Industrial Grade 2G 3G 4G Cellular Router

User Manual

H820 Series

E-Lins Technology Co., Limited

PHONE: +86-755-29230581  83700465

Email: sales@e-lins.com


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

1 Preparation job before configuration .................................................................. 4
   1.1 Learn your router version and feature ...................................................... 4
   1.2 Prepare SIM Card and working condition .............................................. 6
   1.3 Highly recommendation for the configuration ...................................... 6

2 Hardware Installation ......................................................................................... 7
   2.1 Overall Dimension ................................................................................ 8
   2.2 The Ports .................................................................................................. 9
   2.3 Installment ............................................................................................... 9
   2.4 SIM/UIM card installed ......................................................................... 9
   2.5 The installation of terminal blocks ....................................................... 11
   2.6 Grounding ................................................................................................ 11
   2.7 Power Supply .......................................................................................... 11
   2.8 LED and Check Network Status ............................................................ 11

3 Software configuration ....................................................................................... 13
   3.1 Overview .................................................................................................. 13
   3.2 How to log into the Router ..................................................................... 13
   3.3 Router status .......................................................................................... 17
       3.3.1 Status overview ............................................................................. 17
       3.3.2 Network status ............................................................................. 17
       3.3.3 Firewall status ............................................................................. 20
       3.3.4 Routes ........................................................................................... 20
       3.3.5 System log .................................................................................... 21
       3.3.6 Kernel log ..................................................................................... 22
       3.3.7 Realtime graphs .......................................................................... 23
   3.4 System Configuration .............................................................................. 24
       3.4.1 Setup wizard .................................................................................. 24
       3.4.2 System ............................................................................................ 26
       3.4.3 Password ........................................................................................ 27
       3.4.4 NTP ................................................................................................ 28
       3.4.5 Backup/Restore ................................................................. .................. 29
       3.4.6 Upgrade ......................................................................................... 29
       3.4.7 Reset .............................................................................................. 30
       3.4.8 Reboot ............................................................................................ 31
   3.5 Services configuration .............................................................................. 31
       3.5.1 ICMP check ................................................................................... 31
       3.5.2 VRRP .............................................................................................. 32
       3.5.3 Failover (link backup) .................................................................... 33
       3.5.4 DTU ................................................................................................ 34
       3.5.5 SNMP ............................................................................................. 36
       3.5.6 GPS ................................................................................................ 38
       3.5.7 SMS ................................................................................................ 39
       3.5.8 VPN ................................................................................................ 43
3.6.10 Switch

3.6.9 Static Routes

3.6.8.5 Security

3.6.8.4 DMZ

3.6.8.3 traffic rules

3.6.8.2 Port Forwards

3.6.8.1 General Settings

3.6.8 Firewall

3.6.7 Interfaces Overview

3.6.6 WiFi Settings

3.6.5 wired-WAN

3.6.6.4 WiFi AP client

3.6.6.3 WiFi Interface Configuration

3.6.6.2 WiFi Advanced Configuration

3.6.6.1 Wifi General configuration

3.6.6 WiFi Settings

3.6.5 wired-WAN

3.6.4 LAN settings

3.6.3 Cell mobile data limitation

3.6.2 Mobile configuration

3.6.1 Operation Mode

3.6 Network Configuration

3.5.10 Connect Radio Module

3.5.9 DDNS

3.5.8.5 GRE tunnel

3.5.8.4 OpenVPN

3.5.8.3 L2TP

3.5.8.2 PPTP

3.5.8.1 IPSEC

3.5.8 Dynamic Routing

3.5.7 Interface Overview

3.5.6 QoS

3.5.5 cellular-WAN

3.5.4 Static Routes

3.5.3 Security

3.5.2 Port Forwards

3.5.1 Interface Overview
Chapter 1

1 Preparation job before configuration

1.1 Learn your router version and feature

1) H820 series contains different version and option feature. Please learn it before using it. H820 series defines the model as follows,
Notes: please be informed the following features are option. Please indicate with your orders.

1) WiFi Feature
2) GPS feature
3) Serial to cellular feature, RS232 or RS485 can choose one
4) Voice/SMS control
5) DC5V~50V
6) BGP, OSPF, RIP, etc.
7) RMS (Remote Management System)

2) Find the modem type info at the back cover of the router. This will be used while do configuration. For example: the following label indicates the version, type and inside module modem. The module modem name is “ME909s-821”, remember this and will select this module name while do configuration.
1.2 Prepare SIM Card and working condition

1. H820 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 H820 series and how to install and set the configurations.

1. Overall Dimension
2. Accessories Description
3. Installment

2.1 Overall Dimension

[Diagram showing the overall dimensions of the H820 series device]
2.2 The Ports

Back Picture:

ANT1(CELL): for cellular
ANT2(AUX): for cellular diversity receiving MIMO. Notes: the old version ANT2 is for diversity or for GPS.
ANT3 (WiFi): for WiFi
ANT4 (GPS): for GPS. Notes: the old version has no ANT4.
SIM: for sim card
COM: DB9 for serial port.
LAN1~LAN4: LAN RJ45 Ethernet ports.
WAN: WAN RJ45 Ethernet ports.
RST: sys reset button
PWR: DC power socket. DC5~40V, DC5~50V option depends on the router version.

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

Antenna Connection Table

<table>
<thead>
<tr>
<th>Antenna Connector</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell</td>
<td>for main cell antenna</td>
</tr>
<tr>
<td>Aux</td>
<td>for auxiliary cell antenna</td>
</tr>
<tr>
<td>WiFi / WLAN</td>
<td>for WiFi antenna</td>
</tr>
<tr>
<td>GPS</td>
<td>for GPS antenna</td>
</tr>
</tbody>
</table>
2.3 Installment

H820 series should be installed and configured properly before putting in service. The installation and configuration should be done or supervise by qualified engineer.

**Attention:**
Do not install H820 series or connect/disconnect its cable when it is power on.

2.4 SIM/UIM card installed

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

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

2.5 The installation of terminal blocks

This chapter is for version with terminal blocks only. Default, the H820 is with DB9 connector. Please use DB9 cable to connect H820 and the equipment directly.

**The following is for version with terminal blocks only:**
H820 uses pluggable terminals to connect the user’s data and the power supply. Spacing: 3.81mm, 10 Pin; User data and power supply suggestion: 14~24AWG. Please refer to the table 2-4 for the interface definition of the power cable and connection sequence. Specific interface definition of the power cable and connection sequence you can read on the labels of H820 products. Using 14~24AWG cable and referring to H820 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 H820 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
### Attention:

1. The power cable should be connected correctly. We “suggestion double check before switch it on. Wrong connections may destroy the equipment.

2. Power terminals: Pin 1 and Pin 2;

3. Here: Pin 2 is “GND”, PIN 1 is power input “Vin”(DC5~40V, or DV5~50V).

<table>
<thead>
<tr>
<th>PIN</th>
<th>Signal</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VCC</td>
<td>+5-40V DC Input, +5~50V option</td>
<td>Current: 12V/1A</td>
</tr>
<tr>
<td>2</td>
<td>GND</td>
<td>Ground</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>TX</td>
<td>Transmit Data</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>RX</td>
<td>Receive Data</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>PGND</td>
<td>Ground</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RST</td>
<td>Reset</td>
<td>Reset Pin has the same function with reset button. In the usage, it needs to be short connected to the GND. After giving the device a 1 sec low level, it will reboot. 3 seconds, the device will restore factory settings</td>
</tr>
<tr>
<td>7</td>
<td>DIO0</td>
<td>General Purpose I/O</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>DIO1</td>
<td>General Purpose I/O</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>NC</td>
<td>Not connect</td>
<td></td>
</tr>
</tbody>
</table>
I/O Terminal on router | Serial port (RS485 or RS232)
---|---
Port 3 (GND) | Pin 5
Port 4 (RX) | Pin 2
Port 5 (TX) | Pin 3

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

2.6 Grounding

To ensure a safe, stable and reliable H820 series operation, Router cabinet should be grounded properly.

2.7 Power Supply

H820 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, H820 series is designed with advanced power management technology. The DC power supply electronic to the device via the pluggable terminal PIN 2(GND) and PIN 1(Vin). Please refer to the above table for the detail definition of the terminal.

Normally, H820 series input powers supply is +5～+40V (if your H820 support 50V, the option is +5～+50V). In most cases, the standard configuration is 12V/1A.

2.8 LED and Check Network Status

Please connect the antenna after you successfully connect to the cable. And then insert the valid SIM/UIM card and provide the power to the H820 series via the cable. After provide the power to H820, 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 Indications

<table>
<thead>
<tr>
<th>LED</th>
<th>Indication Light</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>On for 25 seconds</td>
<td>On for 25 seconds after power supply</td>
</tr>
<tr>
<td></td>
<td>blink</td>
<td>System set-up normally</td>
</tr>
<tr>
<td></td>
<td>Off or still on after 25 seconds</td>
<td>System set-up failure</td>
</tr>
<tr>
<td>LAN1~LAN4</td>
<td>blink</td>
<td>Data transmission in Ethernet</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Ethernet connection abnormal</td>
</tr>
<tr>
<td></td>
<td>On</td>
<td>Ethernet is connected</td>
</tr>
<tr>
<td>VPN</td>
<td>On</td>
<td>VPN tunnel set-up</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>VPN tunnel set-up failure or unactivated</td>
</tr>
<tr>
<td>CELL</td>
<td>On</td>
<td>Access to the Internet</td>
</tr>
<tr>
<td>WIFI</td>
<td>On</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Disable</td>
</tr>
<tr>
<td>WAN</td>
<td>blink</td>
<td>Data transmission in Ethernet</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Ethernet connection abnormal</td>
</tr>
<tr>
<td></td>
<td>On</td>
<td>Ethernet is connected</td>
</tr>
<tr>
<td>Signal</td>
<td>Off</td>
<td>No signal, or signal checking is not ready</td>
</tr>
<tr>
<td></td>
<td>4s blink 1 time</td>
<td>Signal bar is 1</td>
</tr>
<tr>
<td></td>
<td>3s blink 1 time</td>
<td>Signal bar is 2</td>
</tr>
<tr>
<td></td>
<td>2s blink 1 time</td>
<td>Signal bar is 3</td>
</tr>
<tr>
<td></td>
<td>1s blink 1 time</td>
<td>Signal bar is 4</td>
</tr>
<tr>
<td></td>
<td>1s blink 2 times</td>
<td>Signal bar is 5</td>
</tr>
</tbody>
</table>
3 Software configuration

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

3.1 Overview

H820 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
Way 2) DHCP
Choose “Obtain an IP address automatically” and “Obtain DNS server address automatically”.
After IP setting, check it by ping. Click Windows start menu, run, execute “cmd” command. Input “ping 192.168.1.1” in the DOS window.

This information means the connection is work.

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

3.2.2 Log into Router
Open the Web Browser, and type **http://192.168.1.1** into the address field and press Enter bottom in your computer keyboard.

Type User Name “admin” and Password “admin” in the Login page, and then press the “Login” button.

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

3.3.1 Status overview

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

### Status

<table>
<thead>
<tr>
<th>System</th>
<th>Cell_Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>5600000036000063</td>
</tr>
<tr>
<td>SN</td>
<td>6.216</td>
</tr>
<tr>
<td>Kernel Version</td>
<td>3.18.29</td>
</tr>
<tr>
<td>Local-Time</td>
<td>Mon Aug 8 13:26:47 2015</td>
</tr>
<tr>
<td>Uptime</td>
<td>08:45:11s</td>
</tr>
<tr>
<td>Load Average</td>
<td>0.23, 0.12, 0.15</td>
</tr>
</tbody>
</table>

### Mobile 1

<table>
<thead>
<tr>
<th>Cell Status</th>
<th>Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.181.149.255/255 255.255.255</td>
</tr>
<tr>
<td>DNS 1</td>
<td>119.6.6.6</td>
</tr>
<tr>
<td>DNS 2</td>
<td>202.102.128.68</td>
</tr>
<tr>
<td>Cell Modem</td>
<td>Ericsson_F5521GW (0036_1900)</td>
</tr>
<tr>
<td>IMEI</td>
<td>5673770210131342</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellular Status</td>
<td>Up</td>
</tr>
<tr>
<td>Cell Modem</td>
<td>Ericsson_F6521GW (0BDB_160D)</td>
</tr>
<tr>
<td>IMEI</td>
<td>867377020131342</td>
</tr>
<tr>
<td>SIM Status</td>
<td>SIM Ready</td>
</tr>
<tr>
<td>Strength</td>
<td>9 / 31</td>
</tr>
<tr>
<td>Selected Network</td>
<td>Automatic</td>
</tr>
<tr>
<td>Registered Network</td>
<td>Registered on Home network: &quot;China Unicom&quot;, 2,</td>
</tr>
<tr>
<td>Sub Network Type</td>
<td>UMTS</td>
</tr>
<tr>
<td>Location Area Code</td>
<td>F10E</td>
</tr>
<tr>
<td>Cell ID</td>
<td>0A0EAE7</td>
</tr>
</tbody>
</table>

**Connection Status**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Mobile-PPP</td>
</tr>
<tr>
<td>IPv4 Addr</td>
<td>10.181.174.149/32</td>
</tr>
<tr>
<td>DNS 1</td>
<td>119.6.6.6</td>
</tr>
<tr>
<td>DNS 2</td>
<td>202.132.128.68</td>
</tr>
<tr>
<td>Gateway</td>
<td>0h 0m 10s</td>
</tr>
<tr>
<td>Uptime</td>
<td>0h 3m 40s</td>
</tr>
<tr>
<td>RX</td>
<td>725.33 KB (1607 Pkts)</td>
</tr>
</tbody>
</table>
### WAN Status

<table>
<thead>
<tr>
<th>Port</th>
<th>IPv4 WAN Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>dhcp</td>
</tr>
<tr>
<td>Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>Gateway</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Mac Addr</td>
<td>90:22:00:00:03:00</td>
</tr>
<tr>
<td>RX</td>
<td>0.00 B (0 Pkts.)</td>
</tr>
<tr>
<td>TX</td>
<td>34.61 KB (112 Pkts.)</td>
</tr>
</tbody>
</table>

#### IPv6 WAN Status
- Not connected

#### Active Connections
- 444 / 16384 (2%)

### LAN Status

#### Status Overview
<table>
<thead>
<tr>
<th>Uptime</th>
<th>0h:5m:5s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>static</td>
</tr>
<tr>
<td>Name</td>
<td>bi-lan</td>
</tr>
<tr>
<td>Type</td>
<td>bridge</td>
</tr>
<tr>
<td>Mac Addr</td>
<td>90:22:00:00:03:00</td>
</tr>
<tr>
<td>IPv4 Addr</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>IPv6 Addr</td>
<td>2001:0:1001:100:1001::1/64</td>
</tr>
<tr>
<td>RX</td>
<td>423.41 KB (3487 Pkts.)</td>
</tr>
<tr>
<td>TX</td>
<td>1.29 MB (3156 Pkts.)</td>
</tr>
</tbody>
</table>

#### LAN Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Addr</th>
<th>RX</th>
<th>TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired-LAN</td>
<td>90:22:00:00:03:00</td>
<td>461.26 KB (5755 Pkts.)</td>
<td>1.29 MB (3147 Pkts.)</td>
</tr>
<tr>
<td>WiFi</td>
<td>90:22:00:00:03:00</td>
<td>0.00 B (0 Pkts.)</td>
<td>7.11 KB (62 Pkts.)</td>
</tr>
</tbody>
</table>

#### DHCP Leases

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IPv4-Address</th>
<th>MAC-Address</th>
<th>LeaseTime Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-20100034M01C</td>
<td>192.168.1.171</td>
<td>00:01:66:af:11:b7</td>
<td>50th 3m 8s</td>
</tr>
</tbody>
</table>
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](image)

3.3.4 Routes

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

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

3.4.1 Setup wizard

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

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

### 3.4.3 Password

**Router Password**
Changes the administrator password for accessing the device

```
Password
Confirmation
```

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

NTP is network timing protocol.

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

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

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

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

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

Click button “Choose File” to select a compatible firmware then click button “Upload image…”. Router will do a basic checking for the uploaded file. If it is not compatible file, an error will be generated like this:
If the firmware file is OK, it will go to the verify page, then click button “Proceed”, and system will restart soon.

3.4.7 Reset

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

**System**

**Reboot**

Reboots the operating system of your device

![Reboot button]

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

### 3.5 Services configuration

#### 3.5.1 ICMP check

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

#### ICMP Check

<table>
<thead>
<tr>
<th>Enable</th>
<th>Enable ICMP check feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host1 to ping</td>
<td><a href="http://www.google.com">www.google.com</a></td>
</tr>
<tr>
<td>Host2 to ping</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>Ping timeout</td>
<td>4</td>
</tr>
<tr>
<td>Max retries</td>
<td>10</td>
</tr>
<tr>
<td>Interval between ping</td>
<td>2</td>
</tr>
<tr>
<td>Action when failed</td>
<td>Restart module</td>
</tr>
</tbody>
</table>

![ICMP Check form]

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

### 3.5.2 VRRP

#### VRRP Configuration

**VRRP LAN Configuration Settings**

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

**Failover Settings**

- **Enable**: Enable failover feature
- **Back to high priority**: If checked, when the high priority interface is available, use the high priority interface as WAN port. If unchecked, even if the high priority interface is available, the router will keep the current interface as WAN port and won't switch to the high priority interface.

**Primary Configuration**

- **Primary**: Wired_wan
- **Host 1 to ping**
- **Host 2 to ping**
- **Ping timeout**: 1
- **Max Retries**: 10
- **Interval between ping**: 30

- **Enable**: Enable failover feature
- **Back to high priority**: If checked, when the high priority interface is available, use the high priority interface as WAN port. If unchecked, even if the high priority interface is available, the router will keep the current interface as WAN port and won't switch to the high priority interface.
- **Primary/Secondary/Third**: Interface which can be treated as WAN port. There are 4 options: Wired-WAN, Wifi_client, Cell_mobile, and None.
- **Host 1 to ping / Host 2 to ping**: It is the 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 the system will say this interface is unavailable. If the ping is succeeding, the failed counter will be reset to 0 at anytime.
- **Interval between ping**: The time between twice ping. The unit is second.
3.5.4 DTU

**Notes:**
1) This feature is for H820 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**: Enable DTU feature.
- **Send DTU ID**: Send DTU ID at the front of packet.
- **DTU ID**: The default DTU ID is the SN of router, the final user can re-write it if necessary.
- **Forward delay**: The unit is millisecond. It is delay time that forward data between serial port and network.

#### Serial Setting

- **Serial baudrate**: 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 stopbits**: support 1 bits and 2 bits
- **Protocol**: TCP and UDP is supported.
- **Service mode**: Client and Server is supported.
- **Enable heartbeat**: The heartbeat is used for connection keep alive.
- **Heartbeat interval**: The time between two heartbeat packet.
- **Heartbeat content**: The content of heartbeat packet.
- **DTU center Configuration**: DTU center is the DTU server, the final user can input the center name and click button “Add” to add a new center here.
- **If the center is not needed, the final user can click button “Delete” to delete it, or set it to disabled.**

**Notes:**
The maximum number of DTU center is 32.
3.5.5 SNMP

**SNMP Configuration**

**General Settings**

- **Enable SNMP**: 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**: 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
- **User**: SNMPv3 username
- **Security Mode**: three options: None, private and Authorized. If it is set to None, there is no password required. If it is set to Authorized, only Authentication method and password required.
- **Authentication**: Authentication method, two options: MD5 and SHA.
- **Encryption**: Encryption method, DES and AES supported.
- **Authentication password**: SNMPv3 authentication password, at least 8 characters is required.
- **Encryption password**: SNMPv3 encryption password, at least 8 characters is required.

After all items is setup, click button “Save & Apply” to enable SNMP functionality.
3.5.6 GPS

**GPS Configuration**

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

- **Enable**: please check it once you need to use GPS feature.
- **Only GPRMC**: if check it, only send GPRMC data info (Longitude Latitude altitude)
- **Prefix SN No.**: if check it, add the router SN to the data packet
- **Send interval**: configure the frequency time of updated GPS data packet sending
- **GPS Send to**: Choose “Serial” or “TCP/IP” method. The router only receives the GPS signal, will not process it. It will just send the received GPS signal to your GPS processor devices or servers.
  - If the GPS processor device is connected to the H685 Router via Serial Port, please choose “Serial”.
  - If the GPS processor device is a remote server, please choose “Serial”.

**GPS to TCP/UDP Settings**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>check it to enable SMS command feature.</td>
</tr>
<tr>
<td>SMS ACK</td>
<td>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.</td>
</tr>
<tr>
<td>Reboot Router Command</td>
<td>input the command for “reboot” operation, default is “reboot”.</td>
</tr>
<tr>
<td>Get Cell Status Command</td>
<td>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.</td>
</tr>
<tr>
<td>Set Cell link-up Command</td>
<td>input the command for “router cell link up” operation, default is “cellup”. If router gets this command, the Router Cell will be online.</td>
</tr>
<tr>
<td>Set cell link-down Command</td>
<td>input the command for “router cell link down” operation, default is “celldown”. If router gets this command, the Router Cell will be offline.</td>
</tr>
<tr>
<td>DIO_0 Set Command</td>
<td>input the command for I/O port 0. For SMS feature, please keep the parameter default.</td>
</tr>
<tr>
<td>DIO_0 Reset Command</td>
<td>input the command for I/O port 0. For SMS feature, please keep the parameter default.</td>
</tr>
</tbody>
</table>
**DIO_1 Set Command**: input the command for I/O port 1. For SMS feature, please keep the parameter default.

**DIO_1 Reset Command**: input the command for I/O port 1. For SMS feature, please keep the parameter default.

**DIO Status Command**: input the command for I/O port status. For SMS feature, please keep the parameter default.

**Wifi on Command**: input the command for turning on Wifi. For SMS feature, please keep the parameter default.

**Wifi off Command**: input the command for turning off Wifi. For SMS feature, please keep the parameter default.

- **SMS alarm**
  
  **SMS Alarm**

  - **SMS Alarm**: 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 Configuration

NUM1

- SMS Command: 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.

Send SMS

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

3.5.8.1 IPSEC

**IPsec**

**IPsec Configuration**

- **Enable**: enable IPSEC feature
- **Exchange mode**: IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main mode are supported.
- **Authentication method**: Client and Server. Client is the machine which start the IPSEC connection.
- **Remote VPN endpoint**: domain name or IP address of the remote endpoint. It can be visited from internet.
- **Preshared Keys**: it is known as PSK, the length is 16 to 32.
- **Local subnet**: the subnet of local which connects to IPSEC VPN.
- **Remote subnet**: the subnet of remote which connects to IPSEC VPN.
Phase 1 Proposal
The phase must match with another incoming connection to establish IPSec

- Encryption algorithm: 3DES
- Hash algorithm: SHA1
- DH group: MODP1024

Phase 2 Proposal
The phase must match with another incoming connection to establish IPSec

- Encryption algorithm: AES 128
- PFS group: MODP1024
- Authentication: HMAC_SHA1

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

- **PPTP Client configuration**

  **PPTP Client Instance: Aaaa**

### Main Settings

- **Enable**: enable this instance.
- **Server**: domain name or IP address of PPTP server.
- **Username**: server authentication user name.
- **Password**: server authentication password.
- **MTU**: maximum transmission unit.
- **Keep Alive**: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Use default gateway**: If unchecked, no default route is configured.
- **Use DNS servers advertised by peer**: 

---

E-Lins Technology Co., Limited  
Tel: +86-755-29230581  E-mail: sales@e-lins.com  www.szelins.com  www.e-lins.com
- **Use DNS servers advertised by peer**: If unchecked, the advertised DNS server addresses are ignored.

### PPTP Server Configuration

**PPTP Server Instance:**

**Main Settings**

- **Enable**: [ ]
- **Local IP**: 192.168.0.1
- **Remote IP**: 192.168.0.20
- **Remote IP end**: 192.168.0.30
- **ARP Proxy**: [ ]
- **Debug**: [ ]

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>youruser</td>
<td>*********</td>
</tr>
</tbody>
</table>

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

### 3.5.8.3 L2TP

This page is a list of configured L2TP instance and their state. The final user can click button “Edit” to modify it, or click button “Delete” to delete an instance.
Layer 2 Tunneling Protocol

L2TP Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Enable</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2tpd_server</td>
<td>Server</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

New instance name: [Input Field]  Role: [Dropdown]  Add New

- Enable: enable this L2TP instance.
- Server: domain name or IP address of L2TP server.
- Username: server authentication user name.
- Password: server authentication password.
- MTU: maximum transmission unit.
- Keep Alive: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- Checkup Interval: Number of seconds to pass before checking if the interface is not up since the last setup attempt and retry the connection otherwise. Set it to a value sufficient for a successful L2TP connection for you. It's mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.

L2TP Client Instance: Bbbbbb

Main Settings

- Enable
- Server
- Username
- Password
- MTU
- Keep Alive
- Checkup Interval

L2TP Server configuration
L2TP Server Instance: L2tpd_server

Main Settings

- **Local IP**: indicate server’s IP address.
- **Remote IP range begin**: the remote IP address leases start
- **Remote IP range end**: the remote IP address lease end.
- **Remote LAN IP**: L2TP client IP.
- **Remote LAN netmask**: the mask of L2TP client IP, the default value is 255.255.255.0
- **Username**: server authentication username
- **Password**: server authentication password.

3.5.8.4 OpenVPN

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

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

OpenVPN instances

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

<table>
<thead>
<tr>
<th>enabled</th>
<th>Started</th>
<th>Start/Stop</th>
<th>Tuni/Tap</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom_config</td>
<td>No</td>
<td>no</td>
<td>start</td>
<td>tun</td>
<td>1194</td>
</tr>
<tr>
<td>sample_server</td>
<td>No</td>
<td>no</td>
<td>start</td>
<td>tun</td>
<td>1194</td>
</tr>
<tr>
<td>sample_client</td>
<td>No</td>
<td>no</td>
<td>start</td>
<td>tun</td>
<td>1194</td>
</tr>
</tbody>
</table>

Client configuration for an other: Add

Note: for OpenVPN detail configuration page, you can put mouse on the title on item to get more help information.
If the item you needed is not show in the main page, please check the “Additional Field” dropdown list at bottom of page.

Overview » Instance "sample_server"

Service

- enabled
- verb
- niock
- disable_occ

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

- Additional Field -
3.5.8.5 GRE tunnel

GRE Tunnel

GRE Tunnel Configuration

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

3.5.9 DDNS

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

Dynamic DNS allows your router to 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'.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Hostname/Domain</th>
<th>Enabled</th>
<th>Last Update</th>
<th>Process ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>example_ipv4</td>
<td>153489866a.ikok.la</td>
<td>✔️</td>
<td>Never Verify</td>
<td>PID: 3229</td>
</tr>
<tr>
<td>myddns_ipv6</td>
<td>yourhost.example.com</td>
<td>☐</td>
<td>Never</td>
<td></td>
</tr>
</tbody>
</table>

- **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:
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:
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.
Read the log file of DDNS.

**Notes:**
If use DDNS server no-ip.com, please check the "Use HTTP Secure" referring to following picture.
3.5.10 Connect Radio Module

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

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

Exchange data between radio module and serial

Enable

Connect mode: Serial

Serial baudrate: 115200 bps

Serial parity: None

Serial databits: 8 bits

Serial stopbits: 1 bits

- \textbf{Enable: conflict with DTU, please disable DTU firstly}

- **Connect Mode**: Serial only

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

3.6 Network Configuration
### 3.6.1 Operation Mode

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

#### NAT Enabled
Network Address Translation. Default is Enabling

#### Ethernet wan port role:
- **Wired-WAN port acts as WAN**
  The Ethernet wan port is used as for WAN. Default is Checked
- **Wired-WAN port acts as LAN**
  The Ethernet wan port is used as for lan port to get 5 LAN Ethernet ports. If is WAN RJ45 Ethernet port is used for WAN, please do not check this feature.

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

### 3.6.2 Mobile configuration

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

**Notes:**
the Cell Modem Type was marked on the back of the router.
For example, it shows the following picture. H820 is the router series name,
H820w-W-RS232 is the part number name. And the EM820w Cell Modem is the Cell Modem name.

- **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.

- **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**: support period are Month, Week and Day.  
- **Start day**: the beginning day of period.  
- **SIM data limit(MB)**: the maximum data can be used during this period. If it exceeds, router will disable cell mobile network during this period.  
- **Enable alarm**: enable data limitation alarm.  
- **Phone number**: the phone number receives data limitation alarm SMS.  
- **Warning percent of Data Used**: if the used data arrives this setting, a data limitation alarm SMS will be sent.  
- **Used(MB)**: the data has been consumed during this period.
### 3.6.4 LAN settings

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

#### Common Configuration

<table>
<thead>
<tr>
<th>General Setup</th>
<th>Advanced Settings</th>
<th>Physical Settings</th>
<th>Firewall Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>br-lan</td>
<td>Uptime: 0h 24m 36</td>
<td>MAC-Address: 90:22:00:80:03:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RX: 1.34 MB (13877 Pkts.)</td>
<td>TX: 4.46 MB (12981 Pkts.)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Static address</th>
<th>Really switch protocol?</th>
<th>Switch protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address</td>
<td>192.168.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 netmask</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 broadcast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use custom DNS servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 assignment length</td>
<td>60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 assignment hint</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Protocol**: only static address is supported for LAN
- **Use custom DNS servers**: multiple DNS server supported.
- **IPv6 assignment length**: Assign a part of given length of every public IPv6-prefix to LAN interface
- **IPv6 assignment hint**: Assign prefix parts using this hexadecimal subprefix ID for LAN interface.
• **Bring up on boot**: if checked, LAN interface will be set to up when system bootup. If unchecked, LAN interface will be down. Don't set it to unchecked if don’t have special purpose.

• **Use builtin IPv6-management**: the default is checked. If IPv6 is not needed, it can be set to unchecked.

• **Override MAC address**: override LAN MAC address.

• **Override MTU**: Maximum Transmission Unit.

• **Use gateway metric**: the LAN subnet’s metric to gateway.

---

**Common Configuration**

- **Bridge interfaces**: LAN bridges wired-LAN and WiFi in a same LAN subnet.
- **Enable STP**: enable Spanning Tree Protocol on LAN. The default value is unchecked.
● **Ignore interface**: if it is unchecked, Disable DHCP on LAN.
● **Start**: Lowest leased address as offset from the network address.
● **Limit**: Maximum number of leased addresses.
● **Leasetime**: Expiry time of leased addresses, minimum is 2 minutes (2m). 12H means 12 hours.

**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**: 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

- **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”.

---

E-Lins Technology Co., Limited
Tel: +86-755-29230581  E-mail: sales@e-lins.com  www.szelins.com  www.e-lins.com
After click button “Switch protocol”, the below is shown:

**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

- **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

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

3.6.6.2 WiFi Advanced Configuration

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

### 3.6.6.3 WiFi Interface Configuration

#### Interface Configuration

<table>
<thead>
<tr>
<th>General Setup</th>
<th>Wireless Security</th>
<th>MAC-Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESSID</strong></td>
<td>Cell_AP_0002b2</td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Access Point</td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hide Extended Service Set Identifier</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WMM Mode</strong></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

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

#### Network: Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

- **Hide Extended Service Set Identifier**: hide SSID means this WiFi cannot be scanned by others.
- **WMM Mode**:
**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.

**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.
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**

- **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**

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

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

**Interfaces**

**Interface Overview**

<table>
<thead>
<tr>
<th>Network</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Uptime: 00:50:35s</td>
<td>Connect</td>
</tr>
<tr>
<td></td>
<td>MAC-Address: 94:5.65 KB (9759 Pkts.)</td>
<td>RX: 94.56 KB</td>
</tr>
<tr>
<td>IFMOBILE</td>
<td>MAC-Address: 00:00:00:00:00:00</td>
<td>RX: 0.00 B</td>
</tr>
<tr>
<td>WAN</td>
<td>Uptime: 00:00:00s</td>
<td>Connect</td>
</tr>
<tr>
<td></td>
<td>MAC-Address: 94:5.65 KB (9759 Pkts.)</td>
<td>RX: 94.56 KB</td>
</tr>
<tr>
<td>WANS</td>
<td>Uptime: 00:00:00s</td>
<td>Connect</td>
</tr>
<tr>
<td></td>
<td>MAC-Address: 94:5.65 KB (9759 Pkts.)</td>
<td>RX: 94.56 KB</td>
</tr>
<tr>
<td>WWAN</td>
<td>Uptime: 00:00:00s</td>
<td>Connect</td>
</tr>
<tr>
<td></td>
<td>MAC-Address: 94:5.65 KB (9759 Pkts.)</td>
<td>RX: 94.56 KB</td>
</tr>
</tbody>
</table>
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**: checked
- **Drop invalid packets**: unchecked

**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.
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Match</th>
<th>Action</th>
<th>Enable</th>
<th>Sort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow-IPv4-UDP</td>
<td>From any host in wan to any outer IP at port 68 on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow-DHCP-Renew</td>
<td>From any host in wan to any outer IP at port 68 on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow-IPv4-ICMP</td>
<td>From any host in wan to any outer IP on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow-IPv4-ICMP</td>
<td>From any host in wan to any outer IP on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow-ICMPv6-Input</td>
<td>From any host in wan to any outer IP on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow-ICMPv6-Forward</td>
<td>From any host in wan to any outer IP on this device</td>
<td>Accept input</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Open ports on router and create new forward rules:

#### Open ports on router:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>External port</th>
</tr>
</thead>
<tbody>
<tr>
<td>New input rule</td>
<td>TCP+UDP</td>
<td></td>
</tr>
</tbody>
</table>

#### New forward rule:

<table>
<thead>
<tr>
<th>Name</th>
<th>Source zone</th>
<th>Destination zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>New forward rule</td>
<td>lan</td>
<td>wan</td>
</tr>
</tbody>
</table>
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
- **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 Configuration**

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

- **Enable DMZ**: [ ]
- **IP address**: 
- **Protocol**: All protocols, TCP+UDP, TCP, UDP.

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 or deny users access H820/H685 router from remote side.
- **Ping from WAN to LAN**: allow or deny ping from remote side to internal LAN subnet.
- **HTTPS access from WAN**: allow or deny access router web management page from remote side.
- **Remote network**: Any IP Address, Single IP address, Subnet.
- **IP address**: fill a remote IP address that can access router web management page.
- **Netmask**: 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the illegal value is from 1 to 32.
3.6.9 Static Routes

**Interface:** You can choose the corresponding interface type.

**Target:** the destination host IP or network.

**Gateway:** IP address of the next router.

**Notice:**

- Gateway and LAN IP of this router must belong to the same network segment.
- If the destination IP address is the one of a host, and then the Netmask must be 255.255.255.255.
- If the destination IP address is IP network segment, it must match with the Netmask. For example, if the destination IP is 10.0.0.0, and the Netmask is 255.0.0.0.

3.6.10 Switch

**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**: 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.

<table>
<thead>
<tr>
<th>General Settings</th>
<th>Resolv and Hosts Files</th>
<th>TFTP Settings</th>
<th>Advanced Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Suppress logging**: Suppress logging of the routine operation of these protocols.
- **Allocate IP sequentially**: Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private**: Do not forward reverse lookups for local networks.
- **Filter useless**: Do not forward requests that cannot be answered by public name servers.
- **Localise queries**: Localise hostname depending on the requesting subnet if multiple IPs are available.
- **Expand hosts**: Add local domain suffix to names served from hosts files.
- **No negative cache**: Do not cache negative replies, e.g. for not existing domains.
- **Strict order**: DNS servers will be queried in the order of the resolvfile.
- **Bogus NX Domain Override**: List of hosts that supply bogus NX domain results.
- **DNS server port**: Listening port for inbound DNS queries.
- **DNS query port**: Fixed source port for outbound DNS queries.
- **Max DHCP leases**: Maximum allowed number of active DHCP leases.
- **Max edns0 packet size**: Maximum allowed size of EDNS.0 UDP packets.
3.6.12 Diagnostics

- **Max concurrent queries**: Maximum allowed number of concurrent DNS queries.

**Diagnostics**

Network Utilities

- **Ping**: it is a tool used to test the reachability of a host on an Internet Protocol (IP) network.
- **Traceroute**: it is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- **Nslookup**: it is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
- For example if I want to ping www.google.com, type the target domain name or IP address, then click button “Ping”. Wait couple of seconds, the result will be shown below.

**Diagnostics**

Network Utilities

<table>
<thead>
<tr>
<th><a href="http://www.google.com">www.google.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
</tr>
<tr>
<td>Traceroute</td>
</tr>
<tr>
<td>Nslookup</td>
</tr>
</tbody>
</table>

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

3.6.13 Loopback Interface

**Loopback Interface Configuration**

- **IP address**: 127.0.0.1
- **Netmask**: 255.0.0.0
The default Loopback interface has IP address 127.0.0.1, the final user can change it here.

3.6.14 Dynamic Routing

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

**Dynamic Routing**

**Zebra**

Enable □

Password *****

**OSPF**

Enable □

Password *****

**OSPF6**

Enable □

Password *****
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.

RIPv2: 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:
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**: enable QoS on this interface.
  - **Classification group**: default
  - **Calculate overhead**: off
  - **Half-duplex**: off
  - **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

<table>
<thead>
<tr>
<th>Target</th>
<th>Source host</th>
<th>Destination host</th>
<th>Service</th>
<th>Protocol</th>
<th>Ports</th>
<th>Number of bytes</th>
<th>Comment</th>
<th>Sort</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>22-53</td>
<td></td>
<td>sh, dns</td>
<td></td>
</tr>
<tr>
<td>normal</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>TCP</td>
<td>20-21</td>
<td></td>
<td>ftp, smtp, http(s), imap</td>
<td></td>
</tr>
<tr>
<td>express</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>5190</td>
<td></td>
<td>AOL, Chat, ICQ</td>
<td></td>
</tr>
<tr>
<td>normal</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.