Industrial Grade 2G 3G 4G Cellular Router

User Manual

H820Q Series

E-Lins Technology Co., Limited

PHONE: +86-755-29230581

Email: sales@e-lins.com

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

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

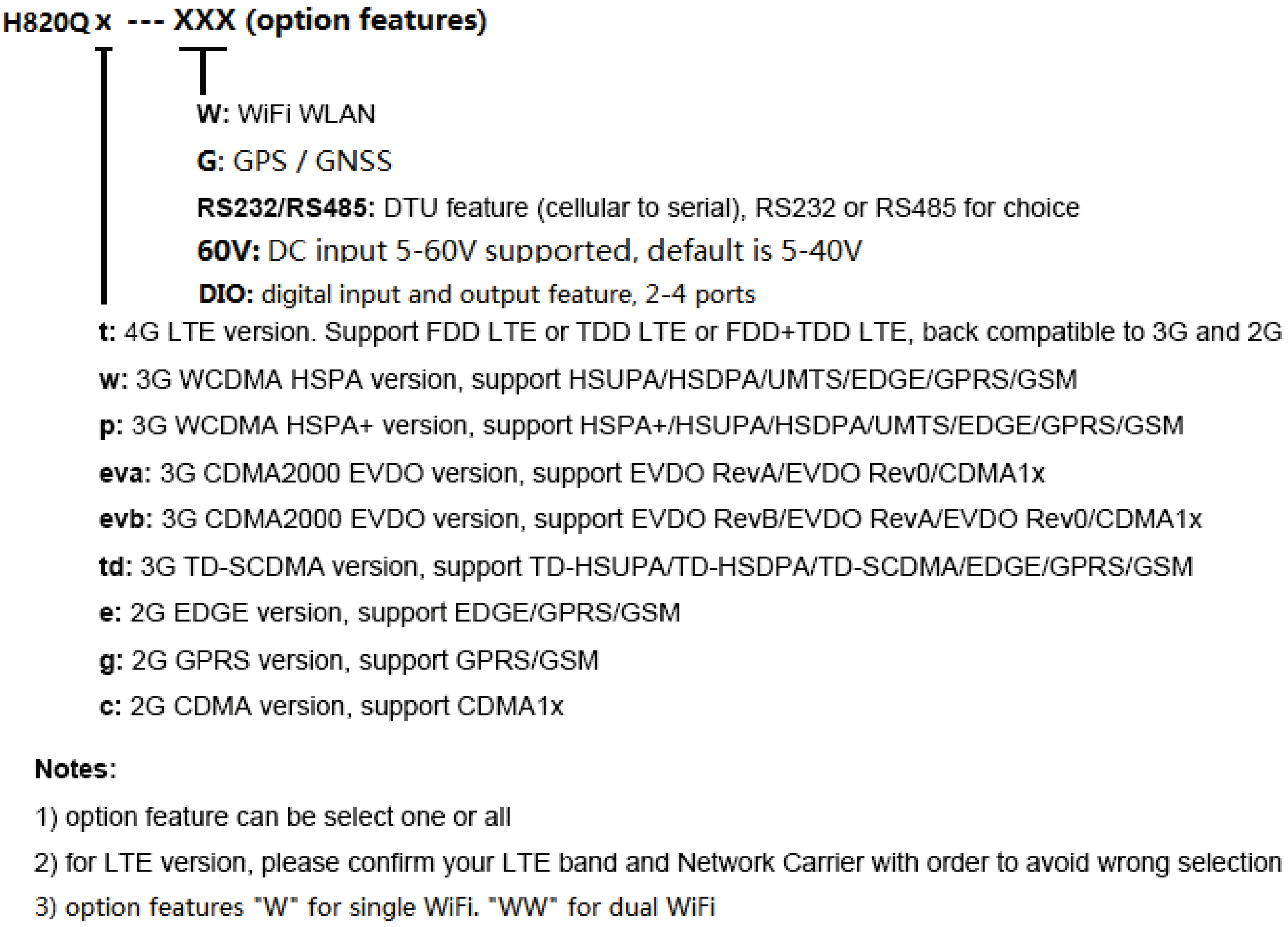
Content

Chapter 1

1 Preparation job before configuration

1.1 Learn your router version and feature

1) H820Q series contains different version and option feature. Please learn it before using it. H820Q series defines the model as follows,



H820Q x --- XXX (option features)

W: WiFi WLAN

G: GPS / GNSS

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

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

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

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

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

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

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

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

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

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

g: 2G GPRS version, support GPRS/GSM

c: 2G CDMA version, support CDMA1x

Notes:

1) option feature can be select one or all

2) for LTE version, please confirm your LTE band and Network Carrier with order to avoid wrong selection

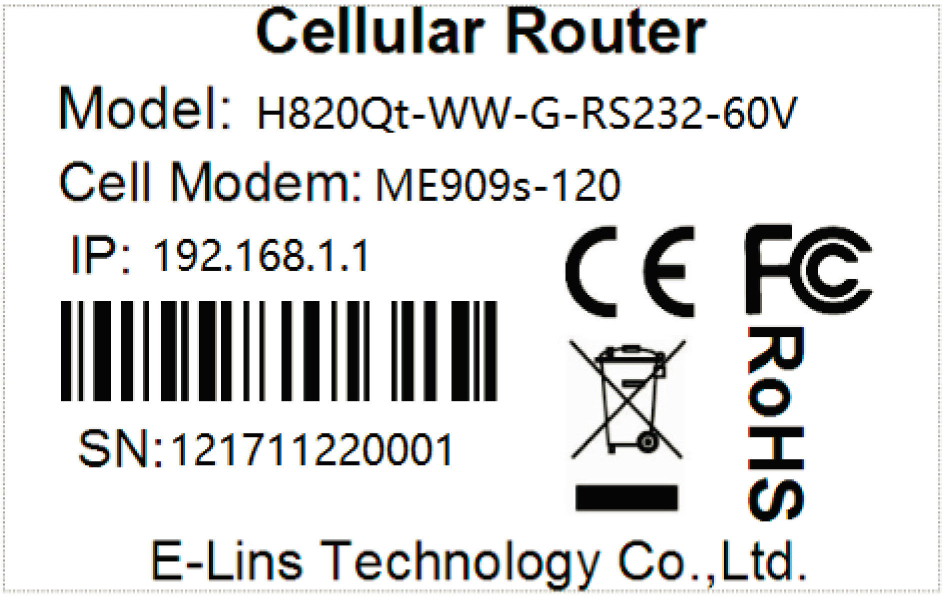
3) option features "W" for single WiFi. "WW" for dual WiFi

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

1) WiFi Feature (Dual WiFi, high gain WiFi)
2) GPS/GNSS feature
3) Serial to cellular feature, RS232 or RS485 can choose one
4) Voice/SMS control
5) DC5V~60V
6) BGP, OSPF, RIP, etc.
7) RMS (Remote Management System)
8) DI/DO (Digital Input /Output): H820Q does not include DI/DO feature default. Please skip this feature in the manual.

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

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



Cellular Router

Model: H820Qt-WW-G-RS232-60V

Cell Modem: ME909s-120

IP: 192.168.1.1

SN:121711220001

CE FC RoHS

E-Lins Technology Co.,Ltd.

1.2 Prepare SIM Card and working condition

1. H820Q router has different version. Study your router version before installation.
2. For GSM/GPRS/EDGE/HSDPA/HSUPA/HSPA/HSPA+/4G LTE version, please get a SIM card with data business.
3. For CDMA2000 EVDO/CDMA1x version, please get a UIM card with data business or inform us before order if the network uses non-ruim (nam-flashing).

4. Make sure the sim card or uim card is with enough data business and balance.
5. Make sure the signal is good enough where you test or install the router. Weak signal will make the router no work. If you find your signal strength is not good, please contact us for high gain antenna.
6. Different countries and carriers use different network band and frequency. E-Lins packs units with free world-wide-use antenna. It can work, but the data speed or signal may not be good at your sites. Please buy dedicated high gain antenna from your local suppliers or contact E-Lins to OEM/ODM the antenna.

1.3 Highly recommendation for the configuration

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

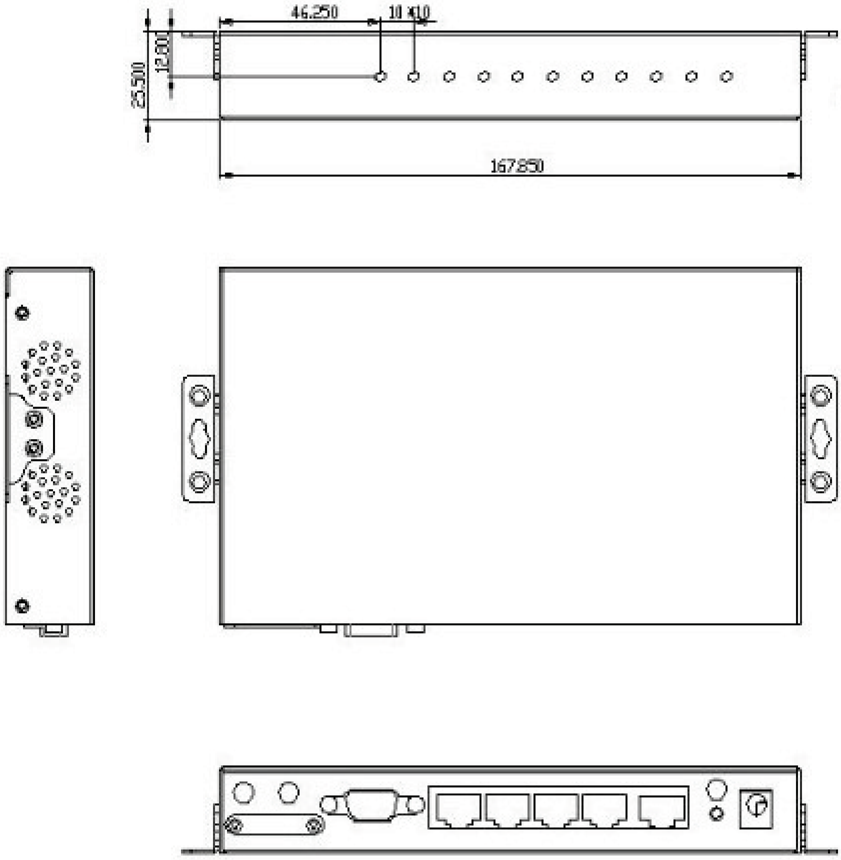
Chapter 2

2 Hardware Installation

This chapter mainly describes the appearance, model and function of H820Q series and how to install and set the configurations.

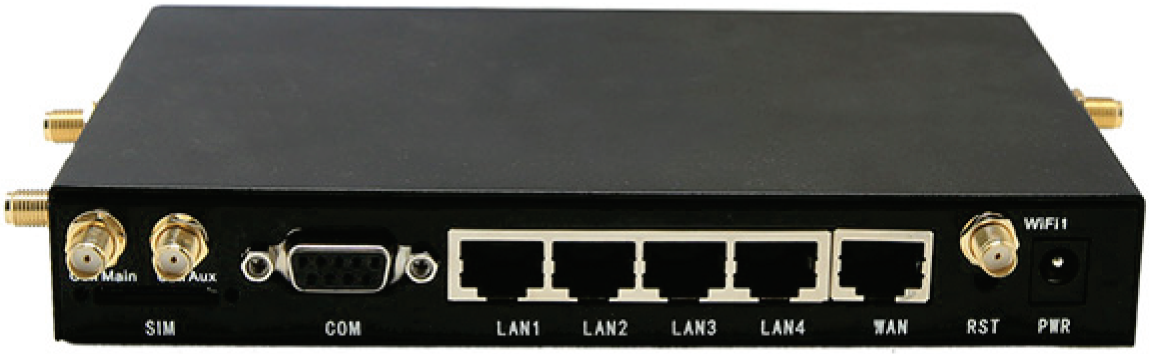
1. *Overall Dimension*
2. *Accessories Description*
3. *Installment*

2.1 Overall Dimension

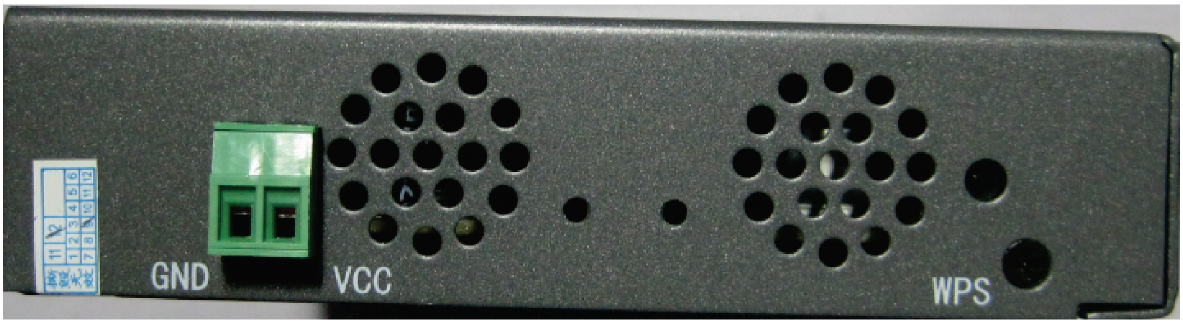


2.2 The Ports

Back Pictures:



CELL Main: for cellular
Cell AUX: for cellular diversity receiving MIMO
WiFi1-5: for WiFi
GPS: for GPS/GNSS
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, DC5~60V option depends on the router version.



GND: DC wire ground
VCC: DC wire positive pole. DC5~40V, DC5~60V option depends on the router version
WPS: WPS button

Antenna Connection Table

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

2.3 Installment

H820Q series should be installed and configured properly before putting in service. The installation and configuration should be done or supervise by qualified engineer.

Notes:
Do not install H820Q 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.

⚠ **Notes:**

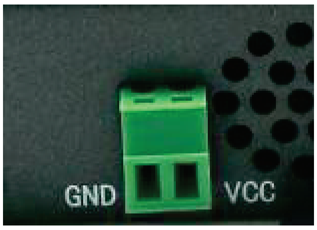
SIM/UIM card does not reach the designated position, the equipment can not find a card, can't work normally, therefore inserted a try to check again for a *SIM Card* is stuck fast.

2.5 The installation of terminal blocks

This chapter is for version with terminal blocks only. Default, the H820Q is with DB9 connector. Please use DB9 cable to connect H820Q and the equipment directly.

The following is for version with terminal blocks only:
H820Q uses pluggable terminals to connect the user’s data and the power supply. Spacing: 3.81mm, 2 Pins; 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 H820Q products. Using 14~24AWG cable and referring to H820Q 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 H820Q 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 "VCC"(DC5~40V, or DV5~60V).

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input, +5~60V option	Current: 12V/1A
2	GND	Ground	

2.6 Grounding

To ensure a safe, stable and reliable H820Q series operation, Router cabinet should be grounded properly.

2.7 Power Supply

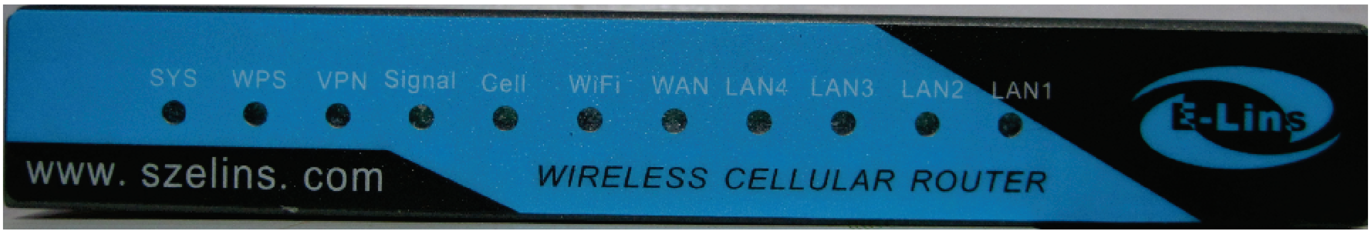
H820Q series can be applied to complicated external environment and usually the power range is very large. So in order to fit the complicated application environment and improve the stability of the system, H820Q series is designed with advanced power management technology. The DC power supply electronic to the device via the pluggable terminal PIN 2(GND) and PIN 1(VCC). Please refer to the above table for the detail definition of the terminal.

Normally, H820Q series input powers supply is +5～+40V (if your H820Q support 60V, the option is +5~+60V). 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 H820Q series via the cable. After provide the power to

H820Q, 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	IPSec VPN tunnel set-up
	Off	IPSec VPN tunnel set-up failure or inactivated
CELL	On	Access to the Internet/Private Network
WiFi	On	Enable
	Off	Disable
WAN	blink	Data transmission in Ethernet
	Off	Ethernet connection abnormal
	On	Ethernet is connected
Signal	Off	No signal, or signal checking is not ready
	blink (2 seconds for on, and 2 seconds for off)	Signal bar is 1
	blink (1 seconds for on, and 1 seconds for off)	Signal bar is 2
	blink (0.5 seconds for on, and 0.5 seconds for off)	Signal bar is 3

3 Software configuration

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

3.1 Overview

H820Q 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.

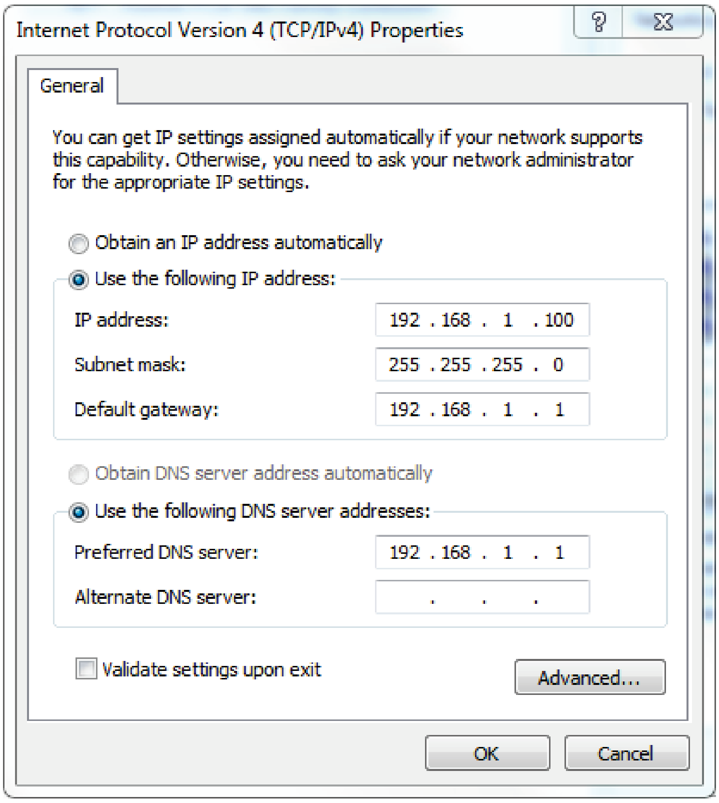
The router default parameters as follow

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

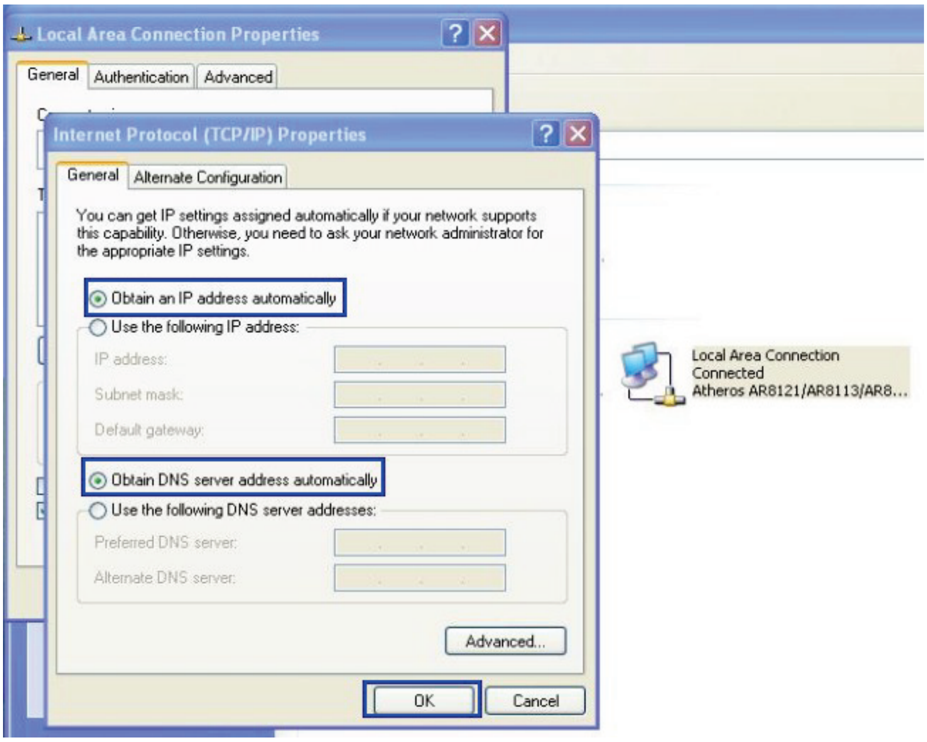
Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

Way 2) DHCP

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



Local Area Connection Properties

General | Authentication | Advanced

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

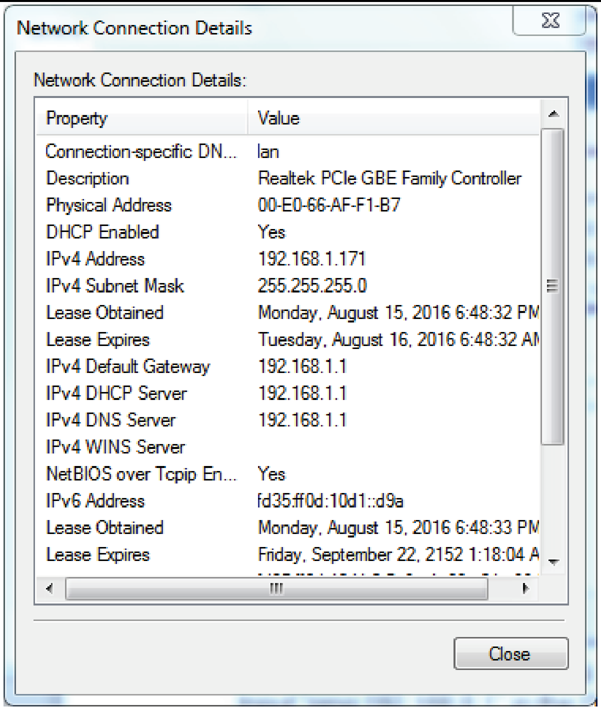
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Local Area Connection
Connected
Atheros AR8121/AR8113/AR8...

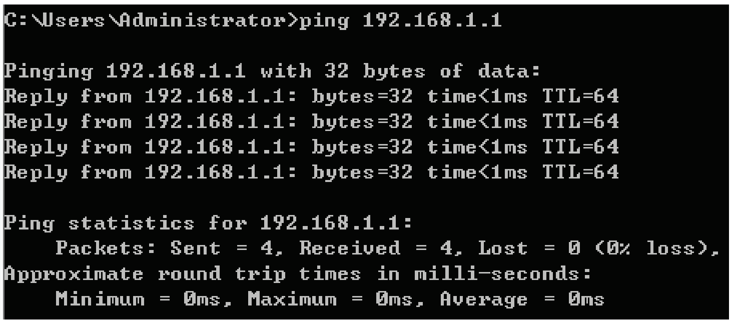


Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	lan
Description	Realtek PCIe GBE Family Controller
Physical Address	00-E0-66-AF-F1-B7
DHCP Enabled	Yes
IPv4 Address	192.168.1.171
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, August 15, 2016 6:48:32 PM
Lease Expires	Tuesday, August 16, 2016 6:48:32 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
IPv6 Address	fd35:ff0d:10d1::d9a
Lease Obtained	Monday, August 15, 2016 6:48:33 PM
Lease Expires	Friday, September 22, 2152 1:18:04 A

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.

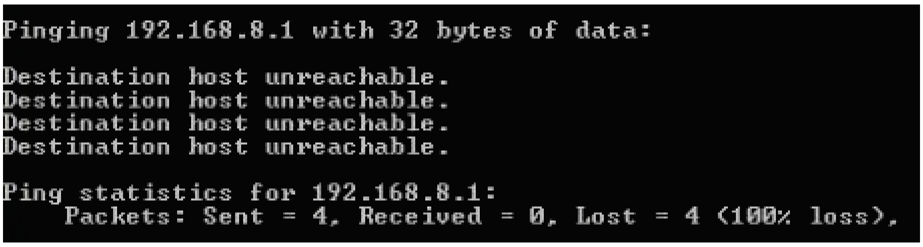


```
C:\Users\Administrator>ping 192.168.1.1

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
```

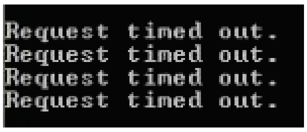
This information means the connection is work.



```
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),
```

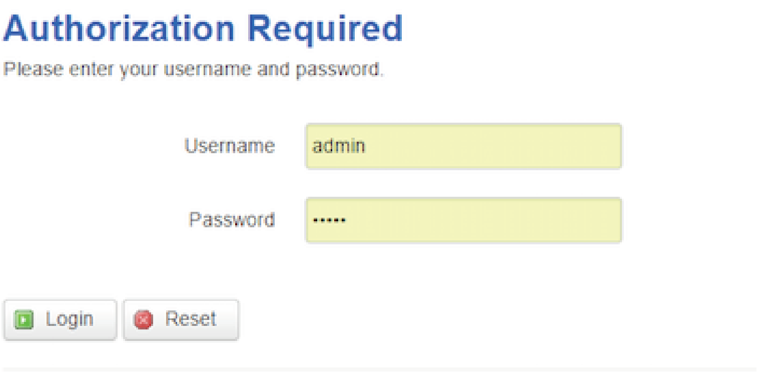


```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

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.

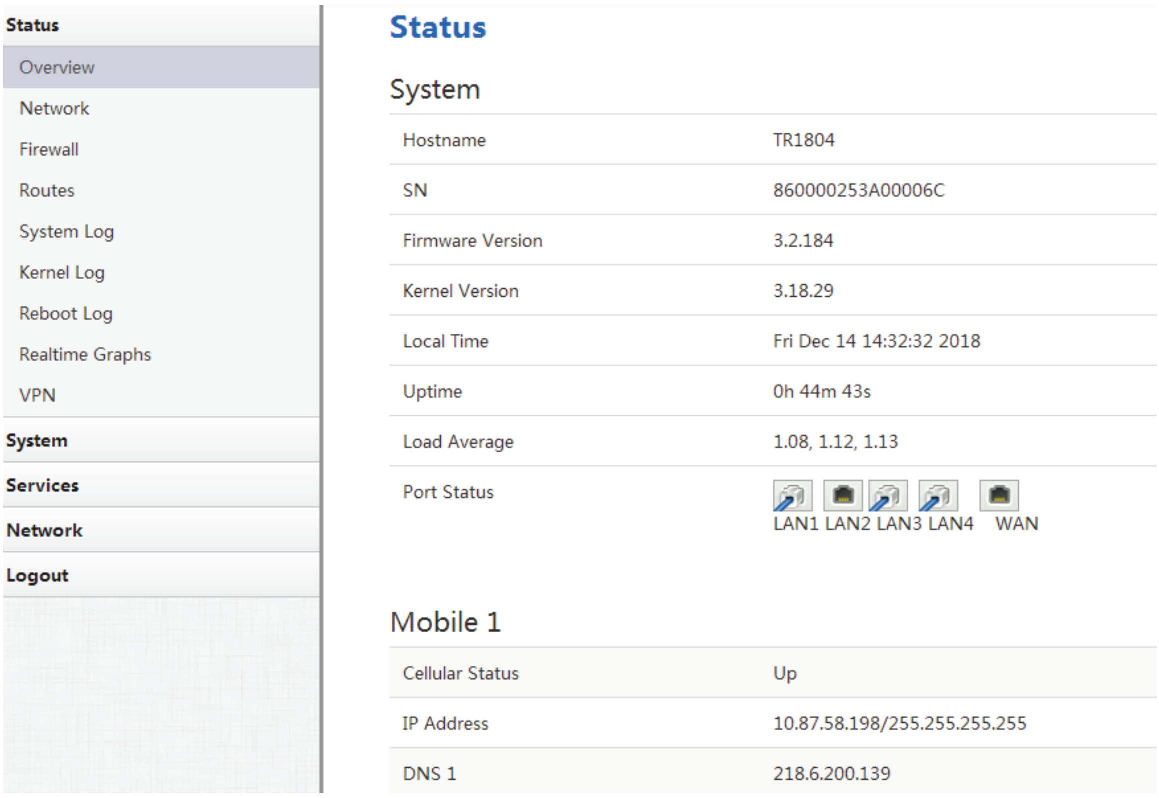


Authorization Required

Please enter your username and password.

Username	admin
Password	•••••

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



Status

System

Hostname	TR1804
SN	860000253A00006C
Firmware Version	3.2.184
Kernel Version	3.18.29
Local Time	Fri Dec 14 14:32:32 2018
Uptime	0h 44m 43s
Load Average	1.08, 1.12, 1.13
Port Status	LAN1 LAN2 LAN3 LAN4 WAN

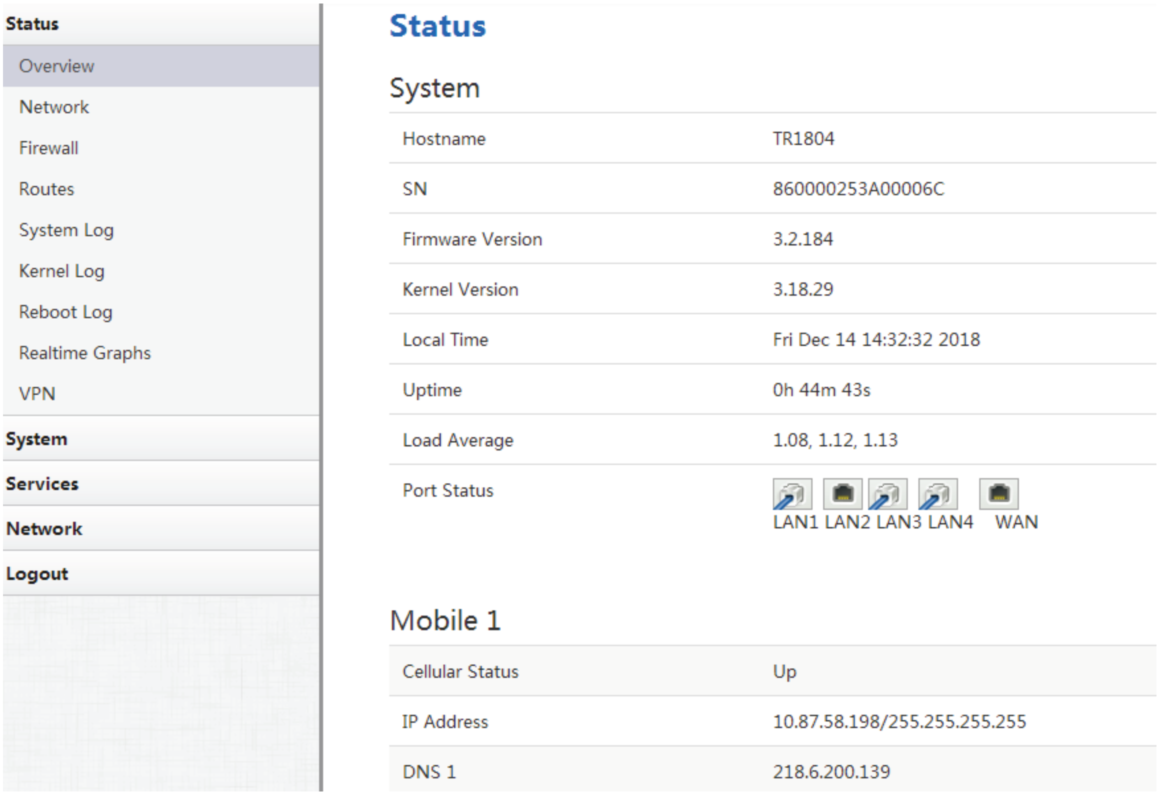
Mobile 1

Cellular Status	Up
IP Address	10.87.58.198/255.255.255.255
DNS 1	218.6.200.139

3.3 Router status

3.3.1 Status overview

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



Status

System

Hostname	TR1804
SN	860000253A00006C
Firmware Version	3.2.184
Kernel Version	3.18.29
Local Time	Fri Dec 14 14:32:32 2018
Uptime	0h 44m 43s
Load Average	1.08, 1.12, 1.13
Port Status	LAN1 LAN2 LAN3 LAN4 WAN

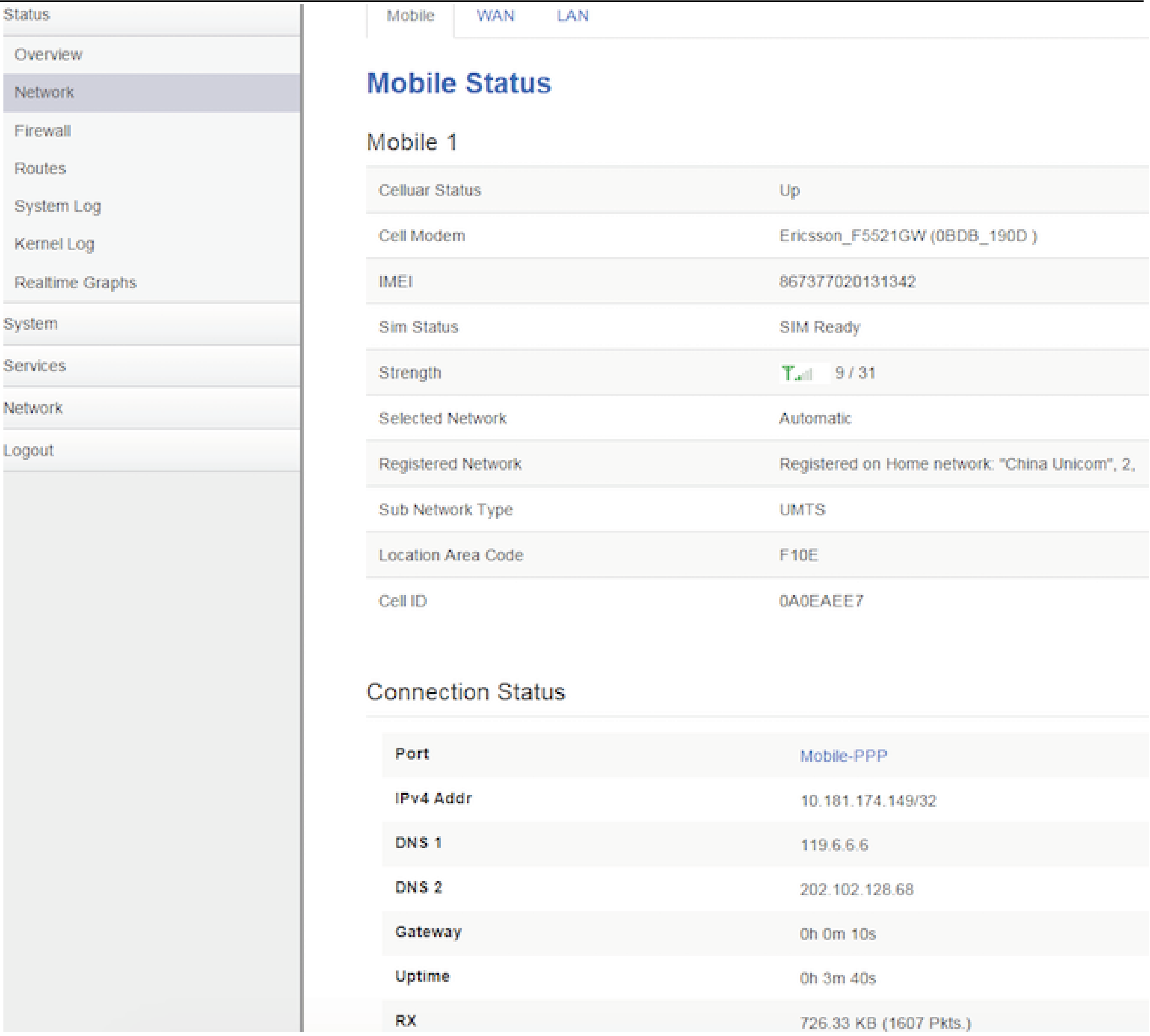
Mobile 1

Cellular Status	Up
IP Address	10.87.58.198/255.255.255.255
DNS 1	218.6.200.139

3.3.2 Network status

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

Cell mobile interface page:



Mobile Status

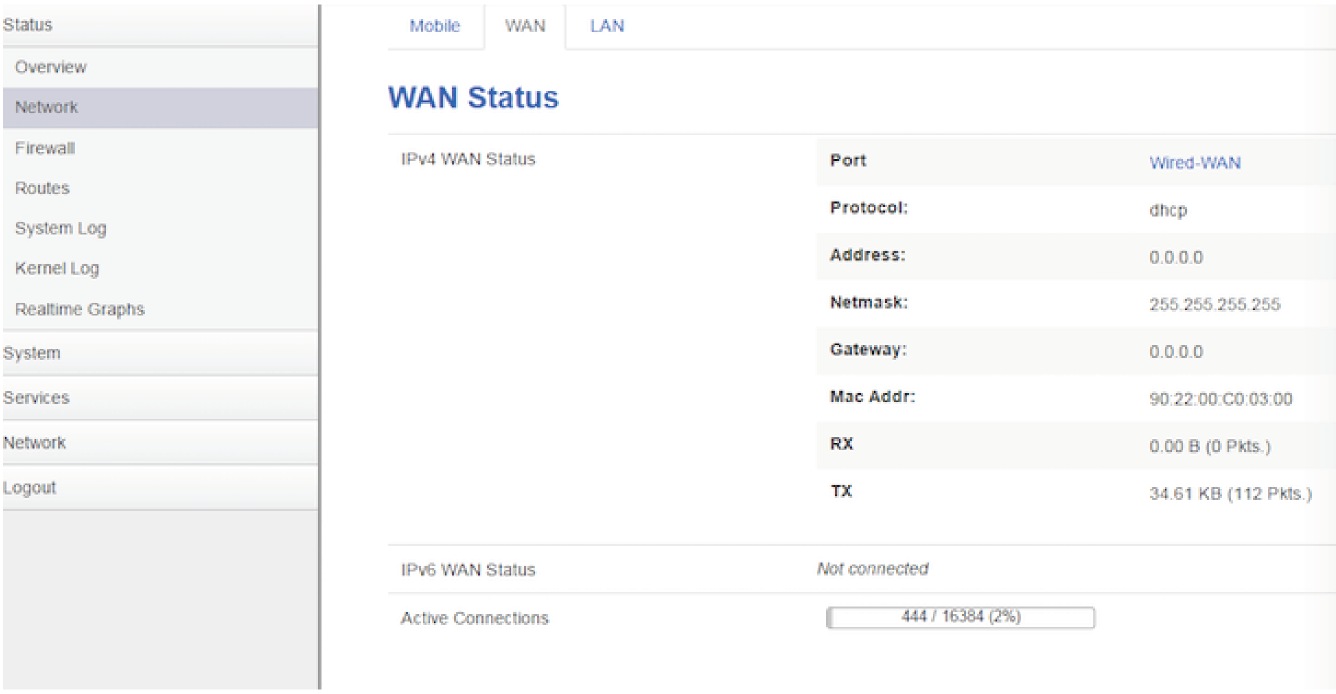
Mobile 1

Celluar Status	Up
Cell Modem	Ericsson_F5521GW (0BDB_190D)
IMEI	867377020131342
Sim Status	SIM Ready
Strength	9 / 31
Selected Network	Automatic
Registered Network	Registered on Home network: "China Unicom", 2,
Sub Network Type	UMTS
Location Area Code	F10E
Cell ID	0A0EAEE7

Connection Status

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:



WAN Status

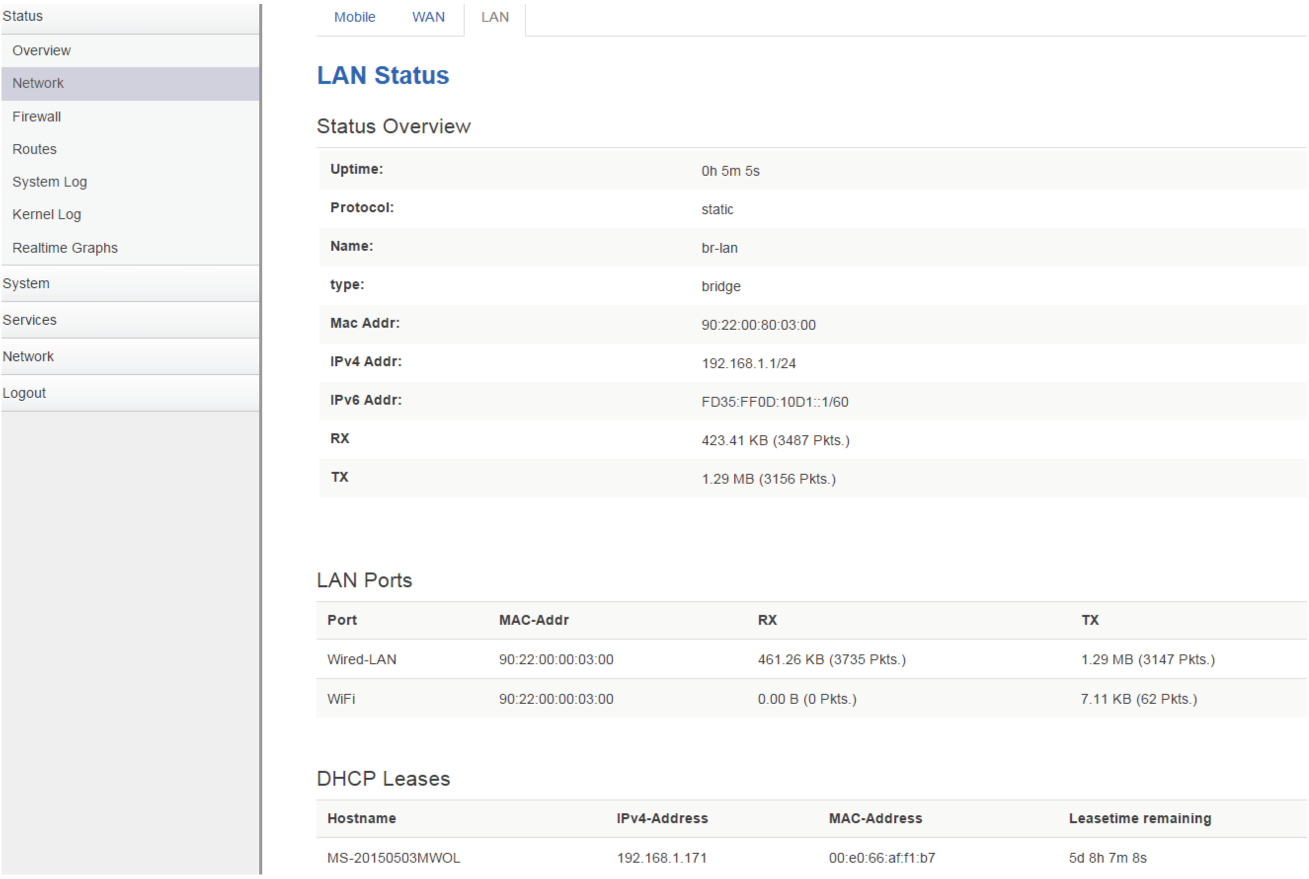
IPv4 WAN Status

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

IPv6 WAN Status *Not connected*

Active Connections 444 / 16384 (2%)

LAN status page:



LAN Status

Status Overview

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

LAN Ports

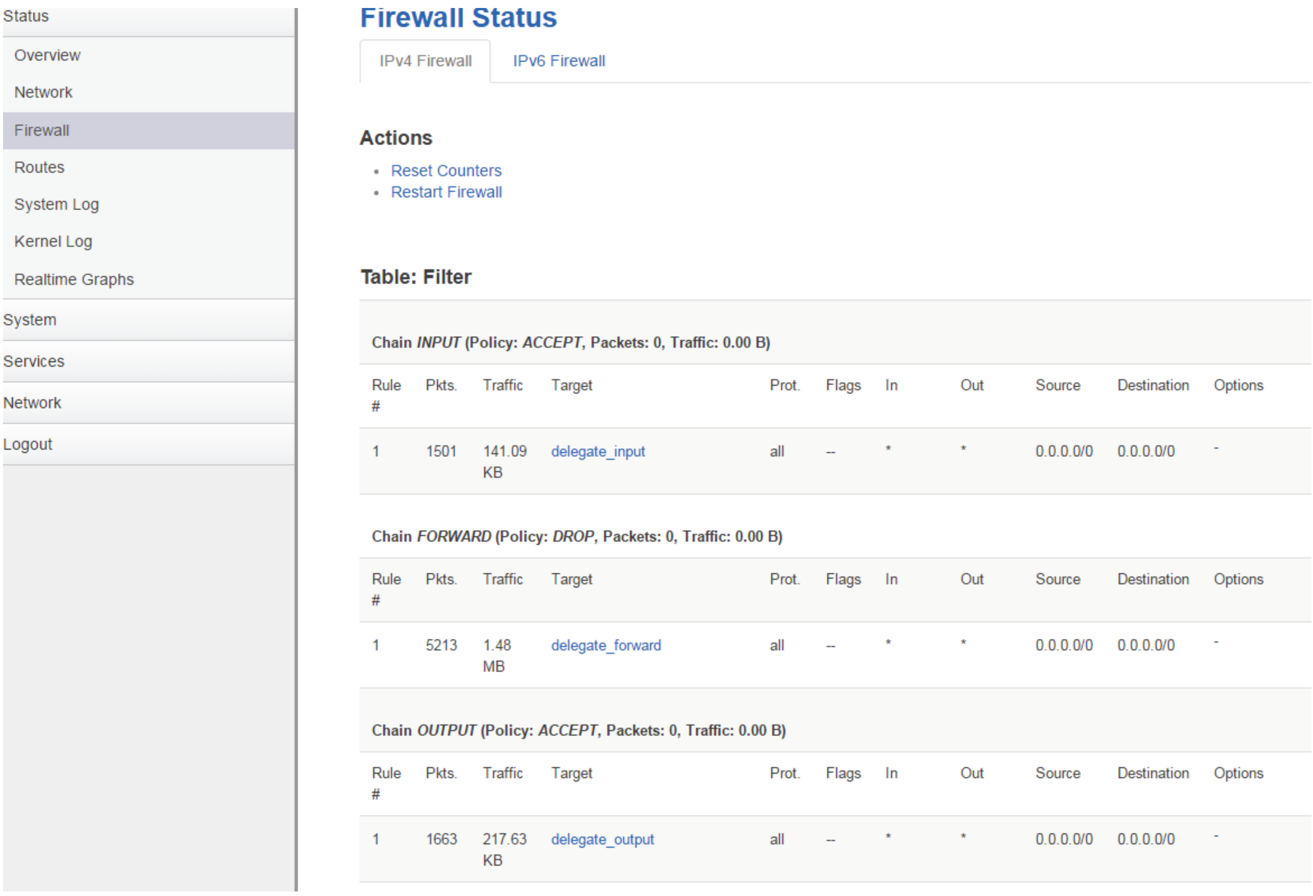
Port	MAC-Addr	RX	TX
Wired-LAN	90:22:00:00:03:00	461.26 KB (3735 Pkts.)	1.29 MB (3147 Pkts.)
WiFi	90:22:00:00:03:00	0.00 B (0 Pkts.)	7.11 KB (62 Pkts.)

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.



Firewall Status

Actions

- Reset Counters
- Restart Firewall

Table: Filter

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1501	141.09 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

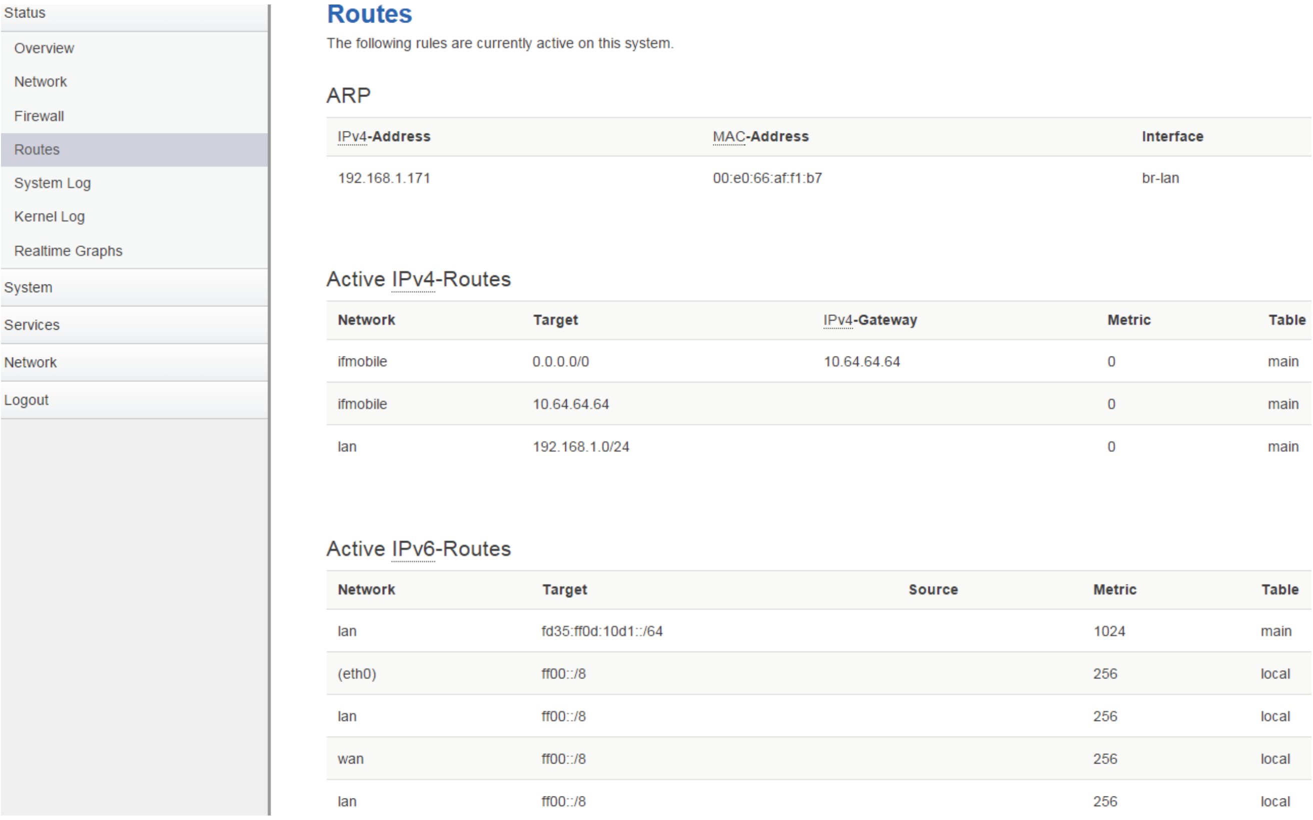
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	5213	1.48 MB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1663	217.63 KB	delegate_output	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.



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

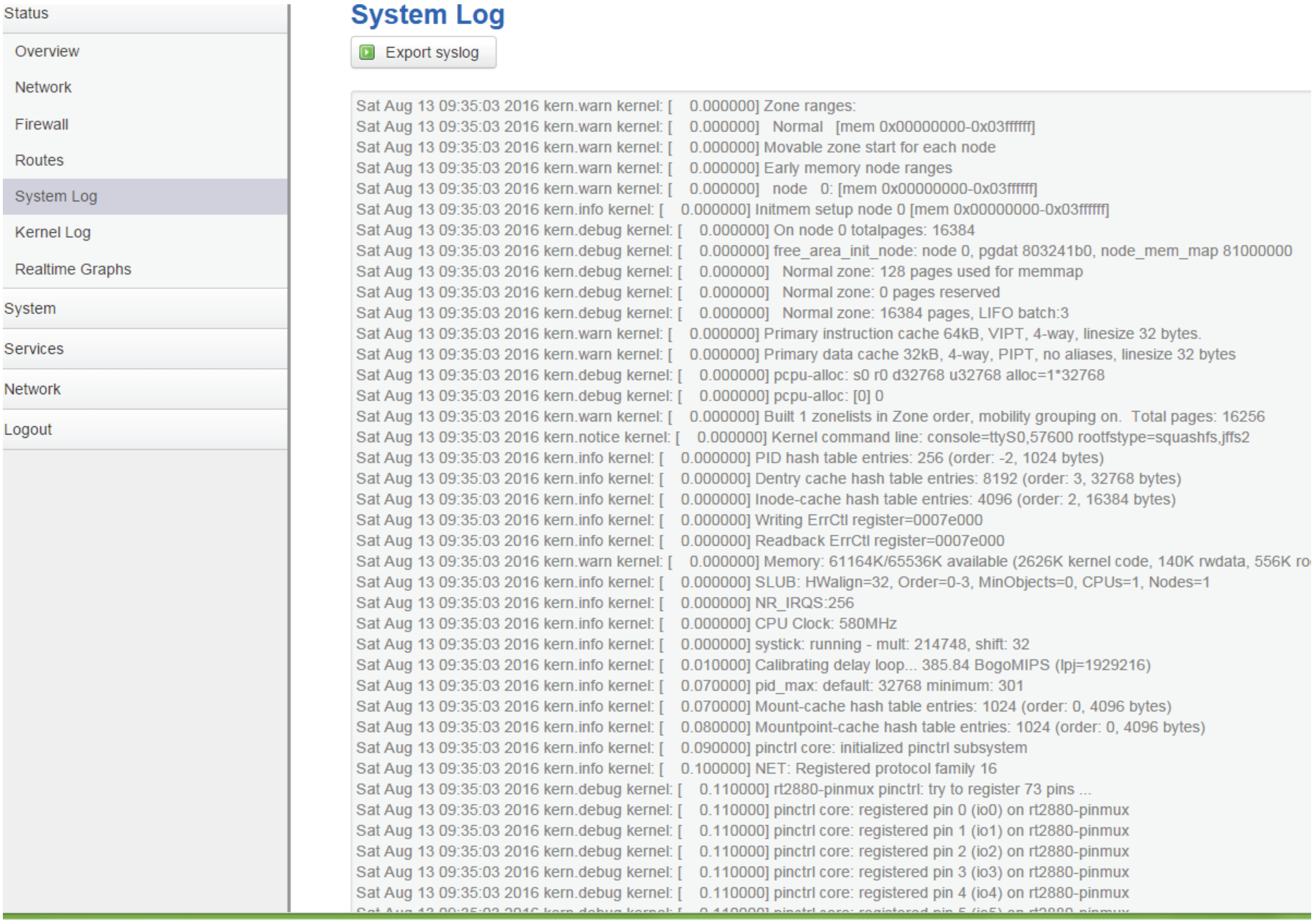
Network	Target	IPv4-Gateway	Metric	Table
ifmobile	0.0.0.0/0	10.64.64.64	0	main
ifmobile	10.64.64.64		0	main
lan	192.168.1.0/24		0	main

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

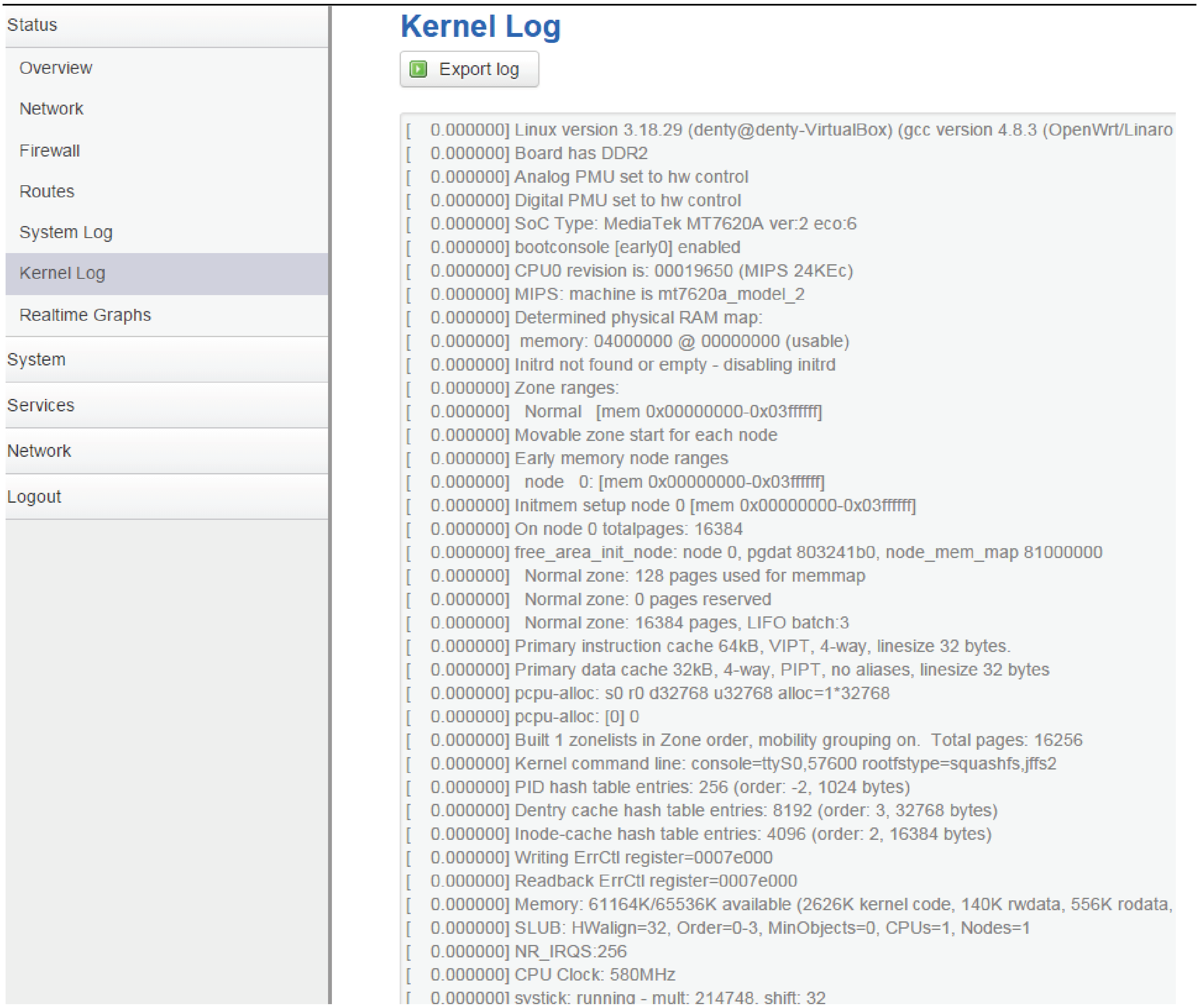
This page shows system log from system boot up. System log is not saved when router restarts. It can be exported by click button “Export syslog”.



```
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

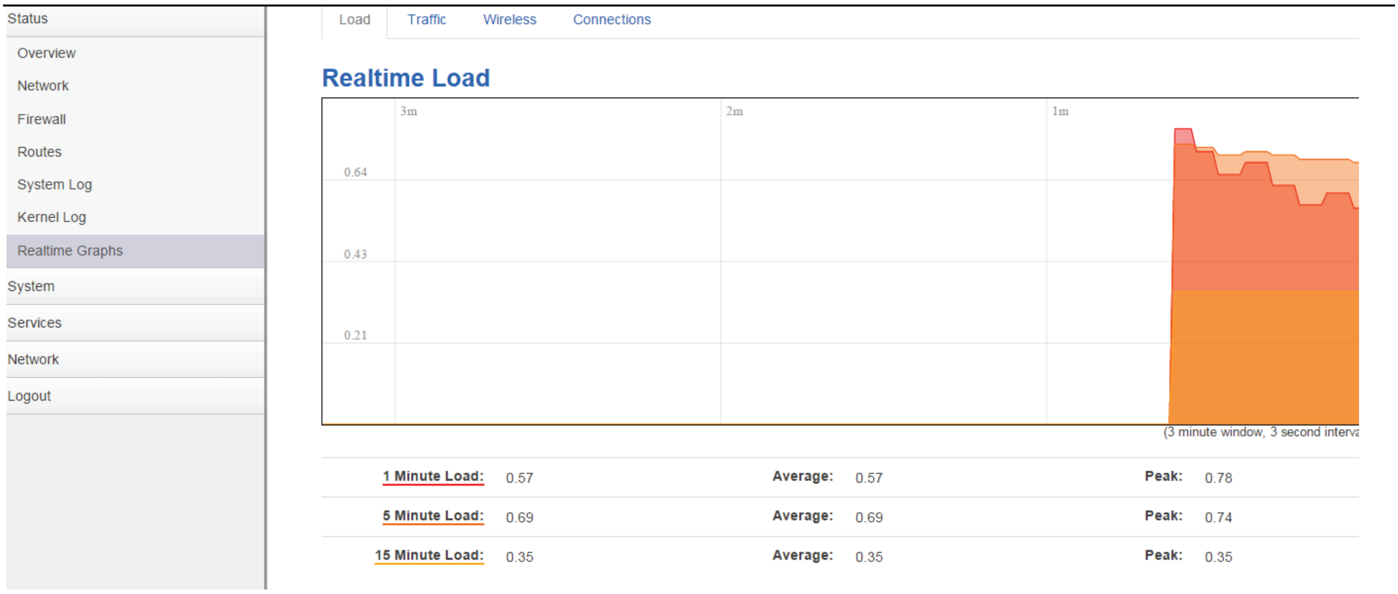
This page shows Kernel log from system boot up. This log is not saved when router restarts. It can be exported by click button “Export syslog”.



```
[    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] systick: running - mult: 214748, shift: 32
```

3.3.7 Realtime graphs

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

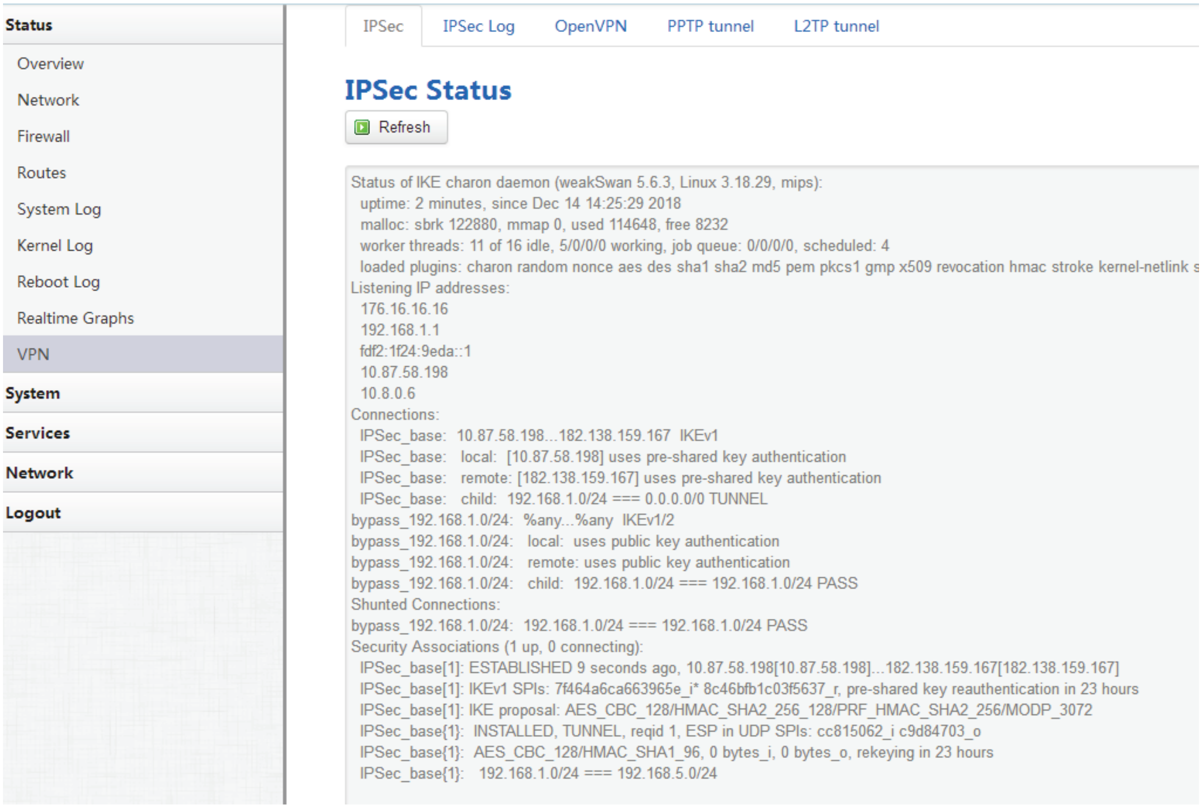


1 Minute Load:	0.57	Average:	0.57	Peak:	0.78
5 Minute Load:	0.69	Average:	0.69	Peak:	0.74
15 Minute Load:	0.35	Average:	0.35	Peak:	0.35

3.3.8 VPN

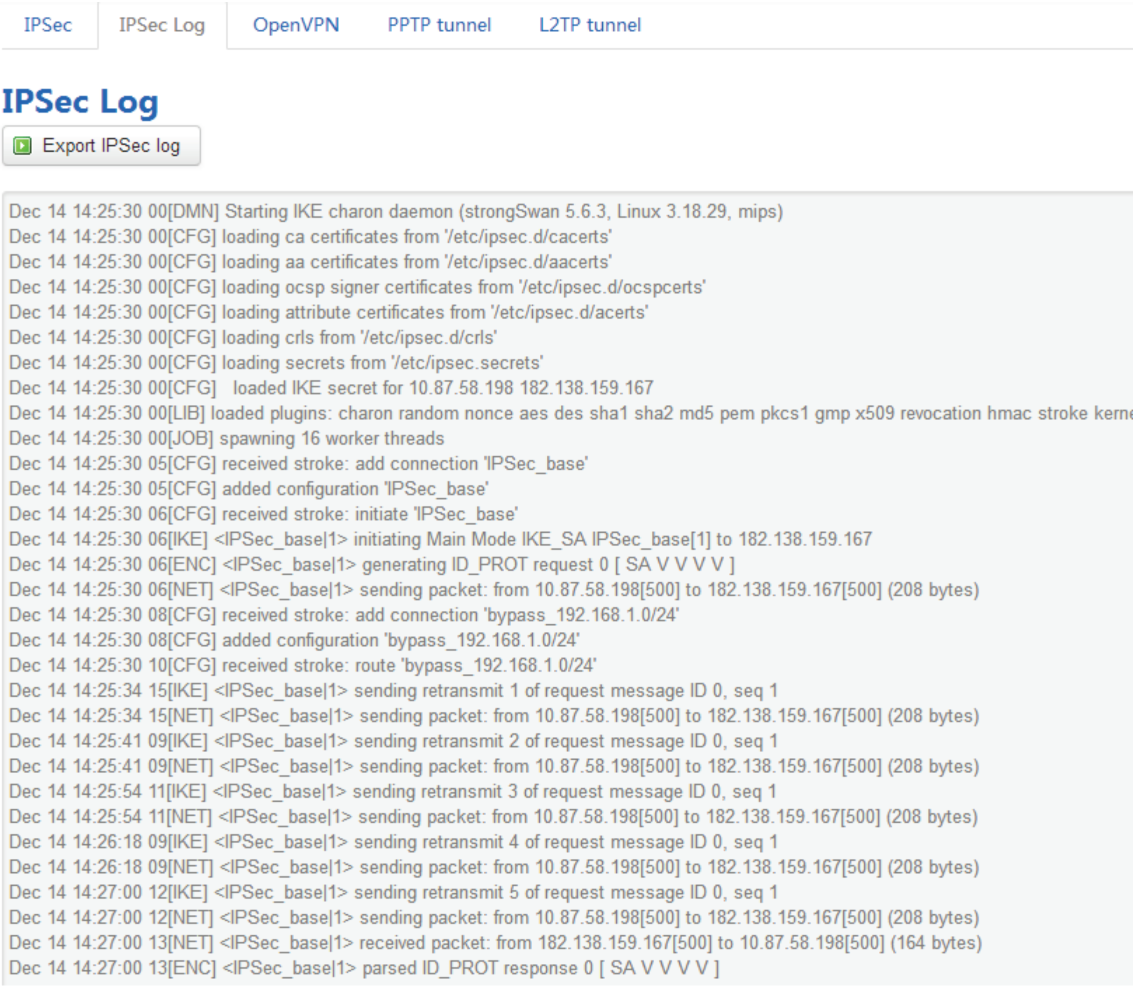
show IPSec status, IPSec log, OpenVPN status, PPTP status and L2TP status.

IPSec Status page



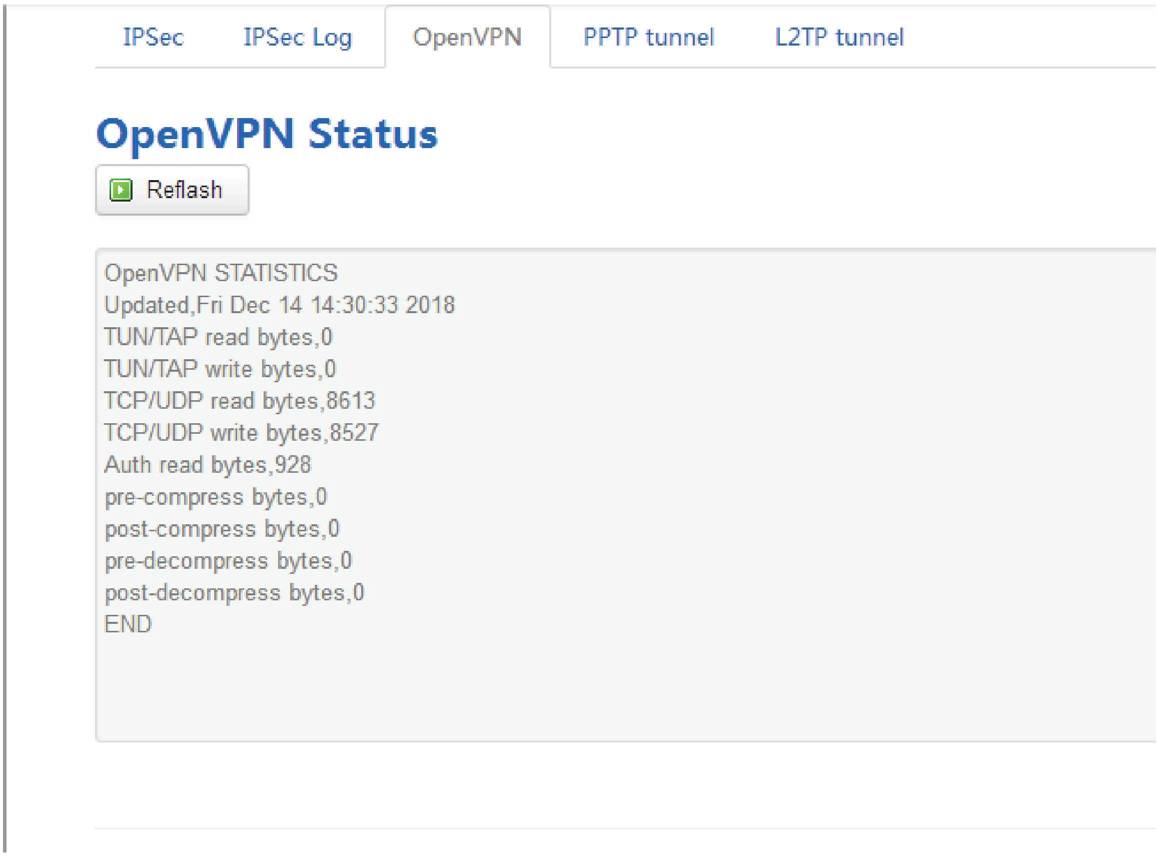
```
Status of IKE charon daemon (weakSwan 5.6.3, Linux 3.18.29, mips):
  uptime: 2 minutes, since Dec 14 14:25:29 2018
  malloc: sbrk 122880, mmap 0, used 114648, free 8232
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink s
Listening IP addresses:
  176.16.16.16
  192.168.1.1
  fdf2:1f24:9eda::1
  10.87.58.198
  10.8.0.6
Connections:
  IPSec_base:  10.87.58.198...182.138.159.167  IKEv1
  IPSec_base:   local:  [10.87.58.198] uses pre-shared key authentication
  IPSec_base:   remote: [182.138.159.167] uses pre-shared key authentication
  IPSec_base:   child:  192.168.1.0/24 === 0.0.0.0/0 TUNNEL
bypass_192.168.1.0/24:  %any...%any  IKEv1/2
bypass_192.168.1.0/24:   local:  uses public key authentication
bypass_192.168.1.0/24:   remote: uses public key authentication
bypass_192.168.1.0/24:   child:  192.168.1.0/24 === 192.168.1.0/24 PASS
Shunted Connections:
bypass_192.168.1.0/24:  192.168.1.0/24 === 192.168.1.0/24 PASS
Security Associations (1 up, 0 connecting):
  IPSec_base[1]: ESTABLISHED 9 seconds ago, 10.87.58.198[10.87.58.198]...182.138.159.167[182.138.159.167]
  IPSec_base[1]: IKEv1 SPIs: 7f464a6ca663965e_i* 8c46bfb1c03f5637_r, pre-shared key reauthentication in 23 hours
  IPSec_base[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
  IPSec_base{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cc815062_i c9d84703_o
  IPSec_base{1}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 23 hours
  IPSec_base{1}:   192.168.1.0/24 === 192.168.5.0/24
```

IPSec Log page



```
Dec 14 14:25:30 00[DMN] Starting IKE charon daemon (strongSwan 5.6.3, Linux 3.18.29, mips)
Dec 14 14:25:30 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Dec 14 14:25:30 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Dec 14 14:25:30 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
Dec 14 14:25:30 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Dec 14 14:25:30 00[CFG] loading crls from '/etc/ipsec.d/crls'
Dec 14 14:25:30 00[CFG] loading secrets from '/etc/ipsec.secrets'
Dec 14 14:25:30 00[CFG]   loaded IKE secret for 10.87.58.198 182.138.159.167
Dec 14 14:25:30 00[LIB] loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kerne
Dec 14 14:25:30 00[JOB] spawning 16 worker threads
Dec 14 14:25:30 05[CFG] received stroke: add connection 'IPSec_base'
Dec 14 14:25:30 05[CFG] added configuration 'IPSec_base'
Dec 14 14:25:30 06[CFG] received stroke: initiate 'IPSec_base'
Dec 14 14:25:30 06[IKE] <IPSec_base|1> initiating Main Mode IKE_SA IPSec_base[1] to 182.138.159.167
Dec 14 14:25:30 06[ENC] <IPSec_base|1> generating ID_PROT request 0 [ SA V V V V ]
Dec 14 14:25:30 06[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:30 08[CFG] received stroke: add connection 'bypass_192.168.1.0/24'
Dec 14 14:25:30 08[CFG] added configuration 'bypass_192.168.1.0/24'
Dec 14 14:25:30 10[CFG] received stroke: route 'bypass_192.168.1.0/24'
Dec 14 14:25:34 15[IKE] <IPSec_base|1> sending retransmit 1 of request message ID 0, seq 1
Dec 14 14:25:34 15[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:41 09[IKE] <IPSec_base|1> sending retransmit 2 of request message ID 0, seq 1
Dec 14 14:25:41 09[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:25:54 11[IKE] <IPSec_base|1> sending retransmit 3 of request message ID 0, seq 1
Dec 14 14:25:54 11[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:26:18 09[IKE] <IPSec_base|1> sending retransmit 4 of request message ID 0, seq 1
Dec 14 14:26:18 09[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:27:00 12[IKE] <IPSec_base|1> sending retransmit 5 of request message ID 0, seq 1
Dec 14 14:27:00 12[NET] <IPSec_base|1> sending packet: from 10.87.58.198[500] to 182.138.159.167[500] (208 bytes)
Dec 14 14:27:00 13[NET] <IPSec_base|1> received packet: from 182.138.159.167[500] to 10.87.58.198[500] (164 bytes)
Dec 14 14:27:00 13[ENC] <IPSec_base|1> parsed ID_PROT response 0 [ SA V V V V ]
```

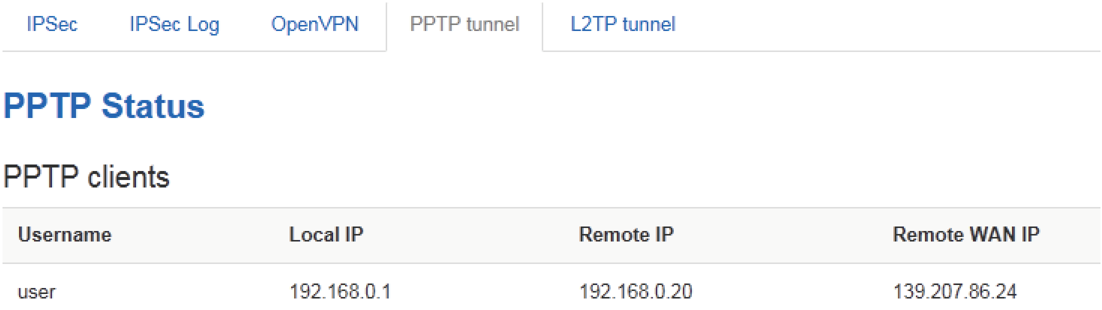
OpenVPN status page



OpenVPN Status

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

PPTP Client Status page

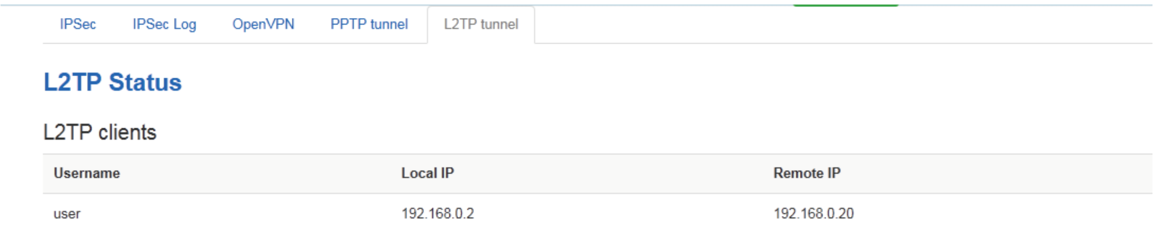


PPTP Status

PPTP clients

Username	Local IP	Remote IP	Remote WAN IP
user	192.168.0.1	192.168.0.20	139.207.86.24

L2TP Client Status page



L2TP Status

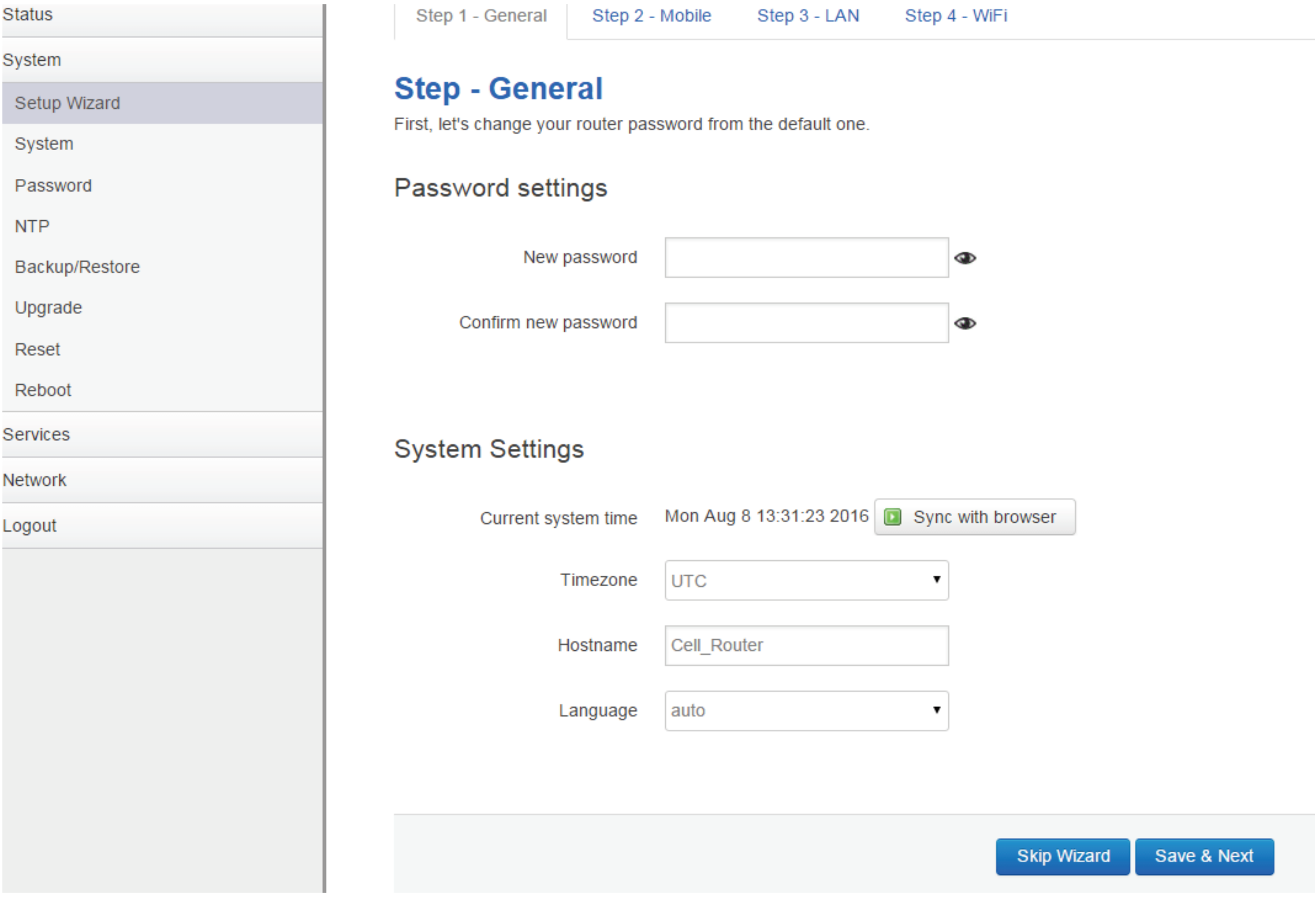
L2TP clients

Username	Local IP	Remote IP
user	192.168.0.2	192.168.0.20

3.4 System Configuration

3.4.1 Setup wizard

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



Step - General

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

Password settings

New password:

Confirm new password:

System Settings

Current system time: Mon Aug 8 13:31:23 2016

Timezone: UTC

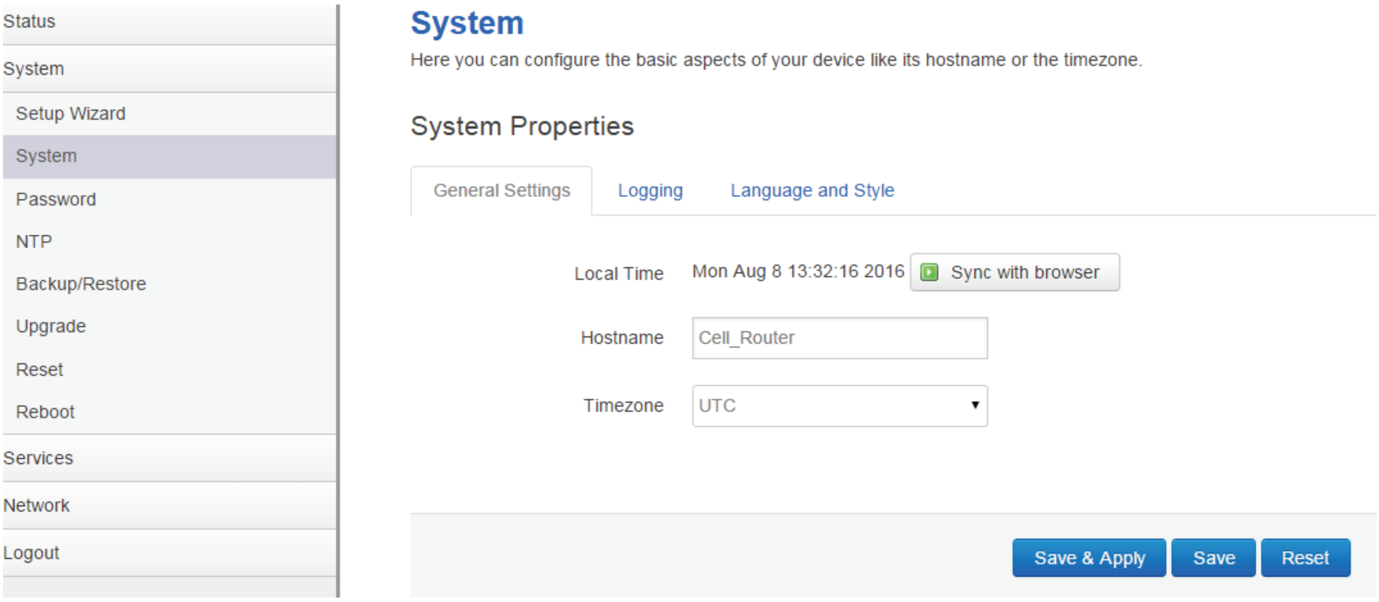
Hostname: Cell_Router

Language: auto

Note:

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

3.4.2 System



System

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

System Properties

Local Time: Mon Aug 8 13:32:16 2016

Hostname: Cell_Router

Timezone: UTC

General Settings

➢ **Local Time**

It displays system time, and the final user can Sync this time with browser by clicking button “Sync with browser”.

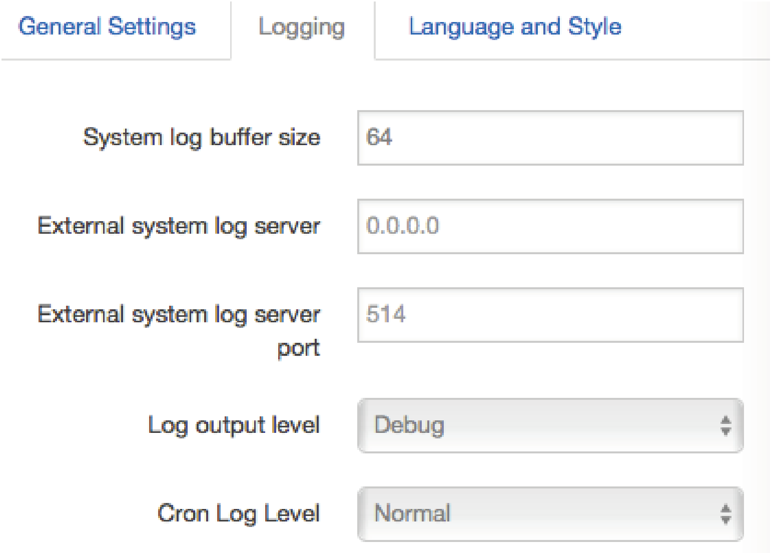
➢ **Hostname**

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



System log buffer size: 64

External system log server: 0.0.0.0

External system log server port: 514

Log output level: Debug

Cron Log Level: Normal

➢ **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**

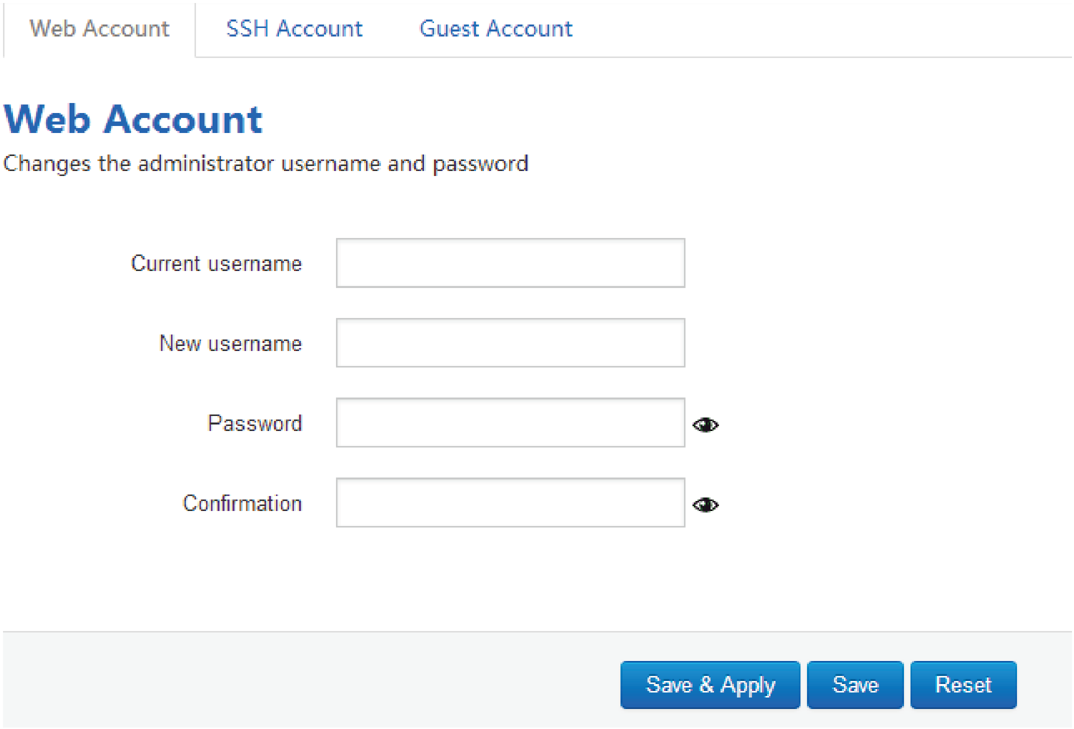
It is log level for process Crond.

Language English

- **Language**

The default language is “Auto”. The final user can choose English or Chinese.

3.4.3 Password



Web Account

Changes the administrator username and password

Current username

New username

Password

Confirmation

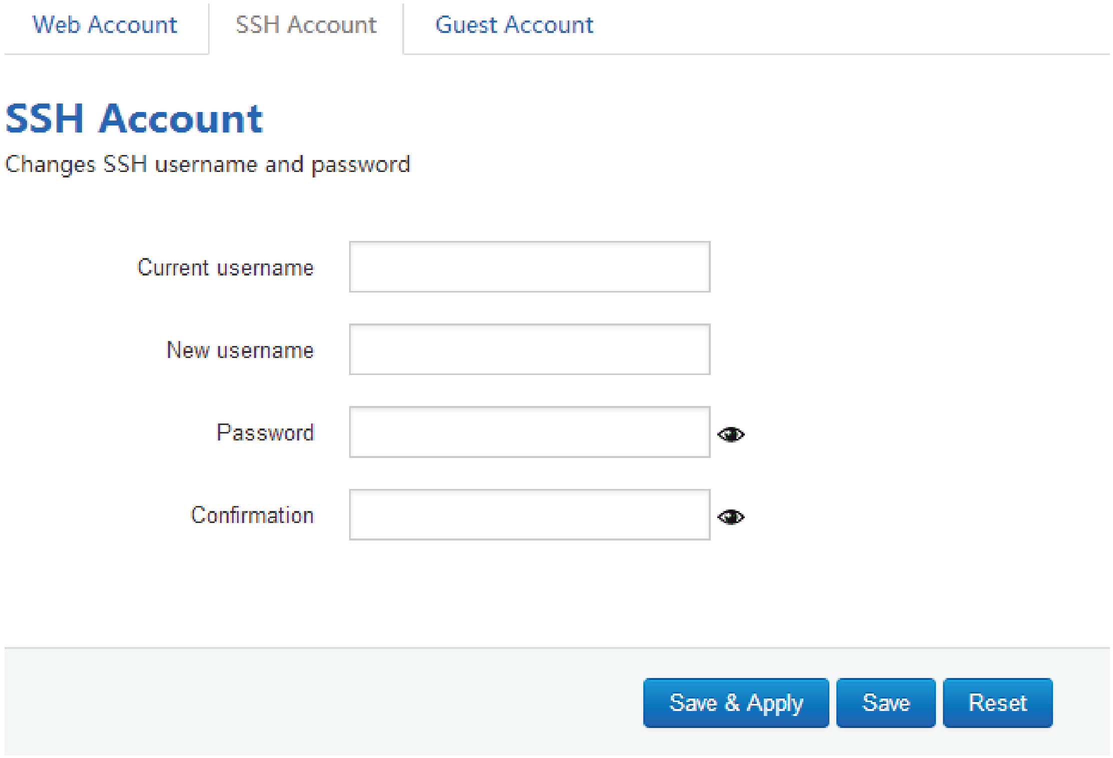
Change username and password for accessing device web. Click “eye button” can show the new password you entered.

Current username. The username of web account is using.

New username: change web account username to the new one.

Password: new password.

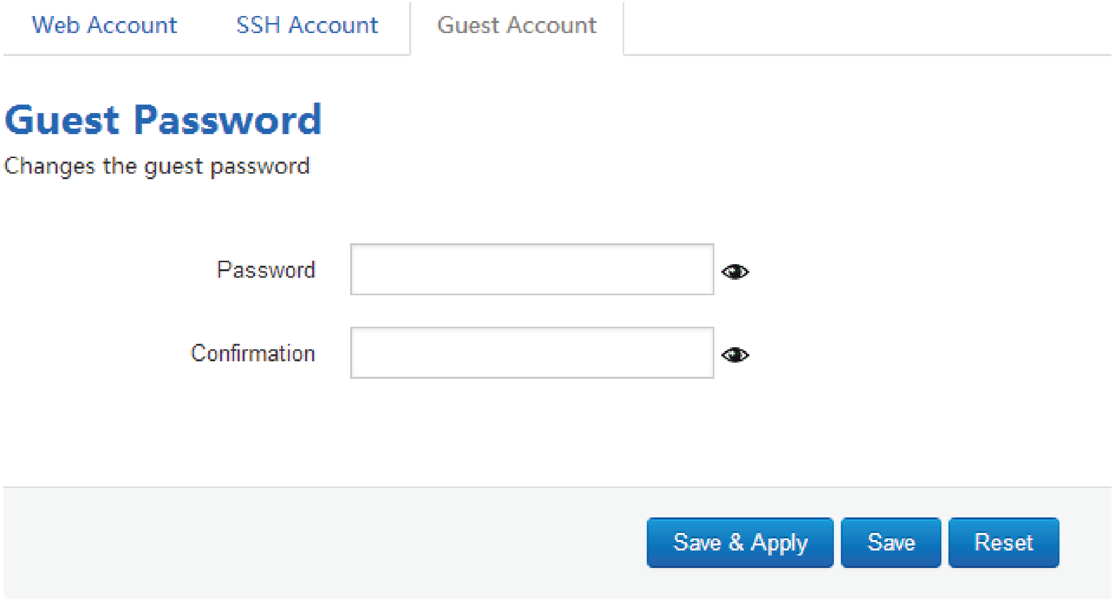
Confirmation: same as Password.



SSH Account

Changes SSH username and password

Change the username and password for ssh access.

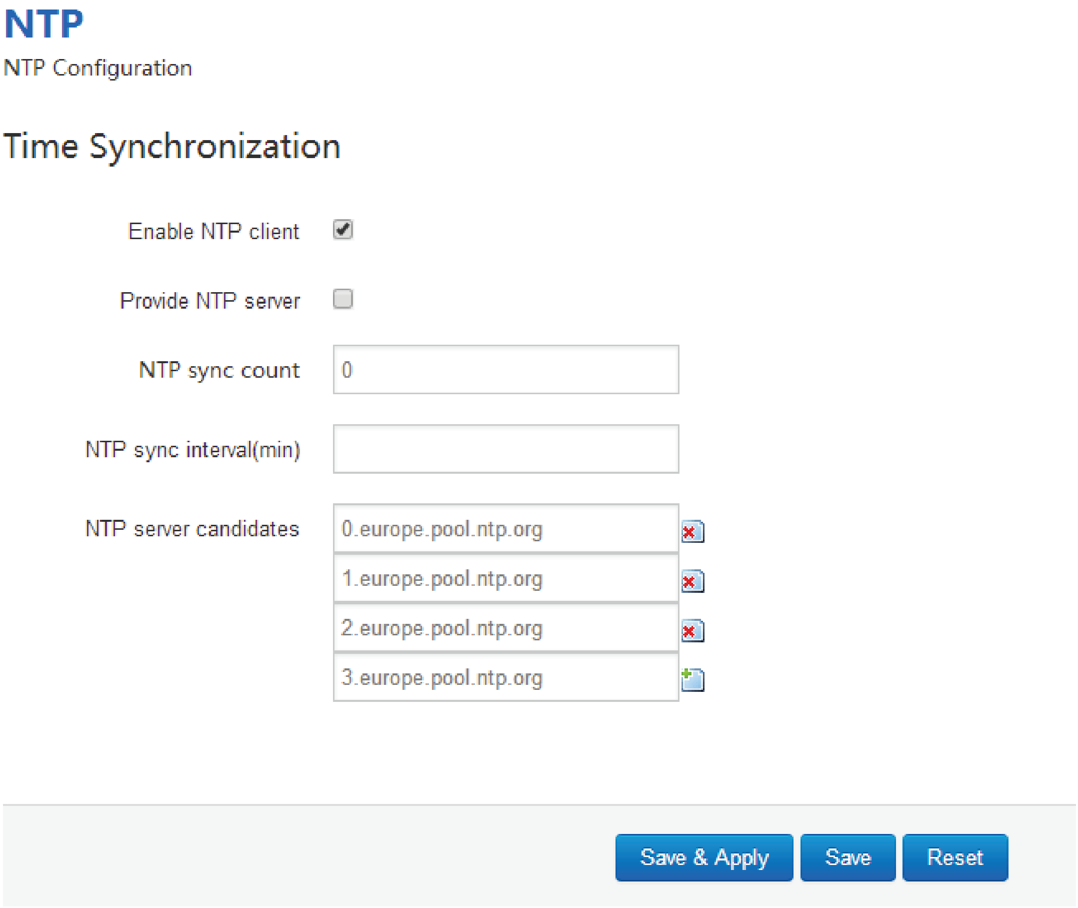


Guest Password

Changes the guest password

Change the password for guest user.

3.4.4 NTP



NTP

NTP Configuration

Time Synchronization

Enable NTP client ☑

Provide NTP server □

NTP sync count: 0

NTP sync interval(min):

NTP server candidates:
0.europe.pool.ntp.org
1.europe.pool.ntp.org
2.europe.pool.ntp.org
3.europe.pool.ntp.org

NTP is network timing protocol.

- **Enable NTP client**

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

- **Provide NTP server**

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

- **NTP sync count**

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

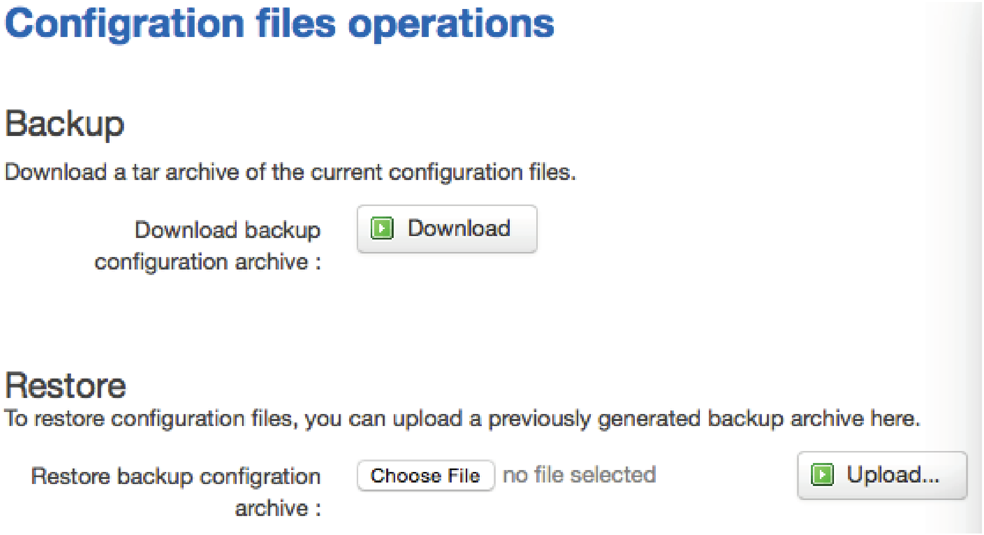
- **NTP sync interval(min)**

The interval time between NTP synchronization.

- **NTP server candidates**

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



Configration files operations

Backup

Download a tar archive of the current configuration files.

Download backup configuration archive : Download

Restore

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

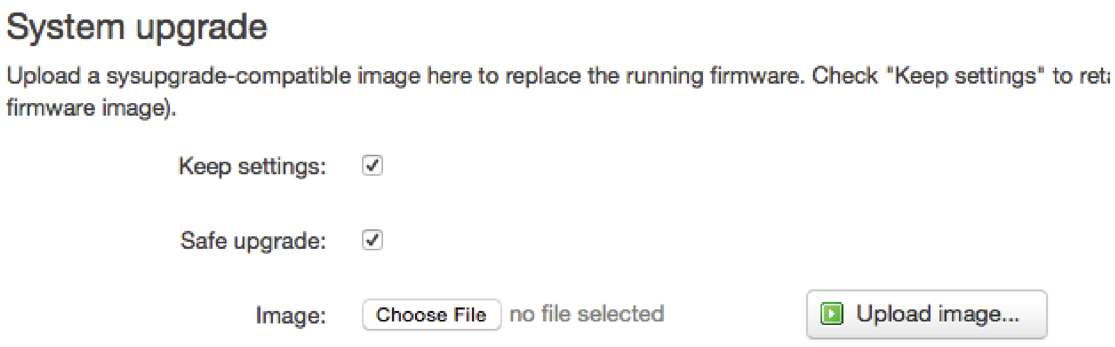
Restore backup configration archive : Choose File no file selected Upload...

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 ret firmware image).

Keep settings: ☑

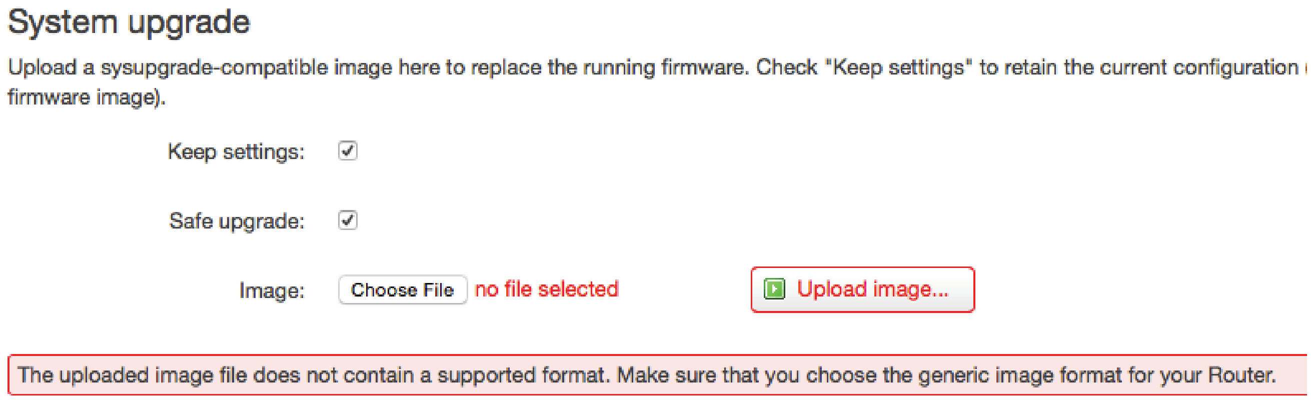
Safe upgrade: ☑

Image: Choose File no file selected Upload image...

Upload a system compatible firmware to replace the running firmware. The default value for "Keep settings" is checked, that means current configuration will be kept after system upgrade, otherwise router will be reset to factory setting. But we highly recommend uncheck "Keep settings", otherwise it may bring uncertain parameters conflicting after updating.

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

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 firmware image).

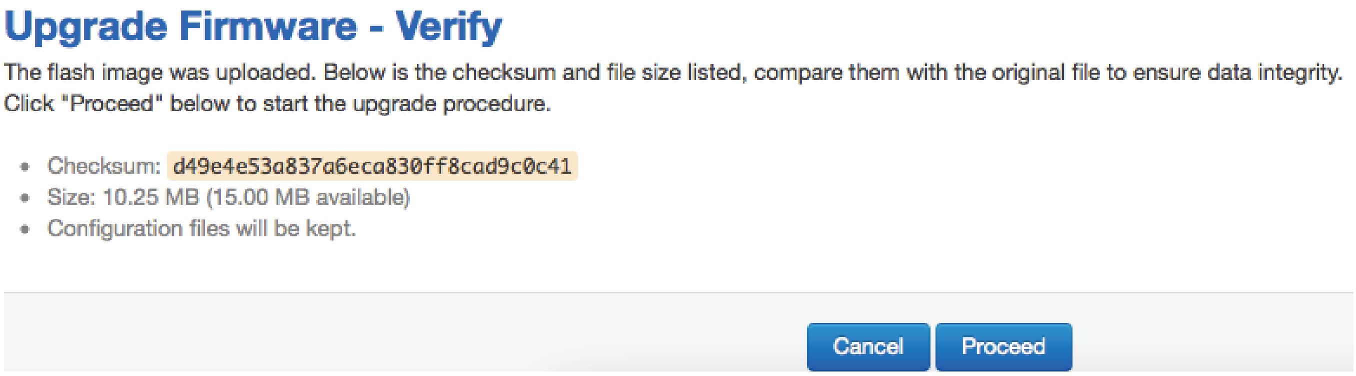
Keep settings: ☑

Safe upgrade: ☑

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.

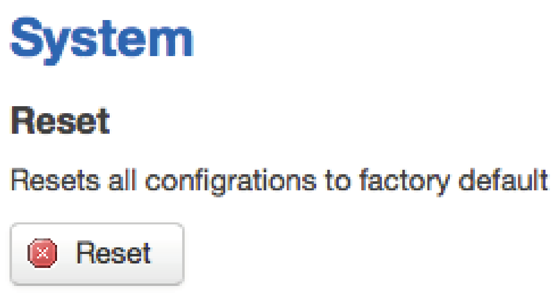


Upgrade Firmware - Verify

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



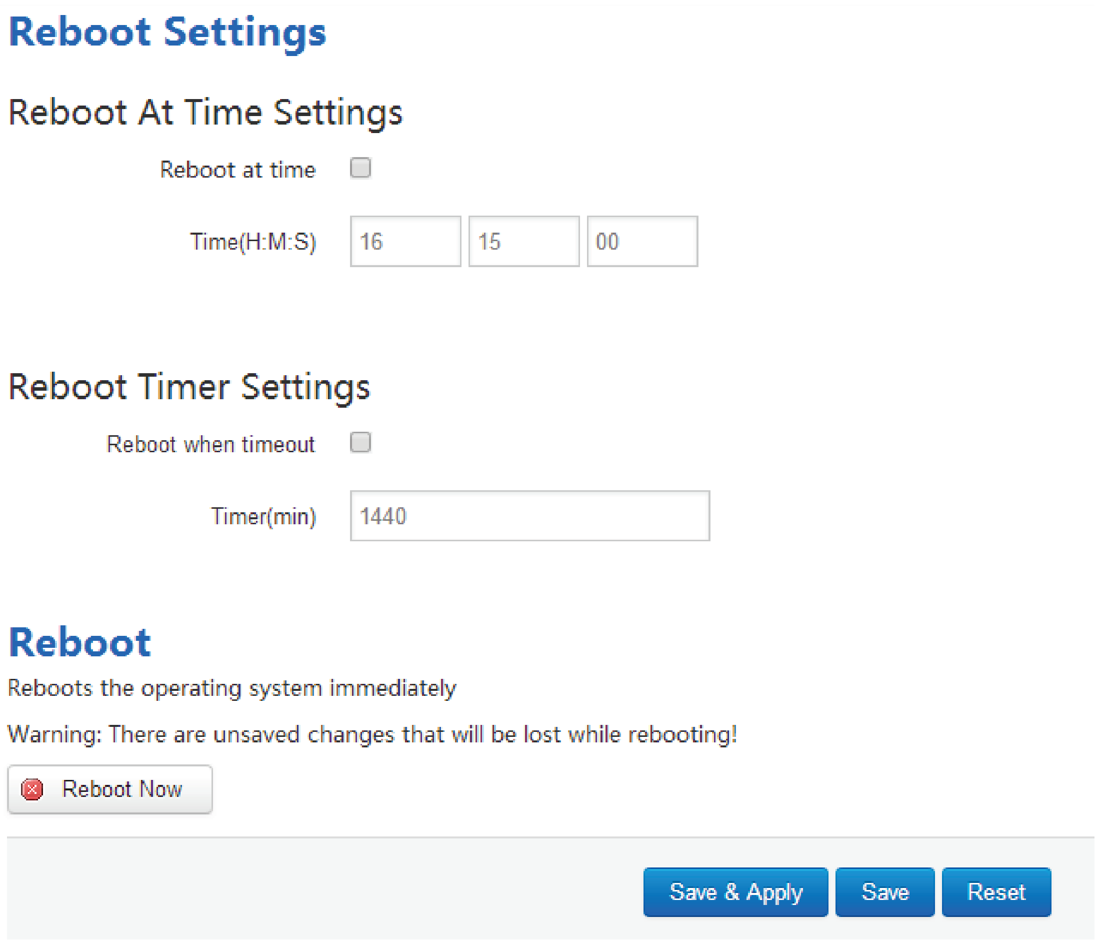
System

Reset

Resets all configrations 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



Reboot Settings

Reboot At Time Settings

Reboot at time □

Time(H:M:S) 16 15 00

Reboot Timer Settings

Reboot when timeout □

Timer(min) 1440

Reboot

Reboots the operating system immediately

Warning: There are unsaved changes that will be lost while rebooting!

Reboot at time: reboot router at a specific time.

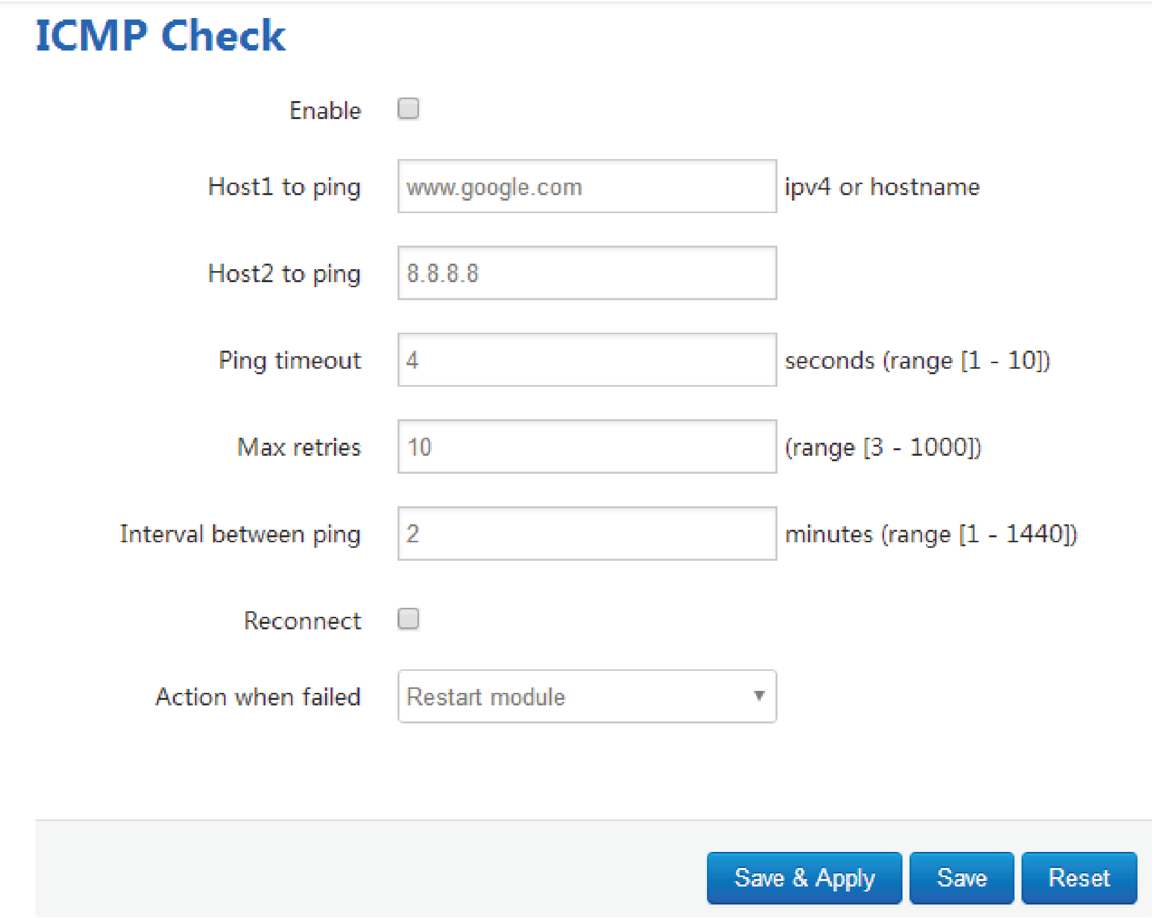
Reboot when timeout: reboot router after timer timeout.

Click button “Reboot Now”, 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	www.google.com	ipv4 or hostname
Host2 to ping	8.8.8.8	
Ping timeout	4	seconds (range [1 - 10])
Max retries	10	(range [3 - 1000])
Interval between ping	2	minutes (range [1 - 1440])
Reconnect	□	
Action when failed	Restart module ▾	

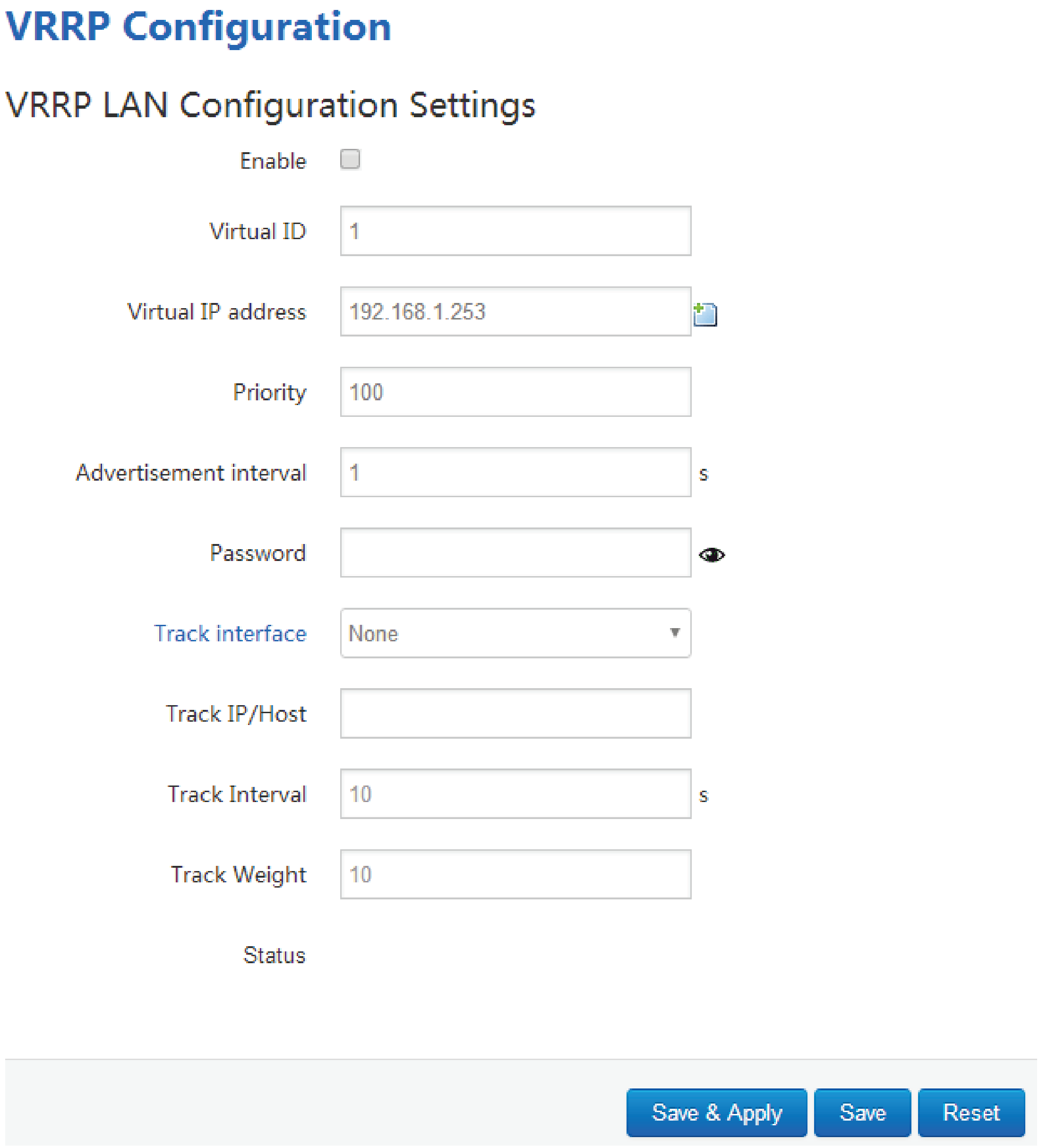
- **Enable**: Enable ICMP check feature
- **Host1 to ping / Host2 to ping**: The domain name or IP address for checking the network connection.
- **Ping timeout**: If ping packet is sent, the response packet is not received before timeout, then this ping is failed.
- **Max retries**: If the ping is failed, the failed counter will add one. If the failed counter is bigger or

equal to the Max retries, then system will say the ICMP check is failed, an action configured in item "Action when failed" will be triggered.

If the ping is succeeding, failed counter will be reset to 0 at anytime.

- **Interval between ping**: The time between twice ping. The unit is minute.
- **Reconnect**: Reconnect cell interface if ping failed.
- **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 ☐

Virtual ID: 1

Virtual IP address: 192.168.1.253

Priority: 100

Advertisement interval: 1 s

Password:

Track interface: None

Track IP/Host:

Track Interval: 10 s

Track Weight: 10

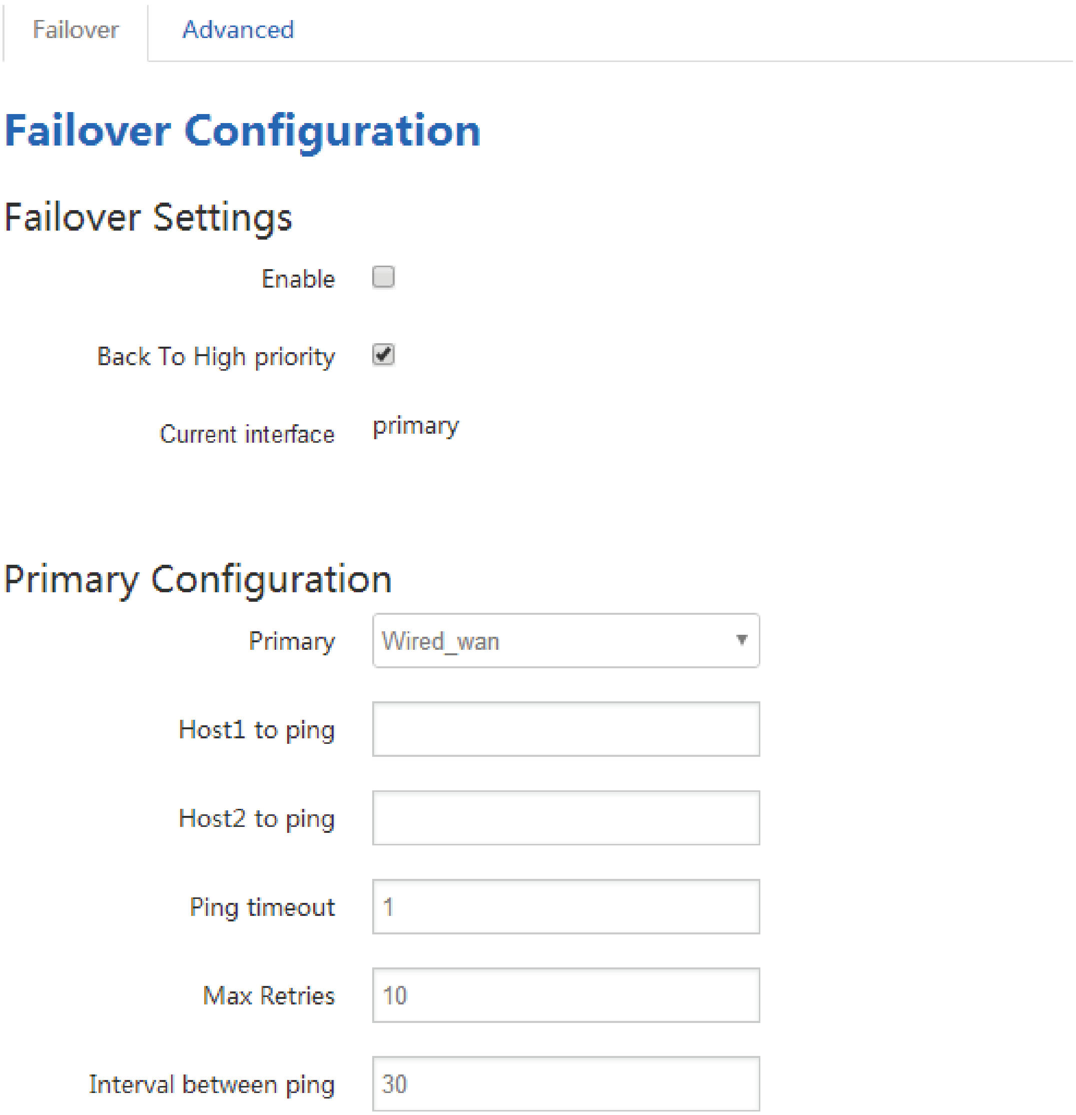
Status

- **Enable**: Enable VRRP(Virtual Router Redundancy Protocol) for LAN.

- **Virtual ID**: Routers with same IDs will be grouped in the same VRRP (Virtual Router Redundancy Protocol) cluster, range [1 - 255].
- **Virtual 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 ⊞.
- **Priority**: Router with highest priority in the same VRRP cluster will act as master. The legal number is from 1 to 255.
- **Advertisement interval:** VRRP send packet to a set of VRRP instances to advertise the device in the MASTER state.
- **Password**: the password string for VRRP accessing. VRRP in our device only supports authentication PASS.
- **Track interface**: Check local interface is up or down.
- **Track IP/Host**: the host or IP address to ping.
- **Track Interval**: ping interval.
- **Track Weight**: priority will be subtracted from the initial priority in case of ping IP/Host failure.
- **Status**: show VRRP status(MASTER/BACKUP).

3.5.3 Failover (link backup)

3.5.3.1 Failover basic settings



Failover Configuration

Failover Settings

Enable □

Back To High priority ☑

Current interface primary

Primary Configuration

Primary: Wired_wan

Host1 to ping:

Host2 to ping:

Ping timeout: 1

Max Retries: 10

Interval between ping: 30

- **Enable**: Enable failover feature
- **Back to high priority**: If back to high priority is checked, when the high priority interface is available, using the high priority interface as WAN port.

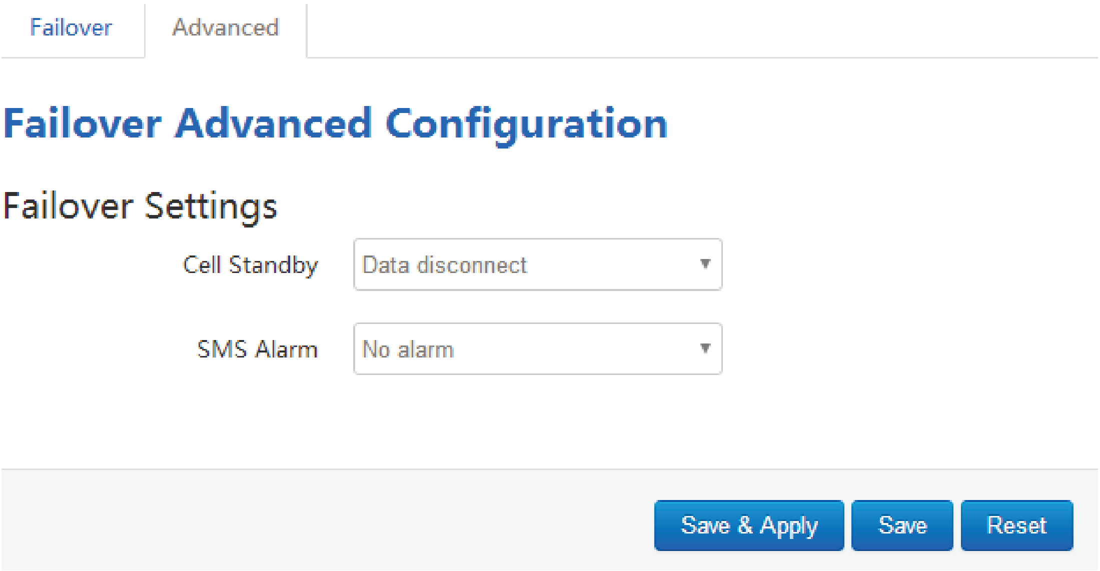
  If back to high priority is unchecked, even if the high priority interface is available, router will keep current interface as WAN port, it won’t switch to high priority interface.

  Primary/Secondary/Third: interface which can be treat as WAN port. There are 4 options, Wired-WAN, WiFi_client, Cell_mobile, and None.
- **Current interface**: show working interface.
- **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.

3.5.3.1 Failover Advanced settings



Failover Advanced Configuration

Failover Settings

Cell Standby: Data disconnect

SMS Alarm: No alarm

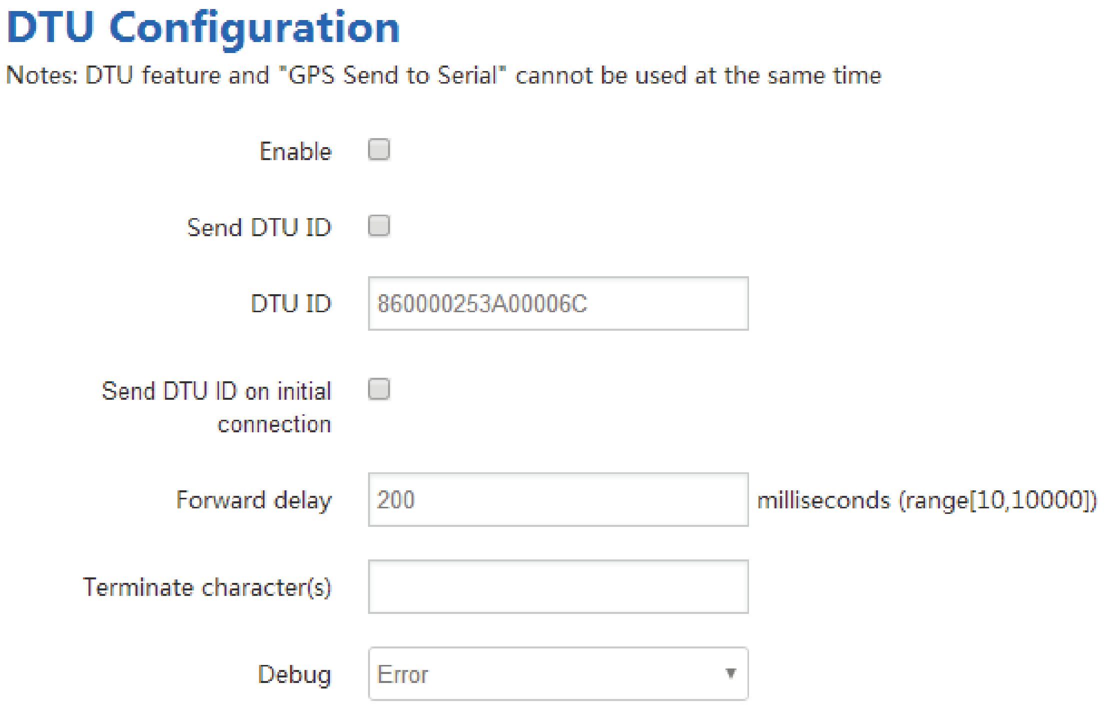
- **Cell Standby**: choose Cell status(connect, disconnect, or radio off) when cell acts as backup interface.
- **SMS Alarm**: if need to send SMS alarm when working interface switchover.

3.5.4 DTU

Notes:

1) This feature is for H820Q 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 860000253A00006C

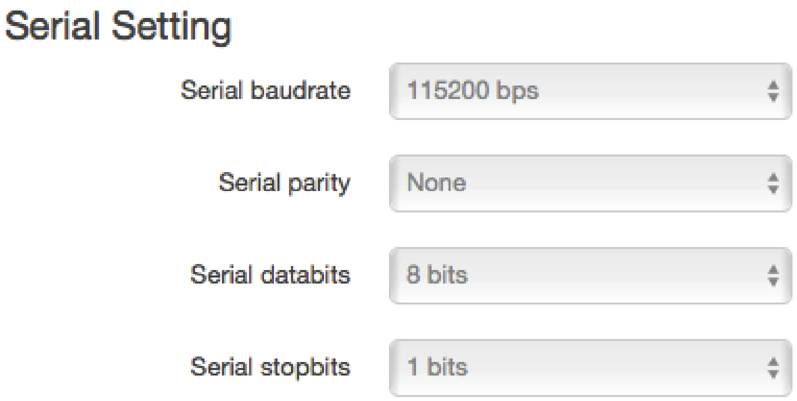
Send DTU ID on initial connection □

Forward delay 200 milliseconds (range[10,10000])

Terminate character(s)

Debug Error

- **Enable**: Enable DTU feature.
- **Send DTU ID**: Send DTU ID at the front of packet.
- **DTU ID**: The default DTU ID is the SN of router, the final user can re-write it if necessary.
- **Send DTU ID on initial connection**: only .
- **Forward delay**: The unit is millisecond. It is delay time that forward data between serial port and network. Set forward delay to empty means no delay.
- **Terminate character**: split serial port data into different packages with terminate character. It can be a string, or hexadecimal which start as 0x,such as 0x0a0d.
- **Debug**: Debug level for log output.



Serial Setting

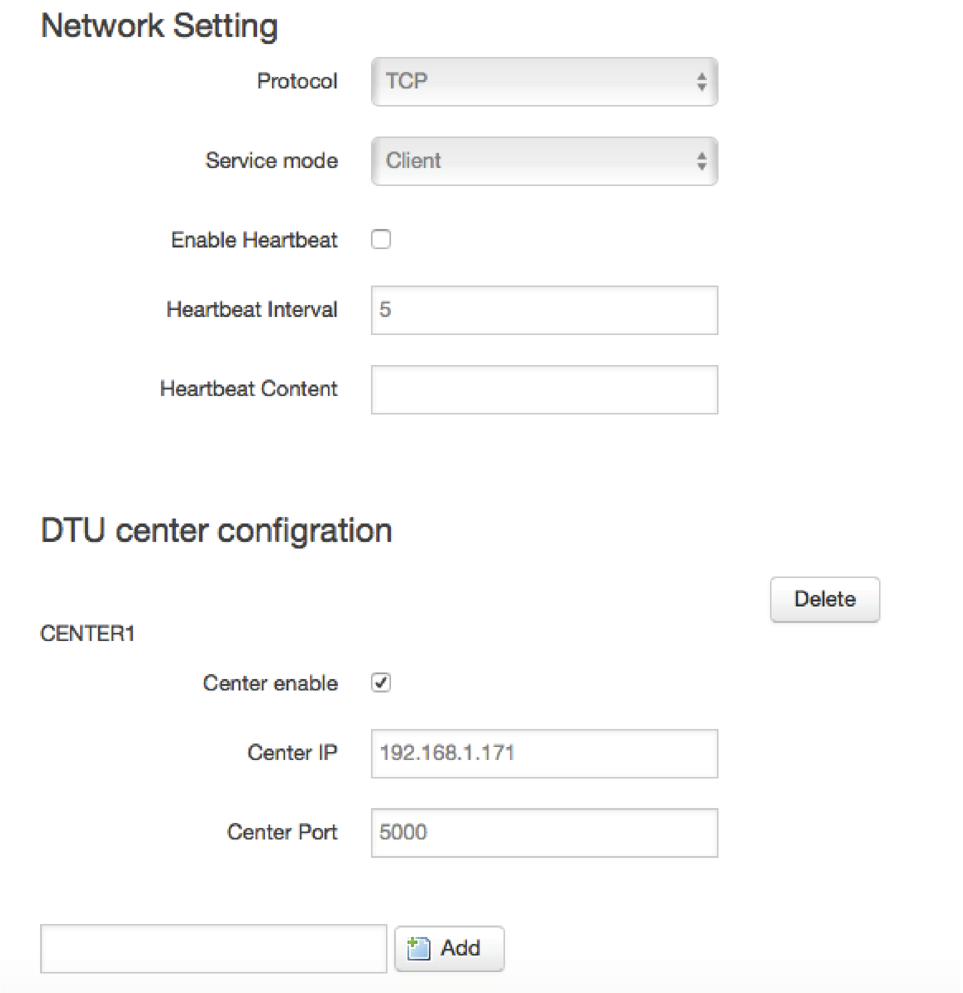
Serial baudrate 115200 bps

Serial parity None

Serial databits 8 bits

Serial stopbits 1 bits

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



Network Setting

Protocol: TCP

Service mode: Client

Enable Heartbeat: □

Heartbeat Interval: 5

Heartbeat Content:

DTU center configration

CENTER1

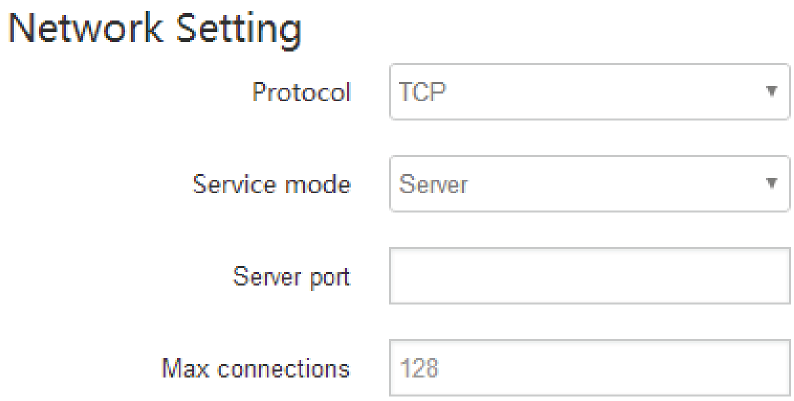
Center enable: ☑

Center IP: 192.168.1.171

Center Port: 5000

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



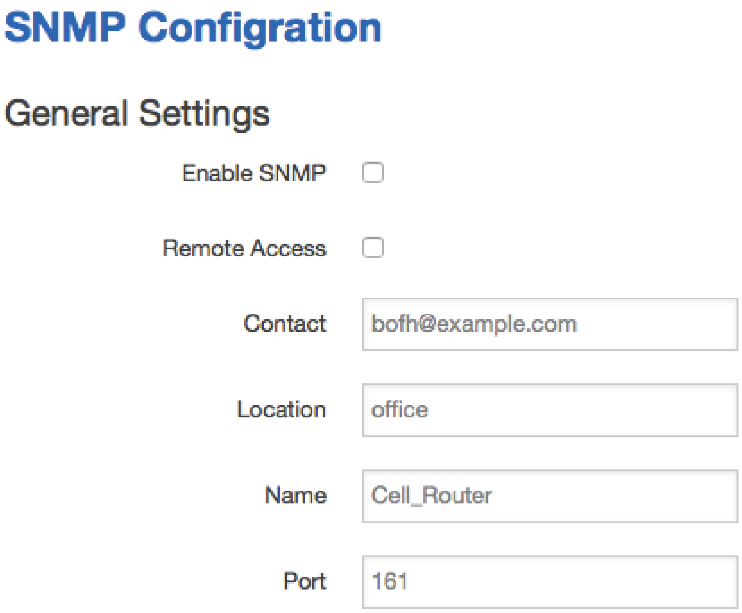
Network Setting

Protocol	TCP ▾
Service mode	Server ▾
Server port	
Max connections	128

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

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

3.5.5 SNMP

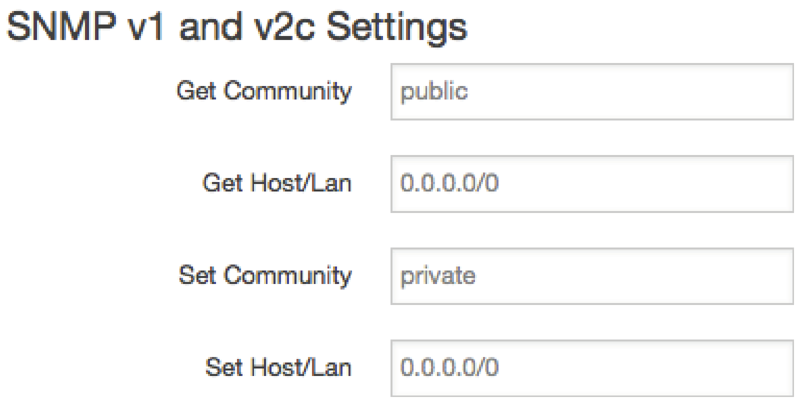


SNMP Configration

General Settings

Enable SNMP	□
Remote Access	□
Contact	bofh@example.com
Location	office
Name	Cell_Router
Port	161

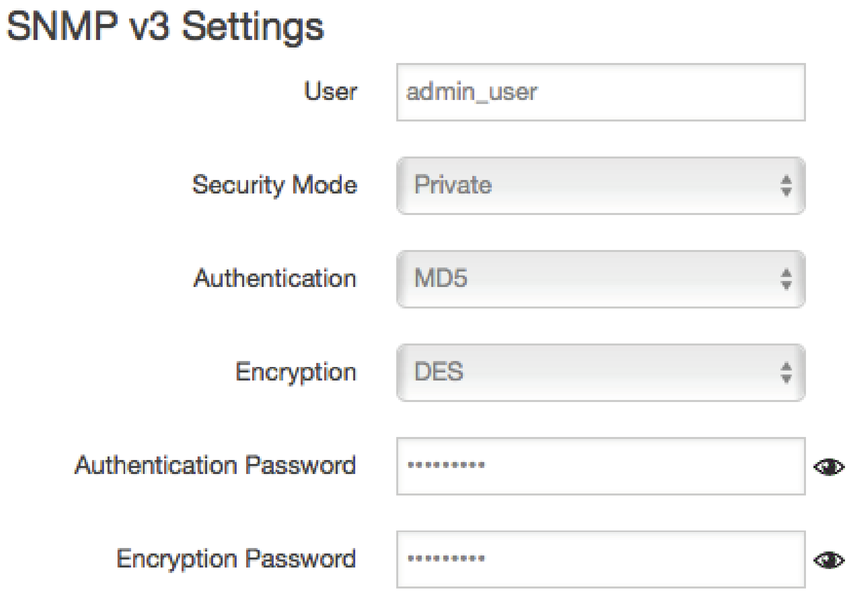
- **Enable SNMP**: Enable SNMP feature
- **Remote Access**: Allow remote access SNMP. If it is unchecked, only LAN subnet can access SNMP.
- **Contact**: Set the contact information here
- **Location**: set router’s installation address.
- **Name**: Set the router’s in SNMP
- **Port**: SNMP service port,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



SNMP v1 and v2c Settings

Get Community	public
Get Host/Lan	0.0.0.0/0
Set Community	private
Set Host/Lan	0.0.0.0/0

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



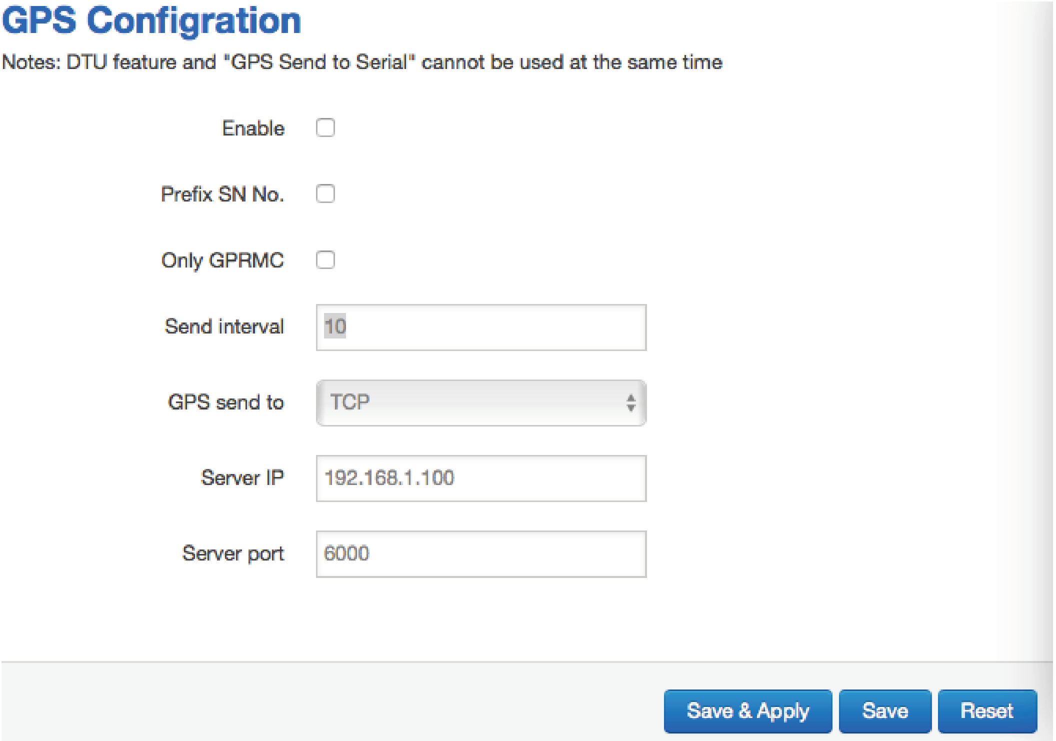
SNMP v3 Settings

User	admin_user
Security Mode	Private
Authentication	MD5
Encryption	DES
Authentication Password	•••••••••
Encryption Password	•••••••••

- **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 Configration

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

Enable □

Prefix SN No. □

Only GPRMC □

Send interval 10

GPS send to TCP

Server IP 192.168.1.100

Server port 6000

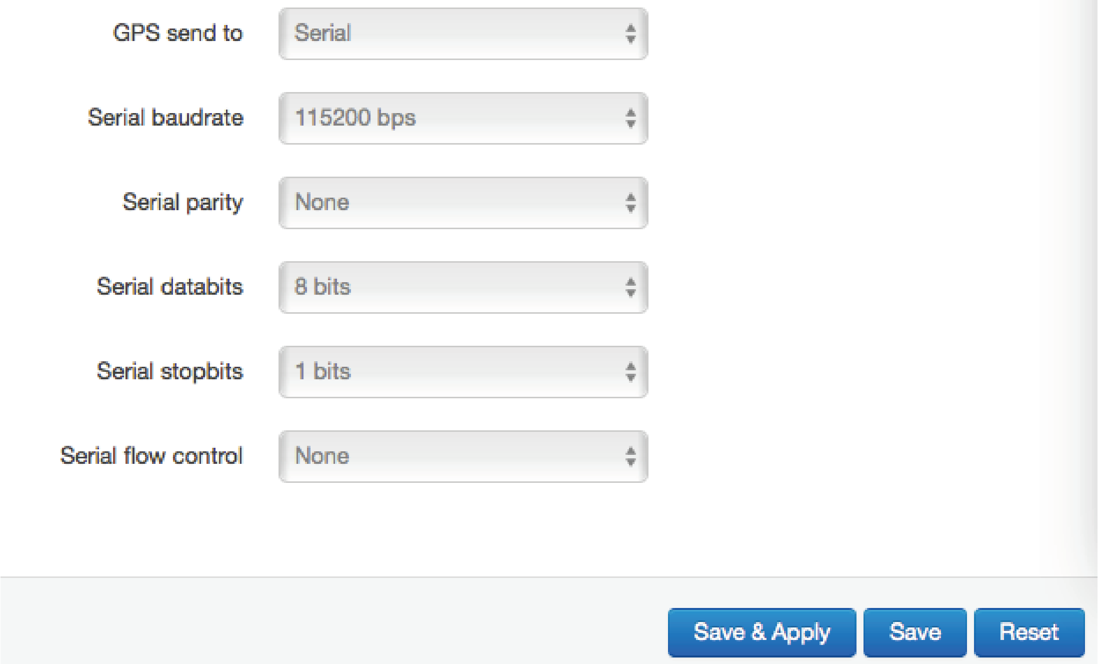
- **Enable**: please check it once you need use GPS feature.
- **Only GPRMC:** if check it, only send GPRMC data info (Longitude Latitude altitude)
- **Prefix SN No.:** if check it, add the router SN to the data packet
- **Send interval:** configure the frequency time of updated GPS data packet sending
- **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 H820Q Router via Serial Port, please choose “Serial”.

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

➢ **GPS to TCP/UDP Settings**

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



GPS send to: Serial

Serial baudrate: 115200 bps

Serial parity: None

Serial databits: 8 bits

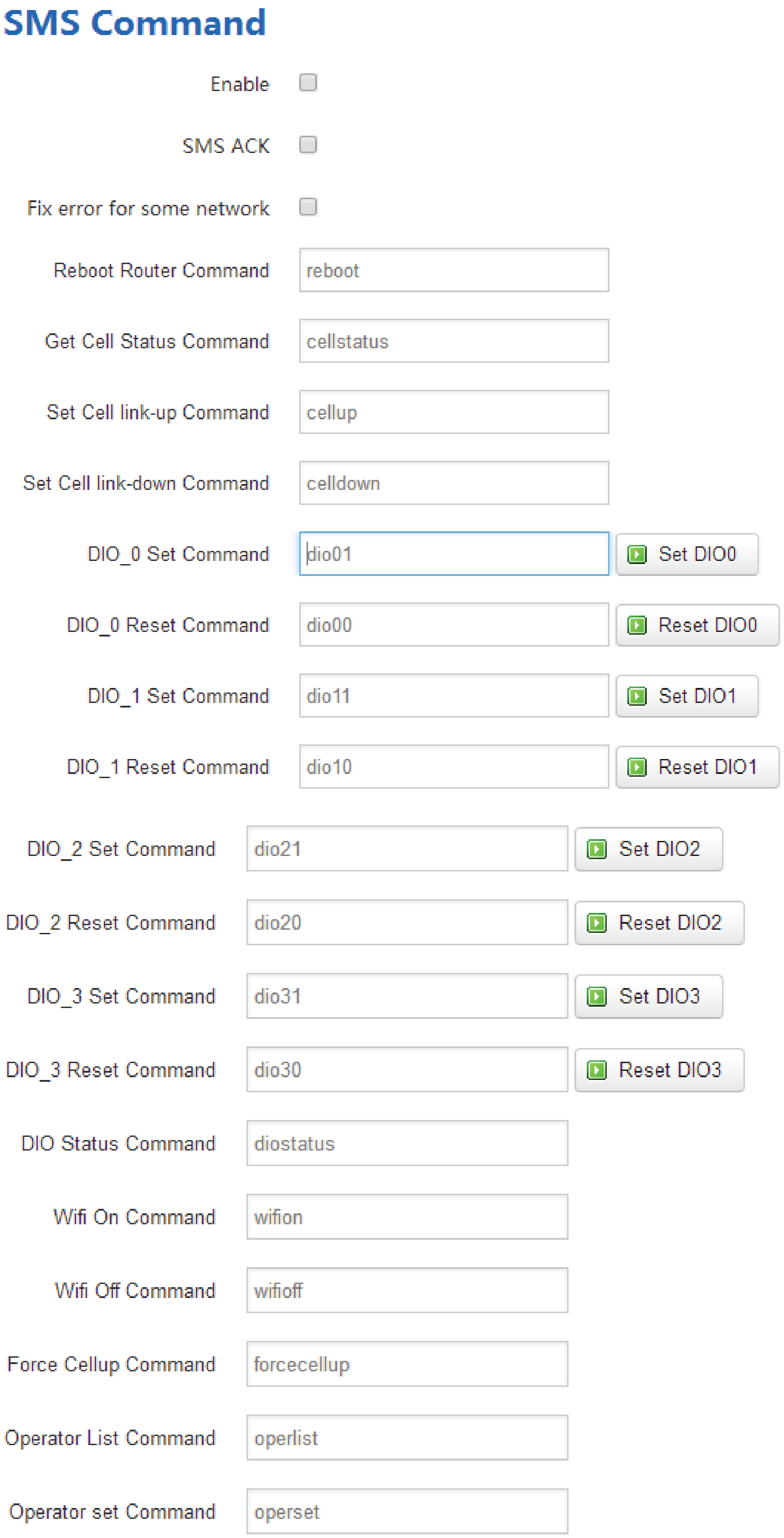
Serial stopbits: 1 bits

Serial flow control: None

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

3.5.7 SMS

➢ **SMS Command**



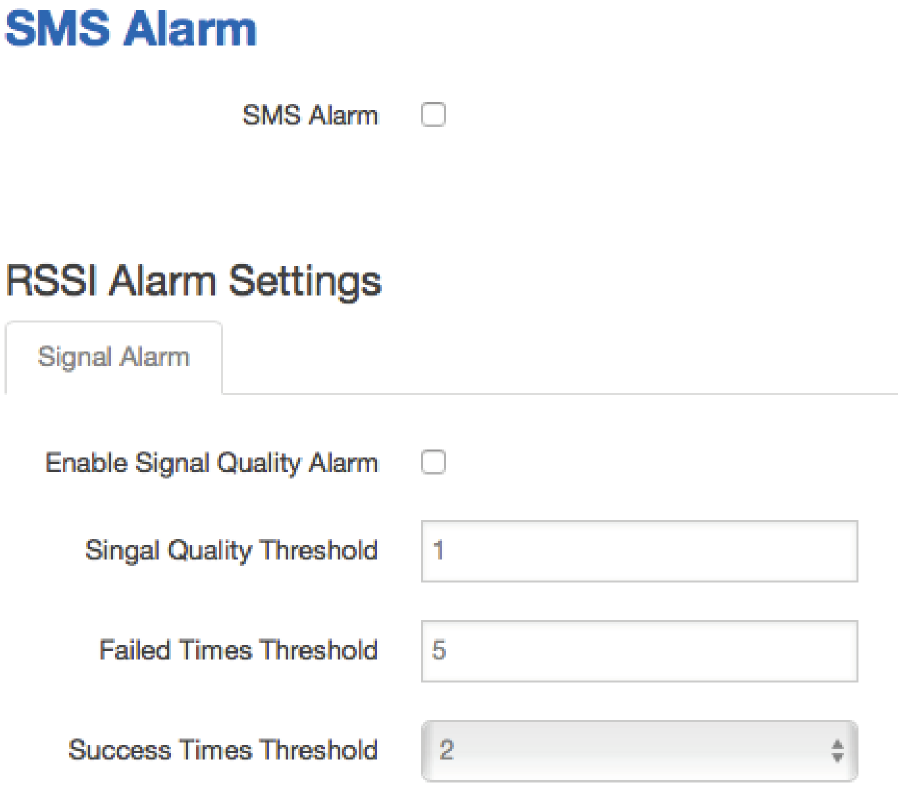
SMS Command

Enable	□	
SMS ACK	□	
Fix error for some network	□	
Reboot Router Command	reboot	
Get Cell Status Command	cellstatus	
Set Cell link-up Command	cellup	
Set Cell link-down Command	celldown	
DIO_0 Set Command	dio01	Set DIO0
DIO_0 Reset Command	dio00	Reset DIO0
DIO_1 Set Command	dio11	Set DIO1
DIO_1 Reset Command	dio10	Reset DIO1
DIO_2 Set Command	dio21	Set DIO2
DIO_2 Reset Command	dio20	Reset DIO2
DIO_3 Set Command	dio31	Set DIO3
DIO_3 Reset Command	dio30	Reset DIO3
DIO Status Command	diostatus	
Wifi On Command	wifion	
Wifi Off Command	wifioff	
Force Cellup Command	forcecellup	
Operator List Command	operlist	
Operator set Command	operset	

- **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. It is not supported by H820Q.
- **DIO_0 Reset Command**: input the command for I/O port 0. For SMS feature, please keep the parameter default. It is not supported by H820Q.
- **DIO_1 Set Command**: input the command for I/O port 1. For SMS feature, please keep the parameter default. It is not supported by H820Q.
- **DIO_1 Reset Command**: input the command for I/O port 1. For SMS feature, please keep the parameter default. It is not supported by H820Q.
- **Button Set/Reset DIO**: set DIO to high or low immediately.
- **DIO Status Command**: input the command for I/O port status. For SMS feature, please keep the parameter default. It is not supported by H820Q.
- **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.
- **Force Cellup Command**: if cell is down since traffic limit, it can be brought up by this command.
- **Operator List Command**: send modem operator list as SMS, it is only supported by some specific modems.
- **Operator set Command**: set modem to operator manually, it is only supported by some specific modems.

➢ SMS alarm



SMS Alarm

SMS Alarm □

RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm □

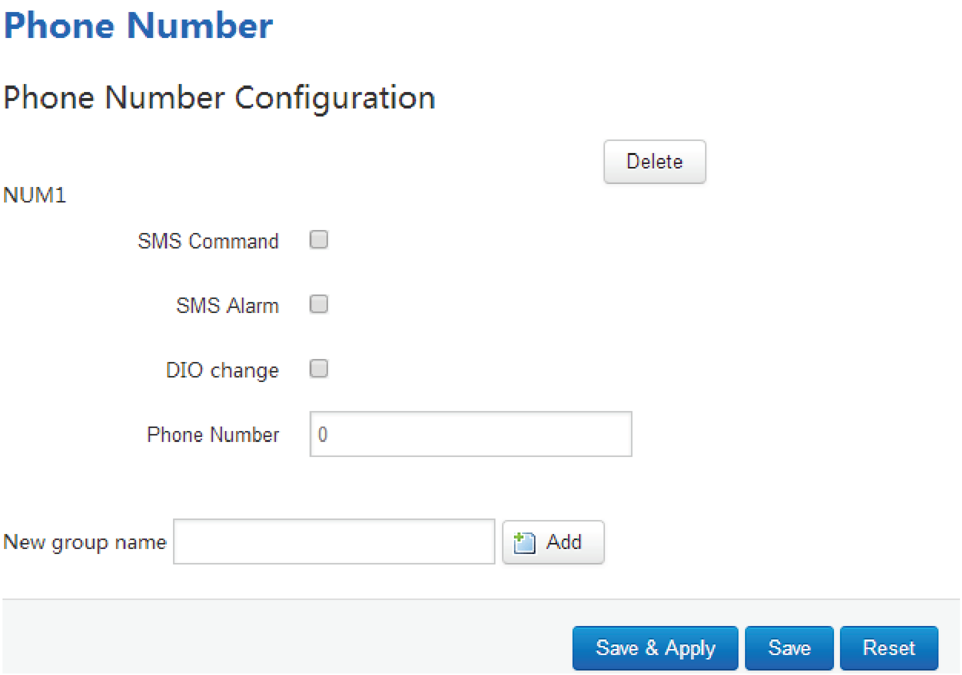
Singal Quality Threshold: 1

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 □

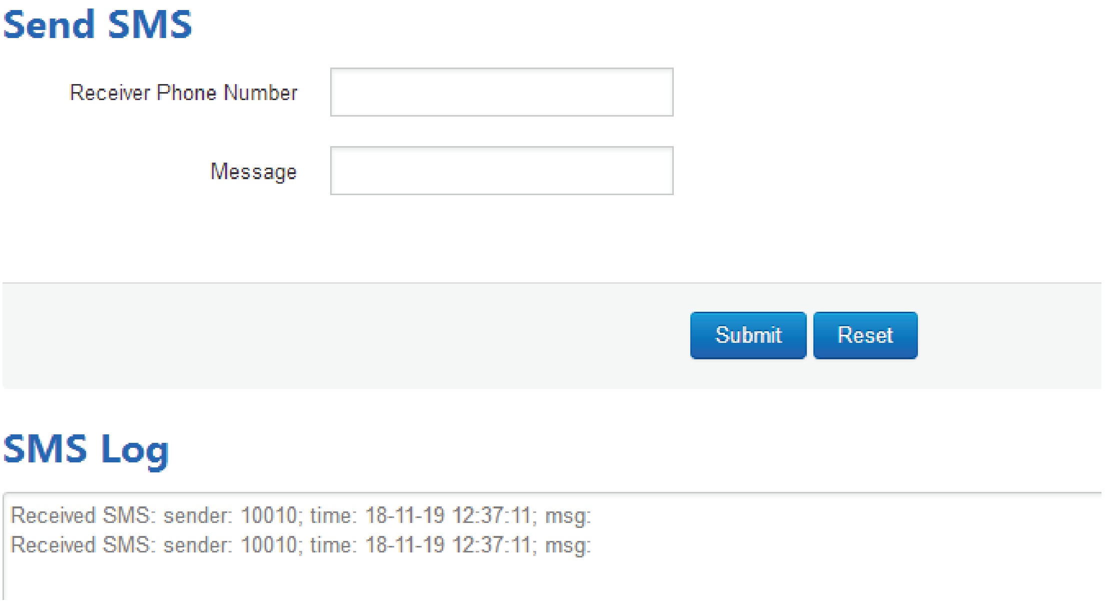
DIO change □

Phone Number 0

New group name

- **Add Phone number**: input a name and click button “Add” to add a new Phone number.
- **Delete Phone number**: click button “Delete”.
- **SMS command**: enable SMS command feature on this phone number.
- **SMS alarm**: this phone number can receive SMS Alarm.
- **DIO change**: DIO change alarm can be sent to this phone number.

➢ **SMS**



Send SMS

Receiver Phone Number

Message

SMS Log

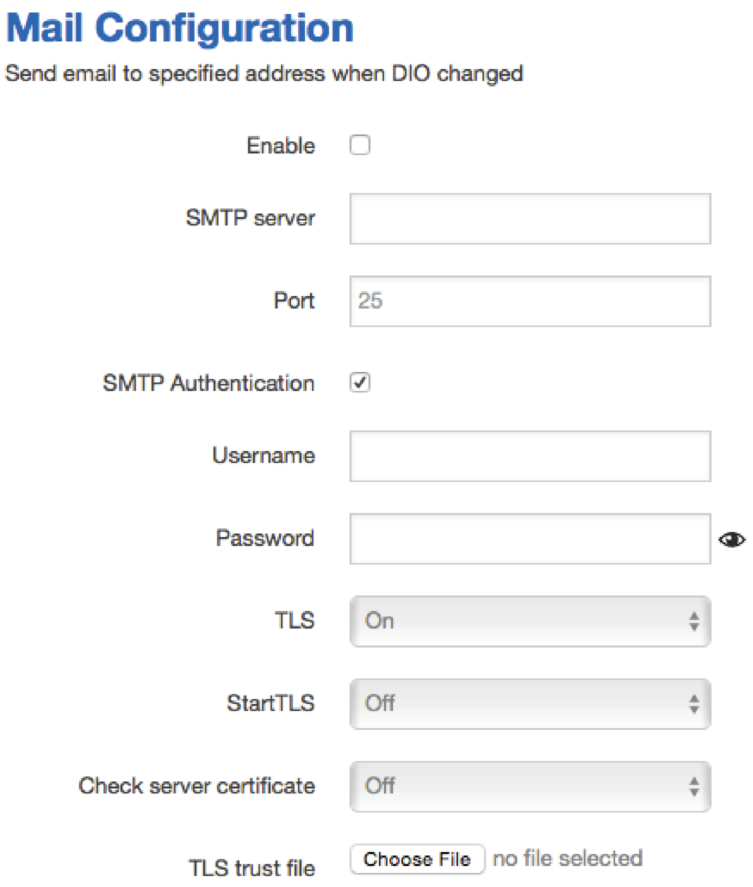
```
Received SMS: sender: 10010; time: 18-11-19 12:37:11; msg:
Received SMS: sender: 10010; time: 18-11-19 12:37:11; msg:
```

- **Receiver Phone Number**: the Phone number that receive message.
- **Message**: the content of message

- **Submit**: click button “Submit” to send message immediately.
- **SMS Log**: SMS send and receive log.

- **DIO Mail**

  Send email to receiver when DIO change.



Mail Configuration

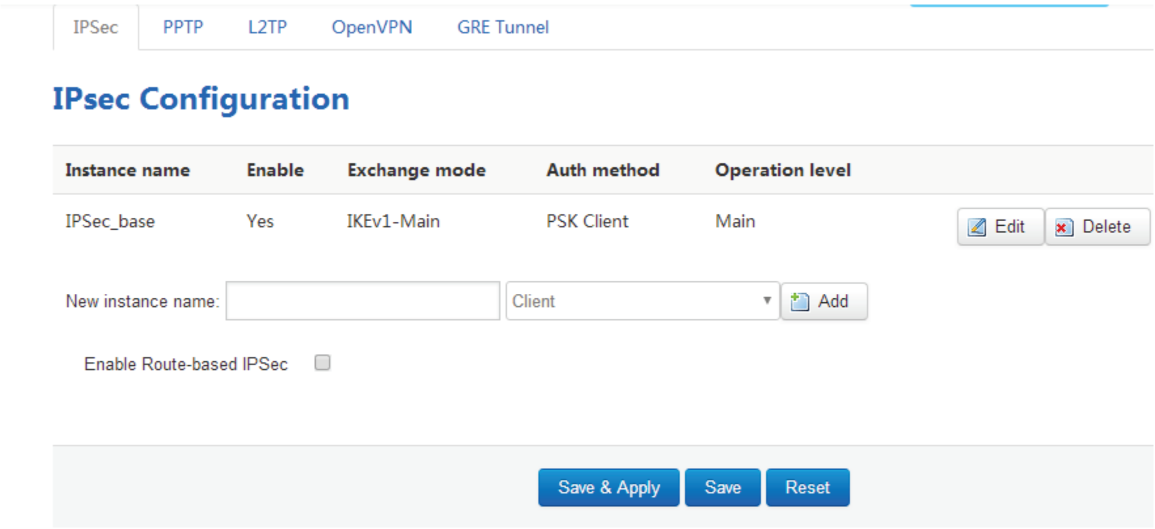
Send email to specified address when DIO changed

Enable	□
SMTP server	
Port	25
SMTP Authentication	☑
Username	
Password	
TLS	On
StartTLS	Off
Check server certificate	Off
TLS trust file	Choose File no file selected

- **Enable**: activate DIO Mail functionality.
- **SMTP server**: SMTP server IP address or URL.
- **Port**: SMTP server port.
- **SMTP Authentication**: If SMTP server requires SMTP Authentication, enable it.
- **Username**: Username for SMTP authentication.
- **Password**: Password for SMTP authentication.
- **TLS**: Enable or disable TLS (also known as SSL) for secured connections.
- **Start TLS**: Choose the TLS variant: start TLS from within the session (‘on’, default), or tunnel the session through TLS (‘off’).
- **Check server certificate**: Activate server certificate verification using a list of trued Certification Authorities (CAs).
- **TLS trust file**: Activate server certificate verification using trusted Certification Authorities (CAs).

3.5.8 VPN

3.5.8.1 IPSEC



IPsec Configuration

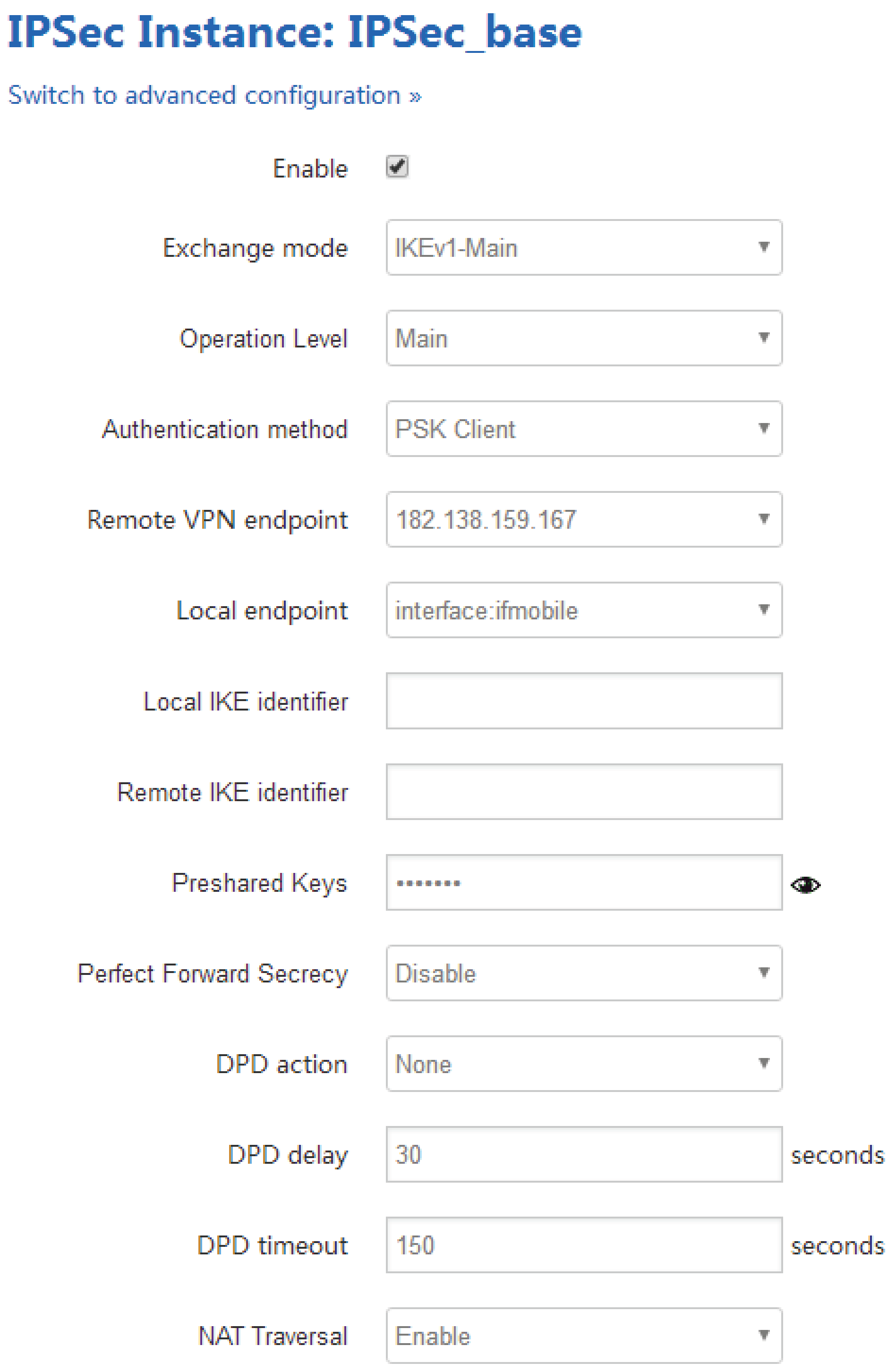
Instance name	Enable	Exchange mode	Auth method	Operation level	
IPSec_base	Yes	IKEv1-Main	PSK Client	Main	Edit Delete

New instance name: Client ▾ Add

Enable Route-based IPSec □

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

The default setting is Policy-based IPSec, if Enable Route-based IPSec is ticked, after save & apply, it will switch to Route-based IPSec.



IPSec Instance: IPSec_base

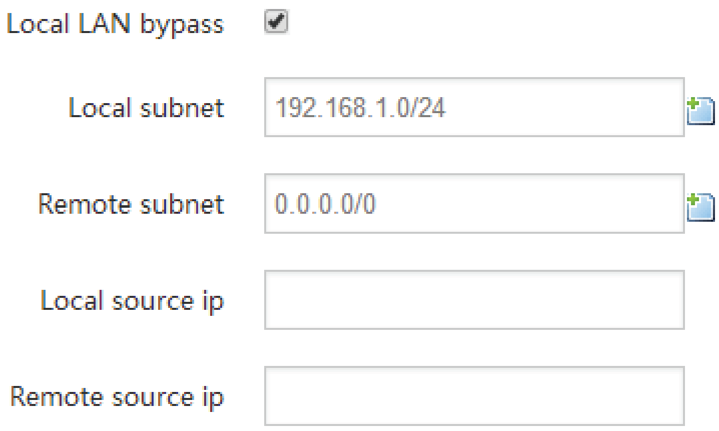
Switch to advanced configuration »

Enable	☑
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Client
Remote VPN endpoint	182.138.159.167
Local endpoint	interface:ifmobile
Local IKE identifier	
Remote IKE identifier	
Preshared Keys	•••••••
Perfect Forward Secrecy	Disable
DPD action	None
DPD delay	30 seconds
DPD timeout	150 seconds
NAT Traversal	Enable

- **Enable**: enable IPSEC feature
- **Exchange mode**: IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main mode are supported.
- **Operation Level**: for IPSec backup. One instance is Main then another instance is Backup. If Main instance is down switch to backup instance.
- **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

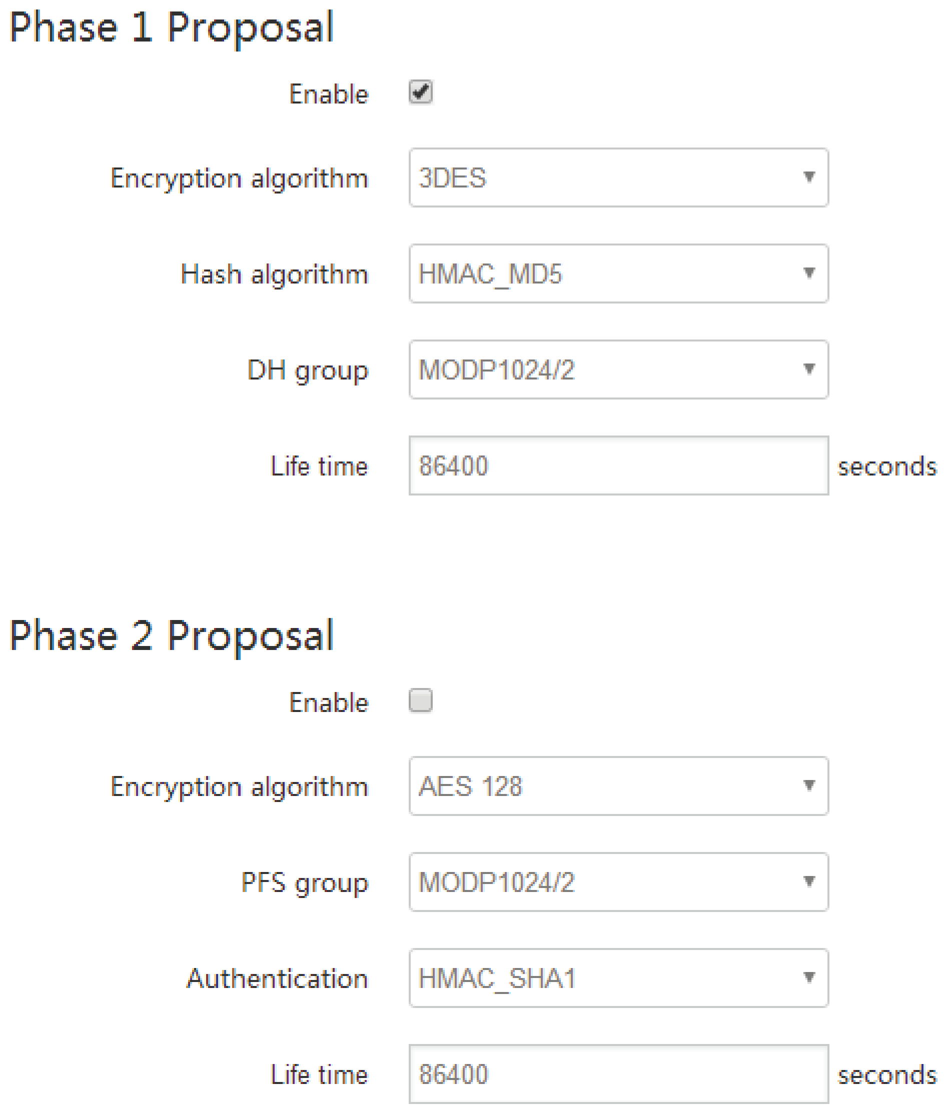
visited from internet.

- **Local endpoint**: domain name or IP address or interface name of this device.
- **Local IKE identifier:** Identity to use for the local device authentication.
- **Remote IKE identifier:** Identity to use for the remote device authentication.
- **Preshared Keys**: it is known as PSK, the length is 16 to 32.
- **Perfect Forward Secrecy:** whether Perfect Forward Secrecy of keys is desired on the connection's keying channel.
- **DPD action:** controls the use of the Dead Peer Detection protocol (DPD, RFC 3706) where R_U_THERE notification messages(IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveliness of the IPsec peer. The values clear, hold, and restart all activate DPD and determine the action to perform on a timeout. With clear the connection is closed with no further actions taken. hold installs a trap policy, which will catch matching traffic and tries to re-negotiate the connection on demand. restart will immediately trigger an attempt to re-negotiate the connection. The default is none which disables the active sending of DPD messages
- **DPD delay**: defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer
- **DPD timeout**: defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
- **NAT Traversal**: indicate device is behind a NAT device or not.



Local LAN bypass	☑
Local subnet	192.168.1.0/24
Remote subnet	0.0.0.0/0
Local source ip	
Remote source ip	

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



Phase 1 Proposal

Enable ☑

Encryption algorithm: 3DES

Hash algorithm: HMAC_MD5

DH group: MODP1024/2

Life time: 86400 seconds

Phase 2 Proposal

Enable □

Encryption algorithm: AES 128

PFS group: MODP1024/2

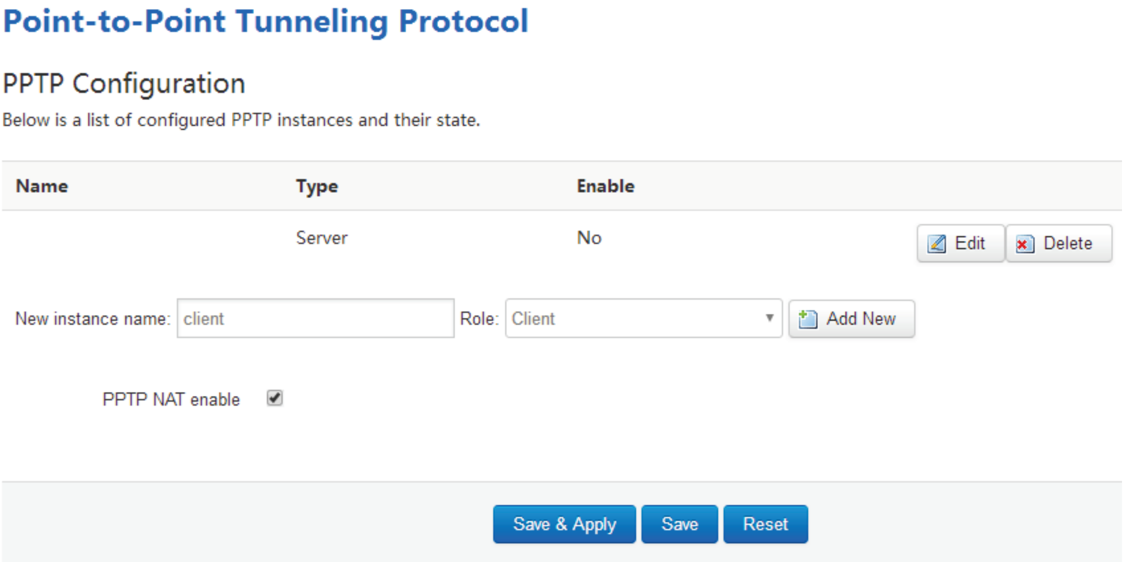
Authentication: HMAC_SHA1

Life time: 86400 seconds

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	Edit Delete

New instance name: client Role: Client

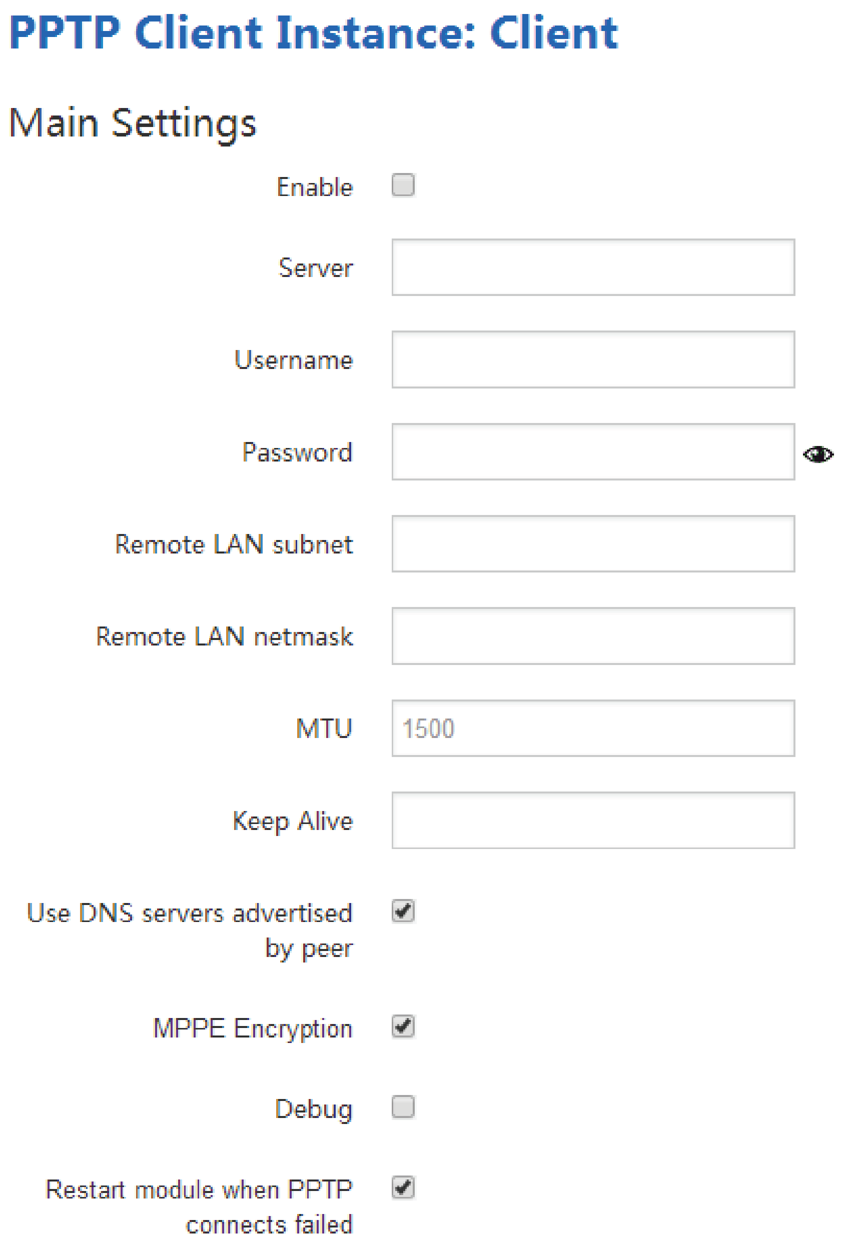
PPTP NAT enable ☑

This page is a list of configured PPTP instance and their state. Click button "Edit" to modify it, or click button "Delete" to delete an instance.

- **PPTP NAT enable**: enable PPTP interface NAT.

.

➢ **PPTP Client configuration**



PPTP Client Instance: Client

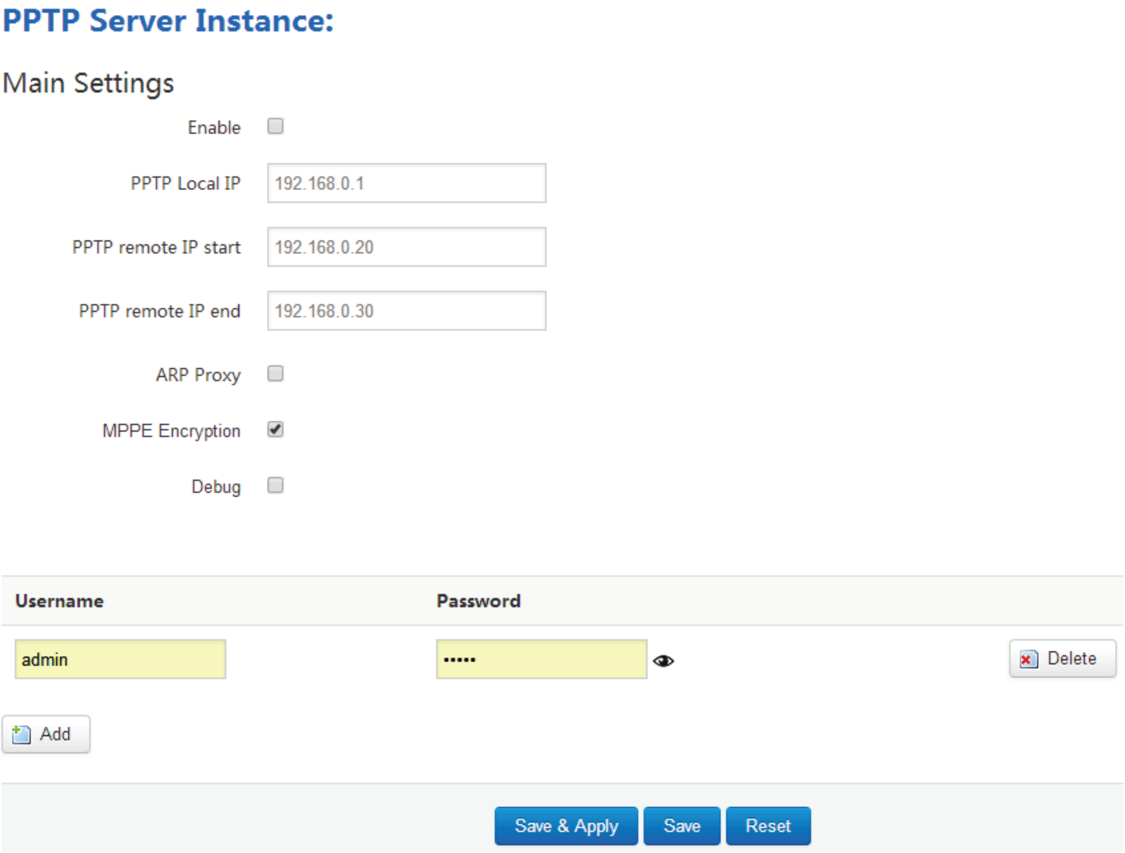
Main Settings

Enable	☐
Server	
Username	
Password	
Remote LAN subnet	
Remote LAN netmask	
MTU	1500
Keep Alive	
Use DNS servers advertised by peer	☑
MPPE Encryption	☑
Debug	☐
Restart module when PPTP connects failed	☑

- **Enable**: enable this instance.
- **Server**: domain name or IP address of PPTP server.
- **Username**: server authentication user name.
- **Password**: server authentication password.
- **Remote LAN subnet**: the remote subnet which can be access via PPTP tunnel.such as 192.168.10.0
- **Remote LAN netmask**: the netmask for remote LAN subnet. Such as 255.255.255.0
- **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 DNS servers advertised by peer**: If unchecked, the advertised DNS server addresses are ignored.

- **MPPE Encryption**: Microsoft Point-to-Point Encryption.
- **Debug**: add verbose PPTP log in system log.
- **Restart module when PPTP connects failed**: in some network PPTP cannot connect until restart module.

➢ **PPTP Server Configuration**



PPTP Server Instance:

Main Settings

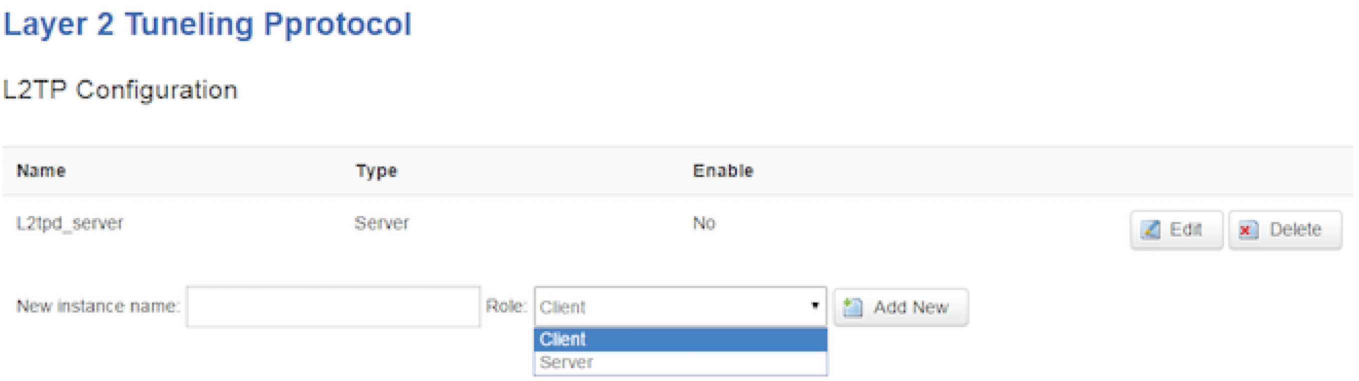
Enable	□
PPTP Local IP	192.168.0.1
PPTP remote IP start	192.168.0.20
PPTP remote IP end	192.168.0.30
ARP Proxy	□
MPPE Encryption	☑
Debug	□

Username	Password	
admin	•••••	Delete

- **PPTP Local IP**: indicate server's IP address.
- **PPTP remote IP start**: the remote IP address leases start
- **PPTP remote IP end**: the remote IP address lease end.
- **ARP Proxy**: if the remote IP has the same subnet with LAN, check it for connecting each other.
- **MPPE Encryption**: Microsoft Point-to-Point Encryption
- **Debug**: add verbose PPTP log 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.



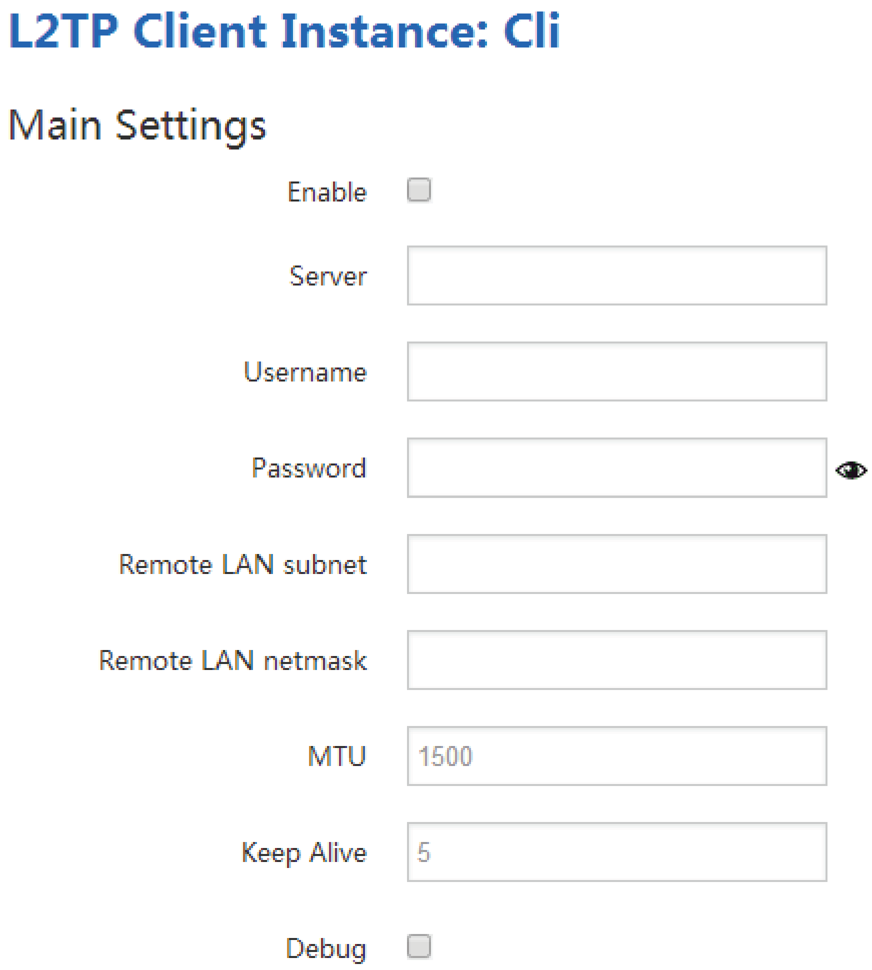
Layer 2 Tuneling Pprotocol

L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	Edit Delete

New instance name: Role: Client ▾ Add New

➢ **L2TP Client configuration**



L2TP Client Instance: Cli

Main Settings

Enable □

Server

Username

Password

Remote LAN subnet

Remote LAN netmask

MTU 1500

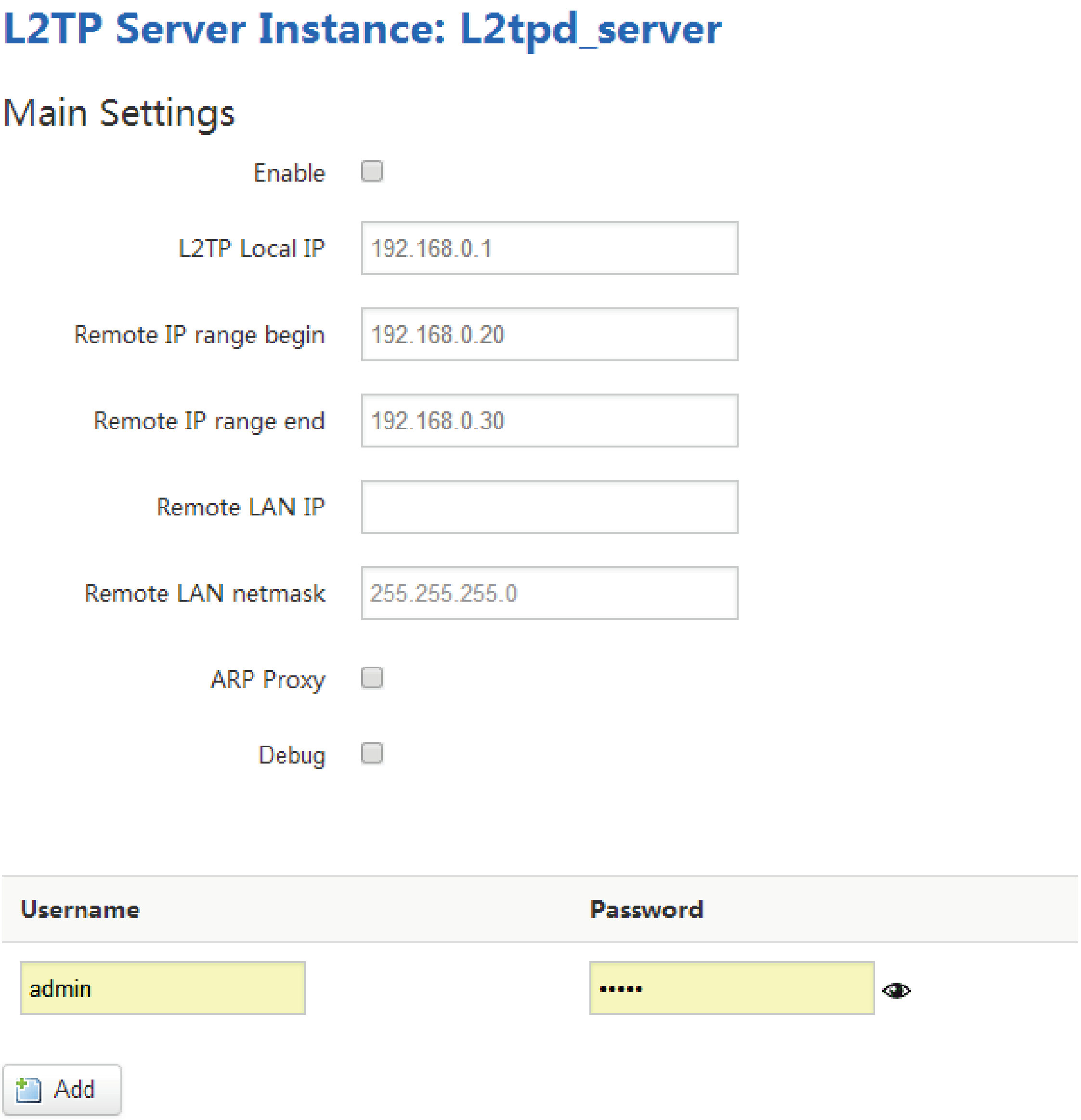
Keep Alive 5

Debug □

- **Enable**: enable this L2TP instance.
- **Server**: domain name or IP address of L2TP server.
- **Username**: server authentication user name.
- **Password**: server authentication password.
- **Remote LAN subnet**: the remote LAN subnet can be accessed via L2TP tunnel, such as 192.168.10.0
- **Remote LAN netmask**: the netmask for remote LAN subnet, such as 255.255.255.0

- **MTU**: maximum transmission unit.
- **Keep Alive**: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Debug**: add L2TP verbose log into system log

➢ **L2TP Server configuration**



L2TP Server Instance: L2tpd_server

Main Settings

Enable	□
L2TP Local IP	192.168.0.1
Remote IP range begin	192.168.0.20
Remote IP range end	192.168.0.30
Remote LAN IP	
Remote LAN netmask	255.255.255.0
ARP Proxy	□
Debug	□

Username	Password
admin	•••••

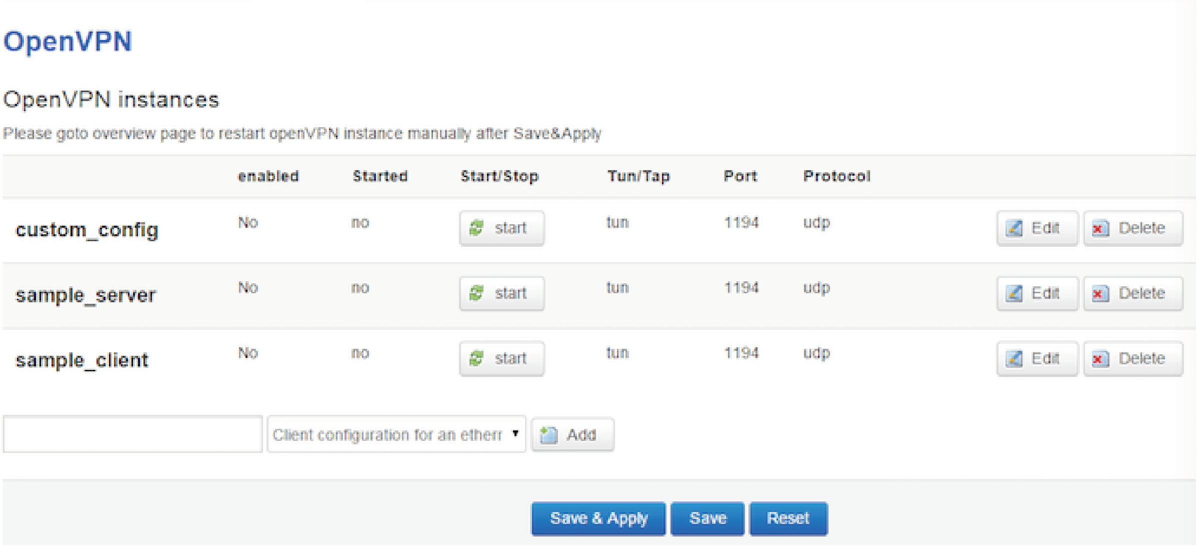
- **Local IP**: indicate server's IP address.
- **Remote IP range begin**: the remote IP address leases start
- **Remote IP range end**: the remote IP address lease end.
- **Remote LAN IP**: the remote LAN subnet can be accessed via L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask**: the mask of L2TP client IP, the default value is 255.255.255.0
- **ARP Proxy**: it allows remote L2TP client to access local LAN subnet. And the remote IP range should be included in LAN subnet. Such as local LAN subnet is

192.168.1.0/24, then configure Remote IP range begin to 192.168.1.20 and Remote IP range end to 192.168.1.30, and enable ARP Proxy.

- **Debug**: add L2TP verbose log into system log.
- **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

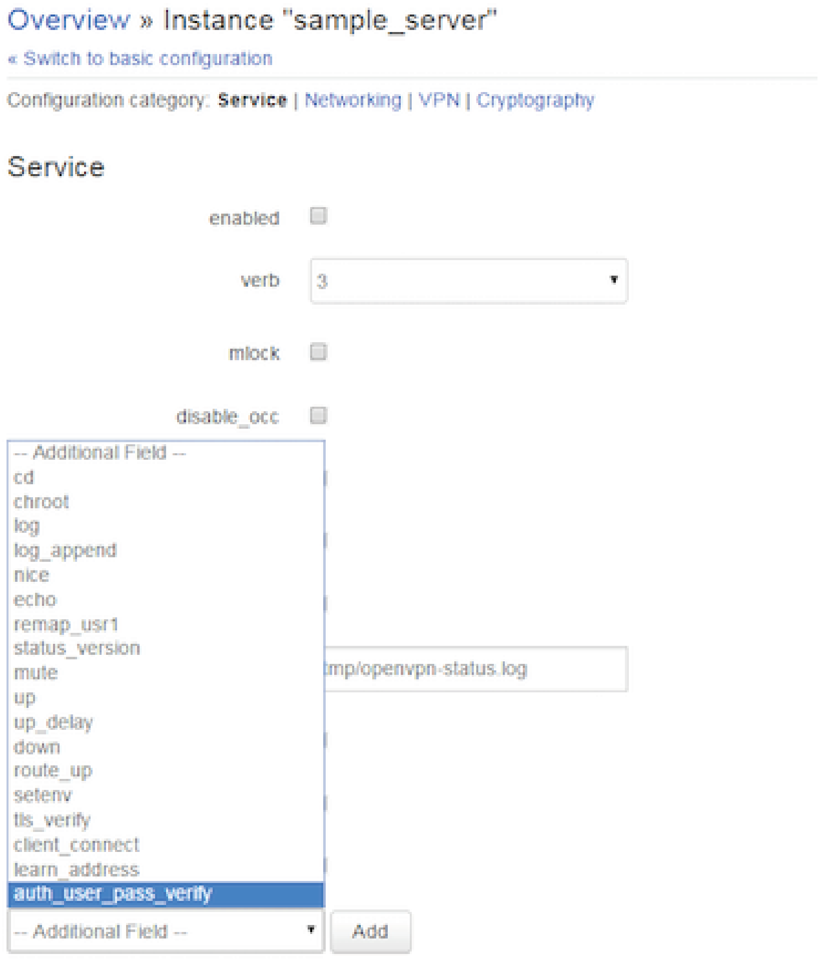
OpenVPN instances

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

Notes:

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" drop down list at bottom of page.



Overview » Instance "sample_server"

« Switch to basic configuration

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

Service

enabled □

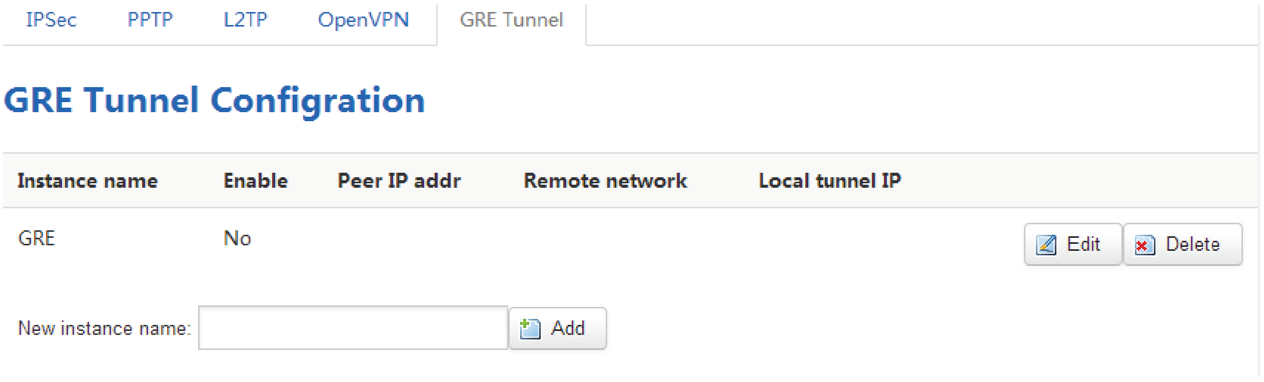
verb 3

mlock □

disable_occ □

tmp/openvpn-status.log

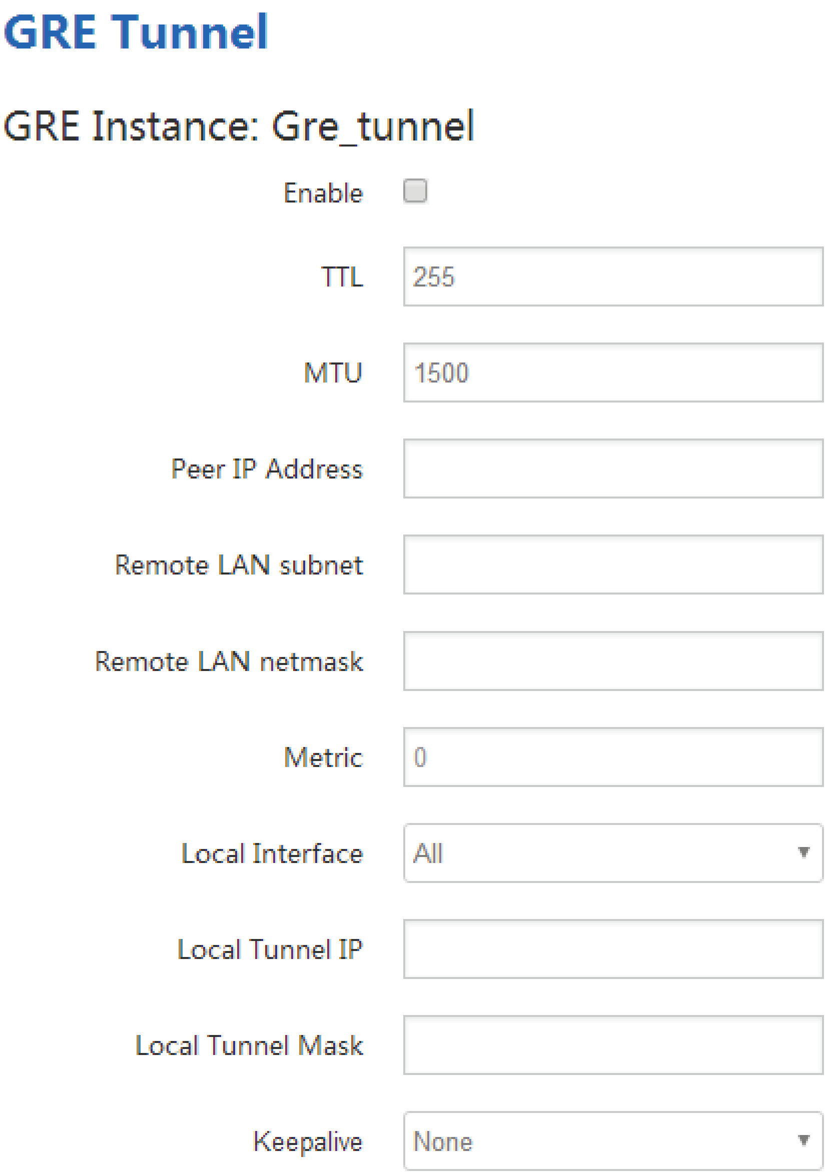
3.5.8.5 GRE tunnel



GRE Tunnel Configration

Instance name	Enable	Peer IP addr	Remote network	Local tunnel IP	
GRE	No				Edit Delete

New instance name: Add



GRE Tunnel

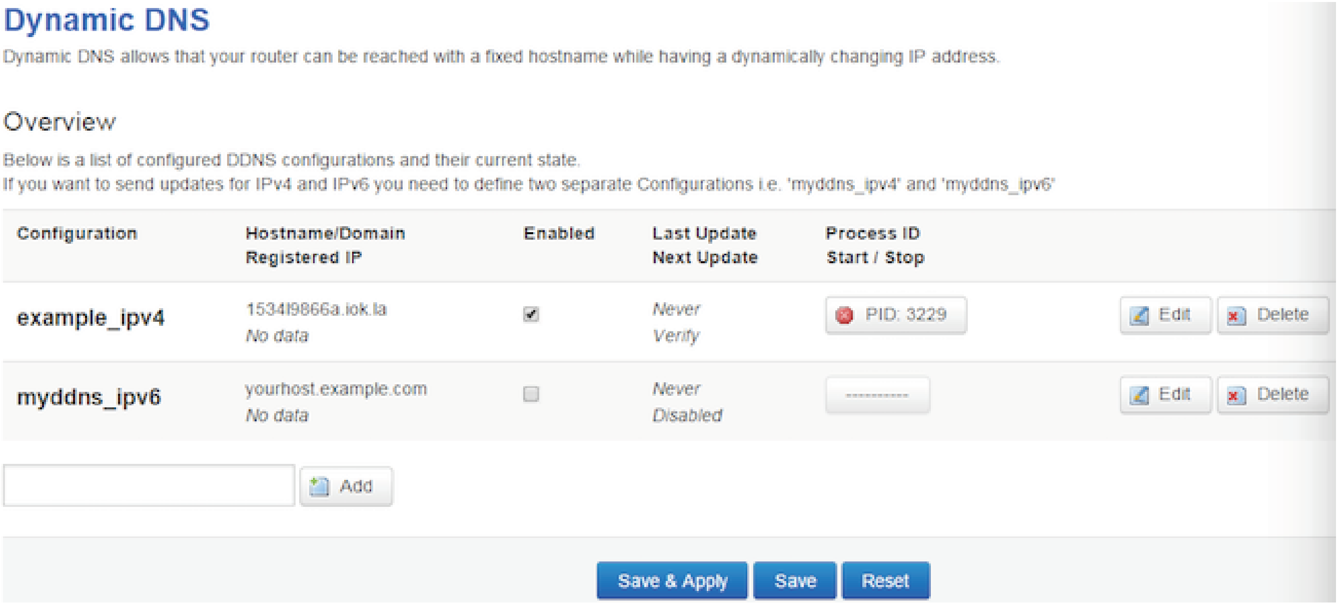
GRE Instance: Gre_tunnel

Enable	□
TTL	255
MTU	1500
Peer IP Address	
Remote LAN subnet	
Remote LAN netmask	
Metric	0
Local Interface	All ▾
Local Tunnel IP	
Local Tunnel Mask	
Keepalive	None ▾

- **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 that can be accessed via GRE tunnel, such as 192.168.10.0
- **Remote Netmask**: remote LAN subnet mask. Such as 255.255.255.0.
- **Local Tunnel IP**: Virtual IP address. It cannot be in same subnet as LAN network.
- **Local Tunnel Mask**: Virtual IP mask.
- **Local Interface**: bond a specific interface for GRE tunnel.
- **Keepalive**: None, receive only, send and receive. If value is None, GRE tunnel will remain up, if value is receive only , if no GRE keepalive message received for peer device, it will set tunnel to up. If value is send and receive, it will send keepalive message to remote peer, and also receive keepalive message from peer.

3.5.9 DDNS

DDNS allows that router can be reached with a fixed domain name while have a dynamically changing IP address.



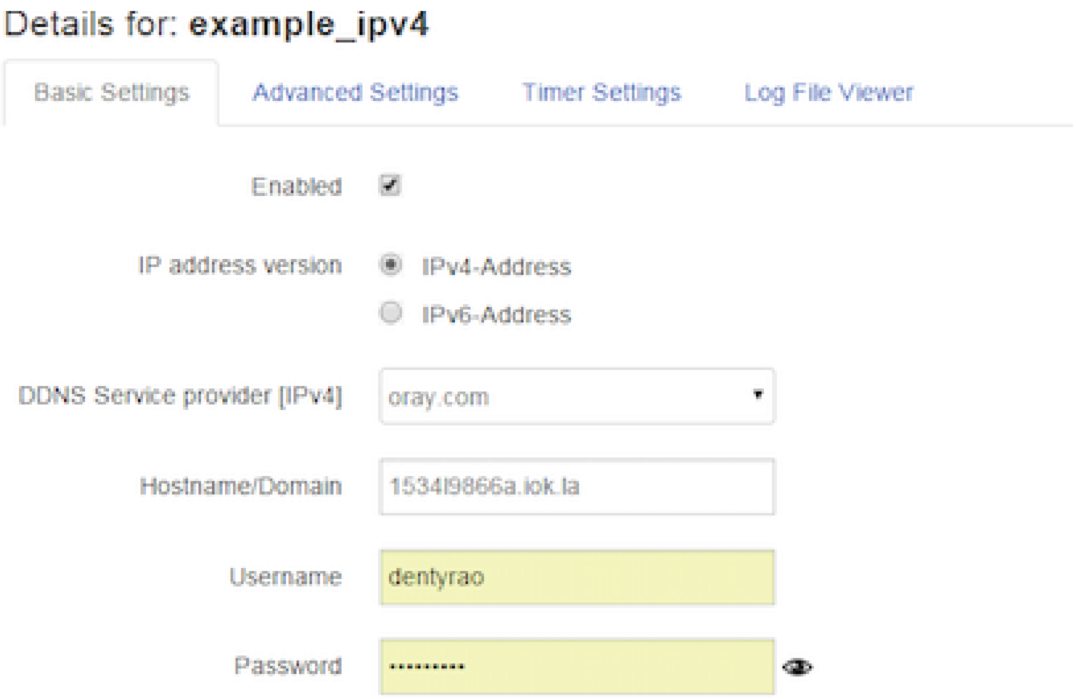
Dynamic DNS

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'

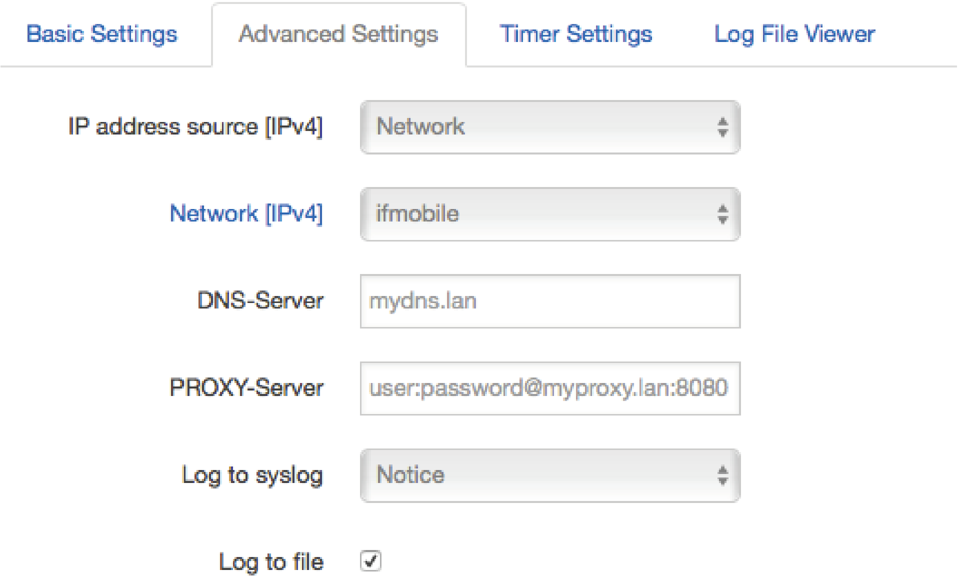
Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop		
example_ipv4	153419866a.iok.la *No data*	☑	*Never* *Verify*	PID: 3229	Edit	Delete
myddns_ipv6	yourhost.example.com *No data*	□	*Never* *Disabled*	----------	Edit	Delete



Details for: example_ipv4

Enabled	☑
IP address version	● IPv4-Address ○ IPv6-Address
DDNS Service provider [IPv4]	oray.com
Hostname/Domain	153419866a.iok.la
Username	dentyrao
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

Network [IPv4]: ifmobile

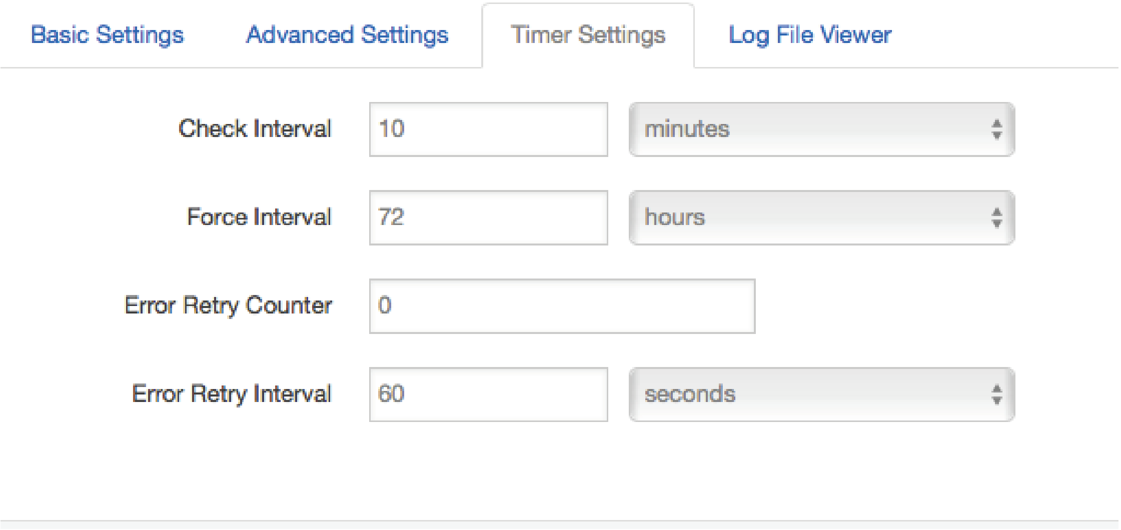
DNS-Server: mydns.lan

PROXY-Server: user:password@myproxy.lan:8080

Log to syslog: Notice

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.



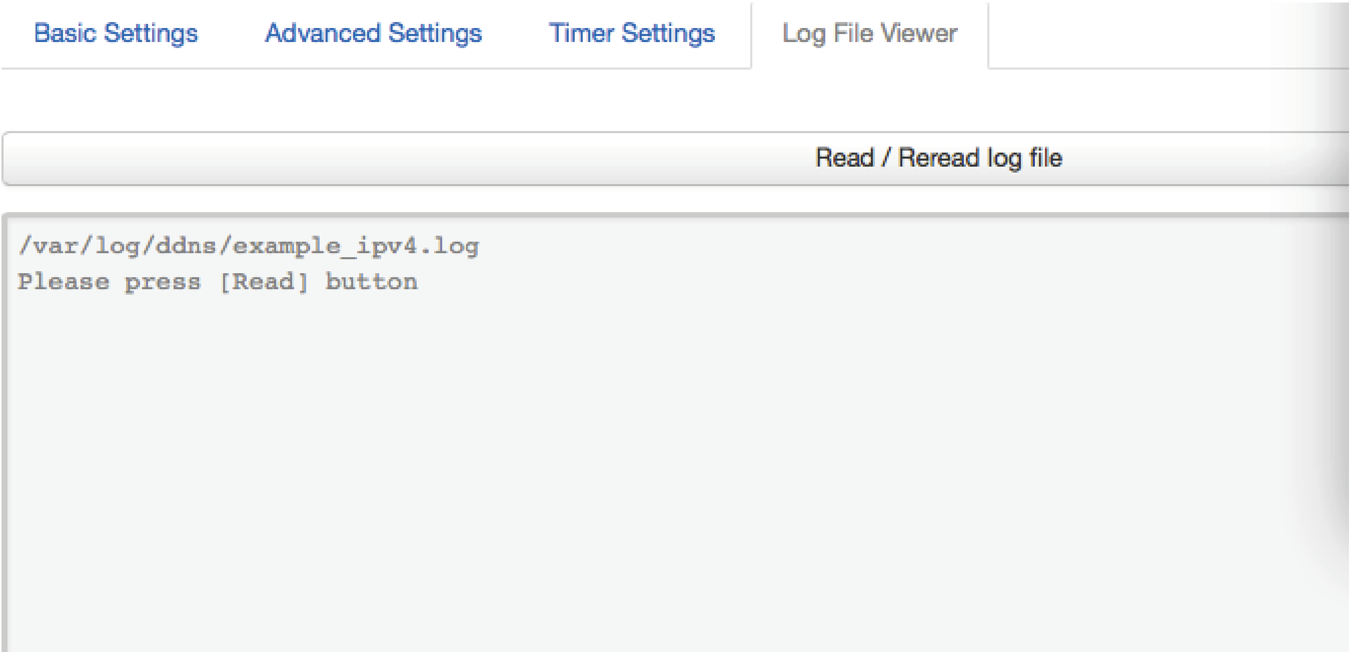
Check Interval: 10 minutes

Force Interval: 72 hours

Error Retry Counter: 0

Error Retry Interval: 60 seconds

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

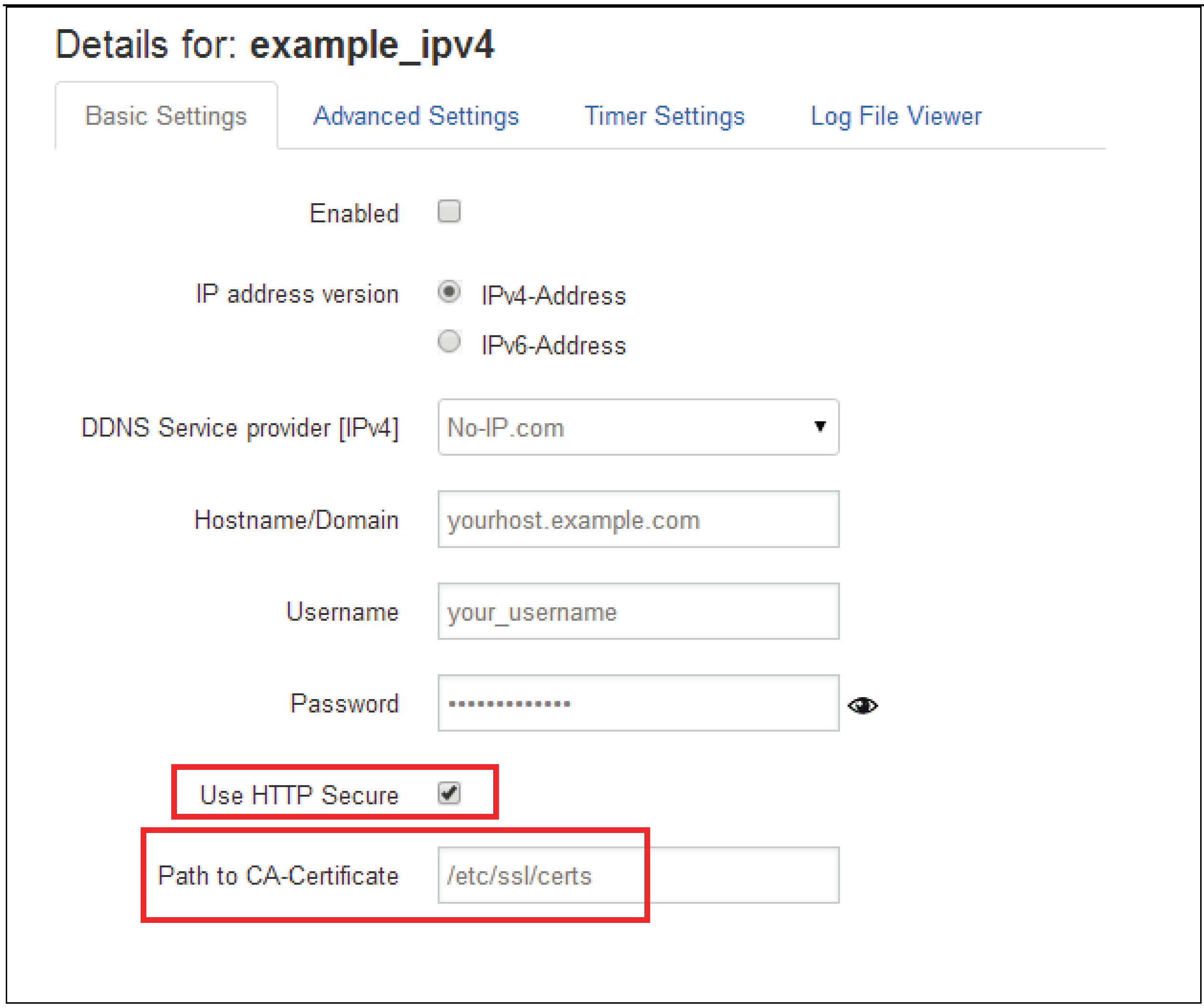


```
/var/log/ddns/example_ipv4.log
Please press [Read] button
```

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**

Enabled □

IP address version ● IPv4-Address ○ IPv6-Address

DDNS Service provider [IPv4] No-IP.com

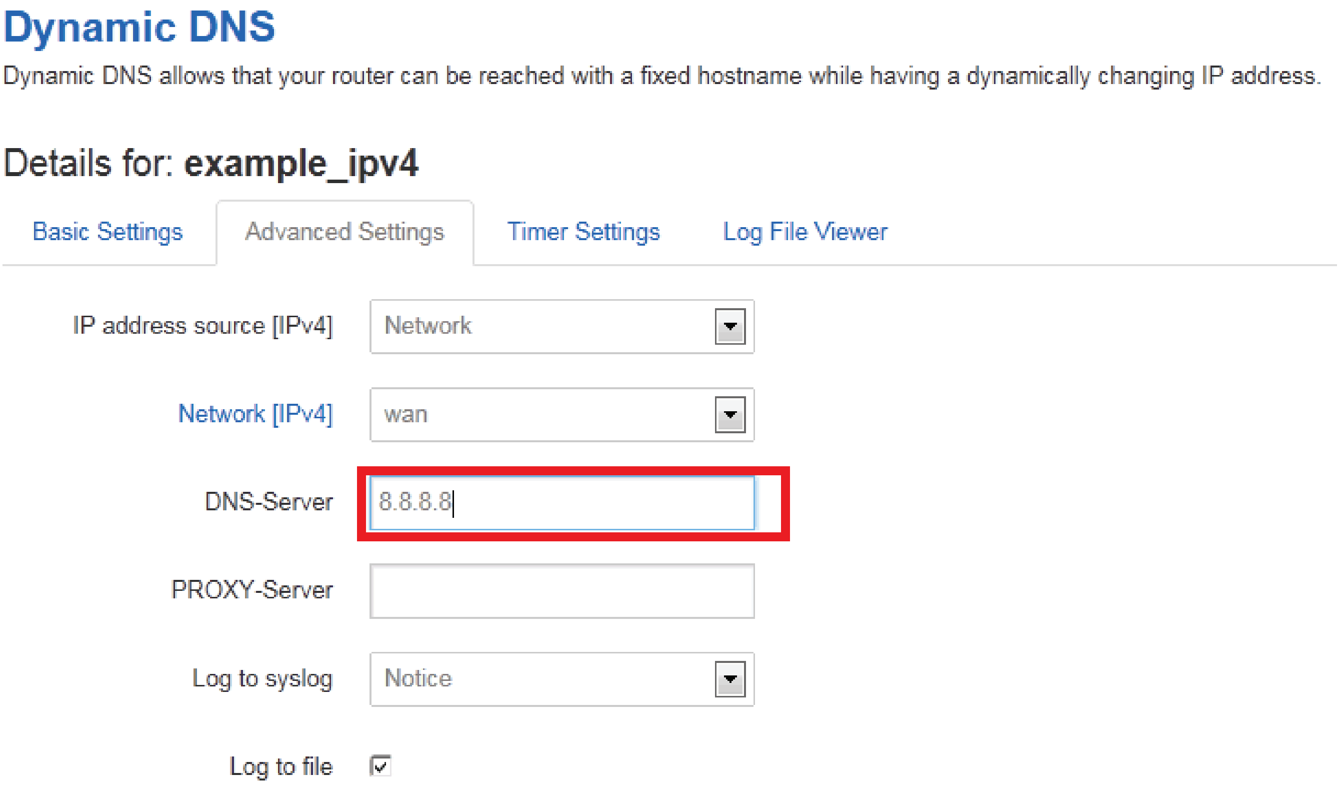
Hostname/Domain yourhost.example.com

Username your_username

Password ••••••••••••••

Use HTTP Secure ☑

Path to CA-Certificate /etc/ssl/certs



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**

IP address source [IPv4]: Network

Network [IPv4]: wan

DNS-Server: 8.8.8.8

PROXY-Server:

Log to syslog: Notice

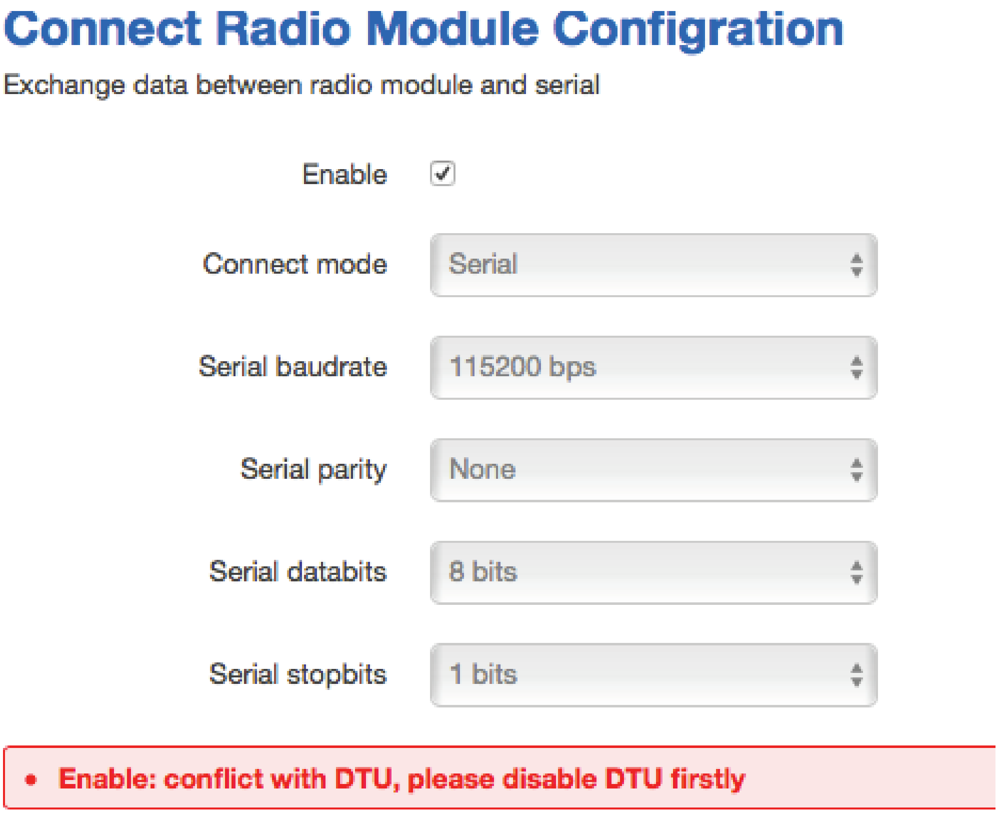
Log to file: ☑

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 Configration

Exchange data between radio module and serial

Enable ☑

Connect mode: Serial

Serial baudrate: 115200 bps

Serial parity: None

Serial databits: 8 bits

Serial stopbits: 1 bits

- Enable: conflict with DTU, please disable DTU firstly

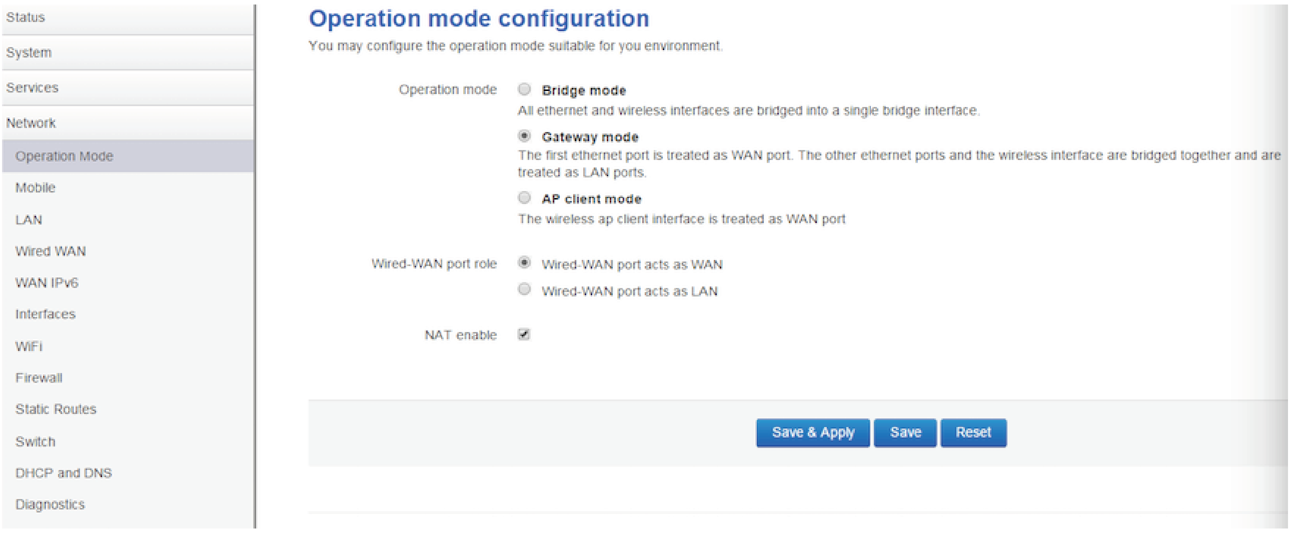
- **Connect Mode:** Serial only

Modem to Serial Settings

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

3.6 Network Configuration

3.6.1 Operation Mode



Operation mode configuration

You may configure the operation mode suitable for you environment.

Operation mode
○ **Bridge mode**
All ethernet and wireless interfaces are bridged into a single bridge interface.
● **Gateway mode**
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 mode**
The wireless ap client interface is treated as WAN port

Wired-WAN port role
● Wired-WAN port acts as WAN
○ Wired-WAN port acts as LAN

NAT enable ☑

➢ **Operation mode**

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

➢ **NAT Enabled**

Network Address Translation. Default is *Enabling*

➢ **Ethernet wan port role:**

Wired-WAN port acts as WAN

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

Wired-WAN port acts as LAN

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

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

3.6.1.1 Gets Five LAN Ethernet Port for H820Q

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

Notes:

1) If checked the " Wired-WAN port acts as LAN ", the H820Q does not have WAN RJ45 port.

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

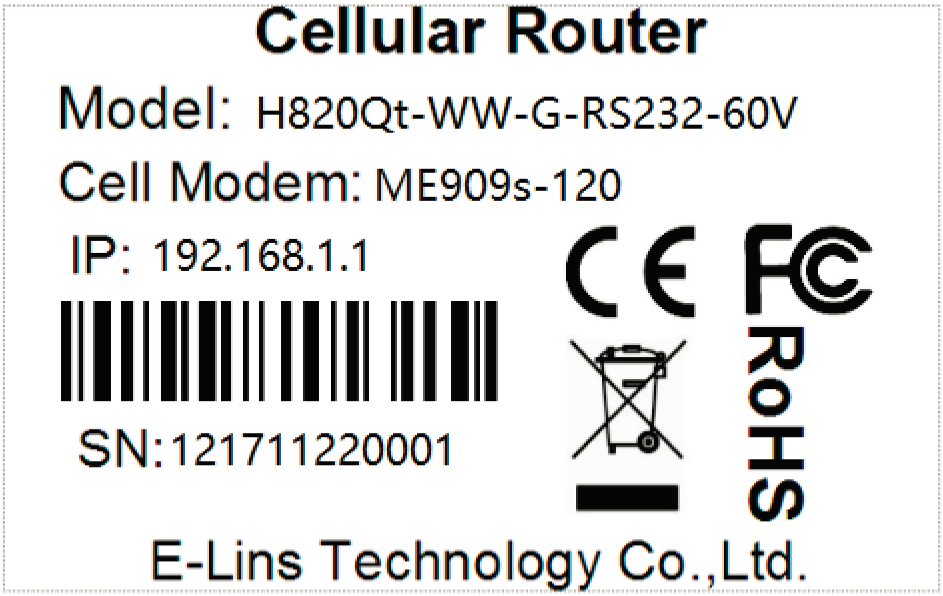
3.6.2 Mobile configuration

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.

⚠**Notes:**

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

For example, it shows the following picture. H820Q is the router series name, H820Qt-WW-G-RS232-60V is the part number name. And the ME909s-120 Cell Modem is the Cell Modem name.



Cellular Router

Model: H820Qt-WW-G-RS232-60V

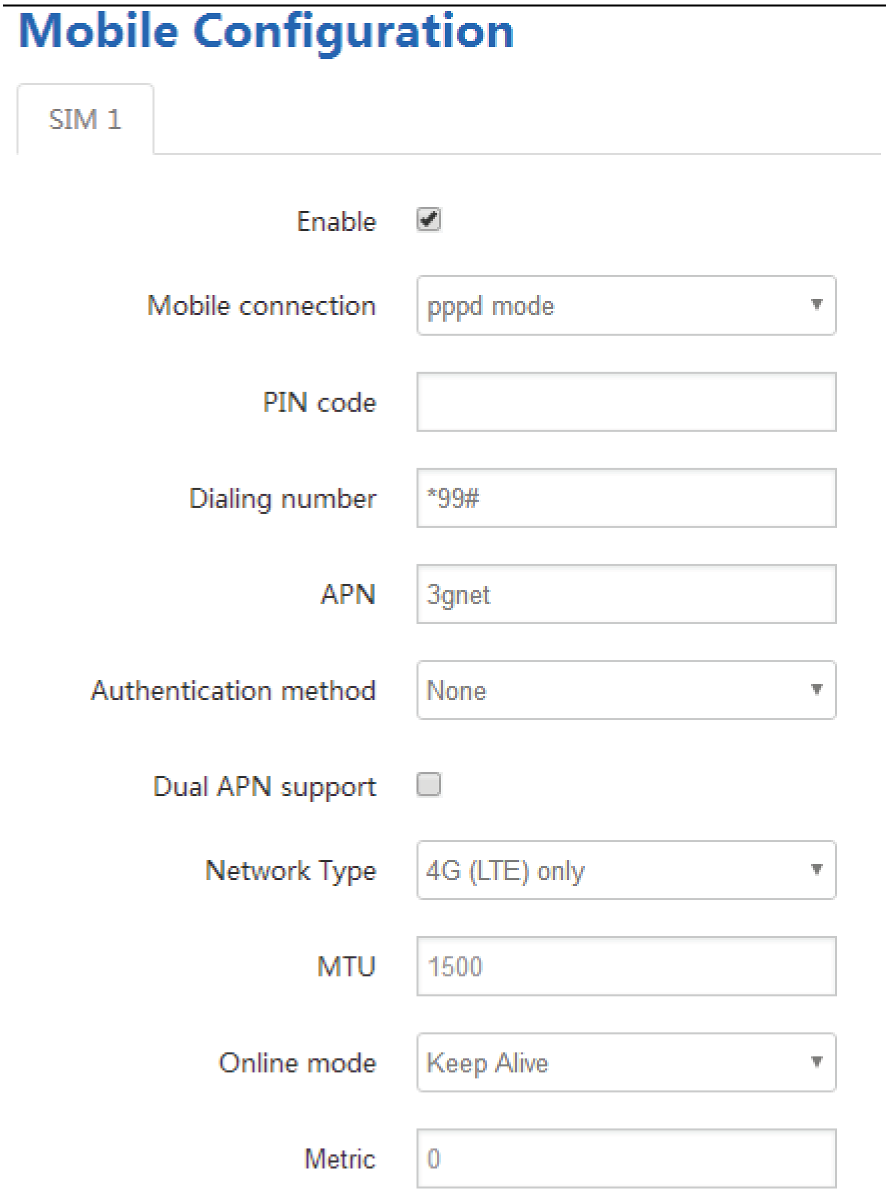
Cell Modem: ME909s-120

IP: 192.168.1.1

SN:121711220001

CE FC RoHS

E-Lins Technology Co.,Ltd.



Mobile Configuration

SIM 1

Enable ☑

Mobile connection: pppd mode ▾

PIN code:

Dialing number: *99#

APN: 3gnet

Authentication method: None ▾

Dual APN support ☐

Network Type: 4G (LTE) only ▾

MTU: 1500

Online mode: Keep Alive ▾

Metric: 0

- **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.

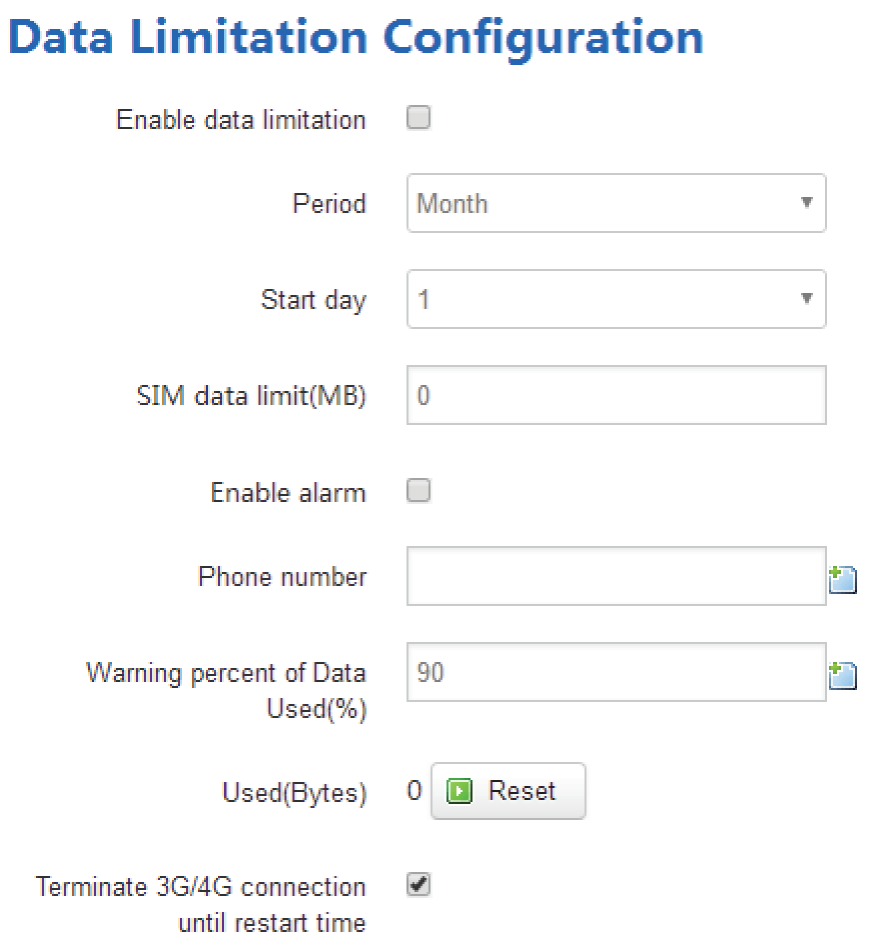
- **Dual APN support:**

  Most of SIM cards or Carriers/Operators just use one APN, but some use two APNs. Check this feature to use.

  Second APN: configure it referring to "APN";
  Second Authentication method: configure it referring to "Authentication method";

- **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

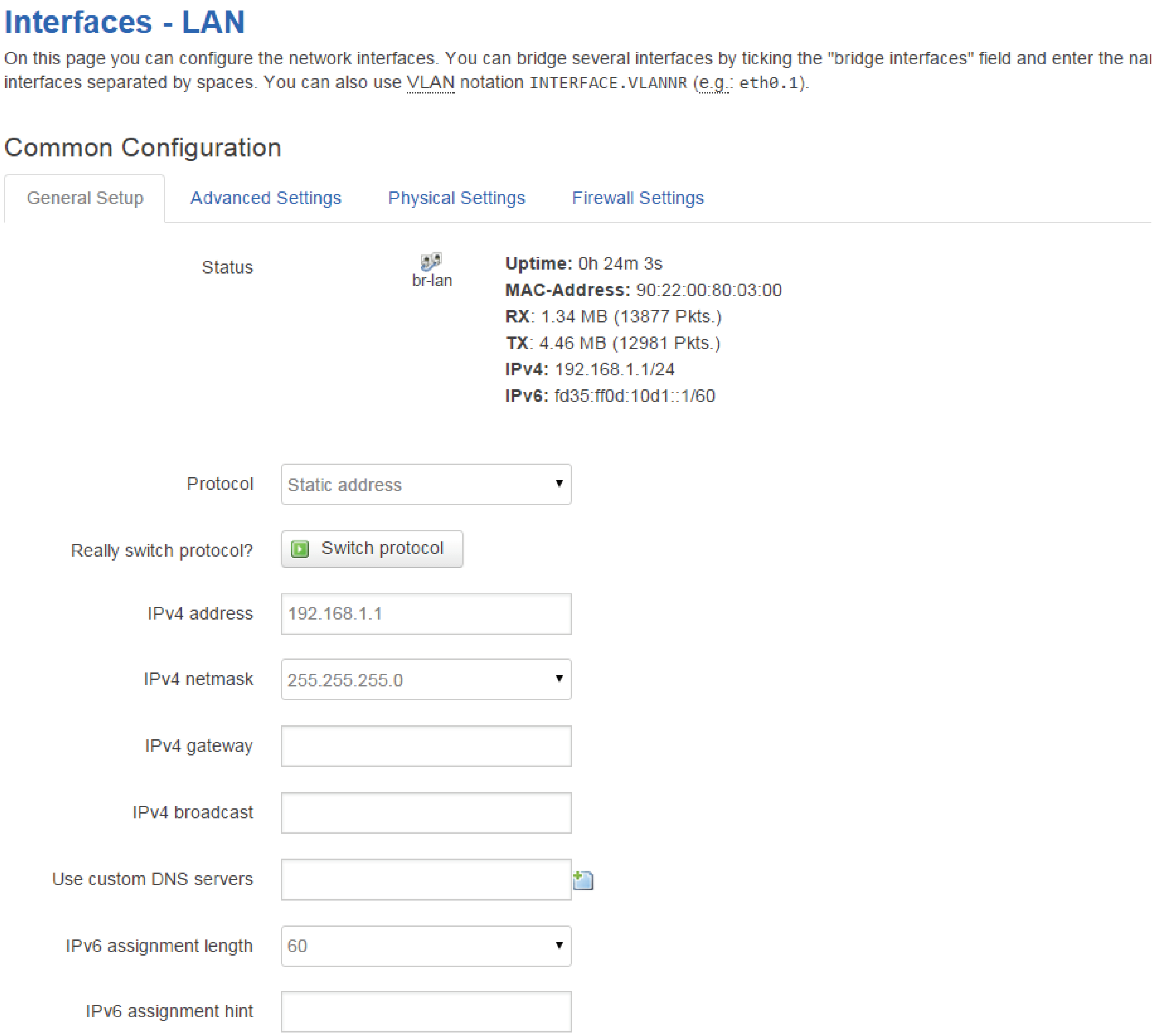


Data Limitation Configuration

Enable data limitation	□
Period	Month ▾
Start day	1 ▾
SIM data limit(MB)	0
Enable alarm	□
Phone number	
Warning percent of Data Used(%)	90
Used(Bytes)	0 Reset
Terminate 3G/4G connection until restart time	☑

- **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.
- **Reset:** press this button to clear all used .
- **Terminate 3G/4G connection until restart time:** if the max data exceed, set cell interface to down.

3.6.4 LAN settings



Interfaces - LAN

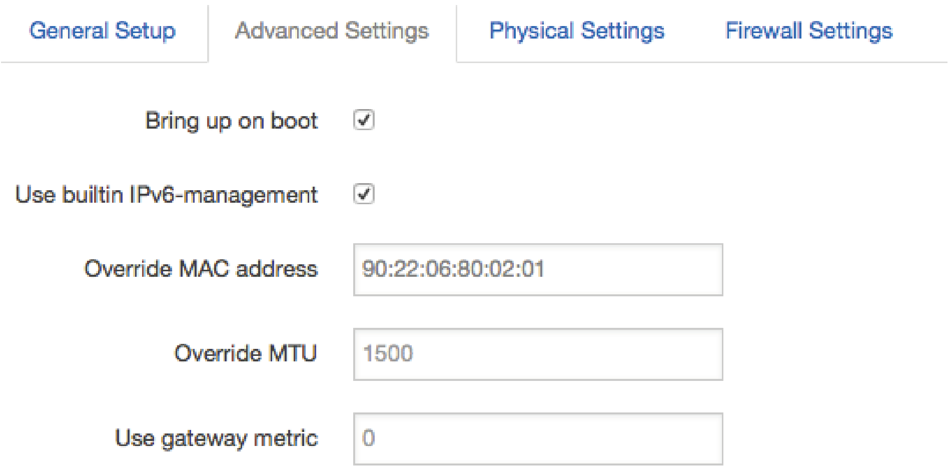
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the nai interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status br-lan
Uptime: 0h 24m 3s
MAC-Address: 90:22:00:80:03:00
RX: 1.34 MB (13877 Pkts.)
TX: 4.46 MB (12981 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd35:ff0d:10d1::1/60

Protocol	Static address
Really switch protocol?	Switch protocol
IPv4 address	192.168.1.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	60
IPv6 assignment hint	

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



Bring up on boot ☑

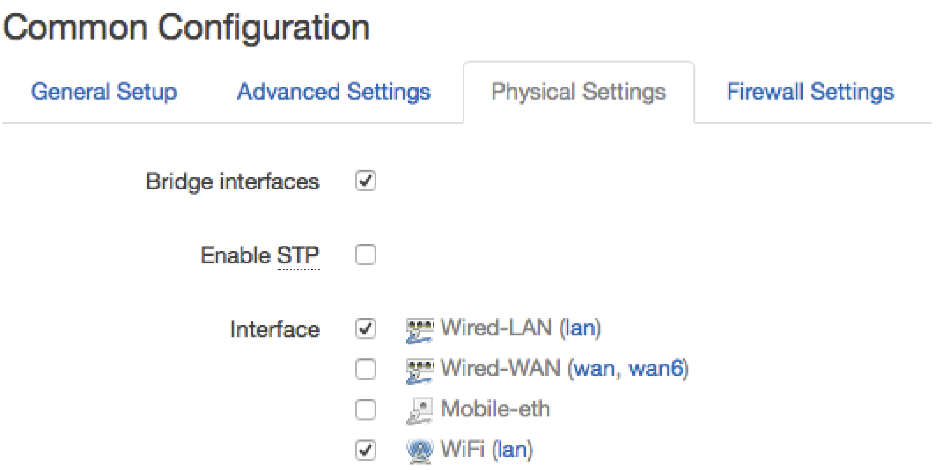
Use builtin IPv6-management ☑

Override MAC address 90:22:06:80:02:01

Override MTU 1500

Use gateway metric 0

- **Bring up on boot**: if checked, LAN interface will be set to up when system boot up. If unchecked, LAN interface will be down. Don't set it to unchecked if don't have special purpose.
- **Use built-in IPv6-management**: the default is checked. If IPv6 is not needed, it can be set to unchecked.
- **Override MAC address**: override LAN MAC address.
- **Override MTU**: Maximum Transmission Unit.
- **Use gateway metric**: the LAN subnet's metric to gateway.

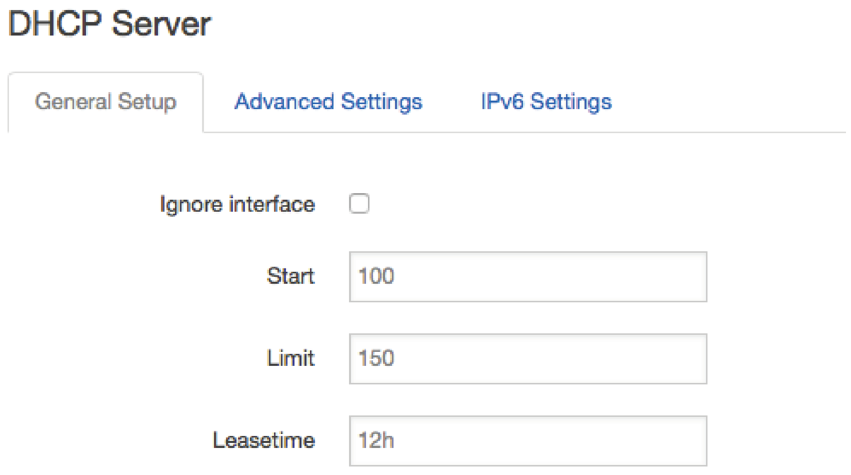


Bridge interfaces ☑

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

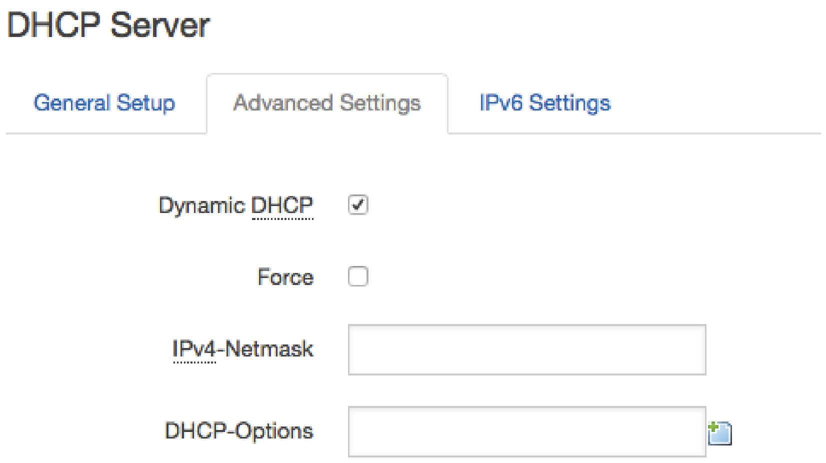
Ignore interface □

Start 100

Limit 150

Leasetime 12h

- **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

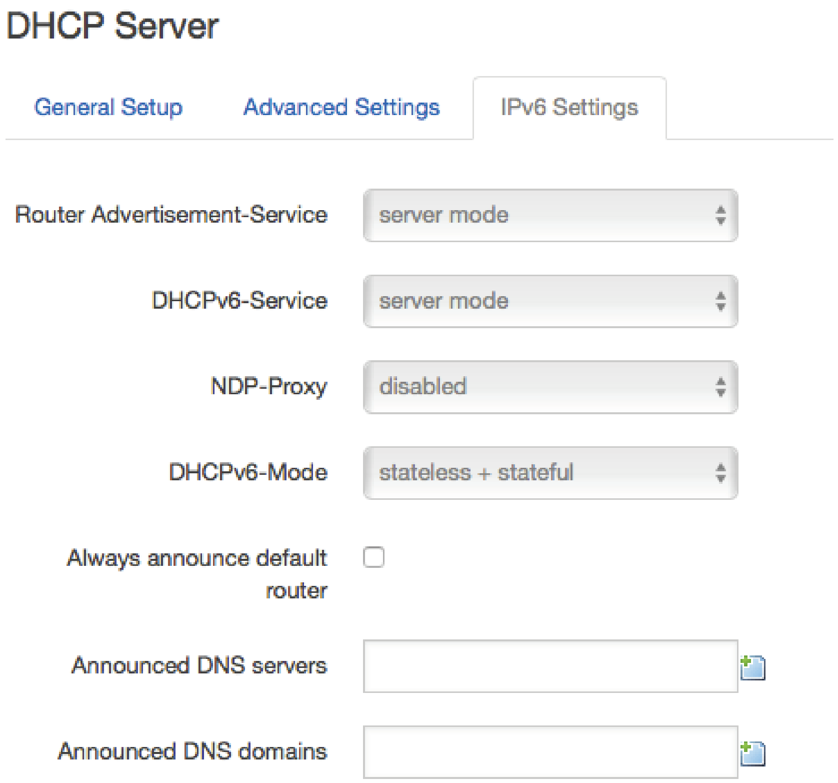
Dynamic DHCP ☑

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

Router Advertisement-Service: server mode

DHCPv6-Service: server mode

NDP-Proxy: disabled

DHCPv6-Mode: stateless + stateful

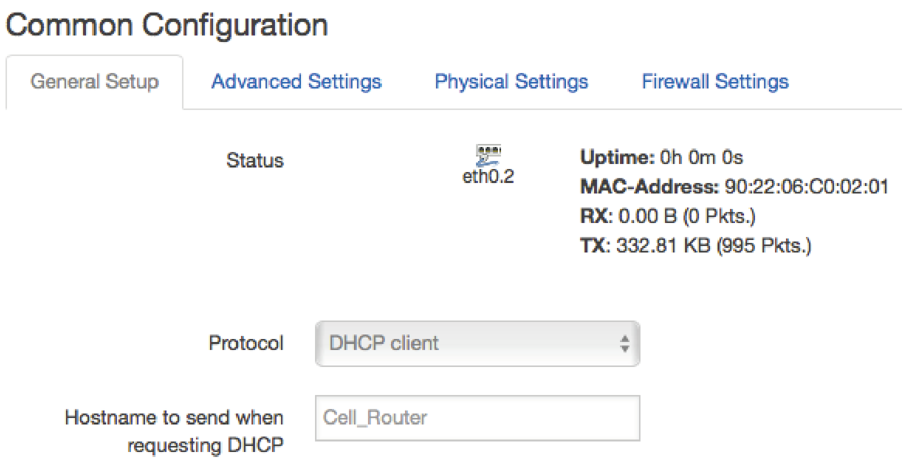
Always announce default router: □

Announced DNS servers:

Announced DNS domains:

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



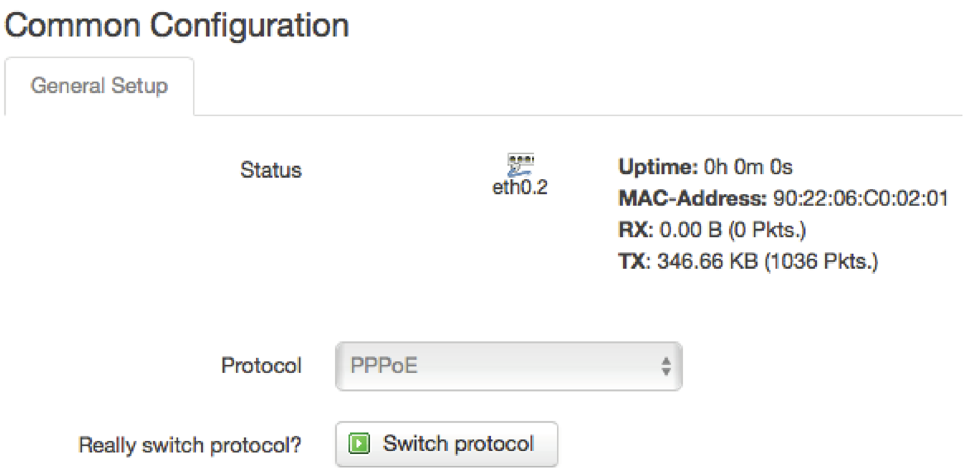
Common Configuration

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”.



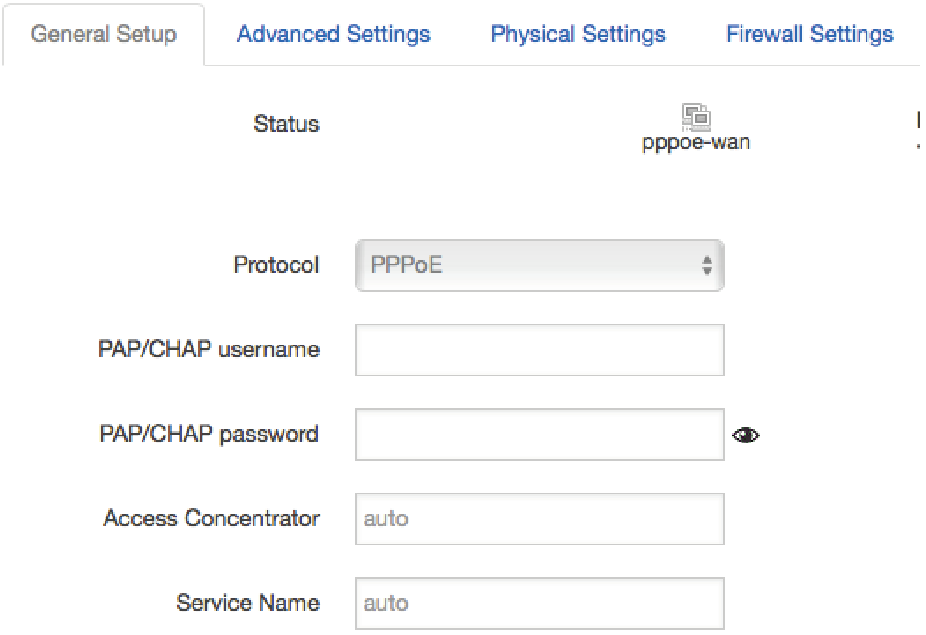
Common Configuration

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

Protocol: PPPoE

Really switch protocol?

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



Status: pppoe-wan

Protocol: PPPoE

PAP/CHAP username

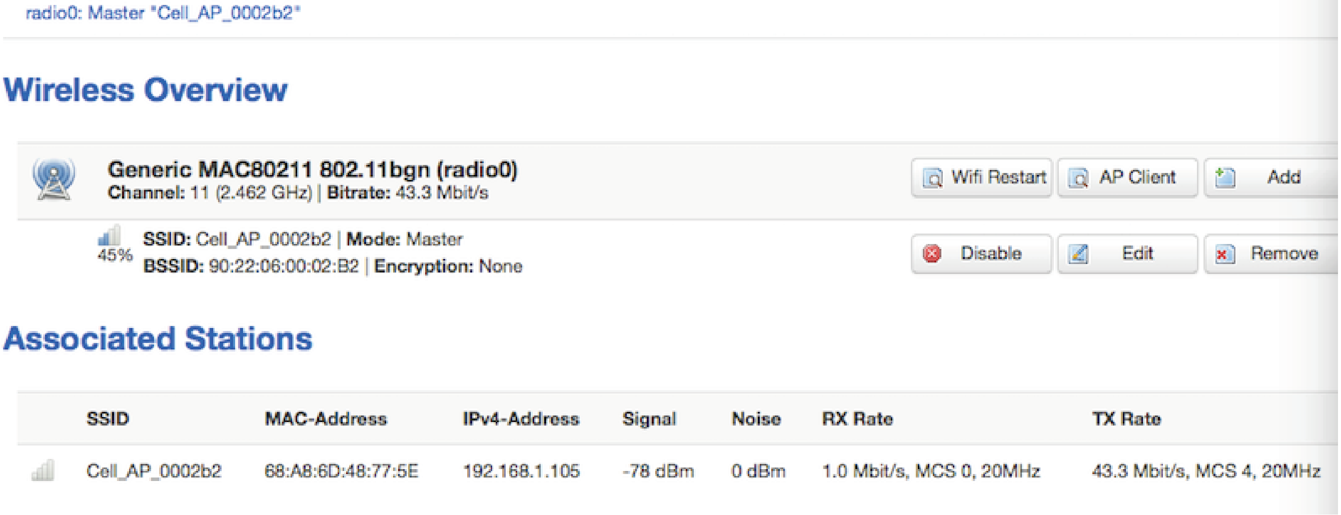
PAP/CHAP password

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

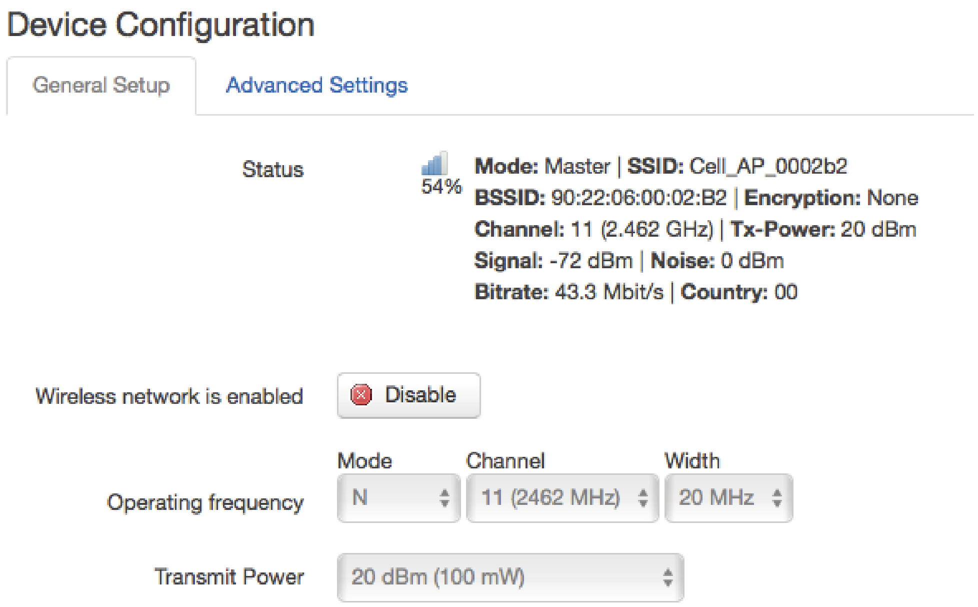
45% **SSID:** Cell_AP_0002b2 | **Mode:** Master
BSSID: 90:22:06:00:02:B2 | **Encryption:** None

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

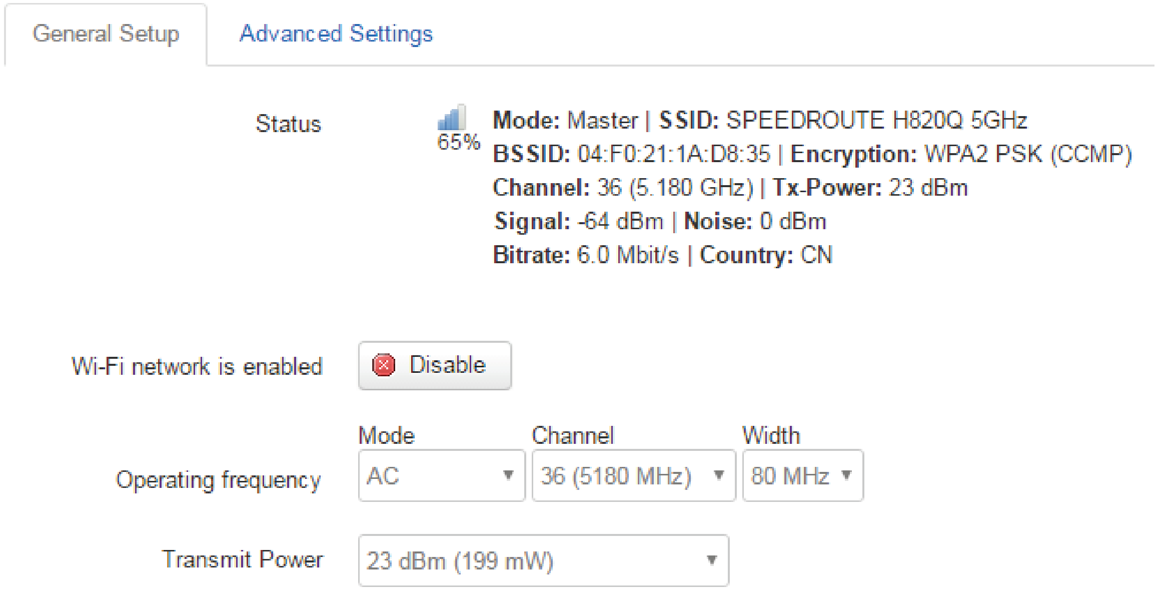
Wireless network is enabled: Disable

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

Transmit Power: 20 dBm (100 mW)

- **Status**: show the WiFi signal strength, mode, SSID 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.

For 5GHz WiFi, the supports channel is from channel 36 to channel 165.



General Setup | Advanced Settings

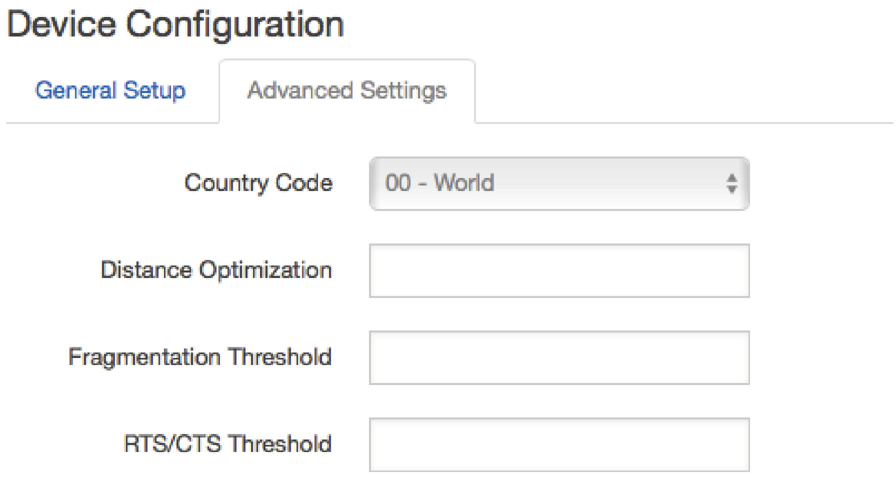
Status
65%
Mode: Master | **SSID:** SPEEDROUTE H820Q 5GHz
BSSID: 04:F0:21:1A:D8:35 | **Encryption:** WPA2 PSK (CCMP)
Channel: 36 (5.180 GHz) | **Tx-Power:** 23 dBm
Signal: -64 dBm | **Noise:** 0 dBm
Bitrate: 6.0 Mbit/s | **Country:** CN

Wi-Fi network is enabled: Disable

Operating frequency: Mode AC; Channel 36 (5180 MHz); Width 80 MHz

Transmit Power: 23 dBm (199 mW)

3.6.6.2 WiFi Advanced Configuration



Device Configuration

Country Code: 00 - World

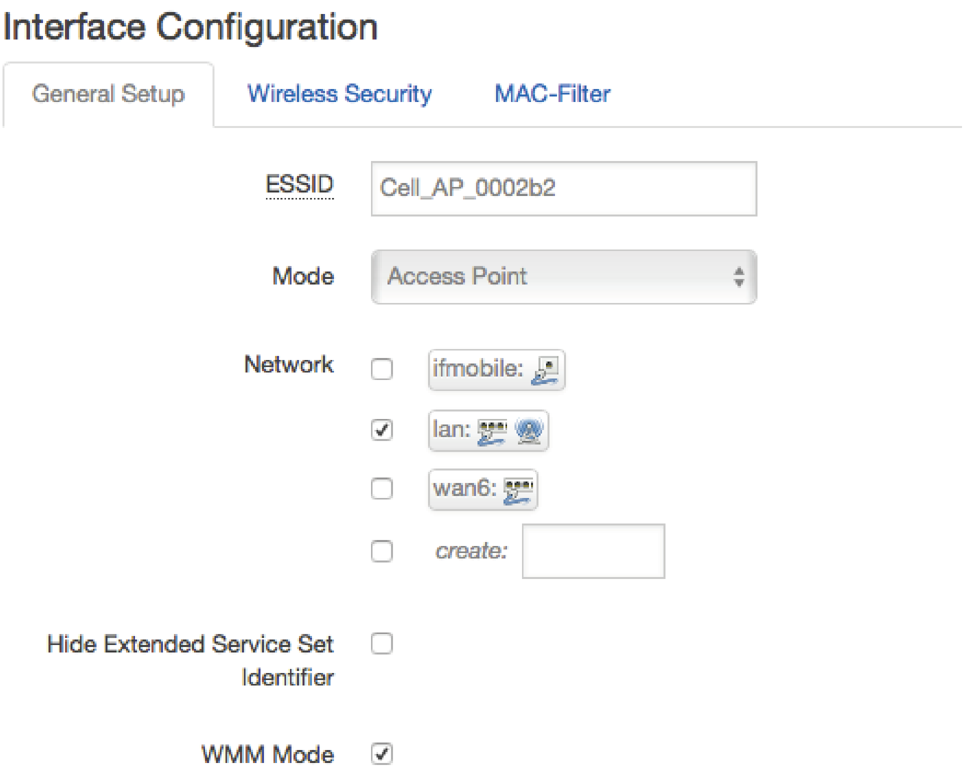
Distance Optimization

Fragmentation Threshold

RTS/CTS Threshold

- **Country Code:** Use ISO/IEC 3166 alpha2 country codes. Different country supports different WiFi channel. For example, United State support channel 1 to channel 11, China supports channel 1 to channel 13.
- **Distance Optimization:** Distance to farthest network member in meters**.**
- **Fragmentation Threshold:**
- **RTS/CTS Threshold:**

3.6.6.3 WiFi Interface Configuration



Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID: Cell_AP_0002b2

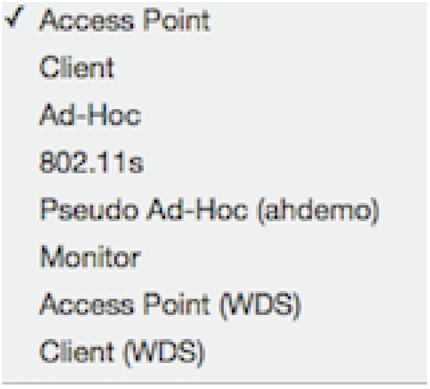
Mode: Access Point

Network:
☐ ifmobile:
☑ lan:
☐ wan6:
☐ *create:*

Hide Extended Service Set Identifier: ☐

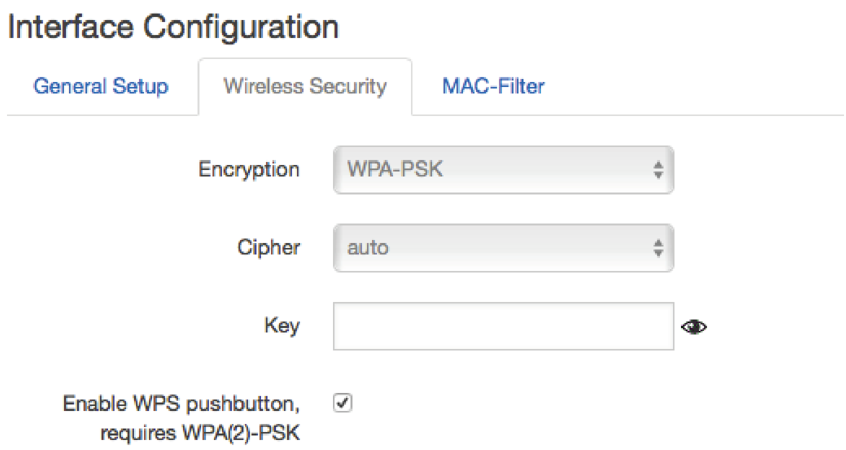
WMM Mode: ☑

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



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

- **Network**: Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
- **Hide Extended Service Set Identifier:** hide SSID means this WiFi cannot be scanned by others.
- **WMM Mode:**



Interface Configuration

General Setup | Wireless Security | MAC-Filter

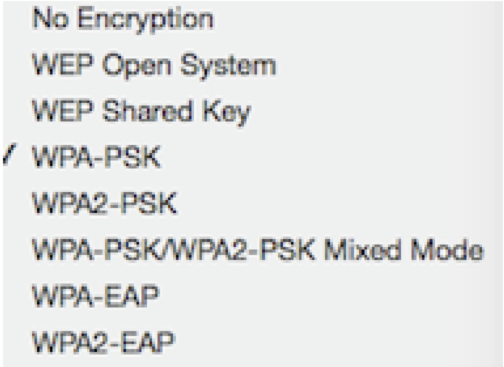
Encryption: WPA-PSK

Cipher: auto

Key:

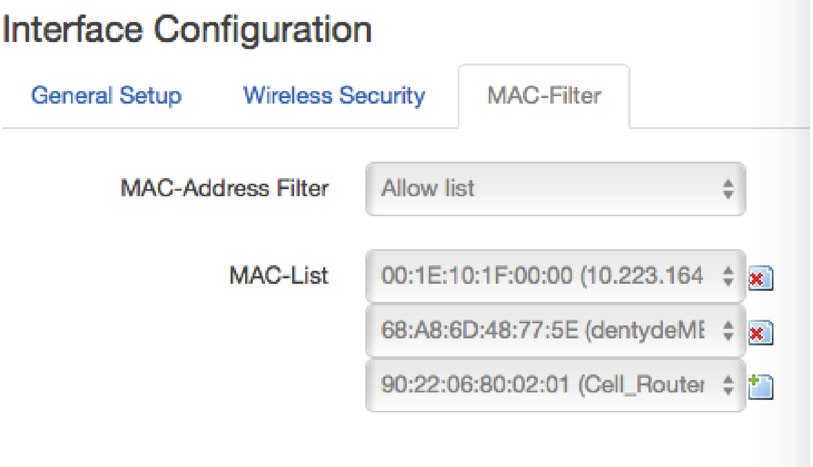
Enable WPS pushbutton, requires WPA(2)-PSK ☑

- **Encryption:**



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

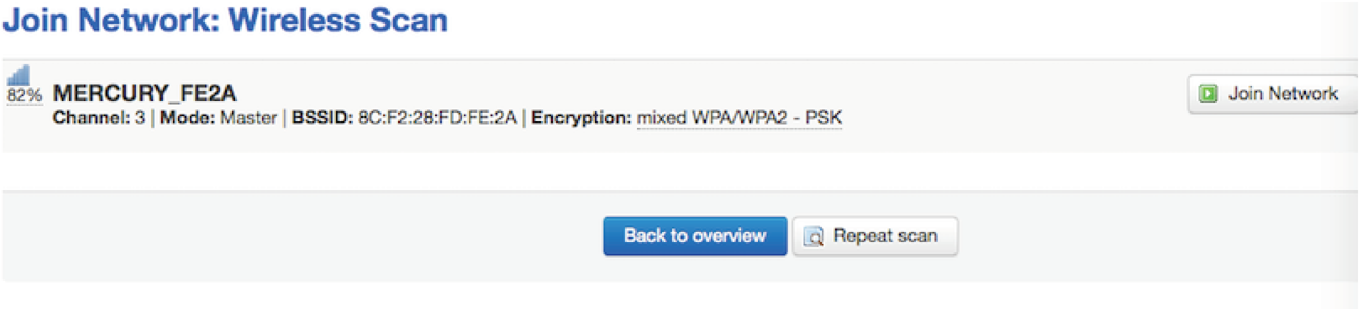
MAC-Address Filter: Allow list

MAC-List: 00:1E:10:1F:00:00 (10.223.164 ☒
68:A8:6D:48:77:5E (dentydeMI ☒
90:22:06:80:02:01 (Cell_Router +

- **MAC-Address Filter**: MAC address access policy. Disabled: disable MAC-address filter functionality. Allow list: only the MAC address in the list is 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

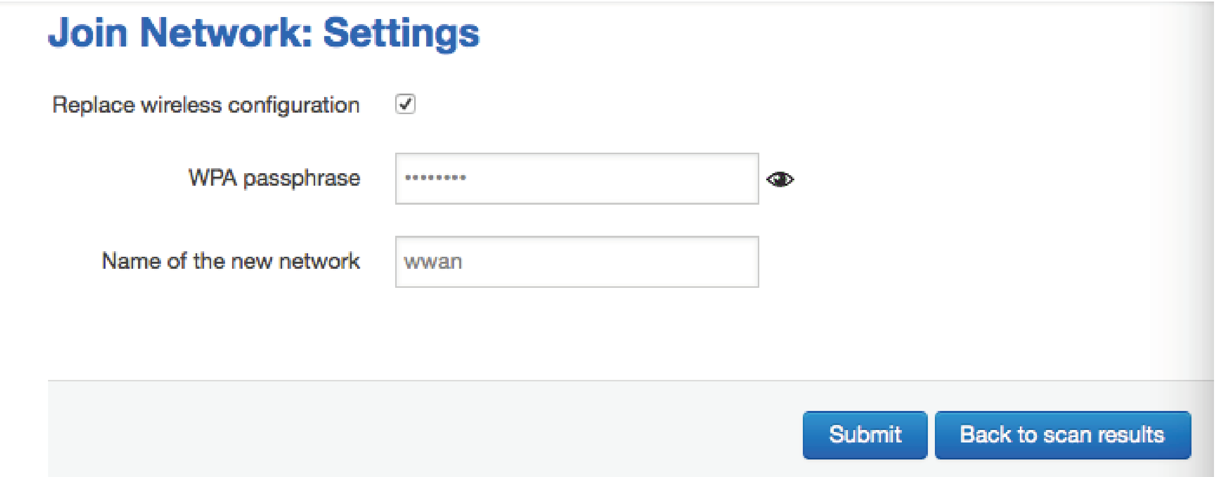
- **Step 1)** click button "AP Client" on wireless overview page, then system start to scan all WiFi signals.



Join Network: Wireless Scan

82% MERCURY_FE2A
Channel: 3 | Mode: Master | BSSID: 8C:F2:28:FD:FE:2A | Encryption: mixed WPA/WPA2 - PSK

- **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.



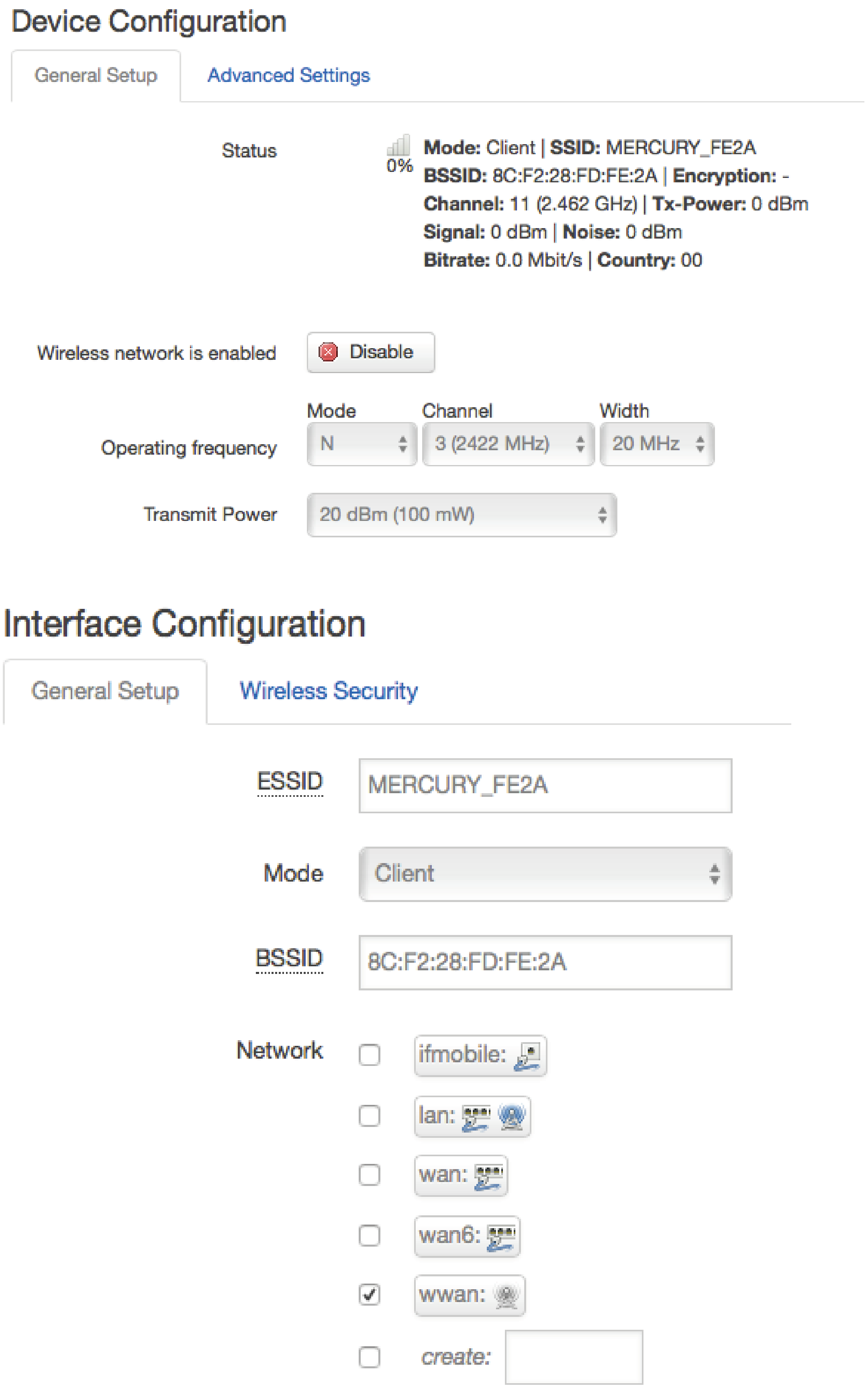
Join Network: Settings

Replace wireless configuration ☑

WPA passphrase ••••••••

Name of the new network wwan

- **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

Status 0% **Mode:** Client | **SSID:** MERCURY_FE2A
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** -
Channel: 11 (2.462 GHz) | **Tx-Power:** 0 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled: Disable

Operating frequency: Mode: N; Channel: 3 (2422 MHz); Width: 20 MHz

Transmit Power: 20 dBm (100 mW)

Interface Configuration

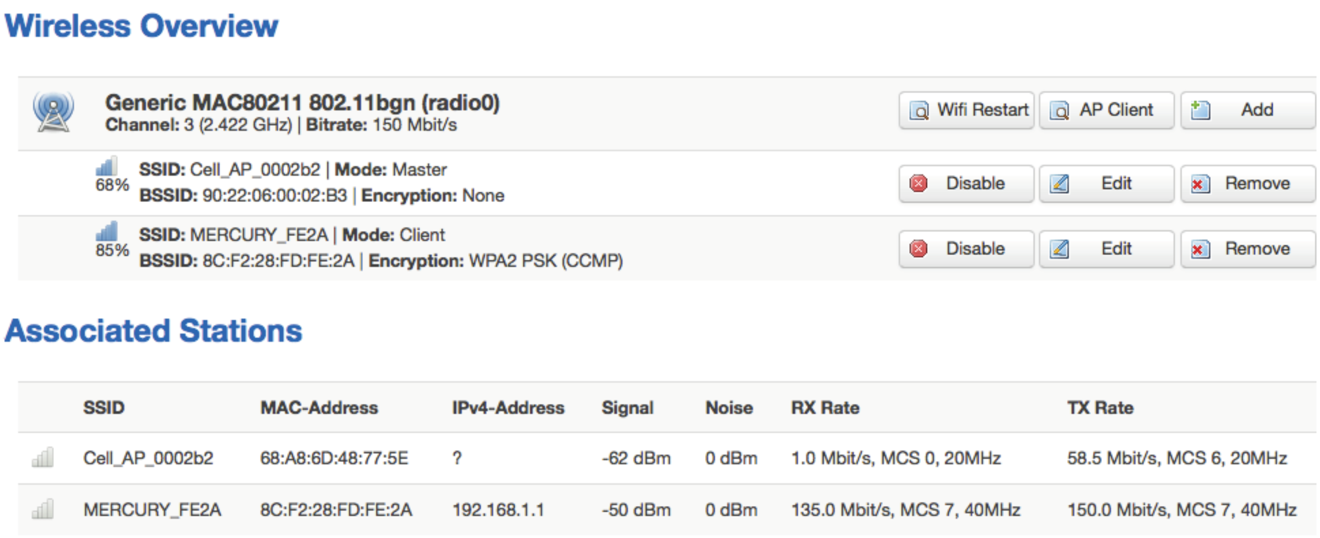
ESSID: MERCURY_FE2A

Mode: Client

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

Network:
□ ifmobile:
□ lan:
□ wan:
□ wan6:
☑ wwan:
□ *create:*

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



Wireless Overview

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

68% **SSID:** Cell_AP_0002b2 | **Mode:** Master
BSSID: 90:22:06:00:02:B3 | **Encryption:** None

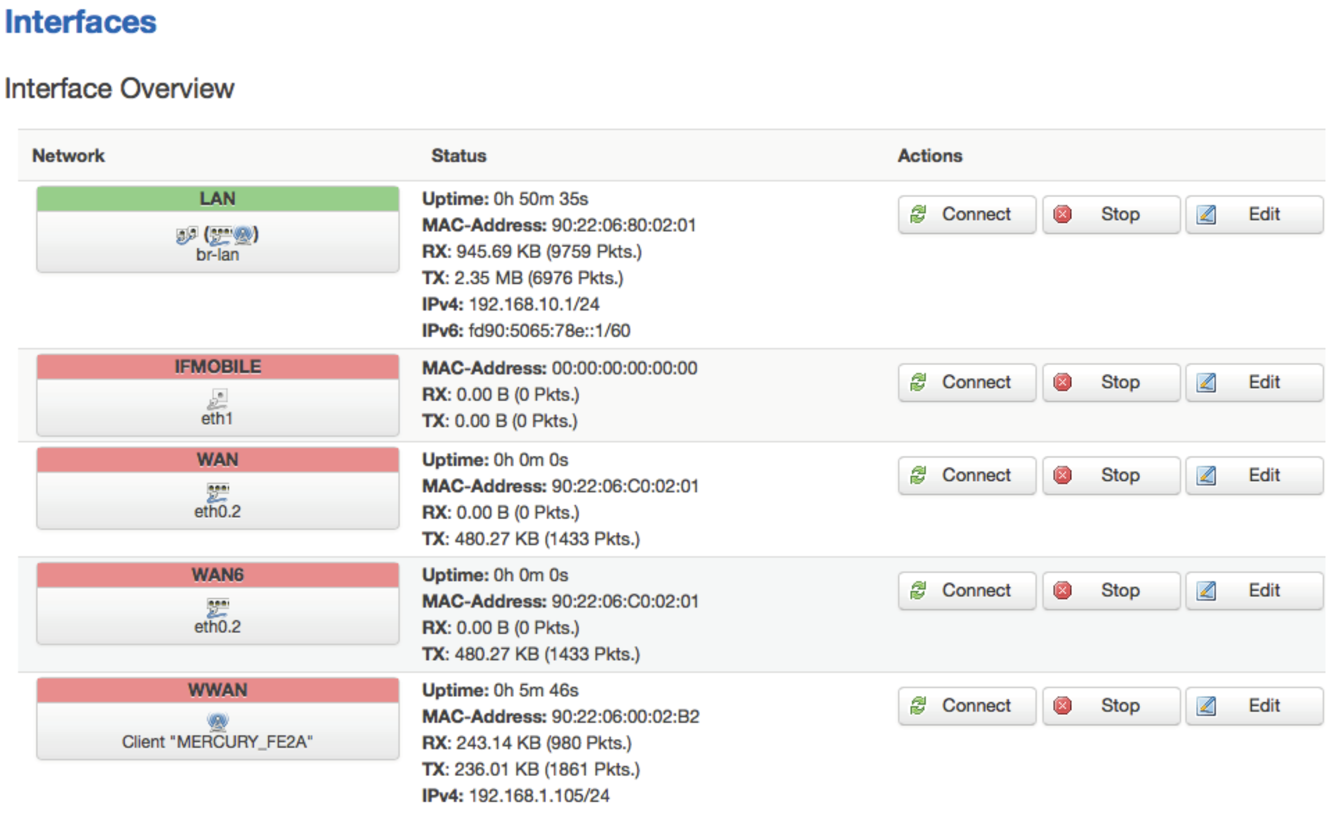
85% **SSID:** MERCURY_FE2A | **Mode:** Client
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** WPA2 PSK (CCMP)

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.



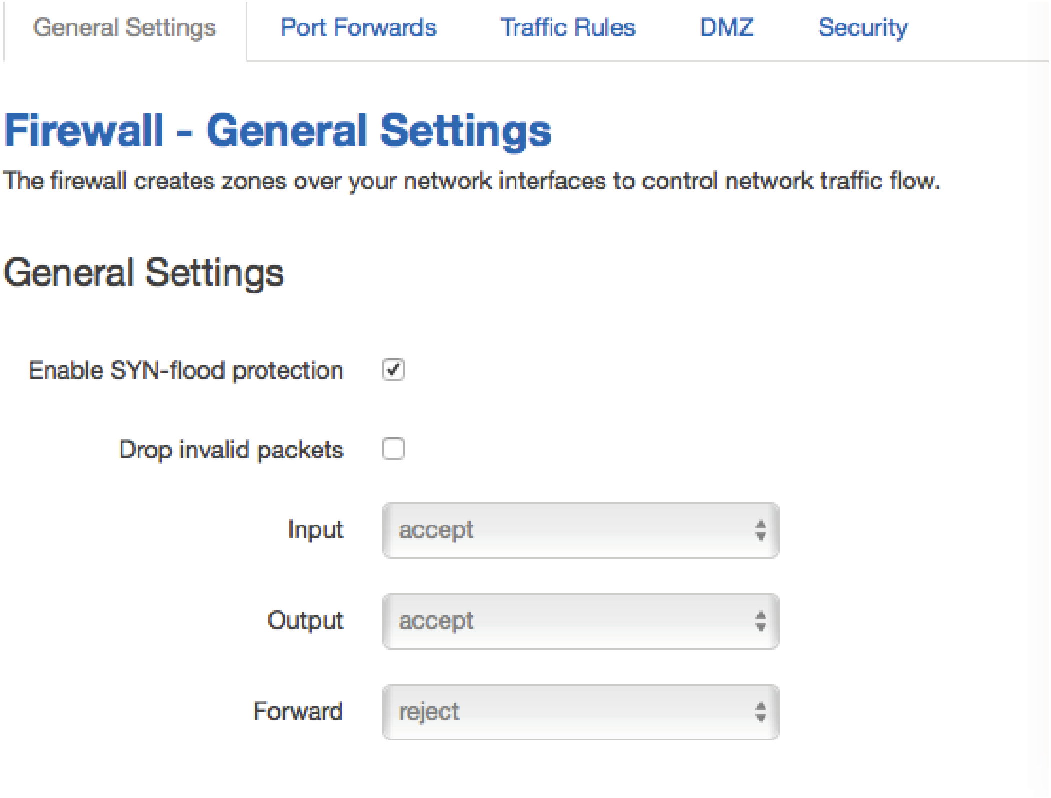
Interfaces

Interface Overview

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

3.6.8 Firewall

3.6.8.1 General Settings



Firewall - General Settings

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

General Settings

Enable SYN-flood protection ☑

Drop invalid packets □

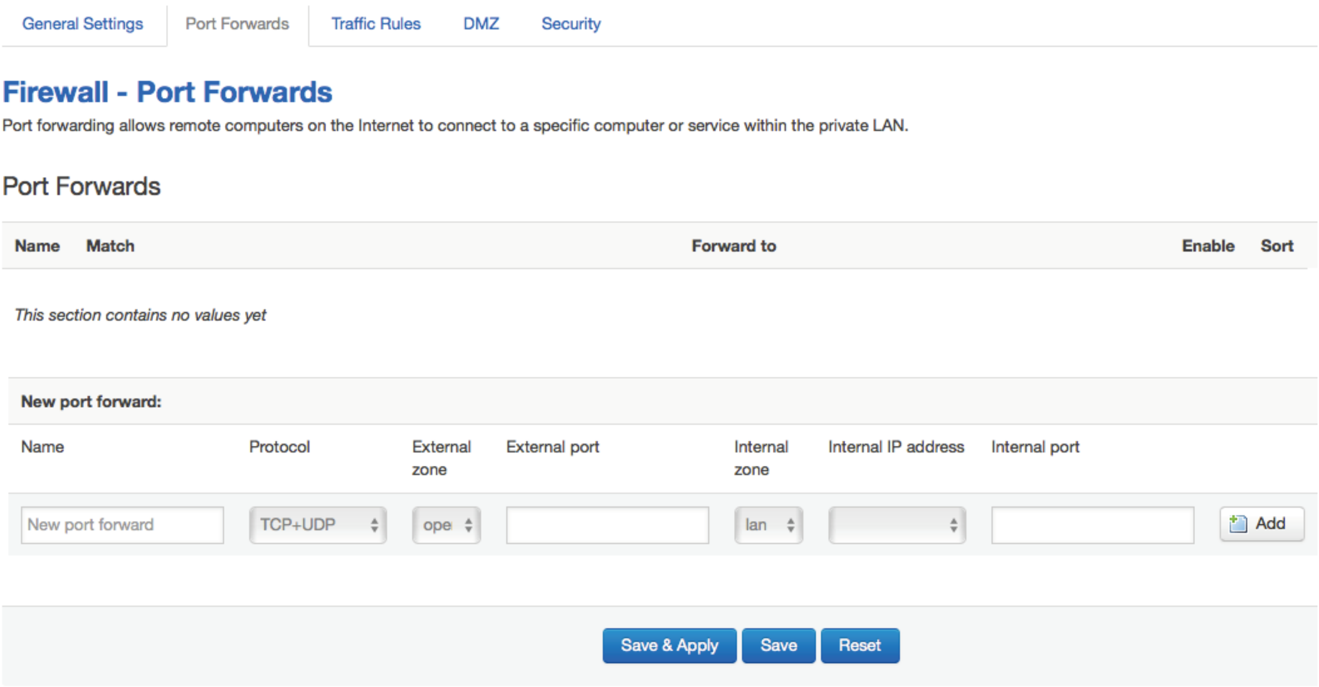
Input: accept

Output: accept

Forward: reject

3.6.8.2 Port Forwards

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



Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort

This section contains no values yet

New port forward:

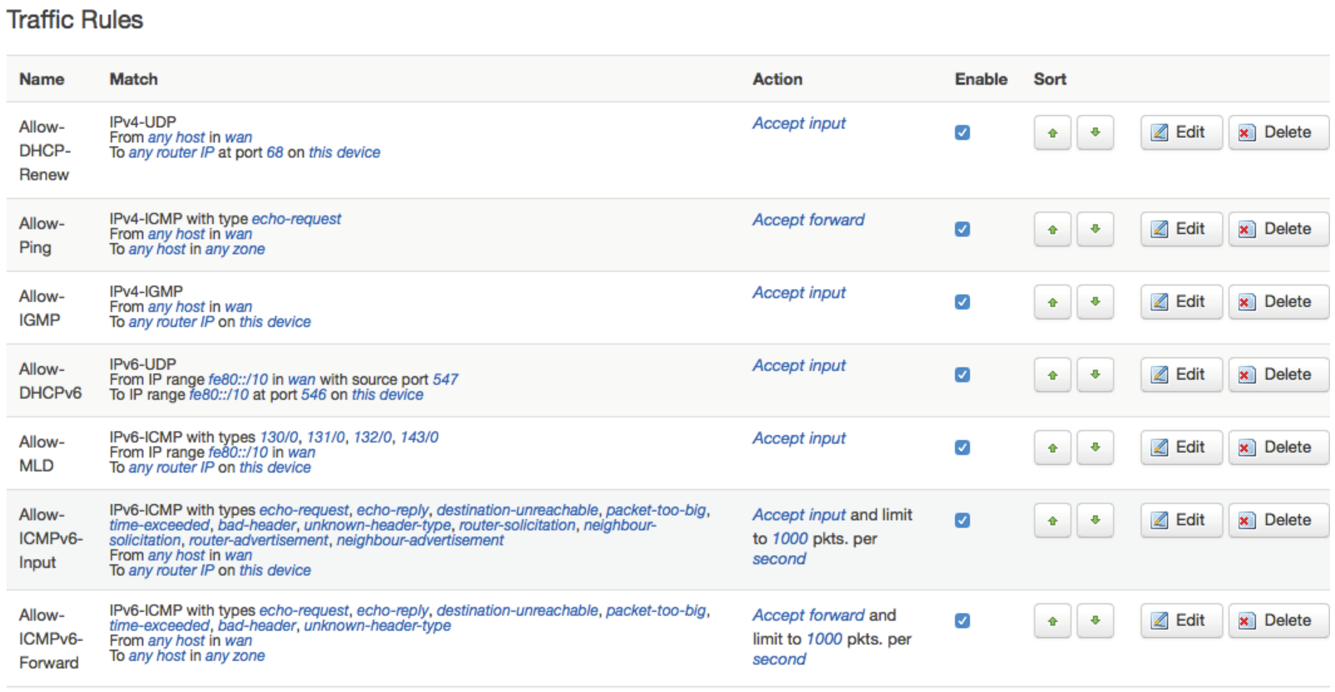
Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
New port forward	TCP+UDP	ope		lan			Add

- **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.

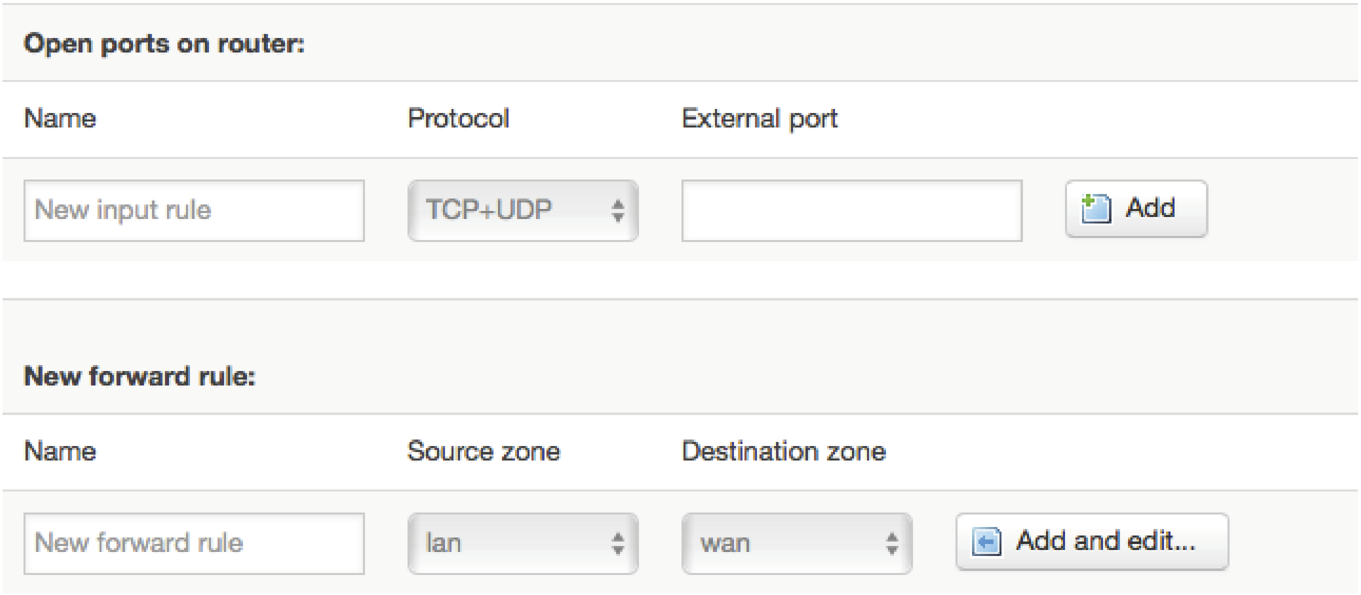
Traffic rules list:



Traffic Rules

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

Open ports on router and create new forward rules:



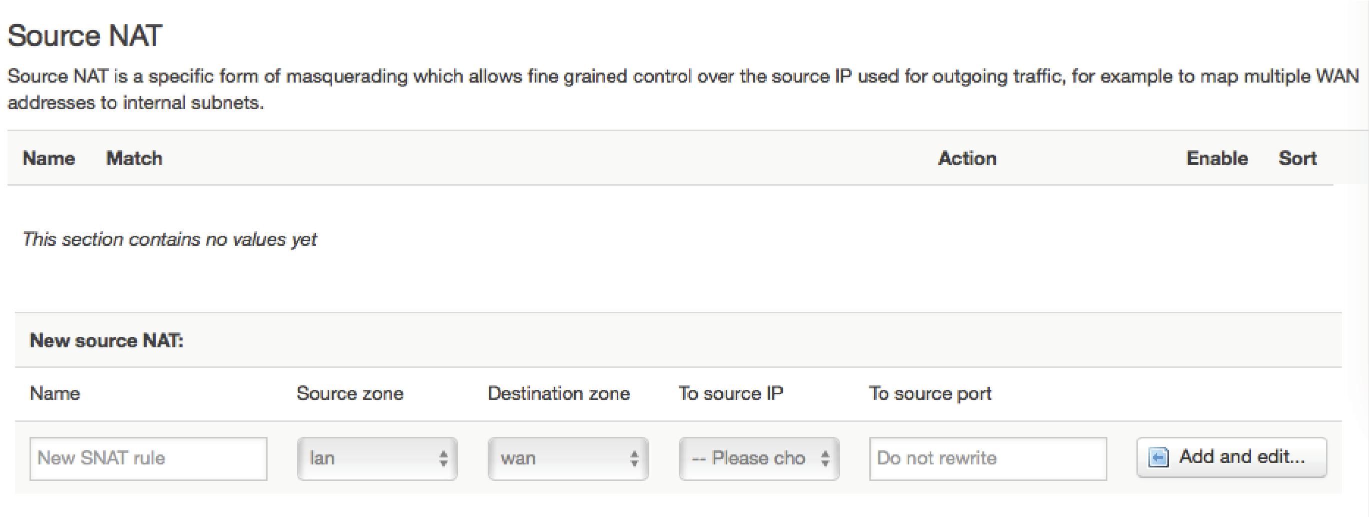
Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

Source NAT list and create source NAT rule:



Source NAT

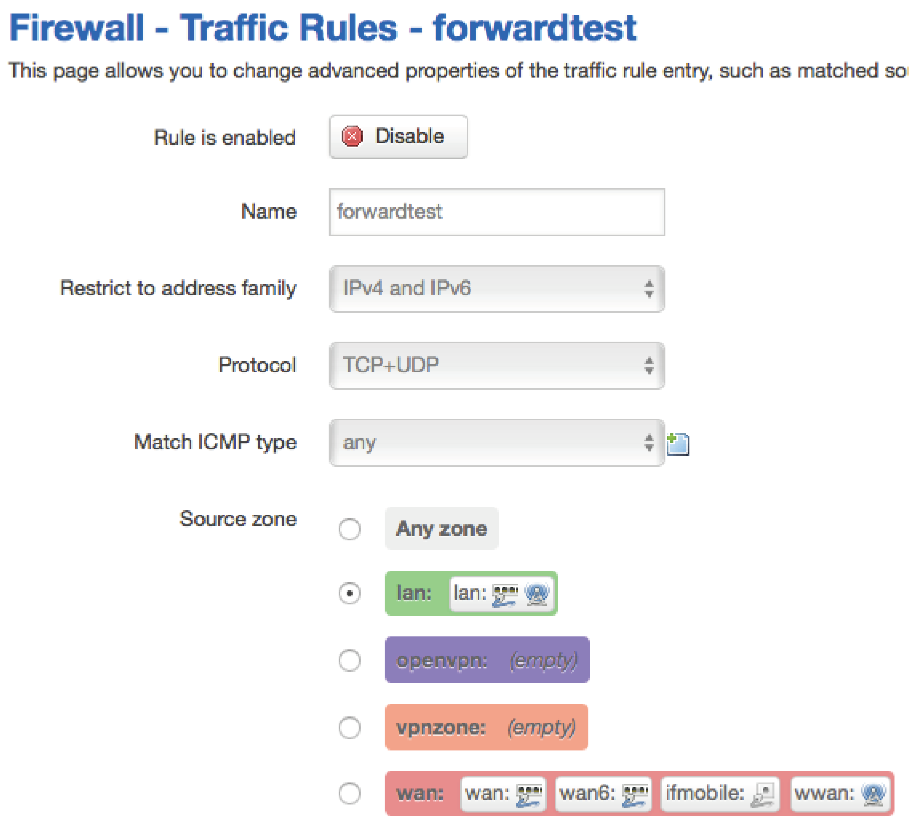
Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	lan	wan	-- Please cho	Do not rewrite	Add and edit...

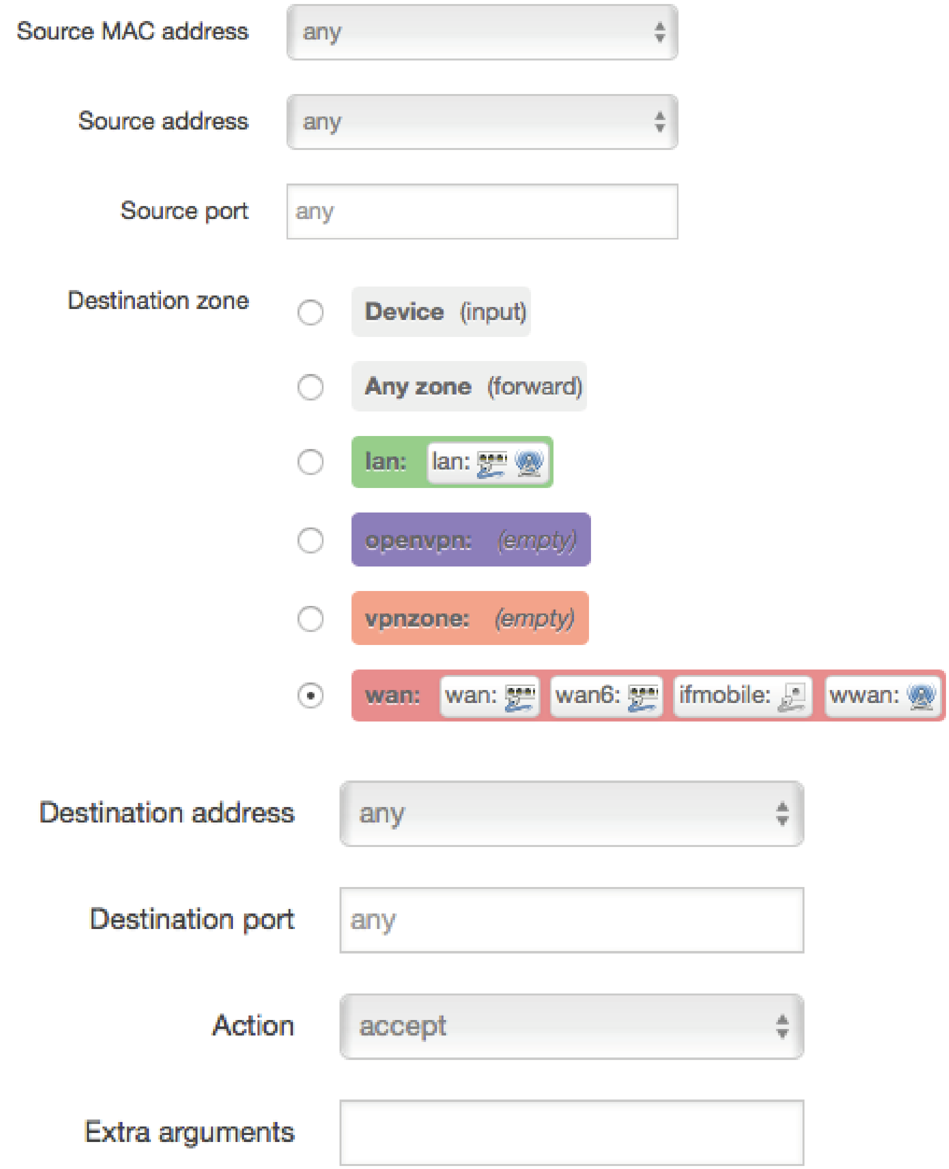
Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.



Firewall - Traffic Rules - forwardtest

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

Rule is enabled	Disable
Name	forwardtest
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ● lan: lan: ○ openvpn: *(empty)* ○ vpnzone: *(empty)* ○ wan: wan: wan6: ifmobile: wwan:



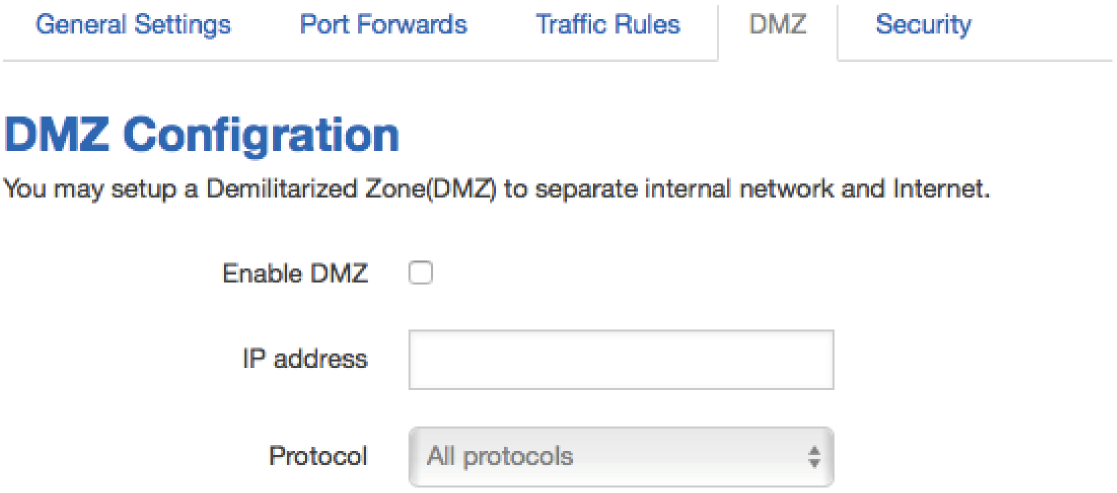
Source MAC address	any
Source address	any
Source port	any
Destination zone	○ Device (input) ○ Any zone (forward) ○ lan: lan: ○ openvpn: (empty) ○ vpnzone: (empty) ● wan: wan: wan6: ifmobile: wwan:
Destination address	any
Destination port	any
Action	accept
Extra arguments	

- **Name**: traffic rule entry name
- **Restrict to address family**: IPv4+IPv6, IPv4 and IPv6 can be selected. 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



DMZ Configration

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

Enable DMZ □

IP address

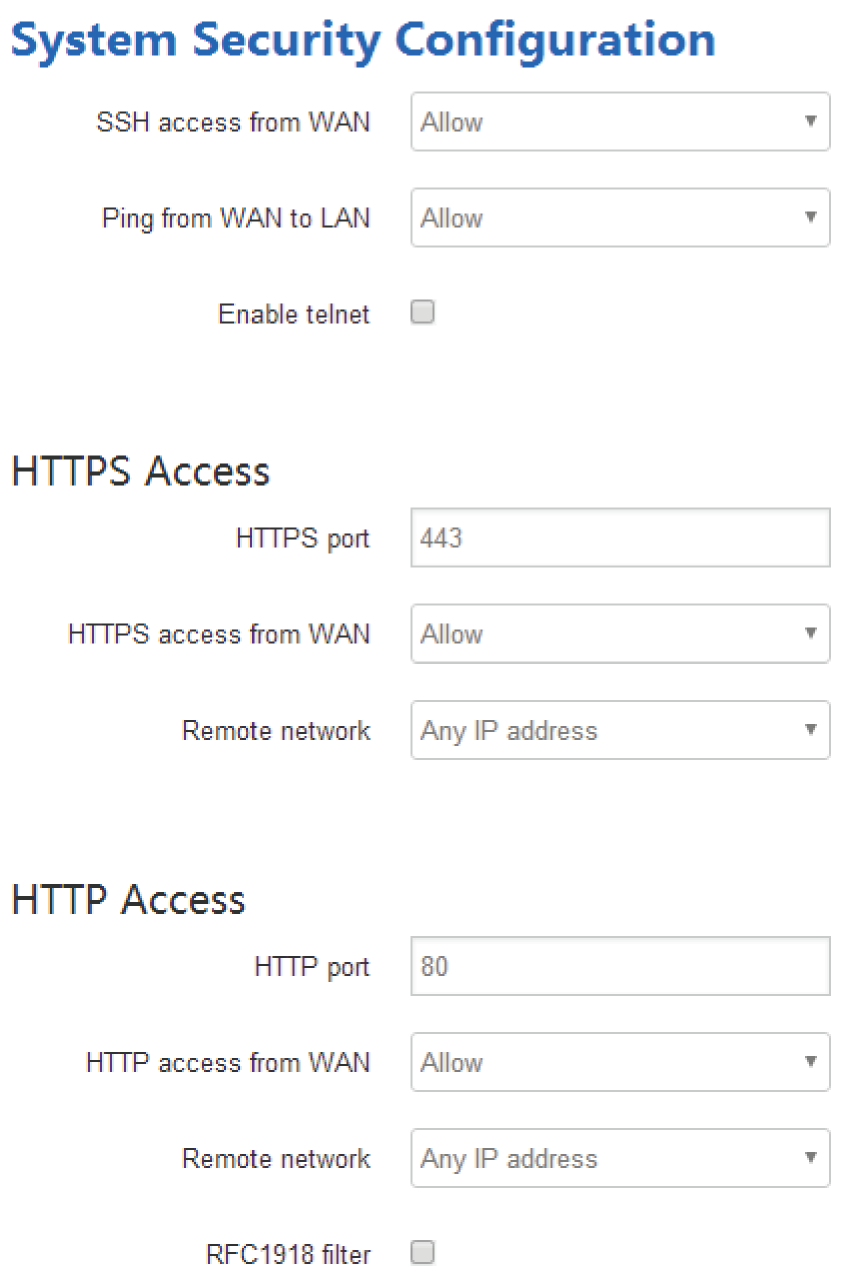
Protocol: All protocols

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

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

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

3.6.8.5 Security



System Security Configuration

SSH access from WAN: Allow

Ping from WAN to LAN: Allow

Enable telnet: □

HTTPS Access

HTTPS port: 443

HTTPS access from WAN: Allow

Remote network: Any IP address

HTTP Access

HTTP port: 80

HTTP access from WAN: Allow

Remote network: Any IP address

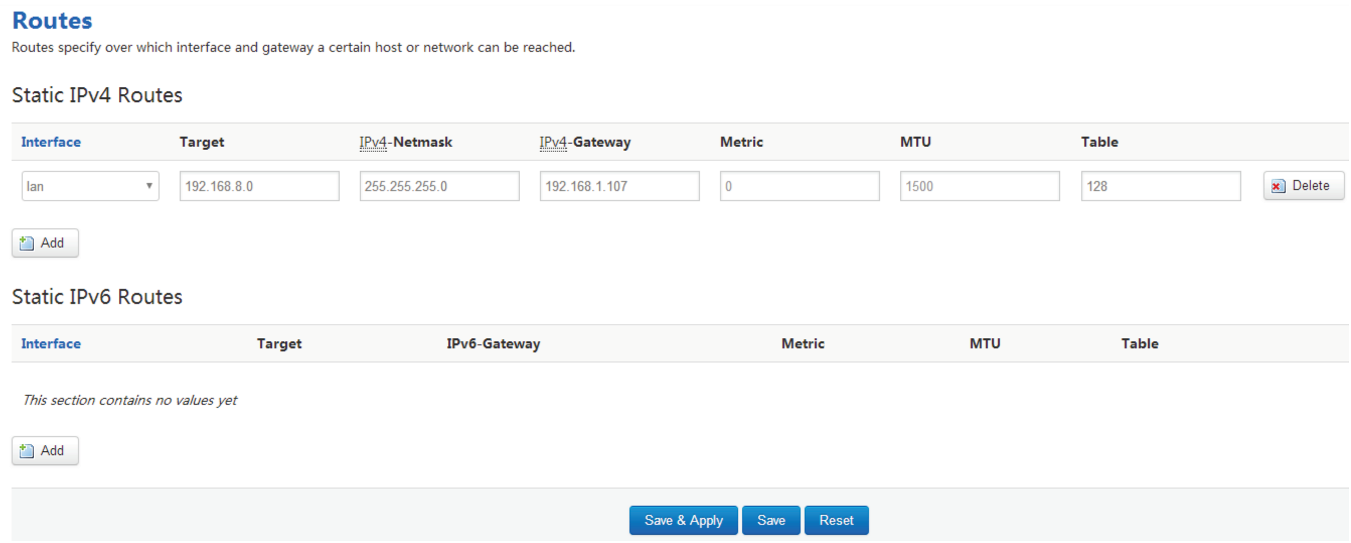
RFC1918 filter: □

- **SSH access from WAN**: allow or deny users access H820Q/H820Q router from remote side.
- **Ping from WAN to LAN**: allow or deny ping from remote side to internal LAN subnet.
- **Enable telnet**: enable telnet connect. The default setting is disabled for security.
- **HTTPS port**: set HTTPS port, the default port is 443.
- **HTTPS access from WAN**: allow or deny access router web management page from remote side.
- **Remote network**: Any IP Address, Single IP address, Subnet.
- **IP address**: fill a remote IP address that can access router web management page.
- **Netmask**: 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the illegal value is

from 1 to 32.

- **HTTP port**: set HTTP port, the default port is 80.
- **HTTP 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.
- **RFC1918 filter**: reject requests from RFC1918 IPs to public server IPs

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	Table	
lan	192.168.8.0	255.255.255.0	192.168.1.107	0	1500	128	Delete

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	Table

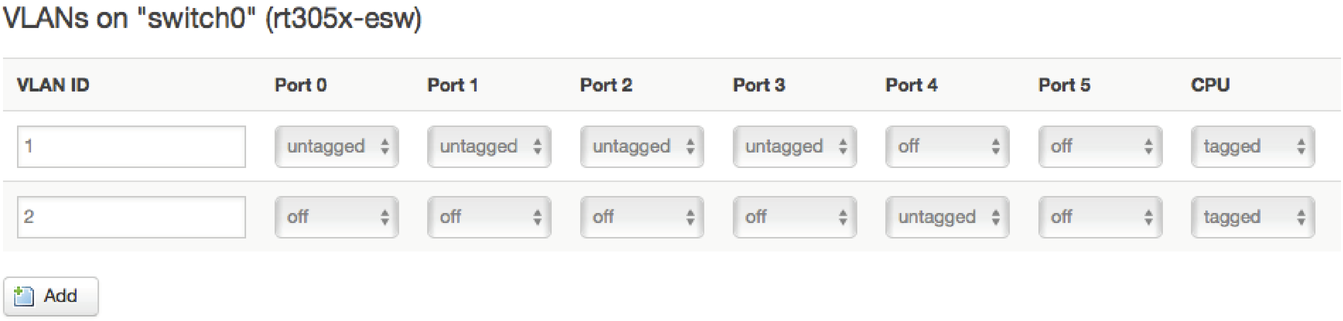
This section contains no values yet

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

  Notice:

  - 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



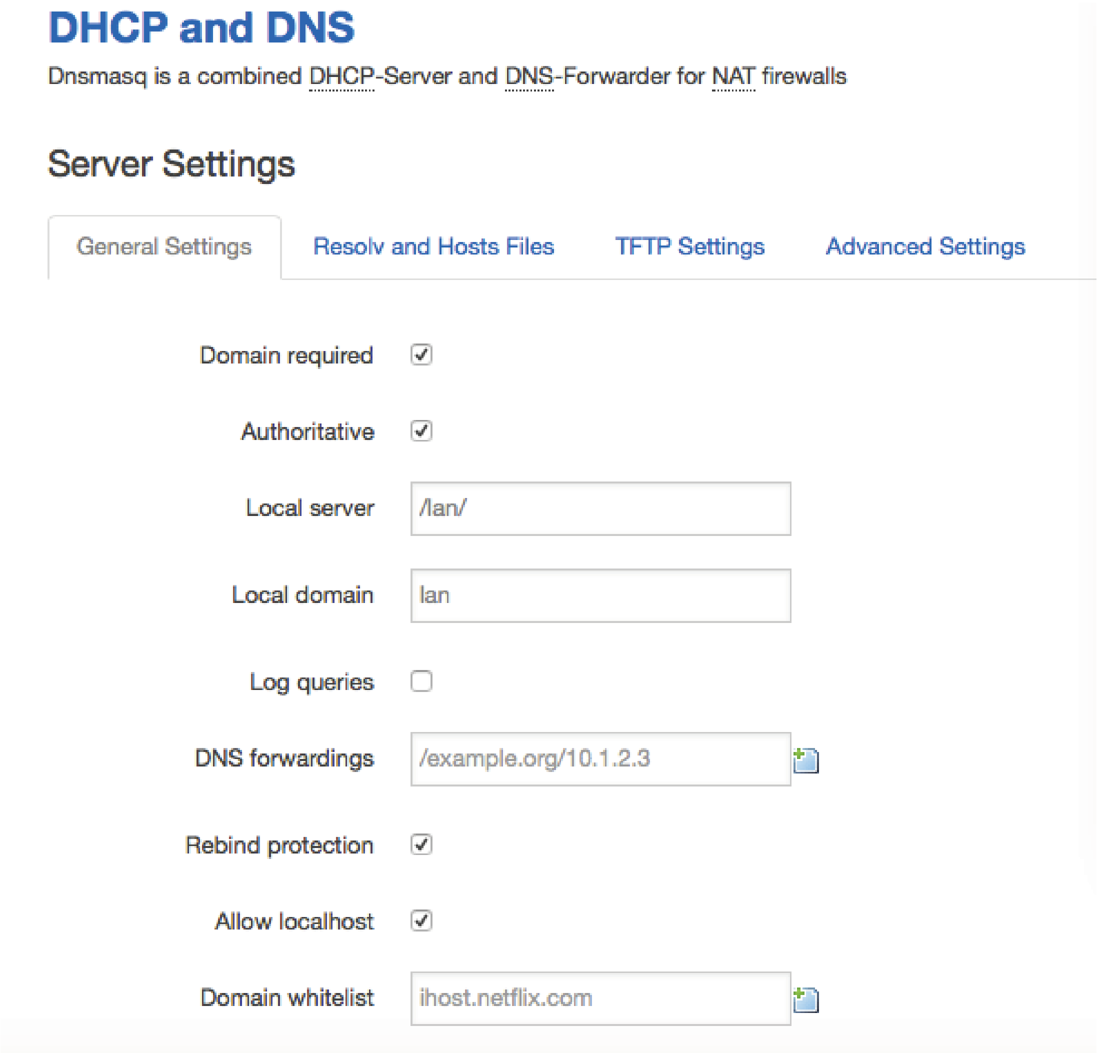
VLANs on "switch0" (rt305x-esw)

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

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

Domain required ☑

Authoritative ☑

Local server /lan/

Local domain lan

Log queries □

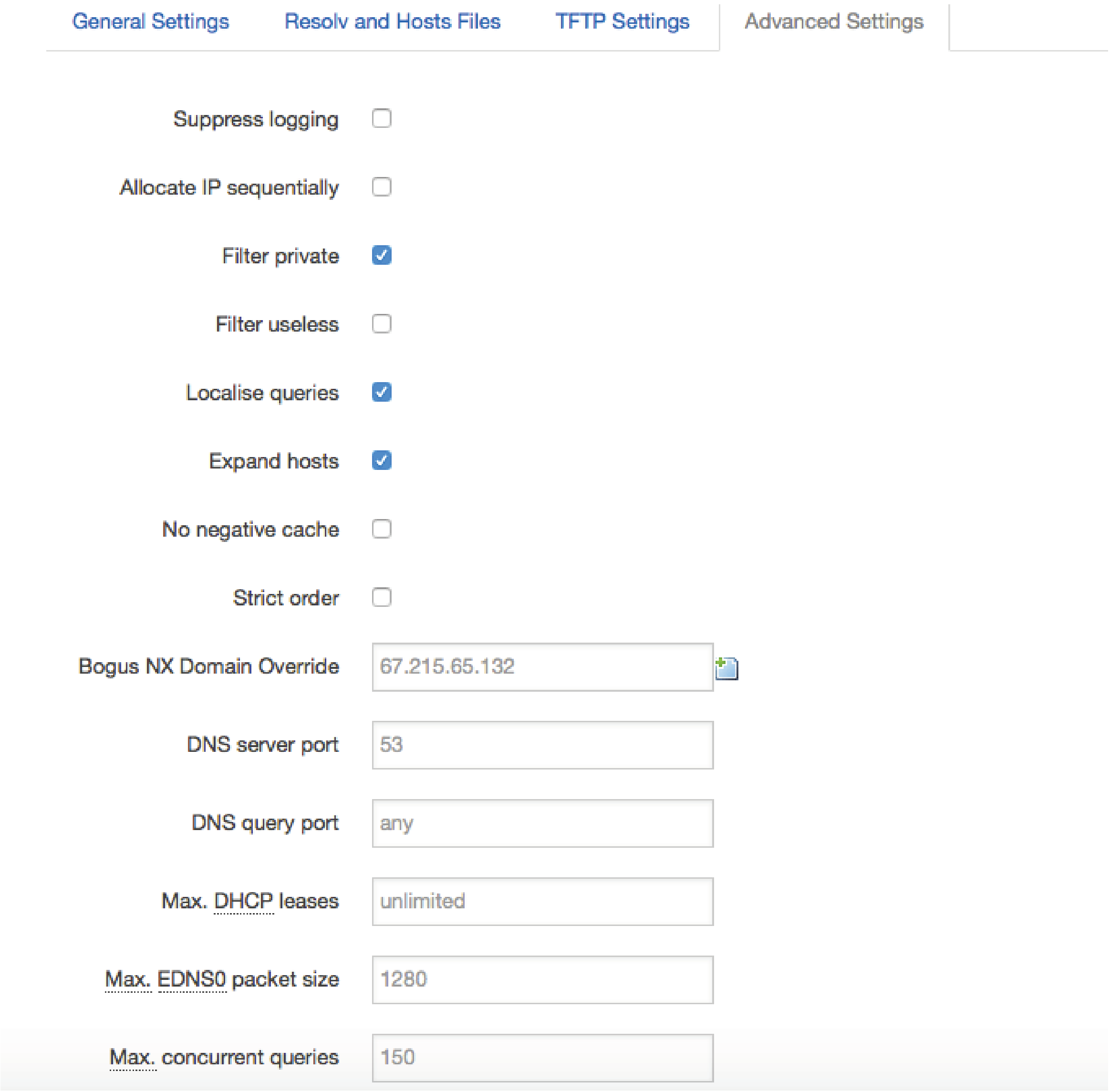
DNS forwardings /example.org/10.1.2.3

Rebind protection ☑

Allow localhost ☑

Domain whitelist ihost.netflix.com

- **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: 67.215.65.132

DNS server port: 53

DNS query port: any

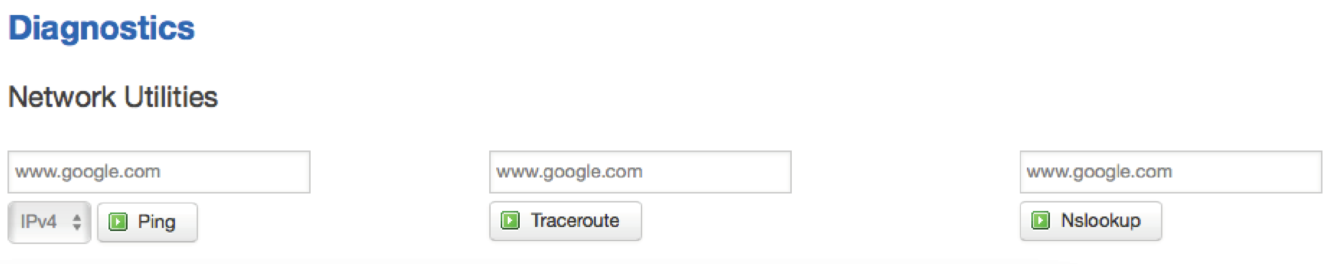
Max. DHCP leases: unlimited

Max. EDNS0 packet size: 1280

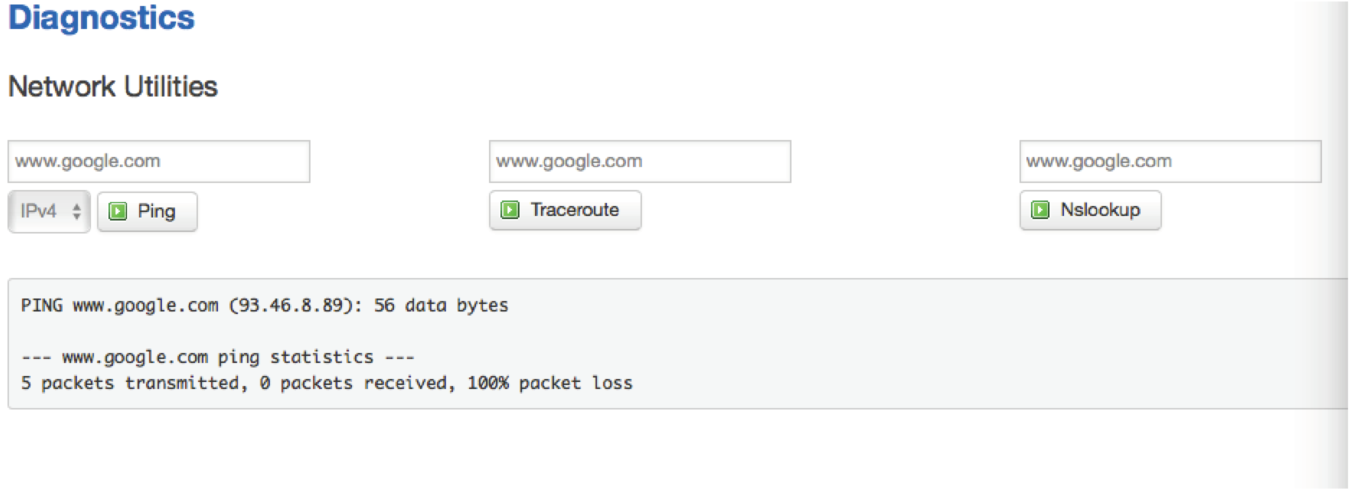
Max. concurrent queries: 150

- **Suppress logging**: Suppress logging of the routine operation of these protocols
- **Allocate IP sequentially**: Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private**: Do not forward reverse lookups for local networks.
- **Filter useless**: Do not forward requests that cannot be answered by public name servers.
- **Localize queries**: Localize 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 resolve file.
- **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



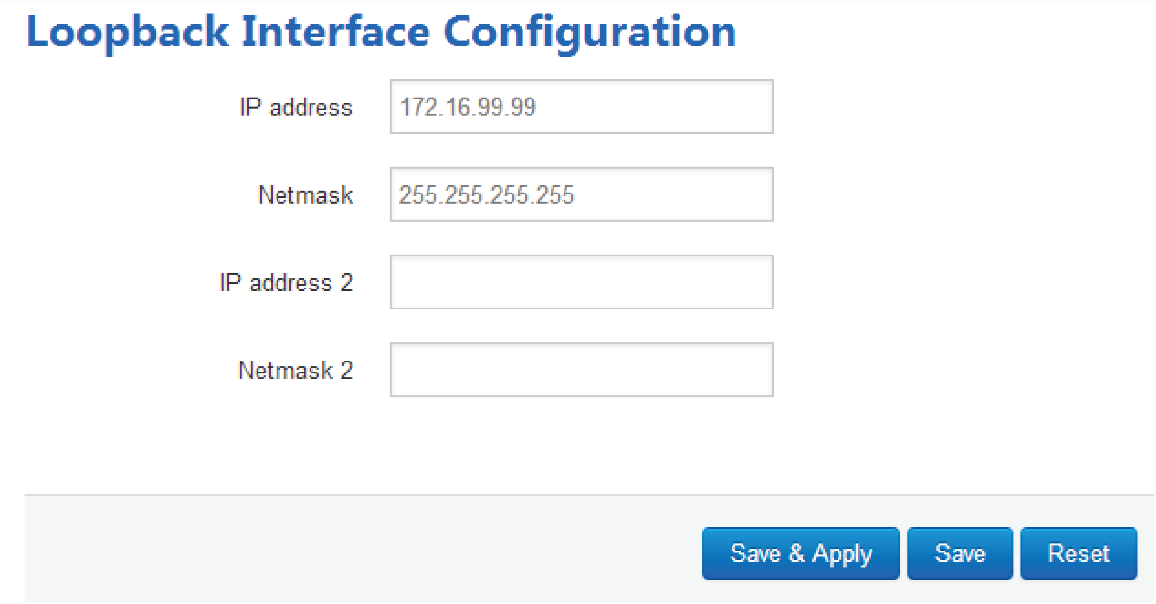
- **Ping** : it is a tool that used to test the reachability of a host on an Internet Protocol (IP) network.
- **Traceroute**: it is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- **Nslookup**: it is a network 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.



```
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: 172.16.99.99

Netmask: 255.255.255.255

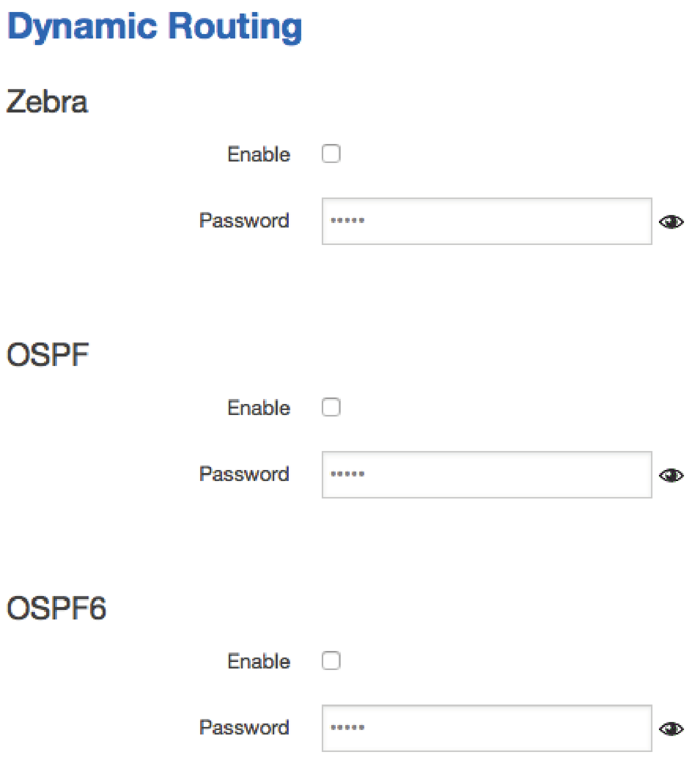
IP address 2:

Netmask 2:

The default Loopback interface has IP address 127.0.0.1, the final user can change it here. The first IP address can be used in IPSec. The secondary can be used as management.

3.6.14 Dynamic Routing

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



Dynamic Routing

Zebra

Enable □

Password ••••• 👁

OSPF

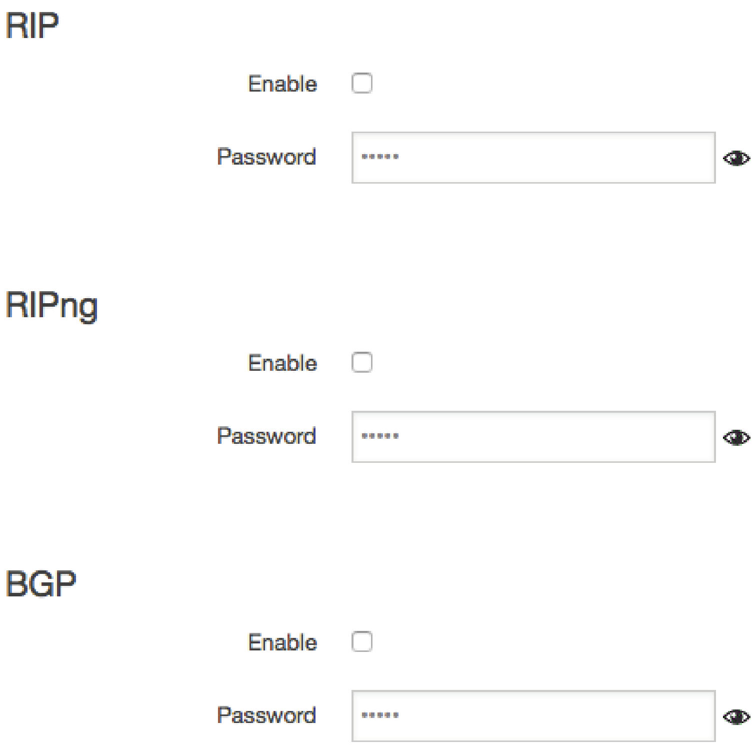
Enable □

Password ••••• 👁

OSPF6

Enable □

Password ••••• 👁



RIP

Enable □

Password ••••• 👁

RIPng

Enable □

Password ••••• 👁

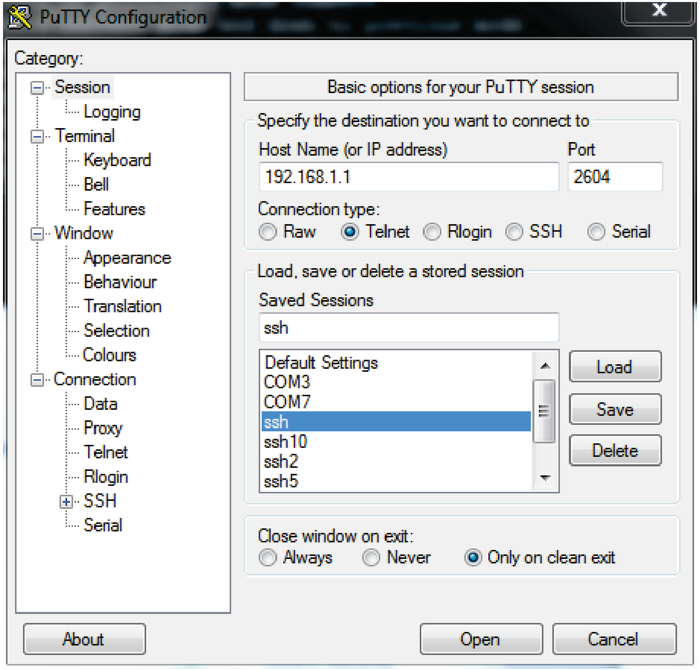
BGP

Enable □

Password ••••• 👁

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

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:



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1
Port: 2604

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

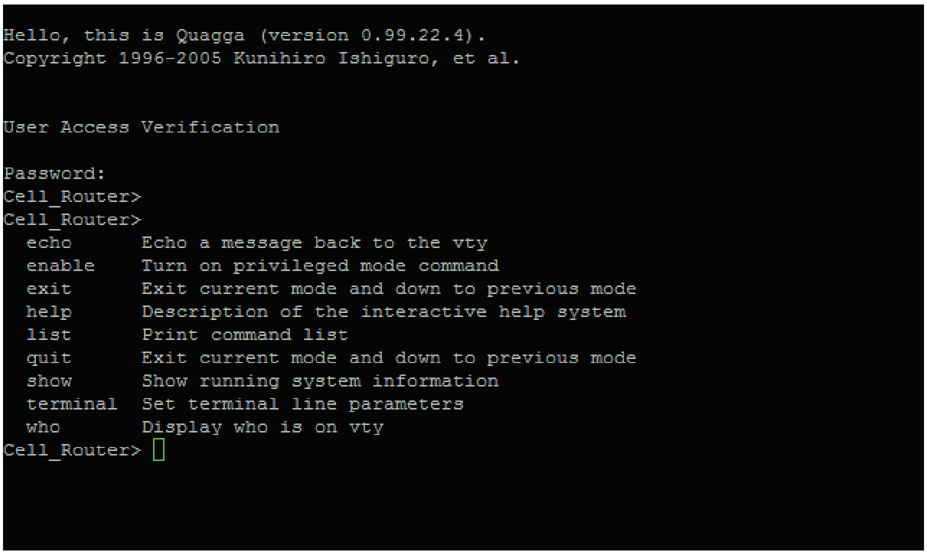
Load, save or delete a stored session

Saved Sessions: ssh

Default Settings
COM3
COM7
ssh
ssh10
ssh2
ssh5

Close window on exit: ○ Always ○ Never ● Only on clean exit

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



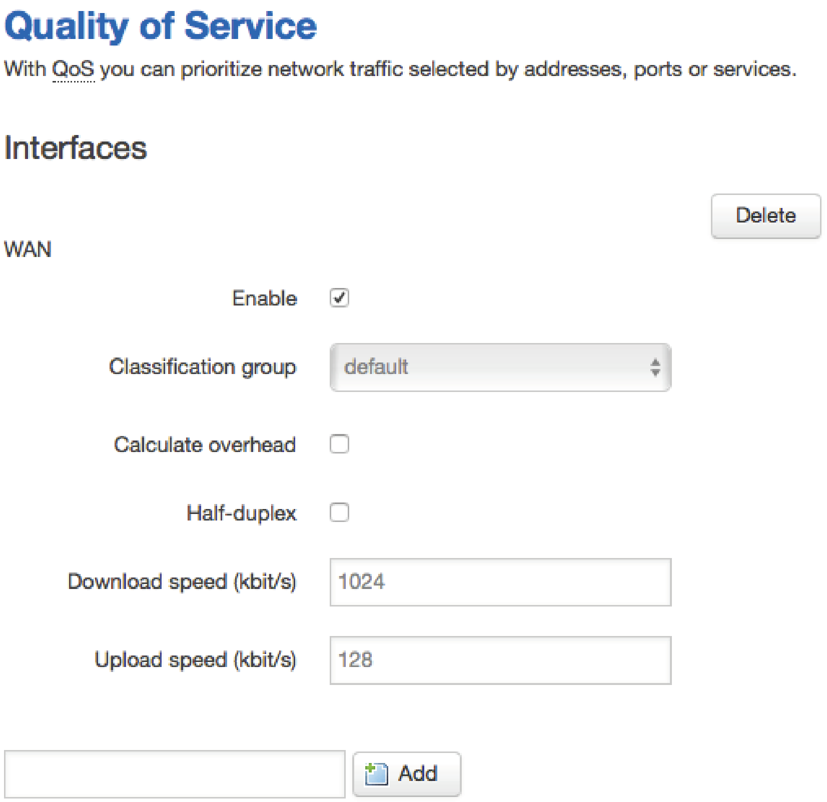
```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


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

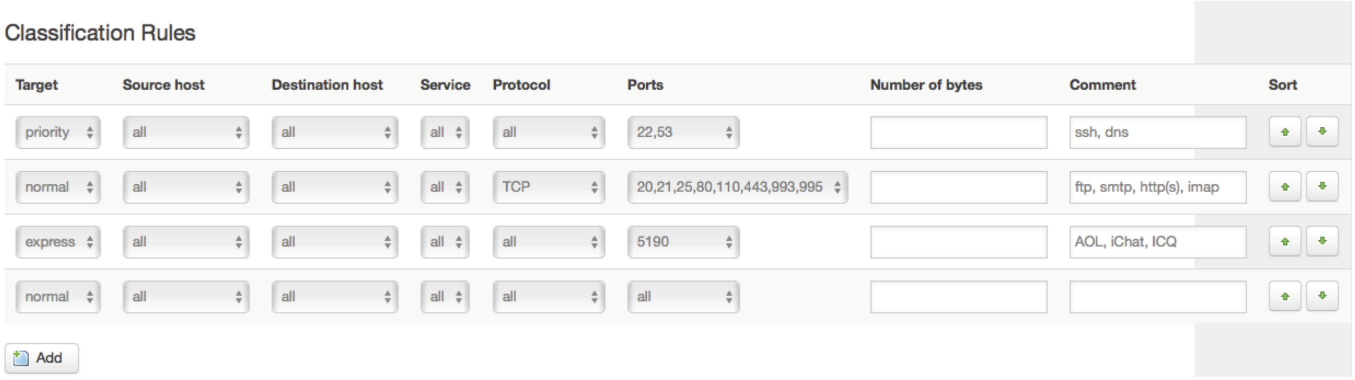
With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

WAN

Enable	☑
Classification group	default
Calculate overhead	□
Half-duplex	□
Download speed (kbit/s)	1024
Upload speed (kbit/s)	128

- **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	
normal	all	all	all	TCP	20,21,25,80,110,443,993,995		ftp, smtp, http(s), imap	
express	all	all	all	all	5190		AOL, iChat, ICQ	
normal	all	all	all	all	all			

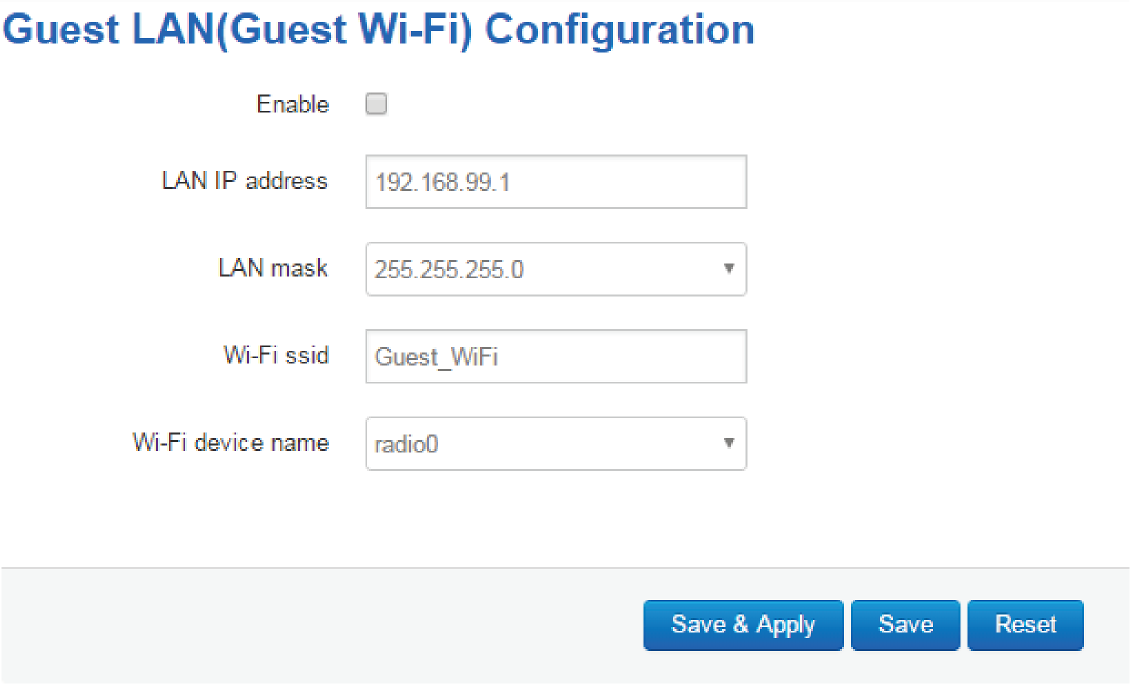
Each classify section defines one group of packets and which target (i.e. bucket) this group belongs to. All the packets share the bucket specified.

- **Target**: The four defaults are: priority, express, normal, low.
- **Source host**: Packets matching this source host(s) (single IP or in CIDR notation) belong to the bucket defined in target.
- **Destination host**: Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in target.
- **Protocol**: Packets matching this protocol belong to the bucket defined in target.

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

3.6.16 Guest LAN(Guest WiFi)

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



Guest LAN(Guest Wi-Fi) Configuration

Enable ☐

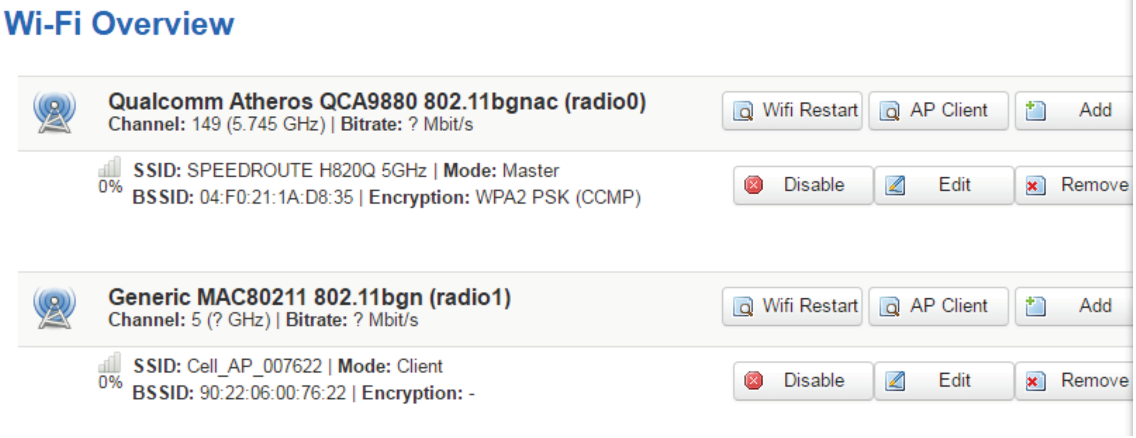
LAN IP address 192.168.99.1

LAN mask 255.255.255.0

Wi-Fi ssid Guest_WiFi

Wi-Fi device name radio0

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



Wi-Fi Overview

Qualcomm Atheros QCA9880 802.11bgnac (radio0)
Channel: 149 (5.745 GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** SPEEDROUTE H820Q 5GHz | **Mode:** Master
BSSID: 04:F0:21:1A:D8:35 | **Encryption:** WPA2 PSK (CCMP)

Generic MAC80211 802.11bgn (radio1)
Channel: 5 (? GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** Cell_AP_007622 | **Mode:** Client
BSSID: 90:22:06:00:76:22 | **Encryption:** -