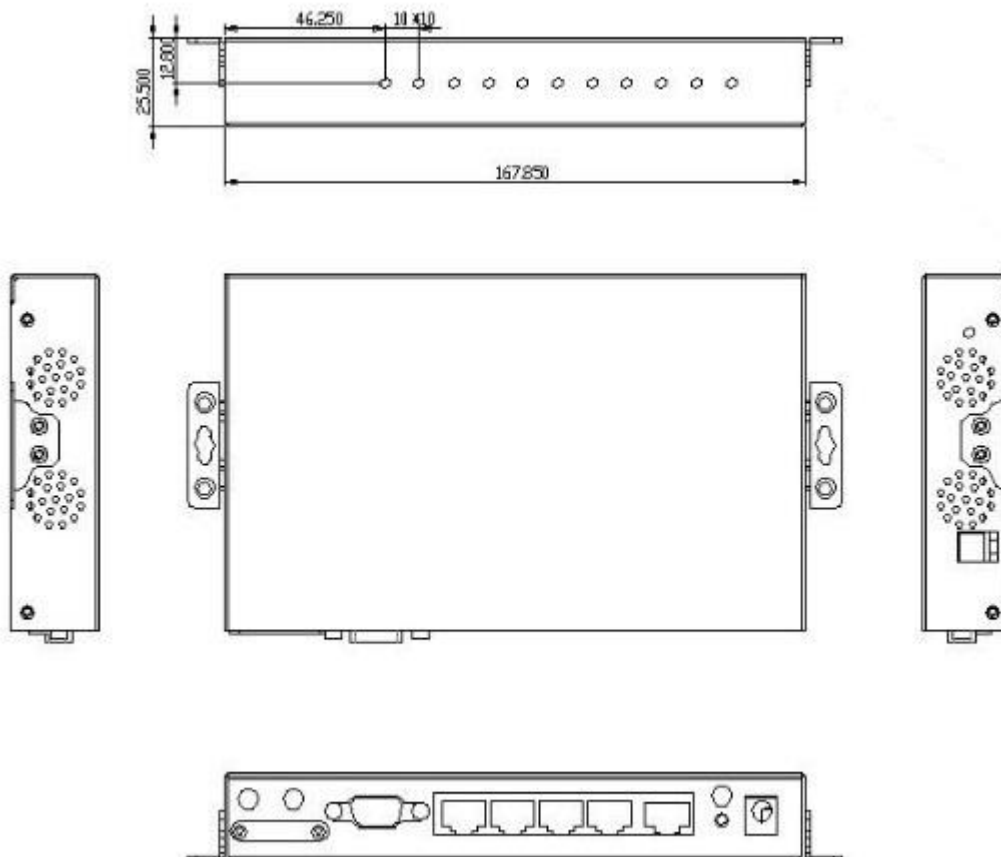
# Chapter 2

## 2 Hardware Installation

This chapter mainly describes the appearance, model and function of TR1803 /TR1804 series and how to install and set the configurations.

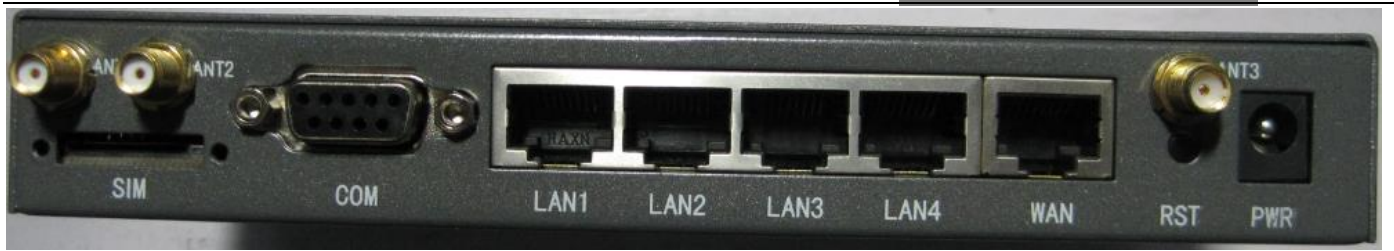
1. *Overall Dimension*
2. *Accessories Description*
3. *Installment*

### 2.1 Overall Dimension



### 2.2 The Ports

Back Picture:



ANT1(CELL): for cellular

ANT2(AUX): for cellular diversity receiving MIMO. Notes: the old version ANT2 is for diversity or for GPS.

ANT3 (WiFi): for WiFi

ANT4 (GPS): for GPS. Notes: the old version has no ANT4.

SIM: for sim card

COM: DB9 for serial port.

LAN1~LAN4: 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.



GND: DC wire ground

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

WPS: WPS button

### Antenna Connection Table

Antenna Connector	Marks
Cell	for main cell antenna
Aux	for auxiliary cell antenna
WiFi / WLAN	for WiFi antenna
GPS	for GPS antenna

## 2.3 Installment

TR1803 /TR1804 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 TR1803 /TR1804 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.*

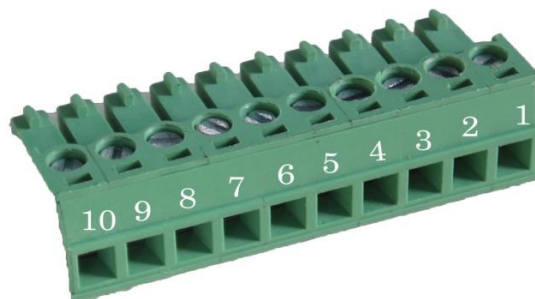
## 2.5 The installation of terminal blocks

This chapter is for version with terminal blocks only. Default, the TR1803 /TR1804 is with DB9 connector. Please use DB9 cable to connect TR1803 /TR1804 and the equipment directly.

**The following is for version with terminal blocks only:**

TR1803 /TR1804 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 TR1803 /TR1804 products. Using 14~24AWG cable and referring to TR1803 /TR1804 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 TR1803 /TR1804 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	

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 TR1803 /TR1804 series operation, Router cabinet should be grounded properly.



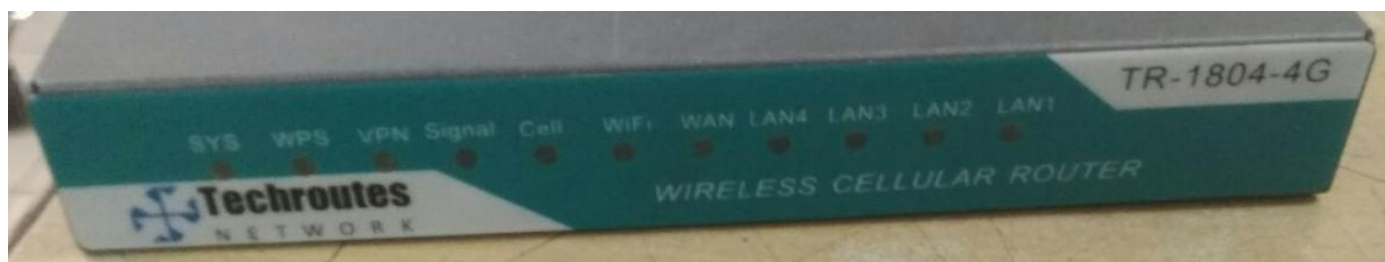
## 2.7 Power Supply

TR1803 /TR1804 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, TR1803 /TR1804 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, TR1803 /TR1804 series input powers supply is +5~+40V (if your TR1803 /TR1804 support 50V, the option is +5~+50V). In most cases, the standard configuration is 12V/1A.

## 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 TR1803 /TR1804 series via the cable. After provide the power to TR1803 /TR1804, 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
LAN1~LAN4	blink	Data transmission in Ethernet
	Off	Ethernet connection abnormal
	On	Ethernet is connected
VPN	On	VPN tunnel set-up
	Off	VPN tunnel set-up failure or unactivated

CELL	On	Access to the Internet
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
	4s blink 1 time	Signal bar is 1
	3s blink 1 time	Signal bar is 2
	2s blink 1 time	Signal bar is 3
	1s blink 1 time	Signal bar is 4
	1s blink 2 times	Signal bar is 5

# Chapter 3

## 3 Software configuration

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

### 3.1 Overview

TR1803 /TR1804 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.

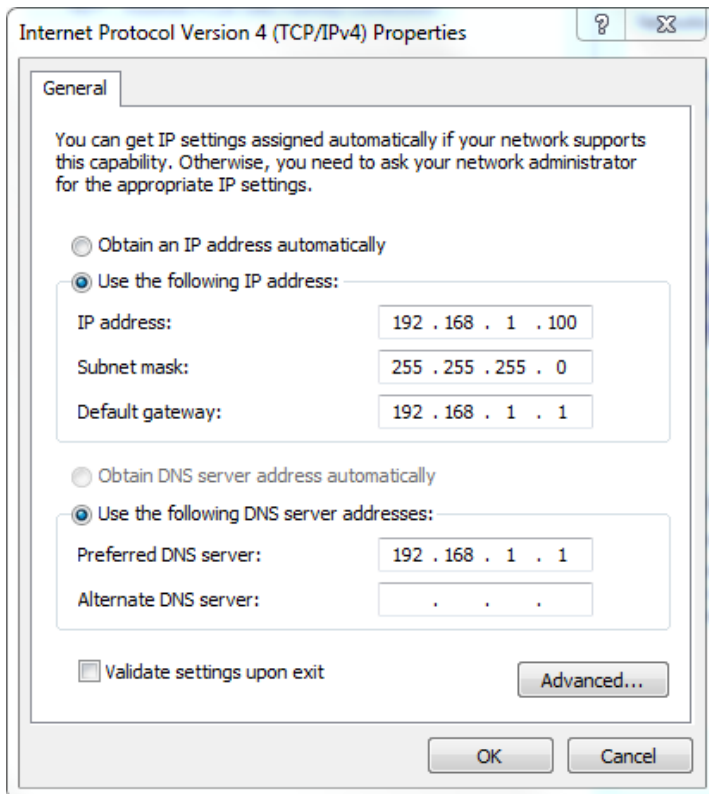
The router default parameters as follow

Default IP: 192.168.1.1, sub mask: 255.255.255.0.

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

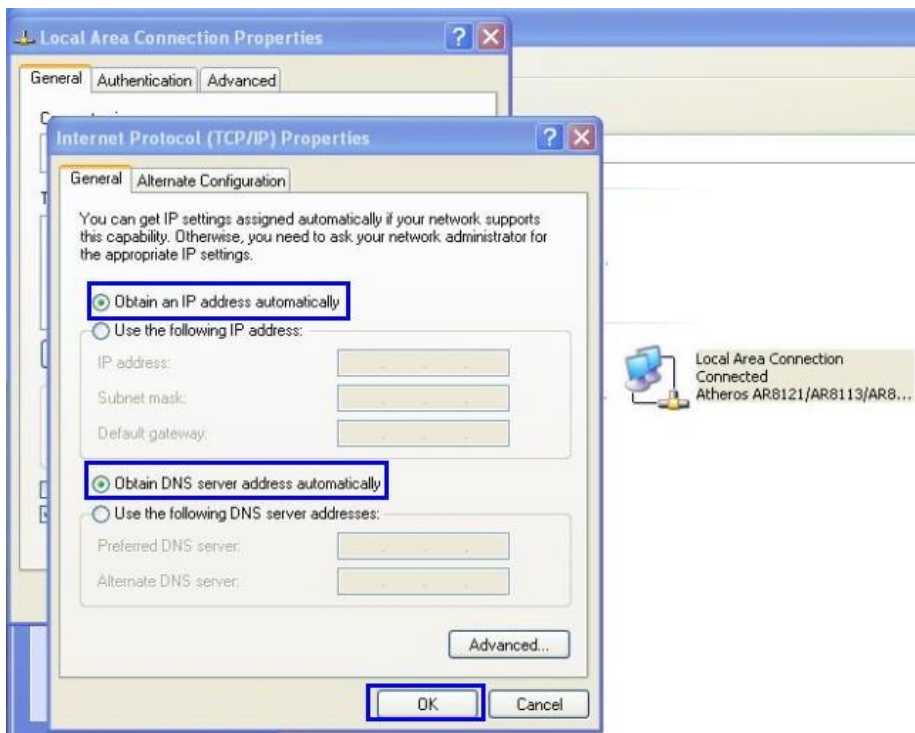
### Way 1) Manual setting

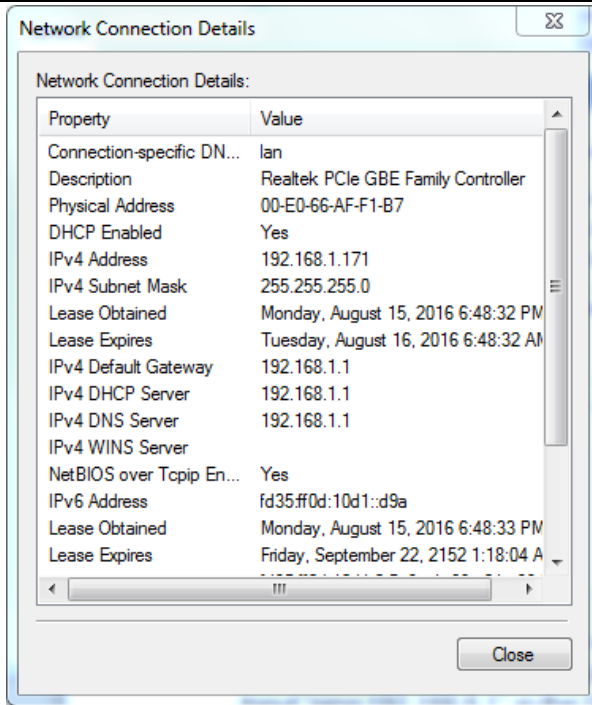
Set the PC IP as 192.168.1.xxx (xxx = 2~254), subnet mask: 255.255.255.0, default gateway: 192.168.1.1, primary DNS: 192.168.1.1.



### 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.

## Authorization Required

Please enter your username and password.

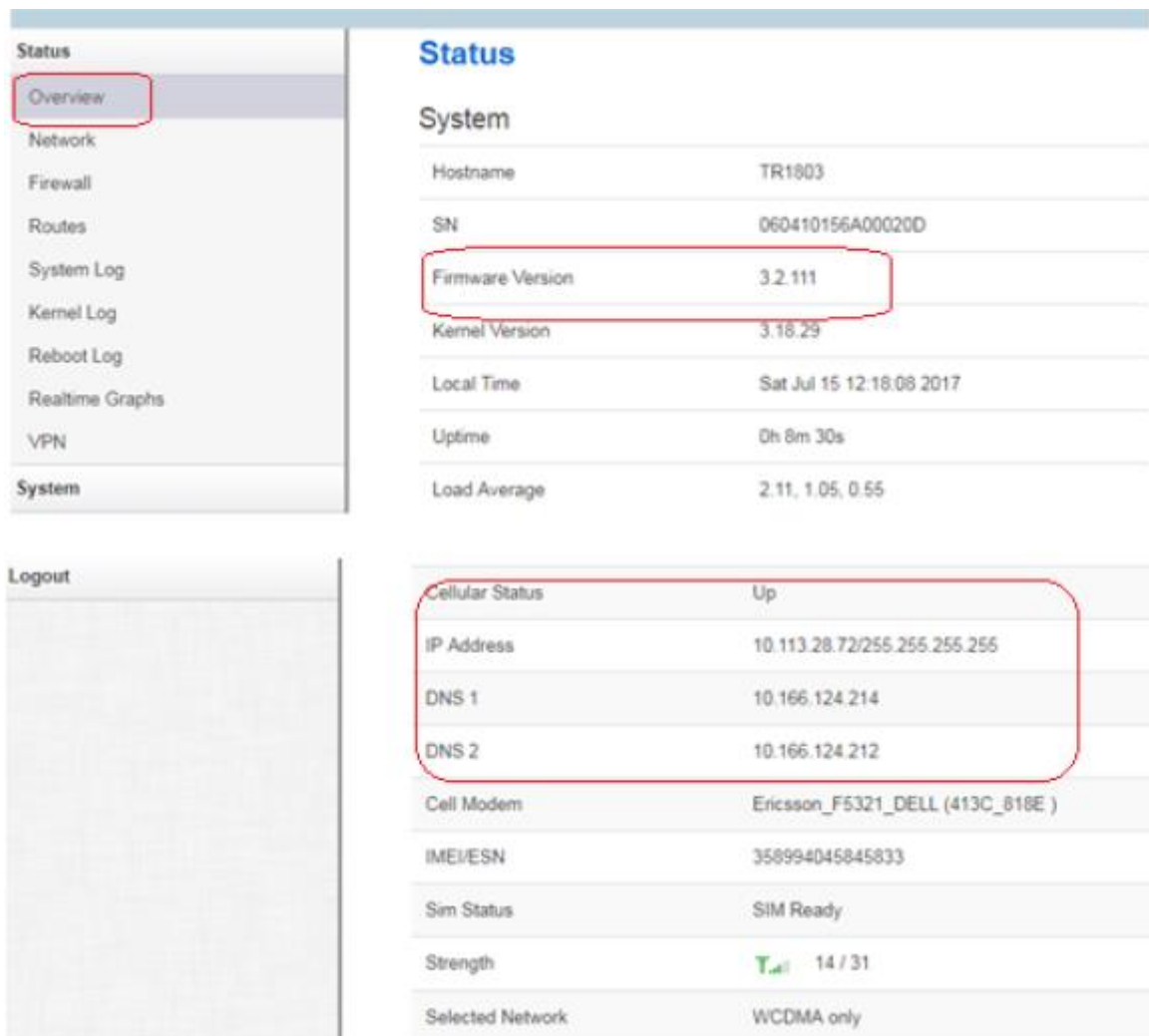
Username

Password

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

### 3.3 Router status3.3.1

**Status overview** Click "Status" in the navigation bar, and then click "Overview".



System	
Hostname	TR1803
SN	060410156A00020D
Firmware Version	3.2.111
Kernel Version	3.18.29
Local Time	Sat Jul 15 12:18:08 2017
Uptime	0h 8m 30s
Load Average	2.11, 1.05, 0.55

Cellular Status	
Cellular Status	Up
IP Address	10.113.28.72/255.255.255.255
DNS 1	10.166.124.214
DNS 2	10.166.124.212
Cell Modem	Ericsson_F5321_DELL (413C_818E )
IMEI/ESN	358994045845833
Sim Status	SIM Ready
Strength	14 / 31
Selected Network	WCDMA only

### 3.3.2 Network status

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

Cell mobile interface page:

Status	Mobile	WAN	LAN
Overview	<h2>Mobile Status</h2>		
Network	<h3>Mobile 1</h3>		
Firewall	Celluar Status	Up	
Routes	Cell Modem	Ericsson_F5521GW (0BDB_190D )	
System Log	IMEI	867377020131342	
Kernel Log	Sim Status	SIM Ready	
Realtime Graphs	Strength	T 9 / 31	
System	Selected Network	Automatic	
Services	Registered Network	Registered on Home network: "China Unicom", 2,	
Network	Sub Network Type	UMTS	
Logout	Location Area Code	F10E	
	Cell ID	0A0EAE7	
	<h3>Connection Status</h3>		
	Port	Mobile-PPP	
	IPv4 Addr	10.181.174.149/32	
	DNS 1	119.6.6.6	
	DNS 2	202.102.128.68	
	Gateway	0h 0m 10s	
	Uptime	0h 3m 40s	
	RX	726.33 KB (1607 Pkts.)	

WAN status page:

Status

Overview

**Network**

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

System

Services

Network

Logout

Mobile
WAN
LAN

## WAN Status

IPv4 WAN Status	<b>Port</b>	Wired-WAN
	<b>Protocol:</b>	dhcp
	<b>Address:</b>	0.0.0.0
	<b>Netmask:</b>	255.255.255.255
	<b>Gateway:</b>	0.0.0.0
	<b>Mac Addr:</b>	90:22:00:C0:03:00
	<b>RX</b>	0.00 B (0 Pkts.)
	<b>TX</b>	34.61 KB (112 Pkts.)

IPv6 WAN Status *Not connected*

Active Connections 444 / 16384 (2%)

### LAN status page:

Status

Overview

**Network**

Firewall

Routes

System Log

Kernel Log

Realtime Graphs

System

Services

Network

Logout

Mobile
WAN
LAN

## LAN Status

### Status Overview

<b>Uptime:</b>	0h 5m 5s
<b>Protocol:</b>	static
<b>Name:</b>	br-lan
<b>type:</b>	bridge
<b>Mac Addr:</b>	90:22:00:80:03:00
<b>IPv4 Addr:</b>	192.168.1.1/24
<b>IPv6 Addr:</b>	FD35:FF0D:10D1::1/60
<b>RX</b>	423.41 KB (3487 Pkts.)
<b>TX</b>	1.29 MB (3156 Pkts.)

### LAN Ports

Port	MAC-Addr	RX	TX
Wired-LAN	90:22:00:00:03:00	461.26 KB (3735 Pkts.)	1.29 MB (3147 Pkts.)
WiFi	90:22:00:00:03:00	0.00 B (0 Pkts.)	7.11 KB (62 Pkts.)

### DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
MS-20150503MWOL	192.168.1.171	00:e0:66:af:f1:b7	5d 8h 7m 8s

## 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.

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

## Firewall Status

IPv4 Firewall IPv6 Firewall

### Actions

- Reset Counters
- Restart Firewall

### Table: Filter

Chain <i>INPUT</i> (Policy: <i>ACCEPT</i> , Packets: 0, Traffic: 0.00 B)										
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1501	141.09 KB	<a href="#">delegate_input</a>	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain <i>FORWARD</i> (Policy: <i>DROP</i> , Packets: 0, Traffic: 0.00 B)										
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	5213	1.48 MB	<a href="#">delegate_forward</a>	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain <i>OUTPUT</i> (Policy: <i>ACCEPT</i> , Packets: 0, Traffic: 0.00 B)										
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1663	217.63 KB	<a href="#">delegate_output</a>	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

## 3.3.4 Routes

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

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

## Routes

The following rules are currently active on this system.

### ARP

IPv4-Address	MAC-Address	Interface
192.168.1.171	00:e0:66:af:f1:b7	br-lan

### Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
ifmobile	0.0.0.0/0	10.64.64.64	0	main
ifmobile	10.64.64.64		0	main
lan	192.168.1.0/24		0	main

### Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fd35:ff0d:10d1::/64		1024	main
(eth0)	ff00::/8		256	local
lan	ff00::/8		256	local
wan	ff00::/8		256	local
lan	ff00::/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”.

Status

- Overview
- Network
- Firewall
- Routes
- System Log**
- Kernel Log
- Realttime Graphs

System

Services

Network

Logout

### System Log

[Export syslog](#)

```
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Zone ranges:
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Normal [mem 0x00000000-0x03ffffff]
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Movable zone start for each node
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Early memory node ranges
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] node 0: [mem 0x00000000-0x03ffffff]
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] Initmem setup node 0 [mem 0x00000000-0x03ffffff]
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] On node 0 totalpages: 16384
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] free_area_init_node: node 0, pgdat 803241b0, node_mem_map 81000000
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] Normal zone: 128 pages used for memmap
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] Normal zone: 0 pages reserved
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] Normal zone: 16384 pages, LIFO batch:3
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.000000] pcpu-alloc: [0] 0
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 16256
Sat Aug 13 09:35:03 2016 kern.notice kernel: [ 0.000000] Kernel command line: console=ttyS0,57600 rootfstype=squashfs,jffs2
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] Writing ErrCtl register=0007e000
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] Readback ErrCtl register=0007e000
Sat Aug 13 09:35:03 2016 kern.warn kernel: [ 0.000000] Memory: 61164K/65536K available (2626K kernel code, 140K rwdata, 556K ro
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] NR_IRQS:256
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] CPU Clock: 580MHz
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.000000] systick: running - mult: 214748, shift: 32
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.010000] Calibrating delay loop... 385.84 BogoMIPS (lpj=1929216)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.070000] pid_max: default: 32768 minimum: 301
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.070000] Mount-cache hash table entries: 1024 (order: 0, 4096 bytes)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.080000] Mountpoint-cache hash table entries: 1024 (order: 0, 4096 bytes)
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.090000] pinctrl core: initialized pinctrl subsystem
Sat Aug 13 09:35:03 2016 kern.info kernel: [ 0.100000] NET: Registered protocol family 16
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] rt2880-pinmux pinctrl: try to register 73 pins ...
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 0 (io0) on rt2880-pinmux
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 1 (io1) on rt2880-pinmux
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 2 (io2) on rt2880-pinmux
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 3 (io3) on rt2880-pinmux
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 4 (io4) on rt2880-pinmux
Sat Aug 13 09:35:03 2016 kern.debug kernel: [ 0.110000] pinctrl core: registered pin 5 (io5) on rt2880-pinmux
```

### 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”.

Status
Overview
Network
Firewall
Routes
System Log
<b>Kernel Log</b>
Realtime Graphs
System
Services
Network
Logout

## Kernel Log

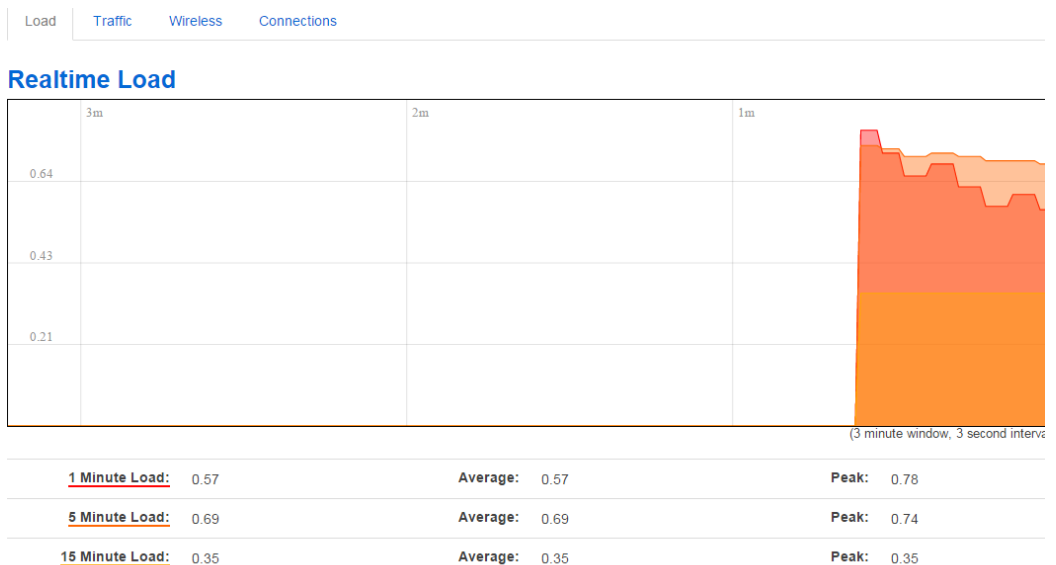
[Export log](#)

```
[ 0.000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro
[ 0.000000] Board has DDR2
[ 0.000000] Analog PMU set to hw control
[ 0.000000] Digital PMU set to 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=ttyS0,57600 rootfstype=squashfs,jffs2
[ 0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)
[ 0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
[ 0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
[ 0.000000] Writing ErrCtl register=0007e000
[ 0.000000] Readback ErrCtl register=0007e000
[ 0.000000] Memory: 61164K/65536K available (2626K kernel code, 140K rwdata, 556K rodata,
[ 0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[ 0.000000] NR_IRQS:256
[ 0.000000] CPU Clock: 580MHz
[ 0.000000] svsttick: runnina - mult: 214748. shift: 32
```

### 3.3.7 Realtime graphs

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

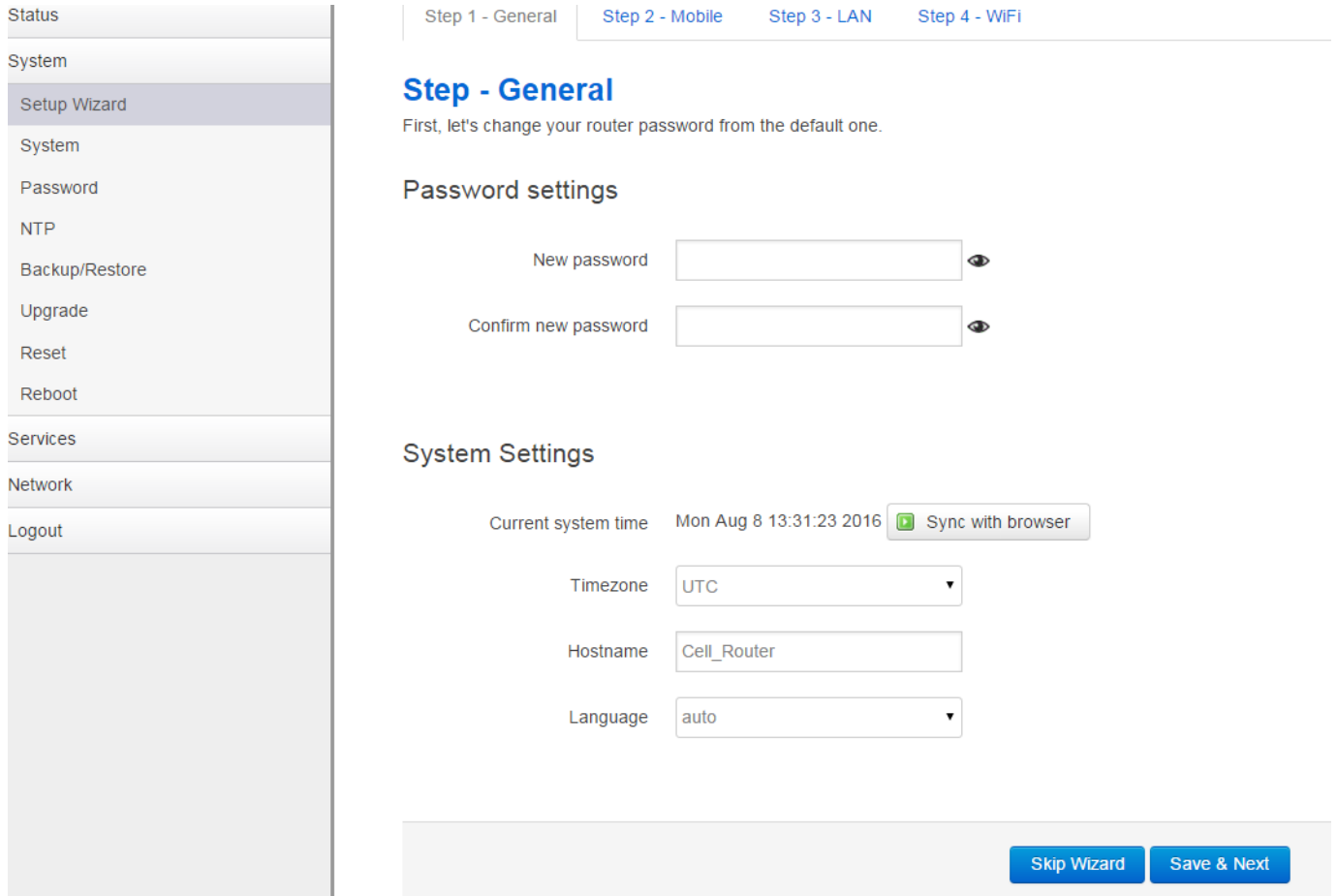
Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
<b>Realtime Graphs</b>
System
Services
Network
Logout



## 3.4 System Configuration

### 3.4.1 Setup wizard

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



The screenshot shows the router's setup wizard interface. On the left is a navigation menu with categories: Status, System (containing Setup Wizard, System, Password, NTP, Backup/Restore, Upgrade, Reset, Reboot), Services, Network, and Logout. The main content area is titled 'Step - General' and includes a progress bar with four steps: Step 1 - General (active), Step 2 - Mobile, Step 3 - LAN, and Step 4 - WiFi. Below the title, a message says 'First, let's change your router password from the default one.' The 'Password settings' section has two input fields: 'New password' and 'Confirm new password', each with an eye icon for visibility. The 'System Settings' section shows 'Current system time' as 'Mon Aug 8 13:31:23 2016' with a 'Sync with browser' button. Below are dropdown menus for 'Timezone' (UTC), 'Hostname' (Cell\_Router), and 'Language' (auto). At the bottom right, there are two buttons: 'Skip Wizard' and '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

Status

System

Setup Wizard

**System**

Password

NTP

Backup/Restore

Upgrade

Reset

Reboot

Services

Network

Logout

### System

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

#### System Properties

General Settings

Logging

Language and Style

Local Time

Mon Aug 8 13:32:16 2016

Hostname

Timezone

### General Settings

#### ➤ Local Time

It displays system 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

### Logging settings

General Settings

Logging

Language and Style

System log buffer size

External system log server

External system log server port

Log output level

Cron Log Level

#### ➤ 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.

Language

➤ **Language**

The default language is “English”.

### 3.4.3 Password

#### Router Password

Changes the administrator password for accessing the device

Password

Confirmation

Change the administrator’ password for accessing the device. Click “eye button” can show the new password you entered.

### 3.4.4 NTP

#### NTP

NTP Configuration

##### Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

0.europe.pool.ntp.org	<input type="button" value="✖"/>
1.europe.pool.ntp.org	<input type="button" value="✖"/>
2.europe.pool.ntp.org	<input type="button" value="✖"/>
3.europe.pool.ntp.org	<input type="button" value="✚"/>

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.

### 3.4.5 Backup/Restore

#### Configuration files operations

##### Backup

Download a tar archive of the current configuration files.

Download backup configuration archive :

##### Restore

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

Restore backup configuration archive :  no file selected

It is used for configuration files backup and restore.

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

For restore configuration files, you can 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.

### 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 an compatible firmware image).

Keep settings:

Image:  no file selected

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 an compatible firmware image).

Keep settings:

Image:  no file selected

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

If the firmware file is OK, 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: **d49e4e53a837a6eca830ff8cad9c0c41**
- Size: 10.25 MB (15.00 MB available)
- Configuration files will be kept.

## 3.4.7 Reset

### System

#### Reset

Resets all configurations to factory default

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

### System

#### Reboot

Reboots the operating system of your device



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

## 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.

### ICMP Check

Enable

Host1 to ping  ipv4 or hostname

Host2 to ping

Ping timeout  seconds (range [1 - 10])

Max retries  (range [3 - 1000])

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

Action when failed

- **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 anytime.



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

### VRRP Configuration

#### VRRP LAN Configuration Settings

Enable

IP address   



Virtual ID

Priority

Save & Apply

Save

Reset

- **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 Settings

Enable

Back To High priority

#### Primary Configuration

Primary

Host1 to ping

Host2 to ping

Ping timeout

Max Retries

Interval between ping

- **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, Wifi\_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 TR1803 /TR1804 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.

## DTU Configuration

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

Enable

Send DTU ID

DTU ID

Forward delay  milliseconds (range[1,10000])

- **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

Serial parity

Serial databits

Serial stopbits

- **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	<input type="text" value="TCP"/>
Service mode	<input type="text" value="Client"/>
Enable Heartbeat	<input type="checkbox"/>
Heartbeat Interval	<input type="text" value="5"/>
Heartbeat Content	<input type="text"/>

## DTU center configuration

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

- **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

### SNMP Configuration

#### General Settings

Enable SNMP

Remote Access

Contact

Location

Name

Port

- **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



Get Host/Lan

Set Community

Set Host/Lan

- **Get Community:** The username for SNMP get. The default value is public. SNMP get is read-only.
- **Get Host/Lan:** The network range to get the router via SNMP, default 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

### GPS Configuration

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

Enable	<input type="checkbox"/>
Prefix SN No.	<input type="checkbox"/>
Only GPRMC	<input type="checkbox"/>
Send interval	<input type="text" value="10"/>
GPS send to	<input type="text" value="TCP"/>
Server IP	<input type="text" value="192.168.1.100"/>
Server port	<input type="text" value="6000"/>

Save & Apply

Save

Reset

- **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	<input type="text" value="Serial"/>
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"/>
Serial flow control	<input type="text" value="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

Enable	<input type="checkbox"/>
SMS ACK	<input type="checkbox"/>
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"/>
DIO_0 Reset Command	<input type="text" value="dio00"/>
DIO_1 Set Command	<input type="text" value="dio11"/>
DIO_1 Reset Command	<input type="text" value="dio10"/>
DIO Status Command	<input type="text" value="diostatus"/>
Wifi On Command	<input type="text" value="wifion"/>
Wifi Off Command	<input type="text" value="wifioff"/>

- **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 Alarm

SMS Alarm

## RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm

Singal Quality Threshold

1

Failed Times Threshold

5

Success Times Threshold

2

- **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**

## Phone Number

### Phone Number Configuration

NUM1

SMS Command

SMS Alarm

Phone Number

- **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.

## ➤ SMS

### Send SMS

Receiver Phone Number

Message

- **Receiver Phone Number:** the Phone number that receive message.
- **Message:** the content of message
- **Submit:** click button “Submit” to send message immediately.

## 3.5.8 VPN

### 3.5.8.1 IPSEC

#### IPsec

##### IPsec Configuration

Enable

Exchange mode

Authentication method

Remote VPN endpoint

Preshared Keys

Local subnet

Remote subnet

- **Enable:** enable IPSEC feature
- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main mode are supported.
- **Authentication method:** 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.
- **Preshared Keys:** it is known as PSK, the length is 16 to 32.
- **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

The phase must match with another incoming connection to establish IPsec

Encryption algorithm

Hash algorithm

DH group

## Phase 2 Proposal

The phase must match with another incoming connection to establish IPsec

Encryption algorithm

PFS group

Authentication

**Notes:**



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

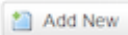
### 3.5.8.2 PPTP

#### Point-to-Point Tunneling Protocol

##### PPTP Configuration

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

Name	Type	Enable	
	Server	No	 

New instance name:  Role:  

- Client
- Server

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

### Main Settings

Enable

Server

Username

Password  

MTU

Keep Alive

Use default gateway

Use DNS servers advertised  
by peer

- **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.

### ➤ PPTP Server Configuration

## PPTP Server Instance:

### Main Settings

Enable


Local IP

Remote IP

Remote IP end

ARP Proxy

Debug

Username	Password
<input type="text" value="youruser"/>	<input type="password" value="*****"/> 
<input type="button" value="Add"/>	
<input type="button" value="Save &amp; Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>	

- **Local IP:** indicate server's IP address.
- **Remote IP:** the remote IP address leases start
- **Remote IP end:** the remote IP address lease end.
- **ARP Proxy:** if the remote IP has the same subnet with LAN, check it for connecting each other.
- **Debug:** for PPTP server debug, the log can be monitored in system log.
- **Username:** server authentication username
- **Password:** server authentication password.

### 3.5.8.3 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 Tuneling Protocol


##### L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
New instance name: <input type="text"/> Role: <input type="text" value="Client"/> <input type="button" value="Add New"/>			
<div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #007bff; color: white; padding: 2px;">Client</span>            Server         </div>			

#### ➤ L2TP Client configuration

## L2TP Client Instance: Bbbbb

### Main Settings

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

- **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.

### ➤ L2TP Server configuration



## L2TP Server Instance: L2tpd\_server

### Main Settings

Enable


Local IP

Remote IP range begin

Remote IP range end

Remote LAN IP

Remote LAN netmask

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

- **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.
- **Remote LAN IP:** L2TP client IP.
- **Remote LAN netmask:** the mask of L2TP client IP, the default value is 255.255.255.0
- **Username:** server authentication username
- **Password:** server authentication password.

### 3.5.8.4 OpenVPN

This page is a list of configured OpenVPN 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

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

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

Client configuration for an etherr Add

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

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 --

### 3.5.8.5 GRE tunnel

## GRE Tunnel

### GRE Tunnel Configuration

Enable

TTL

MTU

Peer IP Address

Remote Network IP

Remote Netmask

Local Tunnel IP

Local Tunnel Mask

Local Gateway

- **Enable:** enable GRE tunnel feature
- **TTL:** Time-to-live
- **MTU:** Maximum transmission unit.
- **Peer IP address:** Remote WAN IP address.
- **Remote Network IP:** remote LAN subnet address
- **Remote Netmask:** remote LAN subnet mask
- **Local Tunnel IP:** Virtual IP address. cannot be in same subnet as LAN network.
- **Local Tunnel Mask:** Virtual IP mask.
- **Local Gateway:**

### 3.5.9 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	1534I9866a.iok.la <i>No data</i>	<input checked="" type="checkbox"/>	Never Verify	PID: 3229	Edit  Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	-----	Edit  Delete

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

### Details for: example\_ipv4

[Basic Settings](#)[Advanced Settings](#)[Timer Settings](#)[Log File Viewer](#)Enabled IP address version  IPv4-Address IPv6-AddressDDNS Service provider [IPv4] Hostname/Domain Username Password 

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

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file

- **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.

Check Interval

Force Interval

Error Retry Counter

Error Retry Interval

- **Check Interval:** the minimum check interval is 1 minute=60seconds.
- **Force interval:** the minimum check interval is 1 minute=60seconds.
- **Error Retry Counter:** On Error the script will stop execution after given number of retries. The default setting of '0' will retry infinite.


[Basic Settings](#)[Advanced Settings](#)[Timer Settings](#)[Log File Viewer](#)[Read / Reread log file](#)

```
/var/log/ddns/example_ipv4.log  
Please press [Read] button
```

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.

**Details for: example\_ipv4**[Basic Settings](#)[Advanced Settings](#)[Timer Settings](#)[Log File Viewer](#)Enabled IP address version  IPv4-Address  
 IPv6-AddressDDNS Service provider [IPv4] Hostname/Domain Username Password  Use HTTP Secure Path to CA-Certificate

## 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 [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file

### 3.5.10 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 Radio Module Configuration

Exchange data between radio module and serial

Enable

Connect mode

Serial baudrate

Serial parity

Serial databits

Serial stopbits

• Enable: conflict with DTU, please disable DTU firstly

- **Connect Mode:** Serial only

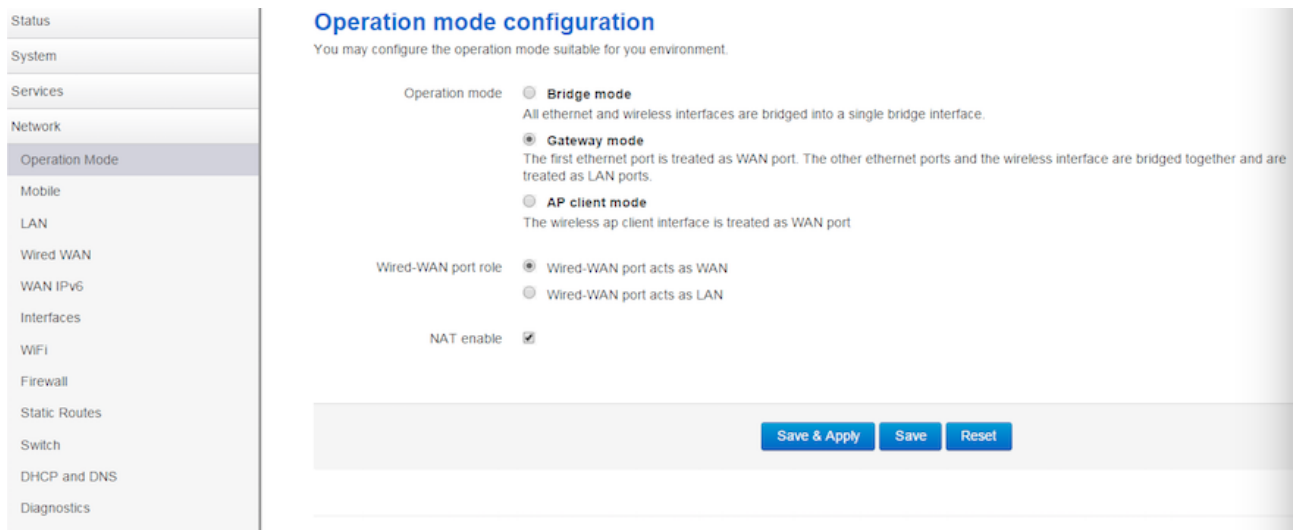
### Modem to Serial Settings

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

## 3.6 Network Configuration



## 3.6.1 Operation Mode



### ➤ Operation mode

- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
- **Gateway:** The first Ethernet port is treated as 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 5 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.

## 3.6.2 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.

Status

System

Services

Network

Operation Mode

**Mobile**

LAN

Wired WAN

WAN IPv6

Interfaces

WiFi

Firewall

Static Routes

Switch

DHCP and DNS

Diagnostics

Loopback Interface

Hostnames

Dynamic Routing

QoS

Logout

General Data Limitation

### Mobile Configuration

SIM 1

Enable

Mobile connection

APN

PIN number

Dialing number

Authentication method

Network Type

MTU

Online mode

- **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.

### 3.6.3 Cell mobile data limitation

#### Data Limitation Configuration

Enable data limitation

Period

Start day

SIM data limit(MB)

Enable alarm

Phone number

Warning percent of Data Used  %

Used(MB)

- **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.

## 3.6.4 LAN settings

### Interfaces - LAN

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

#### Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status



Uptime: 0h 24m 3s

MAC-Address: 90:22:00:80:03:00

RX: 1.34 MB (13877 Pkts.)

TX: 4.46 MB (12981 Pkts.)

IPv4: 192.168.1.1/24

IPv6: fd35:ff0d:10d1::1/60

Protocol

Really switch protocol?

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers  

IPv6 assignment length

IPv6 assignment hint

- **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.

[General Setup](#) [Advanced Settings](#) [Physical Settings](#) [Firewall Settings](#)

Bring up on boot

Use builtin IPv6-management

Override MAC address

Override MTU

Use gateway metric





- **Bring up on boot:** if checked, LAN interface will be set to up when system 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.

## Common Configuration

[General Setup](#) [Advanced Settings](#) [Physical Settings](#) [Firewall Settings](#)

Bridge interfaces

Enable STP

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

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

## DHCP Server

[General Setup](#) [Advanced Settings](#) [IPv6 Settings](#)

Ignore interface

Start

Limit

Leasetime

- **Ignore interface:** if it is unchecked, 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.


## DHCP Server

[General Setup](#)
[Advanced Settings](#)
[IPv6 Settings](#)

Dynamic DHCP

Force

IPv4-Netmask

DHCP-Options  

- **Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force:** Force DHCP on this network even if another server is detected.
- **IPv4-Netmask:** Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options:** Define additional DHCP options, for example '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients.

## DHCP Server

[General Setup](#)
[Advanced Settings](#)
[IPv6 Settings](#)


Router Advertisement-Service


DHCPv6-Service

NDP-Proxy

DHCPv6-Mode

Always announce default router

Announced DNS servers  

Announced DNS domains  

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

### 3.6.5 wired-WAN

#### Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status

 eth0.2

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

Protocol

DHCP client

Hostname to send when requesting DHCP

Cell\_Router

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

#### Common Configuration

General Setup

Status

 eth0.2

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

Protocol

PPPoE

Really switch protocol?

 Switch protocol

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

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status

pppoe-wan

Protocol

PPPoE

PAP/CHAP username

PAP/CHAP password

Access Concentrator

auto

Service Name


auto

**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.

### 3.6.6 WiFi Settings

radio0: Master "Cell\_AP\_0002b2"

#### Wireless Overview


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

45% **SSID:** Cell\_AP\_0002b2 | **Mode:** Master  
**BSSID:** 90:22:06:00:02:B2 | **Encryption:** None

[Wifi Restart](#) [AP Client](#) [Add](#)  
[Disable](#) [Edit](#) [Remove](#)

#### Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cell_AP_0002b2	68:A8:6D:48:77:5E	192.168.1.105	-78 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 4, 20MHz

- **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.



### 3.6.6.1 Wifi General configuration

#### Device Configuration

General Setup **Advanced Settings**

---

Status 54%  
**Mode:** Master | **SSID:** Cell\_AP\_0002b2  
**BSSID:** 90:22:06:00:02:B2 | **Encryption:** None  
**Channel:** 11 (2.462 GHz) | **Tx-Power:** 20 dBm  
**Signal:** -72 dBm | **Noise:** 0 dBm  
**Bitrate:** 43.3 Mbit/s | **Country:** 00

Wireless network is enabled

Operating frequency

Mode	Channel	Width
N	11 (2462 MHz)	20 MHz

Transmit Power

- **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.

### 3.6.6.2 WiFi Advanced Configuration

#### Device Configuration

**General Setup** Advanced Settings

---

Country Code

Distance Optimization

Fragmentation Threshold

RTS/CTS Threshold

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

### 3.6.6.3 WiFi Interface Configuration

#### Interface Configuration




General Setup

Wireless Security

MAC-Filter

ESSID

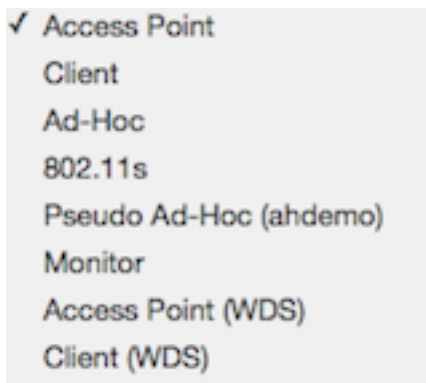
Mode

Network  ifmobile:   
 lan:   
 wan6:   
 create:

Hide Extended Service Set Identifier

WMM Mode

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



- **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

Cipher

Key

Enable WPS pushbutton,   
requires WPA(2)-PSK

- **Encryption:**

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




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



## Interface Configuration

General Setup    **Wireless Security**    MAC-Filter

MAC-Address Filter

MAC-List

00:1E:10:1F:00:00 (10.223.164)	
68:A8:6D:48:77:5E (dentydeME)	
90:22:06:80:02:01 (Cell_Router)	

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

### 3.6.6.4 WiFi AP client

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

signals.

## Join Network: Wireless Scan

82% **MERCURY\_FE2A** Join Network


Channel: 3 | Mode: Master | BSSID: 8C:F2:28:FD:FE:2A | Encryption: mixed WPA/WPA2 - PSK

[Back to overview](#) [Repeat scan](#)

- **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.

## Join Network: Settings

Replace wireless configuration

WPA passphrase  

Name of the new network

[Submit](#) [Back to scan results](#)

- **Step 3)** Join Network Settings  
Replace wireless configuration: An additional wireless network will be created if it is unchecked. Otherwise it will replace the old configuration.  
WPA passphrase: specify the secret encryption key here.  
Name of the new network: the default value is wwan. 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.

## Device Configuration

General Setup

Advanced Settings

Status



**Mode:** Client | **SSID:** MERCURY\_FE2A  
**BSSID:** 8C:F2:28:FD:FE:2A | **Encryption:** -  
**Channel:** 11 (2.462 GHz) | **Tx-Power:** 0 dBm  
**Signal:** 0 dBm | **Noise:** 0 dBm  
**Bitrate:** 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Disable






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

## Interface Configuration

General Setup

Wireless Security

ESSID	MERCURY_FE2A
Mode	Client
BSSID	8C:F2:28:FD:FE:2A

Network	<input type="checkbox"/>	ifmobile: 
	<input type="checkbox"/>	lan: 
	<input type="checkbox"/>	wan: 
	<input type="checkbox"/>	wan6: 
	<input checked="" type="checkbox"/>	wwan: 
	<input type="checkbox"/>	create: <input type="text"/>

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

## Wireless Overview

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

**68%** SSID: Cell\_AP\_0002b2 | Mode: Master  
BSSID: 90:22:06:00:02:B3 | Encryption: None

**85%** SSID: MERCURY\_FE2A | Mode: Client  
BSSID: 8C:F2:28:FD:FE:2A | Encryption: WPA2 PSK (CCMP)

Wifi Restart
AP Client
Add

Disable
Edit
Remove

Disable
Edit
Remove

## Associated Stations






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

## 3.6.7 Interfaces Overview

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

### Interfaces

#### Interface Overview

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

## 3.6.8 Firewall

### 3.6.8.1 General Settings

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

### Firewall - General Settings

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

#### General Settings

Enable SYN-flood protection

Drop invalid packets

Input

Output

Forward

### 3.6.8.2 Port Forwards

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

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

### Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

#### Port Forwards

Name	Match	Forward to	Enable	Sort
<i>This section contains no values yet</i>				

New port forward:

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

- **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.

### 3.6.8.3 traffic rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router. The traffic rules overview page content the follow functionalities.

Traffic rules list:

#### Traffic Rules

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

Open ports on router and create new forward rules:



### Open ports on router:

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

*This section contains no values yet*

### New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
<input type="text" value="New SNAT rule"/>	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 - forwardtest

This page allows you to change advanced properties of the traffic rule entry, such as matched sou


Rule is enabled  Disable

Name

Restrict to address family

Protocol







Match ICMP type

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

Source MAC address

Source address

Source port

- Destination zone
- Device (input)
  - Any zone (forward)
  - lan: lan:  
  - openvpn: (empty)
  - vpnzone: (empty)
  - wan: wan:  wan6:  ifmobile:  wwan: 

Destination address

Destination port

Action

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!

### 3.6.8.4 DMZ

[General Settings](#) [Port Forwards](#) [Traffic Rules](#) [DMZ](#) [Security](#)

## DMZ Configuration

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

Enable DMZ

IP address

Protocol

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

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

**Note:** When DMZ host is settled, the computer is completely exposed to the external

network; the firewall will not influence this host.

### 3.6.8.5 Security

General Settings

Port Forwards

Traffic Rules

DMZ

Security

#### System security configuration

SSH access from WAN

Ping from WAN to LAN

#### HTTPS Remote Access

HTTPS access from WAN

Remote network

IP address

Netmask

#### HTTP Remote Access

HTTP access from WAN

Remote network

- **SSH access from WAN:** allow or deny users access TR1803 /TR1804/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.

### 3.6.9 Static Routes

#### Routes

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

##### Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	
lan		255.255.255.255		0	1500	Delete

Add

##### Static IPv6 Routes

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

This section contains no values yet

Add

Save & Apply Save Reset

- **Interface:** You can choose the corresponding interface type.
  - **Target:** the destination host IP or network.
- Gateway:** IP address of the next router.

Notice:

- 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.

### 3.6.10 Switch

#### VLANs on "switch0" (rt305x-esw)

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

Add

#### Note:

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

## 3.6.11 DHCP and DNS

### DHCP and DNS

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

#### Server Settings

General Settings

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.

Suppress logging Allocate IP sequentially Filter private Filter useless Localise queries Expand hosts No negative cache Strict order Bogus NX Domain Override  DNS server port DNS query port Max. DHCP leases Max. EDNS0 packet size Max. concurrent queries 

- **Suppress logging:** Suppress logging of the routine operation of these protocols
- **Allocate IP sequentially:** Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private:** Do not forward reverse lookups for local networks.
- **Filter useless:** Do not forward requests that cannot be answered by public name servers.
- **Localise queries:** Localise hostname depending on the requesting subnet if multiple IPs are available.
- **Expand hosts:** Add local domain suffix to names served from hosts files.
- **No negative cache:** Do not cache negative replies, e.g. for 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.

## 3.6.12 Diagnostics

### Diagnostics

#### Network Utilities

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

- **Ping** : it is a tool 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

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

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

## 3.6.13 Loopback Interface

### Loopback Interface Configuration

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

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

## 3.6.14 Dynamic Routing

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



## Dynamic Routing

### Zebra

Enable

Password  

### OSPF

Enable

Password  

### OSPF6

Enable

Password  


### RIP

Enable

Password  

### RIPng

Enable

Password  

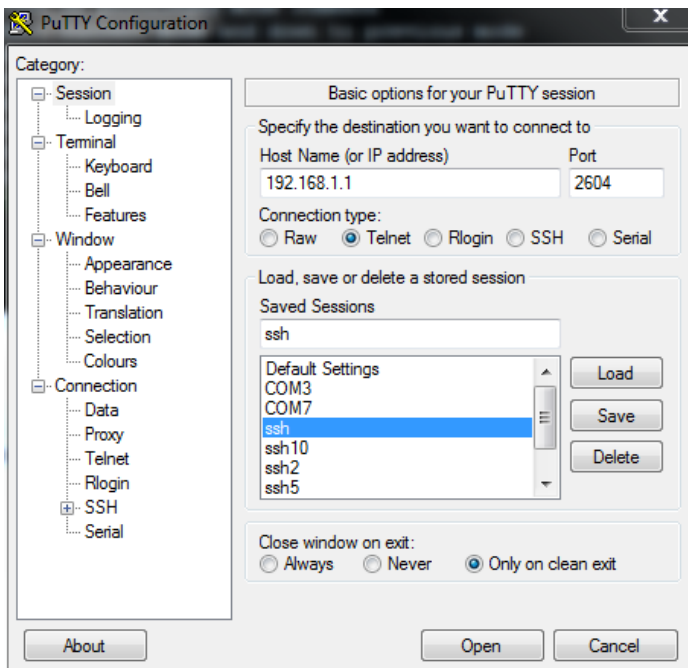
### BGP

Enable

Password  

- **Zebra:** Zebra is an IP routing manager. Telnet port number is 2601.
- **OSPF:** Open Shortest Path First. Telnet port number is 2604.
- **OSPF6:** Open Shortest Path First for IPv6. Telnet port number is 2606.
- **RIP:** Routing Information Protocol. Telnet port number is 2602.
- **RIPng:** it is an IPv6 reincarnation of the RIP protocol. Telnet port number is 2603.
- **BGP:** Border Gateway Protocol. Telnet port number is 2605.

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> █
```

### 3.6.15 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

WAN

Enable

Classification group

Calculate overhead

Half-duplex

Download speed (kbit/s)

Upload speed (kbit/s)

- **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	<input type="button" value="↑"/> <input type="button" value="↓"/>
normal	all	all	all	TCP	20,21,25,80,110,443,993,995		ftp, smtp, http(s), imap	<input type="button" value="↑"/> <input type="button" value="↓"/>
express	all	all	all	all	5190		AOL, iChat, ICQ	<input type="button" value="↑"/> <input type="button" value="↓"/>
normal	all	all	all	all	all			<input type="button" value="↑"/> <input type="button" value="↓"/>

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.

