



User Manual

H8922S 3G/4G Router



We Hongdian provide full support to customers, contact us freely if any questions.

Shenzhen Hongdian Technologies Corporation

Address	F14-16,Headquarter Economic Center Building, Zhonghaixin Science&Tech Park, Bulan Road, Longgang District, Shenzhen
Website	http://www.hongdian.com
Technical Support	+86-0755-88864288-4/8238
Fax Number	0755-83404677
Postcode	518112

Copyright © Shenzhen Hongdian Technologies Corporation. 2017. All rights reserved.

All information in this user manual is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user manual by any means without written authorization from Shenzhen Hongdian Technologies Corporation.

Trademarks and Permissions



and DTU are the trademarks and logos of Shenzhen Hongdian Technologies Corporation. Other trademarks and logos mentioned in this manual belong to other organizations related. Shenzhen Hongdian Technologies Corporation does not own the rights of other trademarks and logos.

Caution

Due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file do not compose any form of guarantee and we Hongdian reserves the right of final explanation.

Introduction

Summary

H8922S 3G/4G Router is a data communication terminal on mobile communication network which independently researched and developed by Hongdian Corporation. The product is based on 3G/4G wireless communication technology. It uses high performance 32-bit embedded operating system and has a full industrial design. It can provide high performance 3G/4G communication speed by accessing the global 3G/4G network via the embedded 4G module. It is widely used for various industries such as telecommunication, finance, information media, electric power, transportation, on-board devices and environmental protection and so on.

The main function of this document is to help readers know the functional characteristics and typical application modes of the product, understand the installation, deployment and configuration operation methods for the product and master the methods for dealing with common faults during usage.

Product Version

The product version corresponding to the document is as shown below.

Product name	Product version
H8922S 3G/4G Router	V12

Readers

The document applies to the following persons:

- R & D engineers
- Technical support engineers
- Customers

You are recommended to start from Chapter One if you know and use any Router product of Hongdian for the first time so as to get a better understanding of the product and the correct usage by reading all the contents of the document.

You are recommended to select any chapter or section you want to know via the contents below if you have known or used any Router product of Hongdian or a similar product of any other company.

Brief Introduction of Contents




The usage of H8922S 3G/4G Router is described in the document.

Section	Contents
1 Product Introduction	H8922S 3G/4G Router and its functional characteristics, product orientation are introduced in the chapter.
2 Product Structure	H8922S 3G/4G Router software, hardware structures are introduced in the chapter.
3 Installation of H8922S 3G/4G Router	How to install H8922S 3G/4G Router is introduced in the chapter.
4 Preparation before Configuration	Preparation before H8922S 3G/4G Router configuration is introduced in the chapter.
5 Router Configuration	H8922S 3G/4G Router functional configuration is introduced in the chapter.
6 Typical Application	Several typical application modes of H8922S 3G/4G Router is introduced in the chapter.
7 FAQ	The causes and handling methods for common faults of H8922S 3G/4G Router during usage are introduced in the chapter.

Conventions

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you address a problem or save your time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in boldface.
<i>Italic</i>	Command arguments are in italics.

Convention	Description
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the "&" sign can be repeated 1 to n times.
#	A line starting with the "#" sign is comments.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface. For example, click OK.
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder.

Keyboard Operations

Format	Description
Key	Press the key. For example, press Enter and press Tab.
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse Operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.

Action	Description
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Contents

Introduction.....	3
Summary	3
Product Version.....	3
Readers	3
Brief Introduction of Contents	4
Conventions	4
Contents	7
Table Contents	11
Figure Contents	13
1 Product Introduction.....	2-1
About This Chapter	2-1
1.1 Summary	2-1
1.2 Product Orientation	2-2
1.3 Functions and Features	2-3
1.4 Technical Indicators and Specifications.....	2-4
2 Product Structure.....	5
About This Chapter	5
2.1 Hardware Structure.....	5
2.1.1 Equipment appearance and dimension.....	5
2.1.2 Equipment configuration and parts.....	7
2.2 Functional Structure	8
3 Installation of H8922S 3G/4G Router	12
About This Chapter	12
3.1 Unpacking.....	12
3.2 Installation and Wiring.....	12
3.2.1 Installation of SIM card.....	12
3.2.2 Ethernet cable connection	13
3.2.3 Serial port line connection	14
3.2.4 Ethernet cable connection	14
3.3 Power Supply.....	15

3.4 Installation Inspection	15
4 Preparation before Configuration	16
About This Chapter	16
4.1 Terminal Panel Indicator Lamp Status	16
4.2 Local Connection Configuration.....	17
4.3 Basic configuration.....	24
4.3.1 Login WEB GUI	24
5 Router Configuration	25
About this chapter	25
5.1 Overview	25
5.2 Network configuration	25
5.2.1 LAN.....	26
5.2.2 WAN	27
5.2.3 Modem.....	30
5.2.4 WLAN.....	36
5.2.5 Parameter select (Recommend to Single module dual SIM version)	40
5.2.6 Link Backup	43
5.2.7 DHCP Service.....	45
5.3 Application program configuration.....	48
5.3.1 ICMP check	48
5.3.2 DDNS configuration	51
5.3.3 SNMP configuration.....	52
5.3.4 M2M configuration.....	54
5.3.5 Timing configuration	56
5.3.6 Wake up configuration.....	59
5.3.7 DTU configuration (Optional).....	61
5.3.8 GPS configuration (Optional).....	64
5.4 Security.....	66
5.4.1 Overview.....	66
5.4.2 Configuration.....	66
5.5 Forward configuration.....	72
5.5.1 Overview.....	72
5.5.2 NAT	73
5.5.3 Static Routing.....	77
5.5.4 QoS (Optional)	80
5.5.5 Dynamic Routing (Optional).....	82
5.6 VPN configuration	87
5.6.1 Overview.....	87
5.6.2 VPDN configuration	88
5.6.3 Tunnel configuration	90
5.6.4 IPSec configuration.....	91

5.6.5 OpenVPN Configuration.....	97
5.7 System configuration.....	101
5.7.1 Overview.....	101
5.7.2 Local Log.....	101
5.7.3 Remote Log.....	102
5.7.4 Clock.....	103
5.7.5 Account.....	104
5.7.6 Network Test.....	106
5.7.7 Files.....	107
5.8 Status.....	113
5.8.1 Overview.....	113
5.8.2 Base Information.....	113
5.8.3 LAN.....	114
5.8.4 WAN.....	115
5.8.5 Modem.....	116
5.8.6 Routing Table.....	118
5.9 RESET button function.....	119
6 Typical application	120
About this chapter	120
6.1 Overview	120
6.2 Awake function.....	120
6.3 Parameter select.....	122
6.4 VPN.....	124
6.5 Timing Task.....	127
6.6 DTU function application	128
7 FAQ	133
About this chapter	133
7.1 Hardware Failure.....	133
7.1.1 All LED dark	133
7.1.2 SIM Slot.....	134
7.1.3 Ethernet Connection	134
7.1.4 Antenna Connection.....	134
7.2 Dial Online Problem	135
7.2.1 Dial discontinue.....	135
7.2.2 No Signal.....	135
7.2.3 Cannot find SIM/UM card	135
7.2.4 Poor Signal.....	136
7.2.5 Compress Protocol not match	136
7.3 VPN Problem	136
7.3.1 VPDN cannot connect	136
7.3.2 VPN cannot communicate.....	137

7.3.3 Router can communicate but subnet cannot	137
7.4 WEB configuration.....	137
7.4.1 Updating firmware failure.....	137
7.4.2 Backup setting problem	138
7.4.3 Updating patch failure	138
7.4.4 CFE Updating failure.....	138
7.4.5 Update failure in WEB GUI	139
7.4.6 Forget Router Password	139

Table Contents

Table 2-1 Specification on Dimension of H8922S 3G/4G Router	6
Table 2-2 List of H8922S 3G/4G Router Parts.....	7
Table 4-1 Table of Illustration of Indicator Lamps	16
Table 5-1 LAN Parameter instruction.....	26
Table 5-2 WAN connection type parameter instruction.....	27
Table 5-3 “Modem” Parameter instruction	31
Table 5-4 WLAN parameter instruction.....	37
Table 5-5 Parameter instruction	41
Table 5-6 Connection type Parameter instruction.....	42
Table 5-7 Link Backup Parameter.....	44
Table 5-8 DHCP Parameter	46
Table 5-9 ICMP check rules Parameter instruction.....	49
Table 5-10 DDNS Parameter instruction.....	51
Table 5-11 SNMP Parameter instruction.....	53
Table 5-12 M2M Parameter instruction	55
Table 5-13 Timing task parameter instruction	57
Table 5-14 Wake up Parameter instruction.....	59
Table 5-15 DTU Parameter instruction	62
Table 5-16 GPS Parameter instruction.....	65
Table 5-17 IP filter parameter instruction.....	68
Table 5-18 Domain Filter parameter instruction.....	70
Table 5-19 MAC Filter explanation	71
Table 5-20 MAC Filter Parameter instruction.....	72
Table 5-21 DNAT Parameter instruction.....	74
Table 5-22 SNAT rule instruction	76
Table 5-23 MASQ rule Parameter instruction.....	77
Table 5-24 Static Routing Parameter Instruction.....	79
Table 5-25 QoS parameter instruction.....	81
Table 5-26 RIP Parameter Instruction.....	83

Table 5-27 RIP parameter instruction	84
Table 5-28 OSPF parameter instruction.....	85
Table 5-29 OSPF route parameter instruction.....	86
Table 5-30 VPDN rule parameter instruction	89
Table 5-31 Tunnel rule parameter instruction.....	91
Table 5-32 IPSec Phase 1 Parameter instruction.....	93
Table 5-33 IPSec Parameter instruction.....	95
Table 5-34 IPSec Parameter instruction.....	96
Table 5-35 OpenVPN parameter instruction.....	98
Table 5-36 Remote log parameter instruction	102
Table 5-37 Clock Parameter instruction	103
Table 5-38 Account parameter instruction	105
Table 5-39 Network Test Parameter instruction.....	106
Table 5-40 Base information Parameter instruction.....	114
Table 5-41 LAN Parameter instruction.....	114
Table 5-42 WAN Parameter instruction.....	116
Table 5-43 Modem Parameter instruction.....	117
Table 5-44 Routing table Parameter instruction.....	118

Figure Contents

Figure 1-1 Schematic Diagram of Application for Financial Industry.....	2-2
Figure 1-2 Schematic Diagram of Dual Modem Online Application	2-3
Figure 2-1 Picture of Actual Appearance of H8922S 3G/4G Router	6
Figure 2-2 Diagram of Lower Cap for H8922S 3G/4G Router	7
Figure 2-3 Diagram of Dual Modem Function Module	9
Figure 2-4 Diagram of Single Mode plus WLAN Functional Structure.....	10
Figure 3-1 Eject SIM Card Set.....	13
Figure 3-2 Schematic Diagram of SIM Card Installation.....	13
Figure 3-3 Single Equipment Direct Connection.....	14
Figure 3-4 Multiple Equipment Connection	14
Figure 4-1 Local Area Connection	17
Figure 4-2 Connection properties	19
Figure 4-3 Internet protocol (TCP/IP)	19
Figure 4-4 Advanced TCP/IP Settings	21
Figure 4-5 TCP/IP address.....	22
Figure 4-6 Connectivity check.....	23
Figure 4-7 User identity page.....	24
Figure 5-1 LAN window	26
Figure 5-2 WAN window	27
Figure 5-3 Modem window	30
Figure 5-4 Modem page.....	31
Figure 5-5 Single module single SIM/dual module dual SIM.....	34
Figure 5-6 Single module dual SIM	34
Figure 5-7 Advanced setting	35
Figure 5-8 AP mode configure interface.....	36
Figure 5-9 Station mode configure interface.....	37
Figure 5-10 Station scan signal interface.....	37
Figure 5-11 Parameter select.....	40
Figure 5-12 Add rule.....	41

Figure 5-13 Connection type window	42
Figure 5-14 Link Backup.....	44
Figure 5-15 DHCP	46
Figure 5-16 ICMP Check tab	48
Figure 5-17 ICMP adding page.....	49
Figure 5-18 DDNS configuration.....	51
Figure 5-19 SNMP configuration	53
Figure 5-20 M2M configuration	55
Figure 5-21 Timing configuration.....	56
Figure 5-22 To add timing task	57
Figure 5-23 Wake up configuration	59
Figure 5-24 DTU configuration	61
Figure 5-25 GPS configuration.....	65
Figure 5-26 IP Filter tab.....	66
Figure 5-27 IP filter “Input” type	67
Figure 5-28 IP Filter “Forward” type.....	67
Figure 5-29 Domain filter tab.....	69
Figure 5-30 Domain filter tab.....	70
Figure 5-31 MAC Filter tab	71
Figure 5-32 MAC Filter configuration.....	72
Figure 5-33 NAT tab	73
Figure 5-34 DNAT rule configuration.....	74
Figure 5-35 SNAT rule configuration	75
Figure 5-36 MASQ configuration.....	77
Figure 5-37 Static Routing Interface.....	78
Figure 5-38 Static Routing Interface.....	78
Figure 5-39 Policy Routing Interface.....	79
Figure 5-40 QoS interface.....	81
Figure 5-41 RIP interface	83
Figure 5-42 RIP route configuration interface	84
Figure 5-43 OSPF Interface.....	85
Figure 5-44 OSPF route configuration interface.....	86
Figure 5-45 VPDN configuration.....	88
Figure 5-46 VPDN rule configuration.....	88
Figure 5-47 L2TP tunnel status	89
Figure 5-48 Tunnel configuration.....	90
Figure 5-49 IPsec tab.....	92

Figure 5-50 IPsec phase 1 configuration.....	93
Figure 5-51 IPsec phase 2 configuration.....	95
Figure 5-52 IPsec configuration tab.....	96
Figure 5-53 OpenVPN configuration page.....	98
Figure 5-54 Local Log tab.....	101
Figure 5-55 Remote Log tab.....	102
Figure 5-56 “NTP” Time Synch.....	103
Figure 5-57 Manual Time Synch. Type	103
Figure 5-58 Account tab.....	105
Figure 5-59 Network Test Tab.....	106
Figure 5-60 Files tab	107
Figure 5-61 Add an IP address	108
Figure 5-62 CFE mode upgrading.....	109
Figure 5-63 CFE upgrading page.....	109
Figure 5-64 Backup setting page	110
Figure 5-65 Factory setting page.....	111
Figure 5-66 Patch operation.....	112
Figure 5-67 Reboot / Refresh.....	113
Figure 5-68 Base Information tab	113
Figure 5-69 “LAN” info	114
Figure 5-70 Static IP WAN status.....	115
Figure 5-71 DHCP WAN status	115
Figure 5-72 PPPoE WAN status	116
Figure 5-73 Modem Status page	117
Figure 5-74 Routing table page	118
Figure 6-1 Wake up/trigger setting example	121
Figure 6-2 Rules setting.....	122
Figure 6-3 Parameter select setting 1	123
Figure 6-4 Parameter select setting 2	124
Figure 6-5 Build IPsec.....	125
Figure 6-6 IPsec Phase 1	125
Figure 6-7 IPsec Phase 2	126
Figure 6-8 IPsec	126
Figure 6-9 IPsec status	127
Figure 6-10 Timing.....	127
Figure 6-11 router online.....	128
Figure 6-12 router off line.....	128

Figure 6-13 router reboot	128
Figure 6-14 DTU Application	129
Figure 6-15 TCP mode configuration.....	130
Figure 6-16 Add text data	131
Figure 6-17 TCP server tool	131

1 Product Introduction

About This Chapter

Section	Brief Introduction of Contents
1.1 Summary	The summary of H8922S 3G/4G Router is briefly introduced in the section.
1.2 Product Orientation	The product orientation of H8922S 3G/4G Router is briefly introduced in the section.
1.3 Functions and Features	The functions and features of H8922S 3G/4G Router are briefly introduced in the section.
1.4 Technical Indicators and Specifications	The technical indicators and relevant specifications for H8922S 3G/4G Router are briefly introduced in the section.

1.1 Summary

H8922S 3G/4G Router is a wireless router gateway researched and developed based on 3G/4G technology. Besides the functions such as VPN, firewall, NAT, PPPoE, DHCP of conventional routers, it can also support 3G/4G wireless dialing to provide wireless high speed bandwidth as high as 100Mbps. H8922S 3G/4G Router has three major forms, namely single mode single card, single mode dual card, dual modem dual card, and all of the three forms support 802.11n to provide local wireless local area network (WLAN) as high as 150Mbps. The most dominant feature of H8922S 3G/4G Router is that it can support simultaneous online and backup switchover among various networks such as WAN, WLAN and 3G/4G. The backup in various networks can guarantee and maintain communication links to the greatest extent so as to avoid business loss caused by communication outage. The simultaneous online of various networks can facilitate strategy diversion based on business so as to realize the bandwidth rationality and adequate utilization of various network channels.

H8922S 3G/4G Router supports the M2M wireless remote comprehensive network management platform independently researched and developed by Hongdian. The M2M

platform is able to realize the statistics of 3G/4G wireless network information and status in the place where H8922S 3G/4G Router is used as well as the remote upgrade and configuration management for H8922S 3G/4G Router.

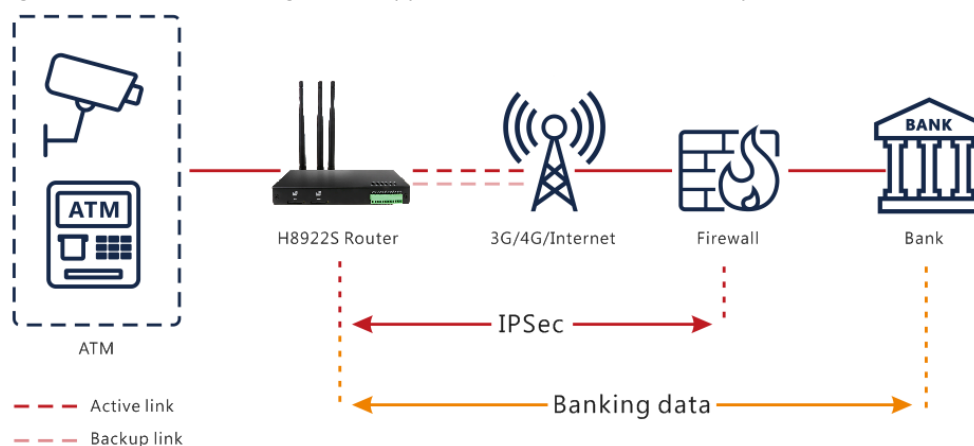
1.2 Product Orientation

H8922S 3G/4G Router is widely used for various industries such as telecommunication, finance, information media, electric power, transportation, on-board devices and environmental protection and so on.

Dual modem backup application for financial industry

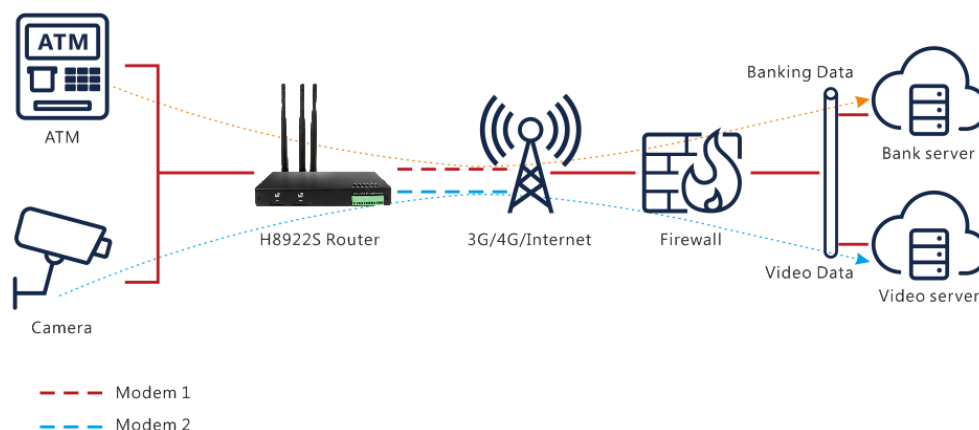
H8922S 3G/4G Router can provide guarantees for highly secure transmission of financial data via ways such as IPSec VPN. The risks of communication outage caused by operators' network faults can be greatly reduced via its dual modem switchover function. The typical network is as shown in Figure 1-1.

Figure 1-1 Schematic Diagram of Application for Financial Industry



Dual modem online application for financial industry

H8922S 3G/4G Router dual modem simultaneous online can simultaneously support the functions such as data transmission for ATM and video monitoring of ATM so as to guarantee the security of ATM operating environment. The typical network is as shown in Figure 1-2

Figure 1-2 Schematic Diagram of Dual Modem Online Application

1.3 Functions and Features

Basic functions

- It supports networks such as LTE, HSPA+, CDMA 2000 EV-DO Rev.A, WCDMA (HSDPA, HSUPA), TD-SCDMA, etc.; in addition, it has downward compatibility for GPRS/EDGE or CDMA 1X networks
- It supports simultaneous online and backup switchover of various networks such as WAN, WLAN, 3G/4G, etc.
- It supports WLAN AP/station client functions; it supports 802.11n to realize wireless local area network transmission rate as high as 150Mbps
- It supports the high speed exchange of 4 LAN interfaces
- It supports PPPoE dialing at a WAN interface
- It supports the access of private networks such as VPDN, APN
- It supports IPSec, GRE(Generic Routing Encapsulation), IPIP, PPTP(Point to Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), and IPSec supports CA digital certificates
- It supports GRE over IPSec, IPSec over PPTP/L2TP/GRE/IPIP
- It supports the multi parameter and multifunction combination switchover functions independently researched and developed by Hongdian to realize the flexible and rapid communication switchover of multiple servers and the switchover of multiple operators on a single card
- It supports DHCP Server
- It supports GPS positioning functions (optional)
- It supports serial port DTU functions (the serial port supports two RS-232 ports as testing ports or data ports) (optional)
- It supports local, long distance, platform firmware upgrade
- It supports local, long distance platform patch upgrade
- It supports firmware upgraded by CFE (The upgrade method after the breakdown of file systems caused by abnormal conditions such as power failure for equipment during business processes such as upgrading, which has higher upgrade efficiency)
- It supports various parameter management methods such as WEB, CLI, SSH and platforms
- It supports M2M platform management, which can make the statistics of equipment flow and monitor the network status of equipment in real time
- It supports the backup and import of parameters and it supports the use of private keys to import or export parameter configurations
- It supports system upgrade and maintenance via USB interfaces
- It supports internal storage of equipment
- It supports DNS proxy and DDNS

- It supports NTP network timing
- It supports SNMP network management
- It supports the delivery local logs and remote logs of systems to realize network monitoring in real time
- It supports Qos (Quality of Service) (optional), and it can perform various types of QoS bandwidth intelligent management for business, protocols and IP network segments
- It supports static routing, RIPv2 (Routing Information Protocol) and OSPF (Open Shortest Path First) dynamic routing, source address strategy routing
- It supports fixed time management to effectively control online surfing flow and duration
- It supports data trigger online and off-line at fixed time or when data is idle
- It supports SMS, voice wakening online, offline and restarting
- It supports the link detection functions such as LCP (Link Control Protocol) detection, ICMP (Internet Control Message Protocol) detection to guarantee the stability and reliability of wireless network
- LED status monitoring (The status of power supply, system, 3G/4G network type and signal strength, etc. is displayed)
- It supports local and remote system running log functions to realize the monitoring of equipment operation in real time

1.4 Technical Indicators and Specifications

Interfaces

- | | |
|-------------------------------|---|
| ● Antenna interface: | 50Ω/SMA female connector |
| ● Serial data interface: | DB9 RS-232(DCE) |
| ● Serial data interface rate: | 115200bps |
| ● Ethernet interface: | 4 RJ45 exchange interfaces,10M/100MBase-T self-adaption |
| ● WAN interface: | 1 RJ45 exchange interface,10M/100MBase-T self-adaption |
| ● RESET interface: | Instant default recovery by pressing the button |

Power supply

- | | |
|------------------------------|--------------------------------|
| ● Voltage: | +9V ~ +36VDC |
| ● Average power consumption: | 170~450mA@12V DC (Dual Modems) |

Other parameters

- | | |
|--------------------------|------------------------|
| ● Net weight: | 400g (Dual Modems) |
| ● Operating temperature: | -30~+75°C |
| ● Storage temperature: | -40~+85°C |
| ● Relative humidity: | <95% (no condensation) |

2 Product Structure

About This Chapter

Section	Brief Introduction of Contents
2.1 Hardware Structure	The hardware structure of H8922S 3G/4G Router is briefly introduced in the section.
2.2 Functional Structure	The functional structure of H8922S 3G/4G Router is briefly introduced in the section.

2.1 Hardware Structure

2.1.1 Equipment appearance and dimension

External view

The actual appearance of Hongdian H8922S 3G/4G Router is as shown in Figure 2-1.

Figure 2-1 Picture of Actual Appearance of H8922S 3G/4G Router

Dimension

Table 2-1 Specification on Dimension of H8922S 3G/4G Router

Equipment name	L×W×H (mm)	Interface description
H8922S 3G/4G Router	191.5×110.4×24.5	<ul style="list-style-type: none">• 1 WAN interface: it is used for connecting Internet via cables• 1 serial port: it is used for serial port and DTU parameter testing• 4 LAN interfaces: they are used for connecting lower computers

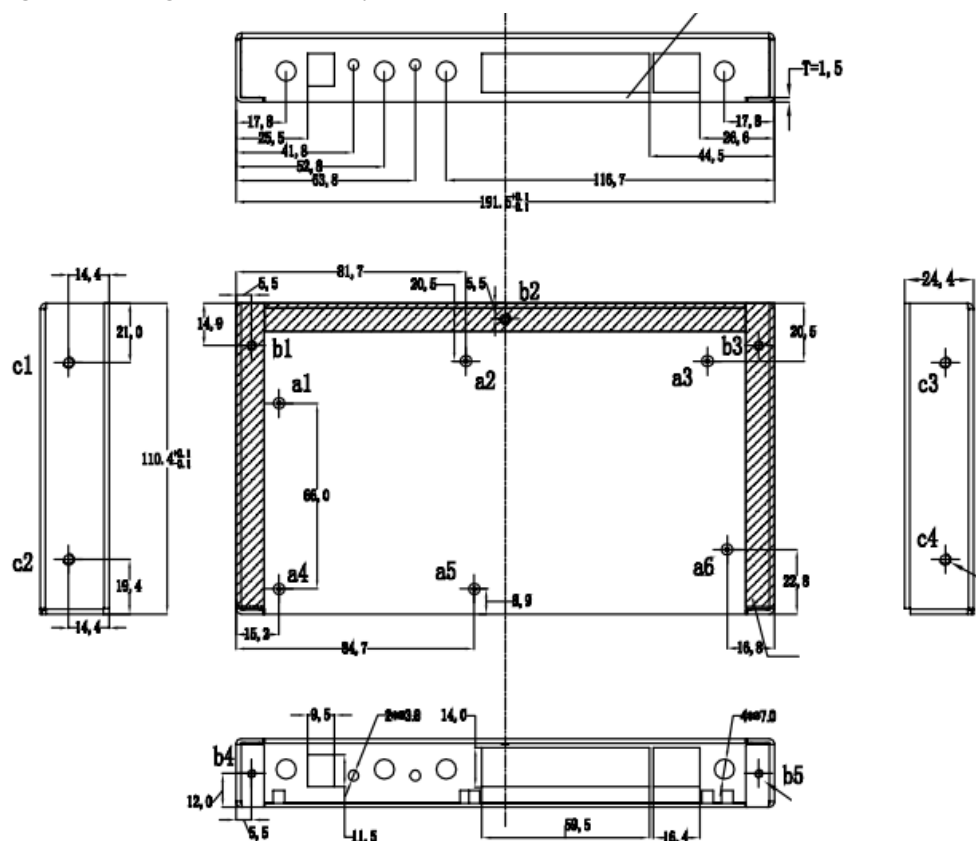
The overall structure and dimension of H8922S 3G/4G Router are as shown in Figure 2-2.



NOTE

In the following diagrams, the dimensions of corresponding objects are expressed in millimeter, and it will not be mentioned hereinafter.

Figure 2-2 Diagram of Lower Cap for H8922S 3G/4G Router



2.1.2 Equipment configuration and parts

Illustration of parts

H8922S 3G/4G Router includes the parts shown in Table 2-2.

Table 2-2 List of H8922S 3G/4G Router Parts

Part name	Quantity	Remarks
Standard configuration		
H8922S 3G/4G Router mainframe	1 piece	Packed as per the order of each customer
CD-ROM	1 piece	Operation manual, the quantity is configured as per the order of each customer
3G/4G antenna	1 piece	Corresponding antennae are equipped as per networks, 2 pieces of antennae are equipped for dual mode

Part name	Quantity	Remarks
WLAN antenna	1 piece	Equipped when WLAN function is available
GPS antenna	1 piece	Equipped when GPS function is available
RJ45 network cable	1 piece	No
Fixed part for installation	1 pair	No
Certificate of quality and warranty card	1 piece	No
+12V power adapter	1 piece	No

Illustration of model

H8922S 3G/4G Router is a wireless routing transmission product researched and developed on the basis of 3G/4G wireless communication technology (in the meantime, it supports wire transmission). It has full industrial grade design, electromagnetic compatibility design and modular design. It is applicable to the application requirements of various industries and the network environments of various operators.

2.2 Functional Structure

H8922S 3G/4G Router has dual modem and single mode plus WLAN, and its functional structures are as shown in Figure 2-3, Figure 2-4.

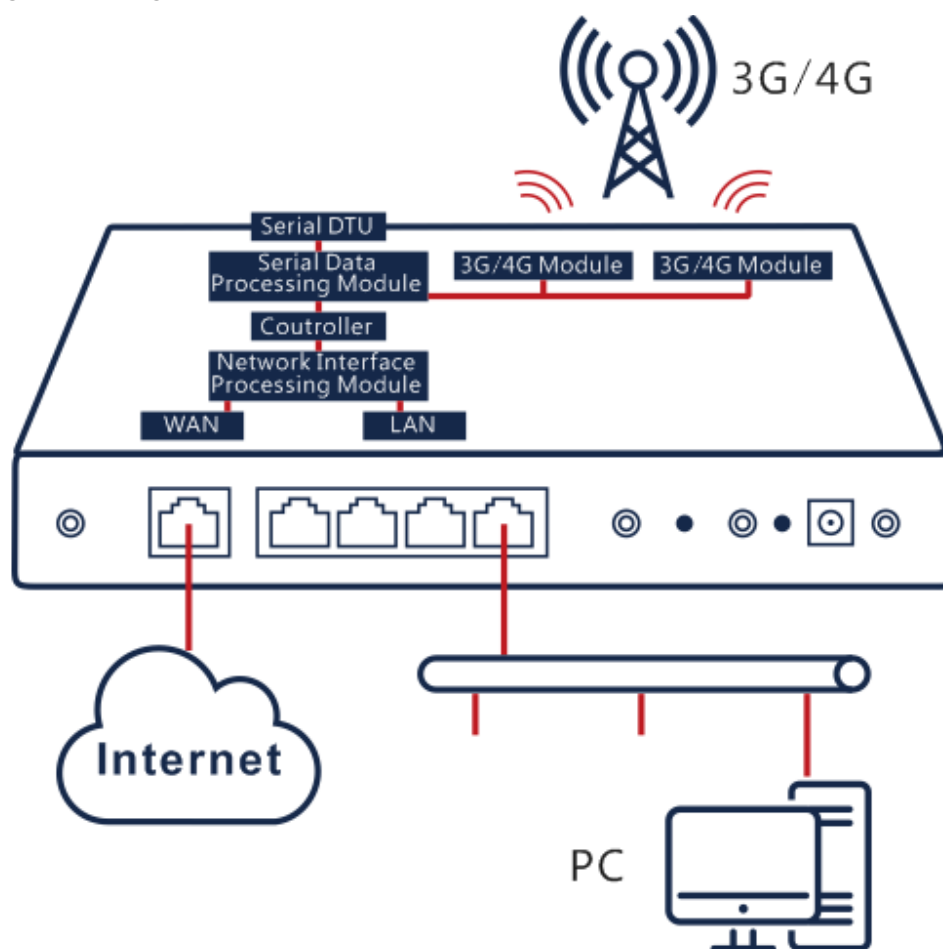
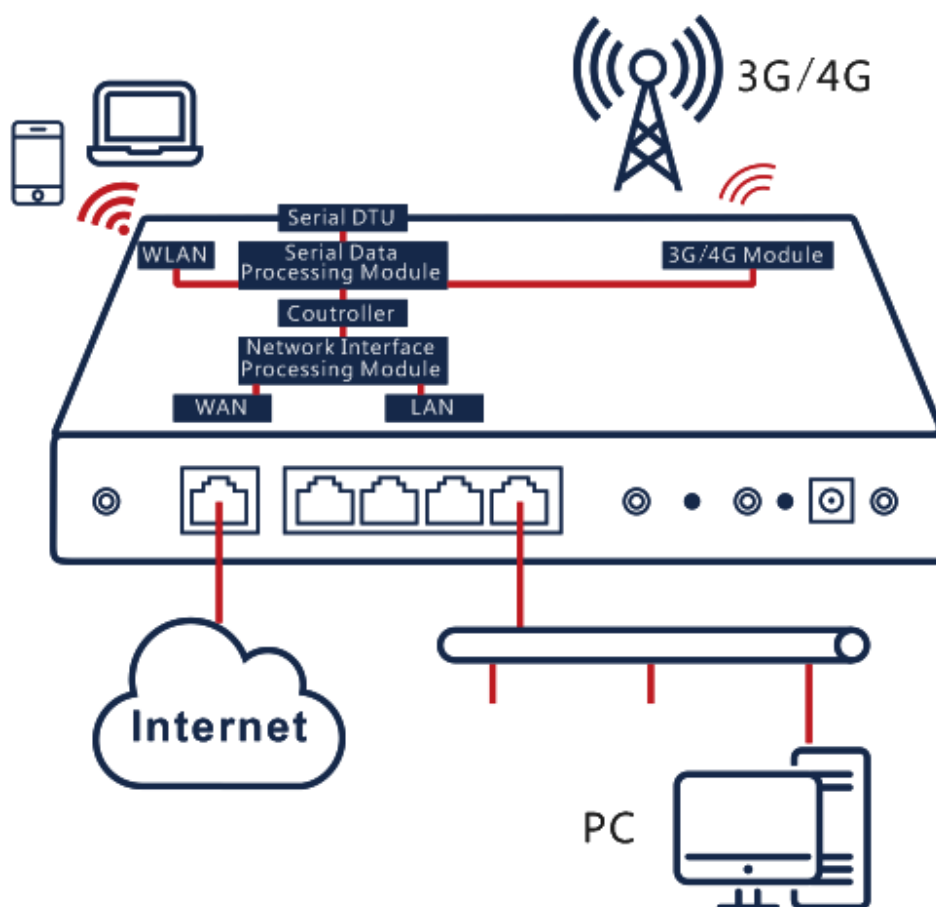
Figure 2-3 Diagram of Dual Modem Function Module

Figure 2-4 Diagram of Single Mode plus WLAN Functional Structure

Master controller module

The module mainly has the following functions:

- It controls 3G/4G module dial-up networking and offline
- It controls the wired connection between routers and Internet
- It transmits IP data packages
- It runs the advanced functions of routing protocols, firewall protocols, VPN protocols, etc.
- It maintains the normal operation of equipment

Serial port

It is mainly used for testing H8922S 3G/4G Router, including: configuration of all kinds of parameters, diagnosis of all types of problems of H8922S 3G/4G Router.

LAN

The internet access data processing module of the router communicates with a lower computer via RJ45 network cable to provide IP data packages forwarding function for the lower computer.

3G/4G module

The module is mainly used for realizing 3G/4G Internet access function so as to realize the forwarding of IP data on terminal products.

WAN

The module is mainly used to make H8922S 3G/4G Router be able to connect Internet via a wire.

WLAN

The module is mainly used for WLAN terminals to connect

- H8922S Wi-Fi hot spots so as to make such WLAN terminals connect external networks. In addition, it also supports two functional modes, bridging and client, to realize connection with other APPs so as to facilitate Internet surfing.

3 Installation of H8922S 3G/4G Router

About This Chapter

Section	Brief Introduction of Contents
3.1 Unpacking	The unpacking operation and the list of equipment to be checked for installation of H8922S 3G/4G Router are briefly introduced in the section.
3.2 Installation and Wiring	The installation of SIM/UIM cards, Ethernet connection, serial port line connection for H8922S 3G/4G Router are briefly introduced in the section.
3.3 Power Supply	The Power supply requirements and methods for H8922S 3G/4G Router are briefly introduced in the section.
3.4 Installation Inspection	The inspection after the installation of H8922S 3G/4G Router is briefly introduced in the section.

3.1 Unpacking

Upon arrival of the equipment, it is necessary to unpack the box and inspect whether the parts are complete. Generally speaking, the complete set of equipment shall include the parts shown in Table 2-2. The packing materials shall be properly kept for future use.

3.2 Installation and Wiring

3.2.1 Installation of SIM card

H8922S 3G/4G Router supports dual SIM card. In normal installation and usage, it is necessary to install a SIM card for two SIM slots respectively. The following content is the illustration of how to install a SIM card in the left-side SIM slot for the front panel.



Please guarantee that the router is off when installing a SIM card.

- Step 1** Use a sharp object to lightly press the button on the SIM card set to eject the set as shown in Figure 3-6.

Figure 3-1 Eject SIM Card Set



- Step 2** Make the SIM card metal face up and insert it into the set, with the unfilled corner end face outward. Then push the card set into the slot as shown in Figure 3-7.

Figure 3-2 Schematic Diagram of SIM Card Installation



---End

3.2.2 Ethernet cable connection

It is easy to use H8922S 3G/4G Router configuration: normal configuration management and data communication can be made via Ethernet cable connection. Ethernet connection can be divided into single equipment direct connection and multiple equipment local area network connection.

Single equipment direct connection

Use Ethernet cable with RJ-45 type connector to directly connect any of four exchange interfaces of H8922S 3G/4G Router with the relevant computer as shown below.

Figure 3-3 Single Equipment Direct Connection

Multiple equipment local area network connection

H8922S 3G/4G Router supports Ethernet switch functions, and it can simultaneously connect to multiple equipment for many LAN (such equipment may not be in the same network segment) as shown below.

Figure 3-4 Multiple Equipment Connection

3.2.3 Serial port line connection

When H8922S 3G/4G Router and a computer are in a joint test, a serial port extension cord shall be prepared; one end of the cord is connected to the serial port of the computer and the other end is connected to the serial port of the router.



The serial port is only for professionals to test the router.
Do not use other Internet access cable such as RJ45 network cable and insert it into the serial port to avoid some impacts on the router.

3.2.4 Ethernet cable connection

H8922S 3G/4G Router supports the LAN/QAN connection of four LAN interfaces and one WAN interface. RJ45 network cable can be used to insert one end into the LAN/WAN interface of the router, and insert the other end into any other equipment.

3.3 Power Supply

+5V~+36V direct current supply is used for H8922S 3G/4G Router

3.4 Installation Inspection

Before installation and power-on, the SIM card shall be pressed to inspect whether it is properly inserted. After power-on, the working status indicator of the router shall be inspected. The LAN interface will be bright as soon as power-on, and the RUN lamp will be bright a while later, which means that the system has been started and working normally.



CAUTION

An antenna must be connected before power-on to avoid the impedance mismatching of RF that causes unsuccessful dial-up and Internet access due to poor signals

Operating steps

- Step 1** Inspect whether the antenna is correctly connected.
- Step 2** Inspect whether the SIM card is correctly and properly installed and confirm whether the SIM card is valid.
- Step 3** Provide power supply for H8922S 3G/4G Router. The following content is about the router dialing of the left-side SIM card, and it is the same for the right-side SIM card.
- After providing power supply, it means that the power supply for the router is normal in case the LAN interface lamp of H8922S 3G/4G Router connected with a lower computer is bright.
 - After a certain period, it means the router system is started in case the RUN indicator lamp of the router is bright.
 - After the RUN indicator lamp is bright for a while, it means that the router has found the module and started dialing in case the NET indicator lamp is bright and flashing quickly.
 - During the dialing process, the SIG lamp will be bright, which means that the router has acquired the signal strength of the SIM card, and the network signal strength can be judged as per the flashing condition of the SIG lamp. See “4.1 Terminal Panel Indicator Lamp Status” for details.
 - Upon the completion of router dialing, in case the 3G/4G lamp is normally on, it means that the connected network is 3G/4G. In case it is flashing slowly, it means that the connected network is 2G/2.5G/2.75G.



NOTE

For different modules, the durations for the router to find all modules are various; in addition, the durations for dialing are various due to different networks. Therefore, for different modules, the durations of router dialing and acquiring IP addresses may vary. However, the router dialing process is exactly as specified above.

---End

4 Preparation before Configuration

About This Chapter

Section	Brief Introduction of Contents
4.1 Terminal Panel Indicator Lamp Status	The terminal panel indicator lamp status of H8922S 3G/4G Router is briefly introduced in the section.
4.2 Local Connection Configuration	The local connection configuration process after installing H8922S 3G/4G Router is briefly introduced in the section.

4.1 Terminal Panel Indicator Lamp Status

There are 12 LED indicator lamps in the front panel of H8922S 3G/4G Router to indicate the working conditions and network conditions of H8922S 3G/4G Router. The illustration of indicator lamp status is as shown in Table 4-1.

Table 4-1 Table of Illustration of Indicator Lamps

Indicator lamp name	Status description
RUN	<ul style="list-style-type: none"> • Normally on: the system is started and working normally • Off: the system is not completely started (within 10 seconds after power-on or during restarting)
WAN	<ul style="list-style-type: none"> • Normally on: the connection of interfaces and other equipment via network cable is normal • Flashing: any interface has data sending and transmission • Off: no network cable is inserted or the connection of interfaces and other equipment via network cable is abnormal
LAN1~4	<ul style="list-style-type: none"> • Same as the status for WAN
SIG1~2	<ul style="list-style-type: none"> • Normally on: the signal strength is good, 21~31 • Quick flashing (0.5s flashing): the signal strength is medium,

Indicator lamp name	Status description
	11~20 • Slow flashing (2s flashing): the signal strength is poor, 1~10 • Off: no signal
3G/4G1~2	• Normally on: the dialing is successful and 3G/4G network is connected • Slow flashing (0.5s flashing): the dialing is successful and 2G/2.5G/2.75G network is connected • Quick flashing (2s flashing): in process of dialing • Off: fail to find any module or dialing is forbidden
WLAN	• It is bright when Wi-Fi function of the router is enabled and it is off when the Wi-Fi function is shut off.
DATA	• It is bright when the router is connected with GPS and it is off when GPS is disconnected.

4.2 Local Connection Configuration

Precondition

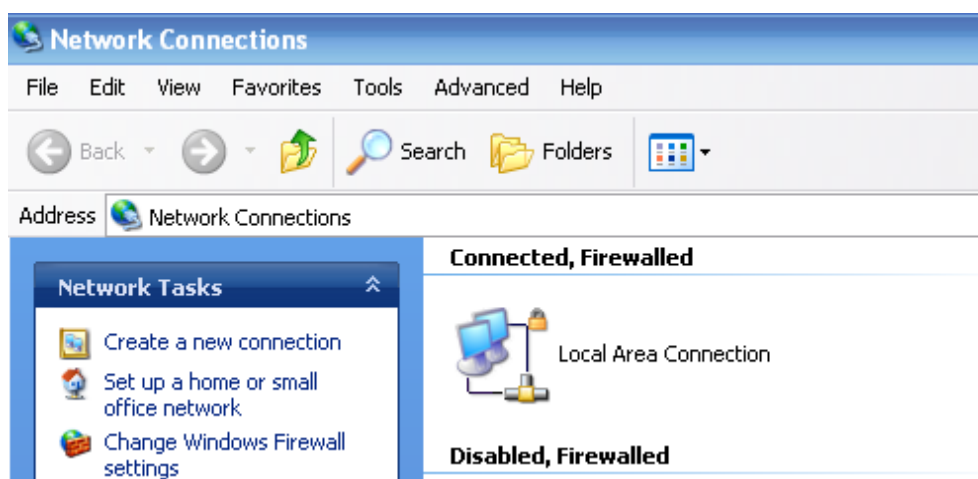
- Already power on H8922S 3G/4G router
- Ethernet cable connect to H8922S 3G/4G router

You could specify a static IP or DHCP get IP for your computer.

Static IP

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

Figure 4-1 Local Area Connection



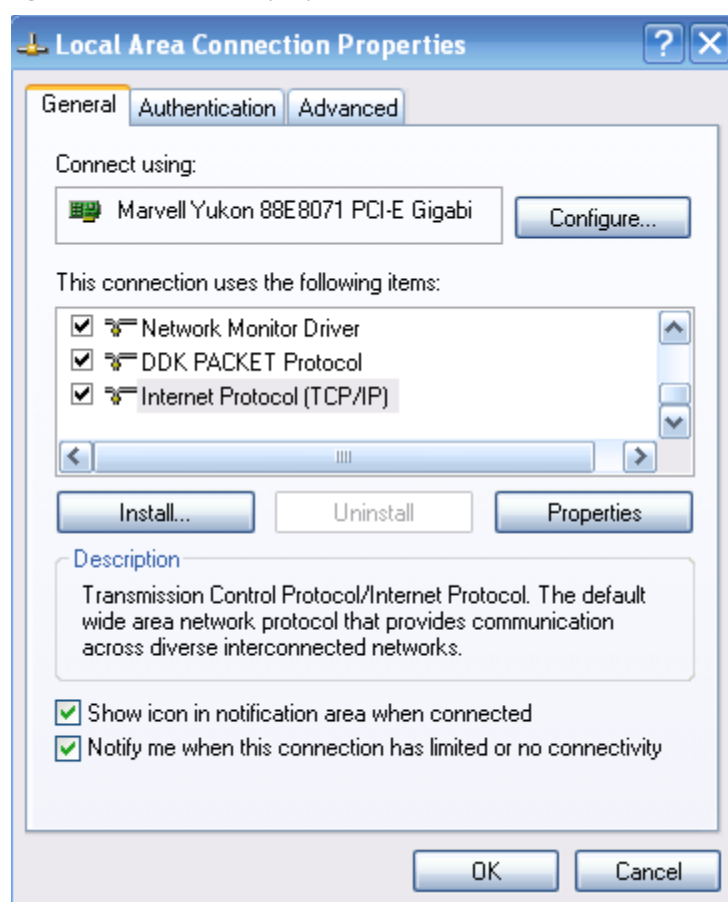
Step 2 Obtain a IP address automatically, or follow below instruction.

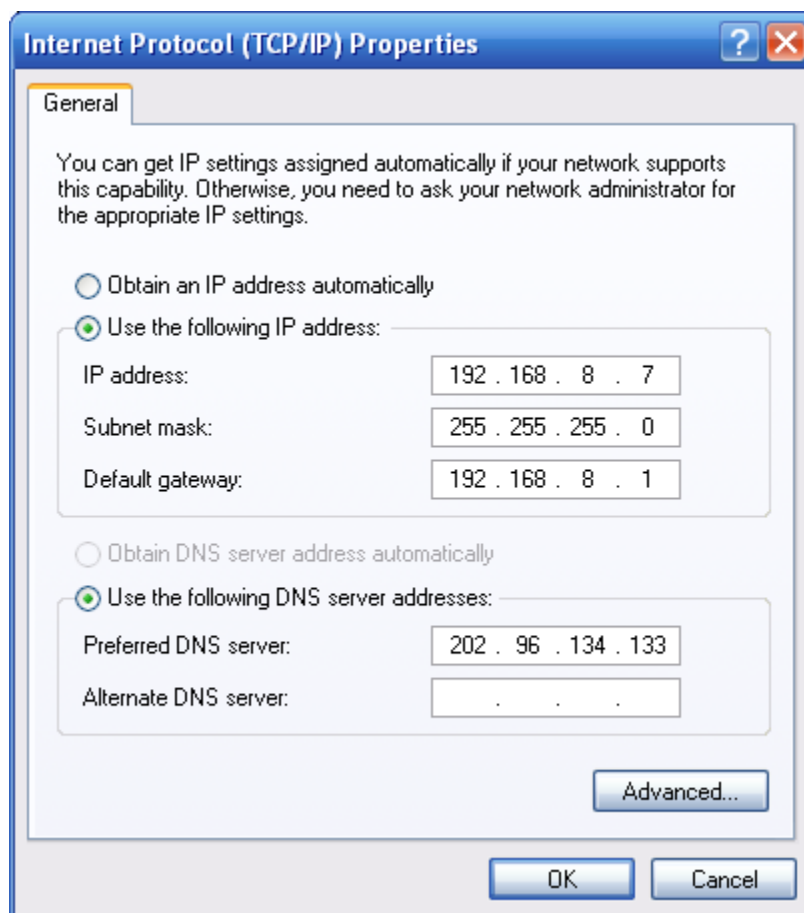


NOTE

H8922S 3G/4G Router default enabled DHCP server. If it has been disabled, DHCP cannot be use .

Step 3 Change or add a IP 192.168.8.* on your computer.

Figure 4-2 Connection properties**Figure 4-3** Internet protocol (TCP/IP)



You could change your IP address or add a IP address in Advanced setting.

- General configuration

This method will temporarily interrupt the communication between the computer under configuration and LAN, and the specific parameter configuration is shown as below:

IP address: 192.168.8.* (*indicates any integral between 2 to 254)

Subnet mask: 255.255.255.0

Default gateway: 192.168.8.1

Remember:

H8922S 3G/4G Router LAN port factory default parameter:

IP address: 192.168.8.1

Subnet mask: 255.255.255.0

H8922S 3G/4G Router factory default login parameter:

Management interface login IP address: 192.168.8.1

Login name: admin

Login password: admin

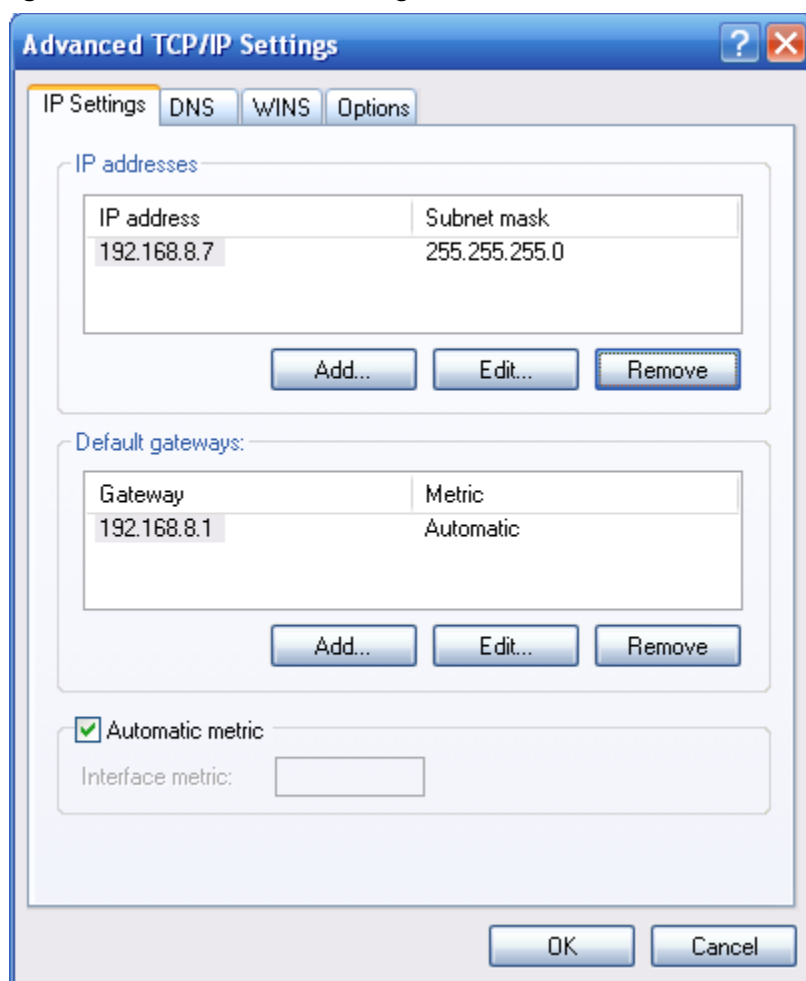
- Advanced configuration

If you don't want to interrupt local PC LAN communication and configure H8922S 3G/4G Router when the former network configuration exists, it is required add route (IP).

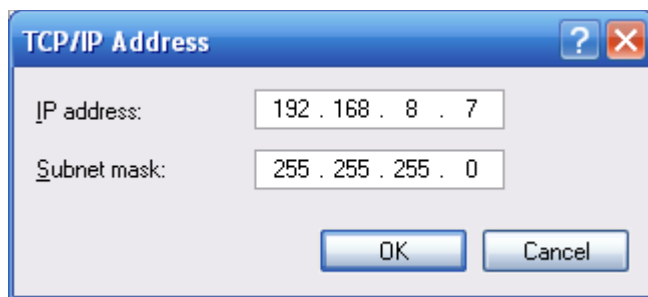
The configuration operation is shown as below:

Click the "Advanced..." button to enter the interface as below:

Figure 4-4 Advanced TCP/IP Settings



Click the "Add (A)" button under the "IP address (R)", and fill in the IP address that you want to add:

Figure 4-5 TCP/IP address

After the configuration is completed, click the “Add”. By now the computer has a route to router H8922S.

Note:

“Default gateway” depends on whether the configuration computer connects with Internet through original local network configuration. If Internet is accessed through original local network, the default gateway setting does not need to be modified; if H8922S 3G/4G Router is used, you need to modify the default gateway and configure it as H8922S 3G/4G Router’s default LAN IP address 192.168.8.1.

---END

Network Check

Step 1 IP configuration check

Use the command of ipconfig to check whether the IP address is correctly set or added. You can enter DOS mode and key-in command: ipconfig, for instance:

```
C:\>ipconfig
```

Windows IP Configuration

Ethernet adapter local connection:

Connection-specific DNS Suffix.:

Auto configuration IP Address . . . : 192.168.8.7

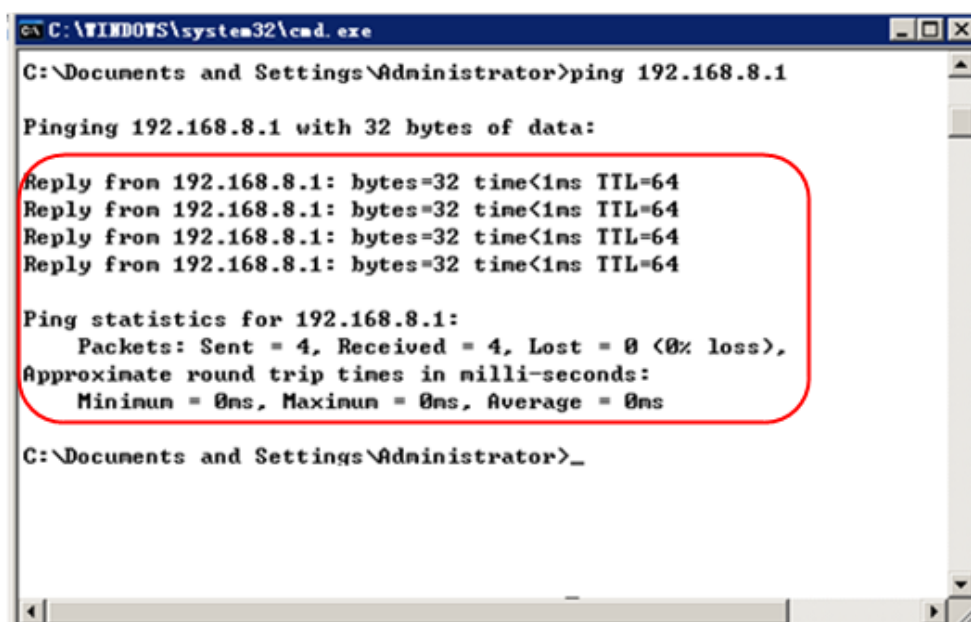
Subnet Mask : 255.255.255.0

Default Gateway : 192.168.8.1

Step 2 Connectivity check

After the configuration is completed, you can check the connectivity between it and Galaxy H8922S 3G/4G router by ping command. Key-in ping command in system command line:

Figure 4-6 Connectivity check



By now, it means that the configuration computer has been connected to the router. You can carry out configuration operation on it.

---END

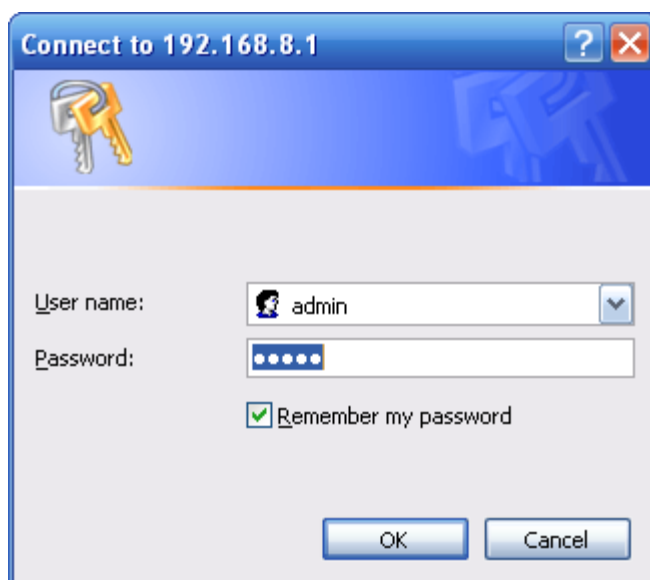
4.3 Basic configuration

Through this chapter, you could achieve basic function: visit internet.

4.3.1 Login WEB GUI

Step 1 Run a Internet Explorer and visit “<http://192.168.8.1/>”, to enter identity page.

Figure 4-7 User identity page



Step 2 User should use default user name and password when log in for the first time:

Step 3 User name: admin

Step 4 Password: admin

---END

5 Router Configuration

About this chapter

Chapter	Content
5.1 Overview	Enter H8922S 3G/4G Router WEB GUI to configure
5.2 Network configuration	Network configuration & function
5.3 Application	Advanced function of router like timing operation, link backup .etc.
5.4 Security	Security setting of H8922S
5.5 Forward	NAT & DMZ setting
5.6 VPN	PPTP, L2TP, IPSec & GRE setting
5.7 System	Updating & maintain
5.8 Status	Router working status

5.1 Overview

H8922S 3G/4G router adopts WEB GUI to configure, all parameter can be modified by this GUI, and it is easy to understand.

5.2 Network configuration

Network connection configuration, including LAN, WAN, cellular network, Wi-Fi(optional), parameter switch, DHCP setting and so on.

5.2.1 LAN

LAN setting used to manage local area network PC which connect to H8922S, make them could visit internet and the network segment connectivity normal.

Step 1 Login H8922S WEB GUI.

Step 2 Single click “Network > LAN”.

Figure 5-1 LAN window

Step 3 LAN parameter.

Table 5-1 LAN Parameter instruction

Parameter	Details	Operation
Host name	router name	Manual input, Maximum length limited to 32 word type character
IP1~4	Divide sub-network, those sub-net could communicate	Manual input Format: A.B.C.D/Mask IP1 default: 192.168.8.1/24
Loopback address	Use for network test, e.g. tunnel test, it won't shutdown with the LAN interface closed	Ping IP address from peer of tunnel

Step 4 Single click “save” icon, done.



After change the LAN IP, if page has no response anymore, please make sure your PC address is in the same network segment, or set a new IP to your PC to insure that.

---END

5.2.2 WAN

Wired connect to Internet by static IP, DHCP or PPPoE.

Step 1 Login H8922S WEB GUI.

Step 2 Single click "network > WAN".

Figure 5-2 WAN window

Step 3 WAN connection type.

Table 5-2 WAN connection type parameter instruction

Parameter	Details	Operation
Connection Type	WAN Connection Type	Dropdown List Selection: <ul style="list-style-type: none"> Static IP: Manual set WAN IP, if set static IP, need manual set gateway, DNS etc. DHCP: DHCP get IP address PPPoE: PPPoE dial to get IP, usually you need connect to a ADSL modem
"Connection Type" select "Static IP"		
IP	Configure the static IP	Manual input Format: A.B.C.D/Mask IP1 default: 192.168.10.1/24
"Connection Type" select "DHCP"		
IP	get IP address from DHCP	Select DHCP

Parameter	Details	Operation
"Connection Type" select "PPPoE"		
Service Name	Configure PPPoE service name, which is usually used for identification and judgment between client and server, and is usually provided by the service side, while ADSL dial-up provided by your ISP	WORD type, up to 64 characters, not blank, please refer to parameters regulation format
Username/Password	PPPoE dial-up user name/password usually provided by the server	WORD type/CODE type, up to 64 characters, not blank, please refer to parameters regulation format
Advanced Settings	Advanced parameters are used in special circumstances, and are generally not recommended for configuration. For the parameters instructions of the "Advanced Settings", please refer to the related parameters in table 5-2	Single click "Display" icon show advanced settings parameters
Authentication (need match server end, default auto-negotiation)		
CHAP	Challenge-Handshake Authentication Protocol, a way to send real password when build ppp link, improved security	<ul style="list-style-type: none"> • Disable • Negotiation CHAP is prior to PAP
PAP	Password Authentication Protocol	<ul style="list-style-type: none"> • Disable • Negotiation
MS-CHAP	MS-CHAP Microsoft Challenge-Handshake Authentication Protocol Based on MPPE	<ul style="list-style-type: none"> • Disable • Negotiation
MS2-CHAP	MS-CHAP second version	<ul style="list-style-type: none"> • Disable • Negotiation
EAP	PPP Extensible Authentication Protocol	<ul style="list-style-type: none"> • Disable • Negotiation
Compress (need match server end, default disable)		

Parameter	Details	Operation
Compression Control Protocol	Negotiate which compress control protocol used on PPP link	<ul style="list-style-type: none"> • Disable • Negotiation
Address/Control Compression	Whether compress IP address	<ul style="list-style-type: none"> • Disable • Negotiation
Protocol Field Compression	Whether compress Whether compress IP address	<ul style="list-style-type: none"> • Disable • Negotiation
VJ TCP/IP Header Compress	Whether allow TCP/IP to communicate by compressing VJ	<ul style="list-style-type: none"> • Disable • Negotiation
Connection-ID Compression	Whether allow TCP/IP to communicate by compressing ID in the first	<ul style="list-style-type: none"> • Disable • Negotiation
More		
Debug	Enable PPP dialing log, default value is enable, in order to check more info about dialing, suggest no changing	<ul style="list-style-type: none"> • Disable • Negotiation
Peer's DNS	Auto get peer DNS when PPP dialing. DNS is necessary if want visit domain name. In order to forbid LAN pc visit domain name, you may disable it	<ul style="list-style-type: none"> • Disable • Negotiation
LCP interval/Retry	After PPP dialing succeed, LCP is needed to keep PPP link alive. Also it could be used to quickly spot network interrupt and reconnect	Value area : 1~512 Unit: second Default value: 30/5
MTU	the number of bytes of the maximum transfer unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
MRU	the number of bytes of the maximum receive unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
Local IP	Set the local IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.1
Remote IP	Set the remote IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.254
Professional	<ul style="list-style-type: none"> • nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp 	Do not suggest modify, please contact us for help if necessary

Parameter	Details	Operation
	• default-asyncmap	

Step 4 Single click “save” icon.

---END

5.2.3 Modem

H8922S 3G/4G Router core function, connect Internet by cellular modem, H8922S 3G/4G Router support single modem single SIM, single modem dual SIM, dual modem dual SIM, those three working type provide internet connection to customers. Usually 3G network bandwidth is 1~5Mbps, 3.5G up to 20Mbps and LTE up to 100Mbps.

Step 1 Login H8922S WEB GUI.

Step 2 Single click “network > Modem”.

Figure 5-3 Modem window

The screenshot displays the 'Modem' configuration window in the H8922S WEB GUI. The top navigation bar includes 'Network', 'Applications', 'VPN', 'Forward', 'Security', 'System', and 'Status'. The 'Network' section is expanded, showing 'LAN', 'WAN', and 'Modem'. The 'Modem' section is further expanded, showing 'Parameter Select', 'Connection Type', 'Link Backup', and 'DHCP Server'. Below this, there are two sections for 'modem1' and 'modem2'. Each section contains a table with columns: Interface Name, APN, Service Code, Username, Simcard, and Operation. For 'modem1', the Interface Name is '0', APN is '---', Service Code is '---', Username is 'card', and Simcard is '---'. For 'modem2', the Interface Name is '2', APN is '---', Service Code is '---', Username is 'card', and Simcard is '---'. The Operation column for both modems contains buttons: 'Mod', 'Del', 'En', and 'Dis'. At the bottom of the window, there are 'Add' and 'Refresh' buttons.

Step 3 Operation:

- add
 1. Single click “add”, and the page shows as below.

Figure 5-4 Modem page

2. Input suitable parameter.

Table 5-3 “Modem” Parameter instruction

Parameter	Details	Operation
Auto-dialup	<ul style="list-style-type: none"> Auto-dialup current modem, if all modem auto-dialup disabled, router will not auto-dialup 	<ul style="list-style-type: none"> Enable Disable
Module type	<ul style="list-style-type: none"> If your router has dual cellular module inside, you could choose which module to use here. 	Dropdown List <ul style="list-style-type: none"> modem modem2 If your router has only one module, no such option.
Interface Name	Interface name, to identify this interface	WORD type, up to 12 characters
APN	APN, provided by local ISP, usually CDMA/EVDO network do not need this parameter	WORD type, up to 64 bytes
Service code	Usually *99***1#, CDMA/EVDO: #777	CODE type, up to 64 bytes
Username/Password	Provided by ISP	WORD type/CODE type, up to 64 bytes
SIM	Only Single module dual SIM router has this option, used to select SIM card	<ul style="list-style-type: none"> SIM1 SIM2

Parameter	Details	Operation
Network type	<ul style="list-style-type: none"> Network type force to 2.5G or 3G/4G 	Dropdown List WCDMA: <ul style="list-style-type: none"> auto wcdma edge EVDO: <ul style="list-style-type: none"> auto evdo cdma For the LTE or HSPA+ module, its network type is not mandatory: selecting "3G" means using 3G or 4G adaptively; selecting "AUTO" means using 2.5G/3G/4G auto (priority is 4G>3G>2.5G)
Advance Setting	<ul style="list-style-type: none"> PPP process advanced parameter, do not suggest to modify the setting. If necessary, contact us for support 	Single click to show advanced setting
Authentication (need match server end, default auto-negotiation)		
CHAP	Challenge-Handshake Authentication Protocol, a way to send real password when build ppp link, improved security	<ul style="list-style-type: none"> Disable Negotiation CHAP is prior to PAP
PAP	Password Authentication Protocol	<ul style="list-style-type: none"> Disable Negotiation
MS-CHAP	MS-CHAP Microsoft Challenge-Handshake Authentication Protocol Based on MPPE	<ul style="list-style-type: none"> Disable Negotiation
MS2-CHAP	MS-CHAP second version	<ul style="list-style-type: none"> Disable Negotiation
EAP	PPP Extensible Authentication Protocol	<ul style="list-style-type: none"> Disable Negotiation
Compress (need match server end, default disable)		
Compression Control Protocol	Negotiate which compress control protocol used on PPP link	<ul style="list-style-type: none"> Disable Negotiation

Parameter	Details	Operation
Address/Control Compression	Whether compress IP address	<ul style="list-style-type: none"> • Disable • Negotiation
Protocol Field Compression	Whether compress Whether compress IP address	<ul style="list-style-type: none"> • Disable • Negotiation
VJ TCP/IP Header Compress	Whether allow TCP/IP to communicate by compressing VJ	<ul style="list-style-type: none"> • Disable • Negotiation
Connection-ID Compression	Whether allow TCP/IP to communicate by compressing ID in the first	<ul style="list-style-type: none"> • Disable • Negotiation
More		
Debug	Enable PPP dialing log, default value is enable, in order to check more info about dialing, suggest no changing	<ul style="list-style-type: none"> • Disable • Negotiation
Peer's DNS	Auto get peer DNS when PPP dialing. DNS is necessary if want visit domain name. In order to forbid LAN pc visit domain name, you may disable it	<ul style="list-style-type: none"> • Disable • Negotiation
LCP interval/Retry	After PPP dialing succeed, LCP is needed to keep PPP link alive. Also it could be used to quickly spot network interrupt and reconnect	Value area : 1~512 Unit: second Default value: 30/5
MTU	the number of bytes of the maximum transfer unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
MRU	the number of bytes of the maximum receive unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
Local IP	Set the local IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.1
Remote IP	Set the remote IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.254
Professional	<ul style="list-style-type: none"> • nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp • default-asynmap 	Do not suggest modify, please contact us for help if necessary

Figure 5-5 Single module single SIM/dual module dual SIM

Auto-Dialup

Basic Settings

Interface Name * Max length is 12

Module Type

APN Max length is 64

Service Code Max length is 64

Username Max length is 64

Password Max length is 64

Network Type

Advanced Settings

Figure 5-6 Single module dual SIM

Auto-Dialup

Basic Settings

Interface Name * Max length is 12

APN Max length is 64

Service Code Max length is 64

Username Max length is 64

Password Max length is 64

PIN Max length is 64

Network Type

Simcard ☒ SIM1 ☐ SIM2

Advanced Settings

Figure 5-7 Advanced setting

Authentication	
CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
PAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
MS-CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
MS2-CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
EAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable

Compress	
Compression Control Protocol	<input type="radio"/> Require <input checked="" type="radio"/> Disable
Address/Control Compression	<input type="radio"/> Require <input checked="" type="radio"/> Disable
Protocol Field Compression	<input type="radio"/> Require <input checked="" type="radio"/> Disable
VJ TCP/IP Header Compress	<input type="radio"/> Require <input checked="" type="radio"/> Disable
Connection-ID Compression	<input type="radio"/> Require <input checked="" type="radio"/> Disable

More	
Debug	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Peer's DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LCP Interval	<input type="text" value="30"/> 1-512 s
LCP Retry	<input type="text" value="5"/> 1-512 times
MTU	<input type="text"/> 128-16384 B
MRU	<input type="text"/> 128-16384 B
Local IP	<input type="text"/> eg. 192.168.8.1
Remote IP	<input type="text"/> eg. 192.168.8.254

Professional	
<p>nomppe: Disable Microsoft Point to Point Encryption.</p> <p>mppe required: Enable Stateful Microsoft Point to Point Encryption.</p> <p>mppe stateless: Enable Stateless Microsoft Point to Point Encryption.</p> <p>nodeflate: Disable Deflate compression entirely.</p> <p>nobsdcomp: Disables BSD-Compress compression.</p> <p>default-asyncmap: Disable asyncmap negotiation.</p>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

3. Single click "save" icon to finish.



NOTE

Grey icon means enabled.

---END

5.2.4 WLAN

H8922S 3G/4G Router provides WLAN AP, Station Client, Repeater three functions, through AP function, H8922S 3G/4G Router can provide wireless LAN hotspots; through Station client function, it allows H8922S 3G/4G Router access to other AP devices, such as H8922S 3G/4G Router downlink machine can access the Internet via the AP connection; Repeater functionality can be other AP WLAN signal amplification device, to achieve WLAN signal repeater, so the clients far away from the AP WLAN can access the AP.

- Step 1** Login H8922S WEB GUI.
- Step 2** Single click “Network > WLAN”.
- Step 3** Open “WLAN” tag, when you select a different WLAN mode (AP, Station, Repeater), respectively, display the page shown in Figure 5-19, Figure 5-20, Figure 5-21. When the WLAN mode select Station and Repeater, need to scan the surrounding AP, an AP access to select, shown in Figure 5-22.

Figure 5-8 AP mode configure interface

The screenshot displays the Web GUI configuration page for the WLAN AP mode. The interface includes a top navigation bar with tabs for Network, Applications, VPN, Forward, Security, System, and Status. Below this is a sub-navigation bar with tabs for LAN, WAN, WLAN (selected), Modem, Parameter Select, Network Type, Link Backup, and DHCP Server. The main content area is divided into several sections:

- WLAN Status:** A section with a toggle switch for "WLAN Status" currently set to "Enable".
- Basic Settings:** A section containing several configuration options:
 - SSID:** A text input field containing "admin" with a red asterisk indicating a maximum length of 32.
 - Wireless Mode:** A dropdown menu set to "ap".
 - Network Mode:** A dropdown menu set to "bgn".
 - Channel:** A dropdown menu set to "auto".
 - Bandwidth:** A dropdown menu set to "20mhz".
 - AP Isolate:** Radio buttons for "Enable" and "Disable", with "Disable" selected.
 - Broadcast Status:** Radio buttons for "Enable" and "Disable", with "Enable" selected.
- Encryption Settings:** A section containing:
 - Security Mode:** A dropdown menu set to "wep".
 - Encryption:** A dropdown menu set to "5 bits ascii".
 - WEP Shared Key:** A text input field containing "admin" with a red asterisk.

At the bottom of the page, there are two buttons: "Save" and "Refresh".

Figure 5-9 Station mode configure interface

The screenshot shows the 'Station mode configure interface' with a top navigation bar containing tabs: LAN, WAN, WLAN, Modem, Parameter Select, Network Type, Link Backup, and DHCP Server. The 'WLAN' tab is selected. Below the tabs, there is a 'WLAN Status' section with 'Enable' and 'Disable' buttons. The 'Basic Settings' section includes: SSID (text input 'admin', note '* Max length is 32'), Wireless Mode (dropdown 'station', 'Scan' button), Network Mode (dropdown 'bgn'), and IP Distribution (dropdown 'dhcp'). The 'Encryption Settings' section includes: Security Mode (dropdown 'wep') and WEP Shared Key (text input 'admin', note '*'). At the bottom are 'Save' and 'Refresh' buttons.

Figure 5-10 Station scan signal interface

The screenshot shows the 'Station scan signal interface'. It features a table titled 'Access Points' with the following data:

ID	BSSID	SSID	Channel	Quality	Bit Rates	Authentication	Encrypt	Operation
0	5C:0E:8B:92:18:82	CMCC-AUTO	3	-88	12	wpa2	tkip	Connect
1	60:C5:A8:00:37:00	9797168.com	1	-82	12	open	none	Connect
2	D6:CA:6D:A4:D2:E2	HDWIFI	5	-88	12	wpa2	aes	Connect

At the bottom of the interface are 'Return' and 'Refresh' buttons.

Step 4 “WLAN” configure parameter instruction, parameter instruction as Table 5-4.

Table 5-4 WLAN parameter instruction

Parameter	Details	Operation
WLAN Status	Enable or disable WLAN feature	Dropdown List <ul style="list-style-type: none"> • Enable • Disable

Parameter	Details	Operation
Basic Setting		
SSID	WLAN server identity	WORD type, max to 32Bytes
Wireless Mode	<ul style="list-style-type: none"> WLAN work mode, support ap/station 	Dropdown List <ul style="list-style-type: none"> ap station
Network Mode	WLAN network mode, different network models are quite different transmission rates, default bgn mixed mode. When operating mode is selected AP, the AP needs to manually set the network mode; When working mode selection station or repeater, AP network mode for the selected network mode, can not be modified manually.	Dropdown List <ul style="list-style-type: none"> n represents the network rate is 150Mbps bgn represents the network rate is 11Mbps,54Mbps(Auto-Negotiation) bgn can support 11Mbps, 54Mbps,150Mbps mixed mode (auto adapt according to the client)
Channel	WLAN work channel, configure according to the specific needs of the network environment, the default value is auto.	Dropdown List <ul style="list-style-type: none"> auto 1~13 auto shows when there is no interference, the default channel is 6, when the same channel interference occur, it can automatically jump out interfere to work with the smaller channel
Bandwidth	Bandwidth configure when WLAN work at 802.11n	Dropdown List <ul style="list-style-type: none"> 20MHz 40MHz 40MHz represents high speed mode
AP Isolate	AP isolate the WLAN client, so the WLAN client can not access each other	Dropdown List <ul style="list-style-type: none"> Enable Disable
Broadcast Status	Used to configure the WLAN SSID is broadcasted so that clients can search the SSID, usually do not want other people to search and disable WLAN function, disable it means hidden SSID function in a network environment, users want to connect, you need to	Dropdown List <ul style="list-style-type: none"> Enable Disable

Parameter	Details	Operation
	manually add the SSID	
IP Distribution (when Wireless Mode is station)	The router is used as station, and the router can get the IP address when it is connected to AP	Dropdown List <ul style="list-style-type: none"> • dhcp: get IP address from DHCP • static: manually set IP address
IP (when Wireless Mode is station)	The router get an IP in correspondence with AP when it is station	Manual input Format: A.B.C.D/Mask
BSSID (when Wireless Mode is repeater)	MAC which the router select AP	WORD type MAC format: XX:XX:XX:XX:XX:XX You can manually set MAC depending on the selected AP
WLAN Encryption		
Security Mode	Configure the WLAN encryption, when encrypted authentication is not required, it can disable. WEP encryption is relatively easy to crack, we recommend using WPA encryption	Dropdown List <ul style="list-style-type: none"> • wep • disable • wpa • wpa2
WEP Encryption (Wired Equivalent Privacy)		
Encryption	WLAN password format <ul style="list-style-type: none"> • 5 bits ASCII • 13 bits ASCII • 10 bits hex digits • 26 bits hex digits 	Dropdown List
WEP shared key	Password connected to WLAN	Configure according to the previous "Encryption" result
wpa/wpa2 (WiFi Protected Access)		
Algorithms	Encryption algorithms <ul style="list-style-type: none"> • tkip • aes 	Dropdown List
WPA Share Key	WLAN encryption key, used to connect the specified SSID	WORD or Number type, refer to "Parameter Specification Table"
WPA Renewal Interval	WLAN client verification interval; If authentication passes, it continues to be a	Value area: 120-86400 Units: Seconds

Parameter	Details	Operation
	WLAN connection, if authentication fails, disconnect the WLAN connection	



When the working mode select station or repeater, H8922S Router will automatically match according to the selected AP and the corresponding encryption algorithm (to keep consistent with AP encryption); shared key update interval is required to fill in the connections of AP key and interval.

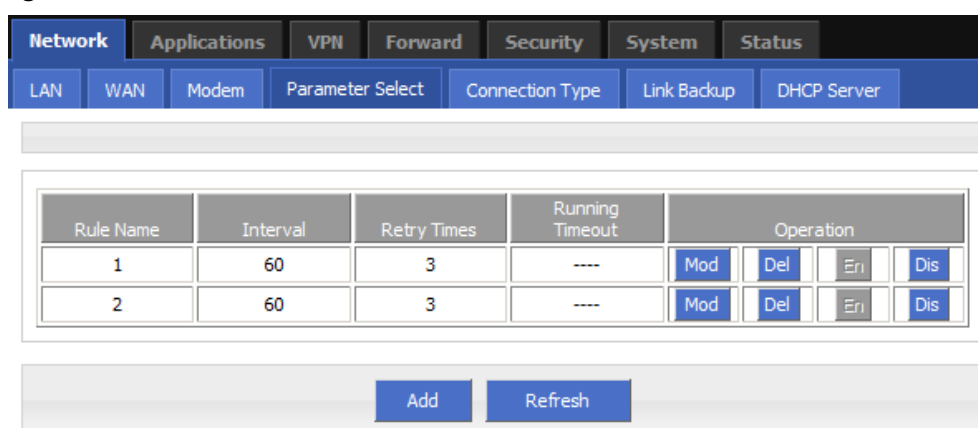
---END

5.2.5 Parameter select (Recommend to Single module dual SIM version)

Router parameter select function is used for multi-function switch, like VPN parameter switch, SIM parameter switch, multi-sever switch etc. You could pre-config several network parameter and switch between them, to achieve multiple Telecom operator backup. This function also could switch VPN setting, for example, when modem 1 online it connects VPN 1, modem 2 online it connects VPN server, they cannot connect at same time because conflict, by this function you could easily switch when network failure.

- Step 1** Login H8922S WEB GUI.
- Step 2** Single click "Network > parameter select".

Figure 5-11 Parameter select



- Step 3** Add, modify, del, enable and disable the parameter select rule.
- add

Figure 5-12 Add rule

Table 5-5 Parameter instruction

Parameter	Details	Operation
Status	For enabled rule: Only one rule is running at one time, when it checks failed, next rule start running For disabled rule: all related interface also disabled	<ul style="list-style-type: none"> • Enable • Disable
Basic settings		
Rule name	Name value decided running order	Value area : [0,9]
Interval/Retry Times	Check interval and retry time, if all check failed, switch to next rule	Value area : 1~512 Units: seconds/time Default: 60/3
Running timeout	<ul style="list-style-type: none"> • Not available for rule 0 • This parameter restrict current rule running time, when timeout, switch to rule0, if do not set, switch to next rule 	Value area : 1~65535 Units: seconds
Select a interface to check		

Parameter	Details	Operation
Interface name	Set related modem interface	Dropdown List to choose, current available option will show below
Check method	If state, router will check link state If ICMP, router will ping the ICMP IP address to check	Dropdown List <ul style="list-style-type: none"> • state • icmp



This function is control how the router online & offline, and use which modem to online. Please notice timing task execute an operation and keep the status, but parameter select only execute a operation. So they do not conflict. But Link backup function may conflict with parameter select function, if you set both, final running result may not as you presume.

---END

Connection type

Step 4 Login H8922S WEB GUI.

Step 5 Single click “Network > Connection type”.

Figure 5-13 Connection type window

Table 5-6 Connection type Parameter instruction

Parameter	Details	Operation
Work mode	Gateway: IP data transfer with MASQ Router: all IP data just transfer, no	Dropdown List <ul style="list-style-type: none"> • gateway

Parameter	Details	Operation
	MASQ Default Gateway, do not suggest to change	<ul style="list-style-type: none"> route
Default route	Default route	Dropdown List
Gateway	If default route is wan static IP, need specify gateway and DNS	Example: 192.168.10.254
DNS type	If Interface, will get DNS automatically	Dropdown List <ul style="list-style-type: none"> interface custom
DNS1/DNS 2	Manual set DNS	Example: 8.8.8.8
Interface name	Router will get DNS address from this interface	Dropdown List <ul style="list-style-type: none"> modem modem2 eth0

Step 6 Single click “save” icon.

---END

5.2.6 Link Backup

This function used to set how to backup network among modem1, modem2, and WAN port, to secure network availability.

There are hot backup and cold backup, hot backup means the backup link will always connect, so switch time is less, but cost extra flow fee.

Please note, when using this feature need to other operation:

- 1) The default route in Forward>>Route need to be delete.
- 2) The Masq of each link need to be added in Forward>>NAT>>MASQ.

Step 1 Login H8922S WEB GUI.

Step 2 Single click “network > Link Backup”.

Figure 5-14 Link Backup

Table 5-7 Link Backup Parameter

Parameter	Details	Operation
Status	Enable or Disable Link Backup feature	<ul style="list-style-type: none"> • Enable • Disable
Rule Name	Link Backup rule name identification Note: 0 can act as chain link or backup link, 1-9 only can act as backup link 1-9 can take the priority according to the number, the smaller the number the greater the priority	<ul style="list-style-type: none"> • Value area: 0-9
Running Mode	Link operate mode include: main: Link operate mode is main link backup: Link operate mode is backup link	Dropdown List <ul style="list-style-type: none"> • main • backup
Backup Mode	Backup mode include: cold and hot Hot refers to the corresponding link treatment enabled, the advantage of hot backup is switching fast, deficiency is when the link online will increase the	<ul style="list-style-type: none"> • Dropdown List • cold • hot

Parameter	Details	Operation
	cost of network overhead and charges. Cold refers to only the interface of current working link is enabled, and the others, as the interfaces of non-working link, are in offline state.	
Running Timeout	<ul style="list-style-type: none"> • If the current link is main link, shows the main link stability time • if the current link is backup link, shows the shortest working time • Note: • Running timeout is only suitable for switching between master and slave 	Value area:1-65535 Units: seconds
Interface Name	Interface used for link switching	<ul style="list-style-type: none"> • Dropdown List • modem 0 • modem 1 • eth1 • eth0
Check IP or Domain	Detection by ping packets IP address or domain name, if not the general principles means the failed test	WORD type, up to 64 characters, please refer to parameters regulation format
Normal Interval/Retry Times	<ul style="list-style-type: none"> • Normal interval means the interval time of the link normal detection. • Retry times means the maximum failure times of the link detection. • When the failure times reach to its maximum, the link will be switched to another. 	<ul style="list-style-type: none"> • Value area:1-65535 • Units: seconds/times

Step 3 Single click “save” icon.

---END

5.2.7 DHCP Service

DHCP(Dynamic Host Configuration Protocol) is a LAN network protocol, enable the DHCP function, a function automatically can obtain the dynamic IP.

Step 1 Login H8922S WEB GUI.

Step 2 Single click “Network > DHCP Server”.

Figure 5-15 DHCP

The screenshot shows the DHCP Server configuration interface. At the top, there are navigation tabs: LAN, WAN, WLAN, Modem, Parameter Select, Network Type, Link Backup, and DHCP Server. The DHCP Server tab is active. Below the tabs, there is a section for the DHCP Server status, with 'Enable' selected over 'Disable'. A 'Basic Settings' section contains four configuration items: IP Pool (dropdown menu showing 'br0'), Gateway Type (dropdown menu showing 'default'), DNS Type (dropdown menu showing 'default'), and Lease Time (text input showing '3600' with a range indicator '* 120-86400 s'). Below the basic settings, there are two rows of input fields for IP and MAC addresses, each with an example value (e.g., 192.168.8.1 for IP and 00:1A:4D:34:B1:8E for MAC) and an 'Add' button. At the bottom, there are 'Save' and 'Refresh' buttons.

Step 3 Configure DHCP parameter.

Step 4 DHCP parameter instructions are as Table 5-8.

Table 5-8 DHCP Parameter

Parameter	Details	Operation
DHCP Server	Enable or Disable DHCP feature	<ul style="list-style-type: none"> • Enable • Disable
Basic Settings (DHCP is not recommended configure in the case of no special network requirement)		
IP Pool	The DHCP client can get the scope of IP address. The IP addresses range assigned for the DHCP client. Selecting interface represents using network segment that the interface belongs to. This option can be configured to specify the IP address range of the lower place machine, for example: only hope at most four machine can automatically obtain the IP	<ul style="list-style-type: none"> • Dropdown List • br0 • custom

Parameter	Details	Operation
Start IP	When IP pool select custom configuration, configure the DHCP pool start IP address	Manual input Format: A.B.C.D/Mask Example: 192.168.8.2
End IP	When IP pool select custom configuration, configure the DHCP pool end IP address	Manual input Format: A.B.C.D/Mask Example: 192.168.8.254
Gateway Type	DHCP client access gateway IP source, divided into default, br0, eth0, custom four categories, associated interface, the interface IP assigned to the DHCP client as a gateway	<ul style="list-style-type: none"> • Dropdown List Default value: default
DNS Type	DHCP client access to the DNS IP source, has a default, modem, modem2, eth0, br0, custom and so on, generally do not recommend to modify the configuration, especially under the dual modem application scenario configuration is not recommended	<ul style="list-style-type: none"> • Dropdown List • default • modem • modem2 • eth0 • br0 • custom • Configuring for the default • is based on DNS address • which is allocated by the • router itself
Lease Time	After the DHCP client obtain an IP on IP lease time, the client usually renegotiates obtain an IP address lease time in more than half the time. IP lease time is mainly used to release idle IP to avoid that IP address resources are also occupied after the DHCP client shutdown	Value area: 120-86400 Units: seconds Default value: 3600
IP, MAC binding is used to assign a fixed MAC within the specified range of IP addresses		
IP	Binding with the specified MAC: when a DHCP client sends a DHCP request, the IP address with the client's MAC binding will be assigned to the DHCP client. The IP address will not be assigned to the other client with different MAC address even if it is not in use.	Manual input Format: A.B.C.D/Mask Example: 192.168.8.2
MAC	Configure DHCP to obtain an IP need to specify the DHCP client's MAC address	WORD Type MAC Format Example: 00:1A:4D:34:B1:8E

---END

5.3 Application program configuration

Based on years of customer experience for different applications, besides SNMP, DDNS, H8922S 3G/4G router has developed many functions for wireless network equipment, such as ICMP check, interface flow check function, M2M terminal management function, task management function and waking on demand function.

5.3.1 ICMP check

There is fake link (can get IP after dialing, but cannot link to destination address). Usually LCP is used to avoid this. Besides LCP, H8922S 3G/4G router can use another more reliable checking way ICMP which check the link by PING. When abnormal link is checked, the preset action will be executed to recover the link and systems quickly. Initially ICMP is to check wireless link, and now it can be used to check VPN link and supports simultaneous check in different rules. It supports maximum 10 ICMP check rules.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “applications > ICMP Check”.

Open “ICMP Check” tab.

Figure 5-16 ICMP Check tab

Network	Applications	VPN	Forward	Security	System	Status
ICMP Check	DDNS	SNMP	M2M	Timing	Wake Up	

Rule Name	Destination Address	Destination Backup	Timeout Action	Operation			
2	www.goog...	8.8.8.8	modem-reset	Mod	Del	En	Dis
1	192.168.1.1	8.8.8.8	reboot	Mod	Del	En	Dis

Add

Refresh

Step 3 “Add”, “Modify”, “Delete”, “Enable” “Disable” the function of “ICMP Check”.

- Add

Figure 5-17 ICMP adding page

ICMP Check Service

Basic Settings

Rule Name * Max length is 12

Destination Address * Max length is 64

Destination Backup Max length is 64

Retry Times * 1-65535

Normal Interval * 1-65535 s

Source Type ▼

Failed Interval * 1-65535 s

Timeout Action ▼

1. Configure the ICMP check parameter.

Table 5-9 ICMP check rules Parameter instruction

Parameter	Details	Operation
ICMP check service	To enable or disable ICMP check rules, multiple rules can be used simultaneously, and one specific rule can be disabled	Button <ul style="list-style-type: none"> • Enable • Disable
Basic Config		
Rule Name	ICMP Check rule name, just to distinguish different rules	WORD type, max 12 bytes
Destination address	Destination address of ICMP check, can be domain name and also can be IP address. If domain name, DNS of the router shall be configured correctly	WORD type, max 64 bytes
Destination backup	A backup destination address of ICMP check, if "destination address" cannot be linked by ICMP check, the "destination backup" address will be checked, if still cannot linked, the router will	WORD type, max 64 bytes

Parameter	Details	Operation
	recognize ICMP check fails	
Retry times/normal interval	Check time interval and max check failure times when link is OK, if check failure times reaches the max times, then "timeout action" will be executed, e.g. "modem reset"	Value area : 1~65535 Unit: second/time
Source Interface	Router sends an ICMP detected packet's source address	Dropdown List options <ul style="list-style-type: none"> • br0 • modem • modem2
Timeout action	<ul style="list-style-type: none"> • An action when check failure times reach max failure times. Can be modem-reset, reboot, custom 	Dropdown List options <ul style="list-style-type: none"> • modem-reset: modem redials • modem2-reset: modem2 redials • reboot: router reboots • custom: customized action
Run commands	If "Timeout action" is "custom", this shall be configured. Commands are BGO operation. It is not suggested to use, if need, please contact our technical engineers	WORD type, max 64 bytes

2. Single click "save" to finish a ICMP check rule.



If ICMP is normal, ICMP packet is sent at "normal interval". When abnormal, packet will be sent continuously at "failed interval". If "destination address" cannot be linked and checking times reach "retry times", "destination backup" will be checked. If "destination address" can be linked in checking "destination backup", "destination address" will be checked again. If "destination backup" cannot be linked and checking times reach "retry times", "Timeout action" will be executed.

- Modify
- Delete
- Enable



If already enabled, the button "EN" is gray.

- Disable



If already disabled, the button "DIS" is gray

- Refresh

Click “refresh” to refresh the page.

---END

5.3.2 DDNS configuration

Network of SIM/UIM shall be a public address so that router can be visited for a DDNS.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Applications” > “DDNS”.

Figure 5-18 DDNS configuration

The screenshot shows the DDNS configuration interface. At the top, there are tabs for Network, Applications (selected), VPN, Forward, Security, System, and Status. Under Applications, there are sub-tabs: ICMP Check, DDNS (selected), SNMP, M2M, Timing, and Wake Up. The main content area has a 'DDNS Service' section with 'Enable' and 'Disable' buttons. Below this is the 'Basic Settings' section with the following fields:

- Service Provider: A dropdown menu showing '88ip'.
- Server Port: A text input field with a range indicator '1-65535'.
- Username: A text input field with a note '* Max length is 64'.
- Password: A text input field with a note '* Max length is 64'.
- User Domain: A text input field with a note '* Max length is 64'.
- Update Interval: A text input field with a note '* 120-86400 s'.

At the bottom of the form are 'Save' and 'Refresh' buttons.

Step 3 Configure DDNS parameter.

Table 5-10 DDNS Parameter instruction

Parameter	Details	Operation
DDNS Service	Set whether enable DDNS service function	Button Enable Disable
Basic Config		
Service Provider	Select the DDNS service provider that router currently supports, don't support other providers	Dropdown List options 3322 88ip Dnsexit Dyndns Zoneedit changeip

Parameter	Details	Operation
		custom
Server IP or Domain	When “custom” in “service provider” is selected, “Server IP or Domain” will be configured. Default is standard DDNS protocol. for customized protocol, please contact our engineer	WORD type, max 64 bytes
Server Port	Set the port number of the DDNS server provided by the service provider. The default port number is 80	Value area: 1~65535 If empty, it means 80 port
User name/Password	Set user name/password of the DDNS service registered in the service provider	Normal WORD type/CODE type, max 64 bytes
User Domain	Set the domain of the DDNS service provided by the service provider	Normal WORD type, max 64 bytes
Update Interval	Set the interval of the DDNS client obtains new IP, suggest 240s or above	Value area: 120~86400 Unit: seconds

Step 4 Click “Save” to complete DDNS configuration



DDNS in China: 88IP (www.88ip.net), 3322 (www.3322.org)
 DDNS outside of China: DNSEXIT (www.dnsexit.com), ZONEEDIT(www.zoneedit.com),
 CHANGEIP(www.changeip.com), DYNDNS(www.members.dyndns.org)
 After router reboots, IP address which SIM/UM gets from ISPs will change. If user uses DDNS in remote login, no matter the IP address changes, he can Log-on the router.

---END

5.3.3 SNMP configuration

SNMP (Simple Network Management Protocol) can monitor routers remotely and get to know the status of routers (Support interface status check, like VPN, modem etc. MIB of our company shall be used).

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Applications>SNMP” to open the “SNMP” tab.

Figure 5-19 SNMP configuration

Step 3 Configure SNMP parameter.

Table 5-11 SNMP Parameter instruction

Parameter	Details	Operation
SNMP service	To enable or disable SNMP service	Options: <ul style="list-style-type: none"> • Enable • Disable
Basic Config		
Port	SNMP port, suggest to be default port161	Value area: 1~65535 Default: 161
Community	Community Password of SNMP client to router SNMP, Used for identification	WORD type, max 16 bytes
Trap IP	Link-state router report server address	Manual input Format: A.B.C.D/Mask
Trap Port	Link-state router report server address's port	Value area: 1~65535 Default: 162

Parameter	Details	Operation
Loopback Status	Match with "LAN" page loopback address, in the "Loopback Status" to "Enable", means loopback address configuration successfully, the router reported Trap IP packet source address is the loopback address, If the "Loopback Status" to "Disabled" means router IP packet source address for the LAN port address	Options: <ul style="list-style-type: none"> • Enable • Disable

Step 4 Single click "save" icon to finish SNMP configuration.



NOTE

MIB for SNMP can be downloaded from our website, if necessary, please contact our technical engineers.

---END

5.3.4 M2M configuration

H8922S 3G/4G router has embedded a WMMP (Wireless Machine-to-Machine Protocol) protocol to realize communication with M2M (Machine-to-Machine) platform which can remotely monitor and manage the routers and its network, e.g. visit the router, patch upgrading, firmware upgrading, parameter configuration, monitor the network strength, time delay, flow. Its configuration is as follows:

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click "Applications > M2M" to open M2M configuration tab.

Figure 5-20 M2M configuration

The screenshot shows the M2M configuration interface. At the top, there are tabs for Network, Applications, VPN, Forward, Security, System, and Status. The Applications tab is selected, and within it, the M2M sub-tab is active. Below the tabs, there is a section for M2M Service with 'Enable' and 'Disable' buttons. The 'Disable' button is highlighted. Below this is a 'Basic Settings' section with several input fields and their constraints:

- Server IP or Domain: * Max length is 64
- Server Port: * 1-65535
- Login Times: * 1-5
- Heartbeat Interval: * 1-65535 s
- Retry Times: * 1-5
- Task Failure Time: * 1-65535 s

At the bottom of the form, there are 'Save' and 'Refresh' buttons.

Step 3 Configure M2M parameter.

Parameter instruction is shown.

Table 5-12 M2M Parameter instruction

Parameter	Details	Operation
M2M service	To enable or disable M2M function. This function shall be used with our M2M platform	Button <ul style="list-style-type: none"> • Enable • Disable
Basic Config		
Server IP or Domain	Set the server IP or domain of M2M platform	Normal WORD type, max 64 bytes
Server Port	WMMP port No, shall be the same with Port No of M2M platform server	Value area: 1~65535
Login Times	Max retry-times of router to login M2M platform. If login times reach max times, the router will reboot, M2M will initialize and login again	Value area: 1~5 Unit: times
Heartbeat Interval	Time interval to send heartbeat which maintains the like with M2M platform server. The heartbeat includes the network status info which will update the network info of the M2M platform	Value area: 1~65535 Unit: seconds

Parameter	Details	Operation
Retry Times	There is a retry mechanism for package exchange between router and M2M platform. When exchange times reach retry times, router will judge the exchange fails and usually no operation will be made	Value area: 1~5 Unit: seconds
Task Failure Time	The time to judge an exchange fails, if an exchange uses time which exceeds the “task failure time”, router will judge the exchange fails and will retry to send the exchange	Value area: 1~65535 Unit: seconds

Step 4 Single click “save” icon to finish the configuration.

---END

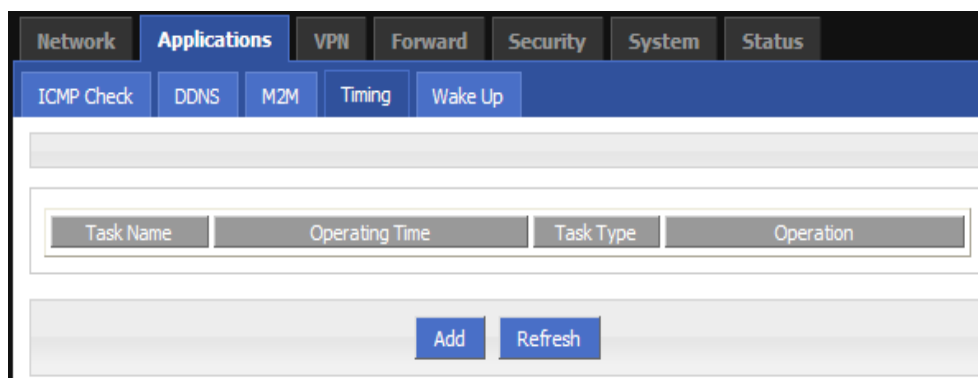
5.3.5 Timing configuration

This application is to control the online time of the router to better manage network and save 3G/4G flow. H8922S can add several online periods as per the user's requirement (e.g. hours of some day). in addition, this application can support to begin some tasks at a time point (e.g. redial or reboot at 00:00). 10 tasks max.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Applications > M2M” to open M2M configuration tab.

Figure 5-21 Timing configuration



Step 3 To add a timing task, please click “Add”.

Figure 5-22 To add timing task

Network Applications VPN Forward Security System Status

ICMP Check DDNS M2M Timing Wake Up

Status

Basic Settings

Task Name * Max length is 12

Task Type ▼

Schedule * Max length is 64

Set Time

Time Type ▼

Clock : - : eg. 00:00-23:59

Day - eg. 01-31

Week - eg. 1-7

Step 4 Configure timing task parameter.

Table 5-13 Timing task parameter instruction

Parameter	Details	Operation
Status	To enable or disable a timing task. Some task shall be enabled together with NTP	options <ul style="list-style-type: none"> • Enable • Disable
Basic Config		
Task name	Name of a timing task	Max 12 digits
Task type	Task type has action task and status task. Action task is for time point or time interval, while status task is for time period (for “modem-online” and “modem2-online”), which means that the modem will be online (if down, modem will automatically redial)	Dropdown List options: <ul style="list-style-type: none"> • modem-online • modem2-online • reboot • custom if select “custom”, “schedule” will be shown to input command (can be dialup or other command). Max 64 bytes

Parameter	Details	Operation
	during the configured time period. Modem will be offline (no dialing) for other time	
Schedule	This is Linux shell command. Usually suggested not to use it. In case of need, please contact our technical engineers	WORD type. Max 64 digits
Set time		
Time type	Range or interval for status task or action task	Dropdown List options: <ul style="list-style-type: none"> • range • interval
When “time type” select “range”		
Clock	To input hour and minute. When beginning and end hour and minute are the same, it means a time point for action task	Value area: [00:00,23:59] Format: HH:mm-HH:mm
Day	Days in a month for task	Value area: [01,31] Format: XX-XX
Week	Days in a week for task. When “day” and “week” are both input, it means only if both conditions meet, the task will begin	Value area: [1,7] Format: X-X 1 for Monday
When “time type” select “Interval”		
Interval	Time interval for action task	Value area: 1~65535 Unit: minutes

Step 5 Single click “save” icon to finish “Timing” configuration

The “range” selection requires system clock enable (that is to say the NTP server), while the “interval” selection does not require. For the system clock configuration, see the section “5.6.4 Clock”.

---END

5.3.6 Wake up configuration

3G/4G fee is mostly based on flow. H8922S 3G/4G router can get on/off line on demand. It supports on/offline or reboot triggered by voice, SMS or data. It supports max 10 cell phone Nos.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Applications > Wake up” to open “Wake up” tab.

Figure 5-23 Wake up configuration

Step 3 Configure “wake up” parameter.



Click “Save” to write in the flash memory, after finishing “basic setting” parameter.

Table 5-14 Wake up Parameter instruction

Parameter	Details	Operation
Wake up service	To enable or disable the service.	Options: <ul style="list-style-type: none"> • Enable • Disable

Parameter	Details	Operation
Add phone Number		
Phone Number	Phone No to trigger the router action. One phone No for one action of one modem.	WORD type. Max 32 digits.
Task type	<ul style="list-style-type: none"> Triggered action includes modem-up, modem-down, reboot. 	Dropdown List options <ul style="list-style-type: none"> modem-down modem-up modem2-down modem2-up reboot
Basic setting		
Wake up method	To configure actions triggered, it supports phone and data. If choose phone, please be sure that the SIM card has opened voice or SMS service. Usually recommend voice wakeup with high efficiency and don't need SMS charge.	Dropdown List options <ul style="list-style-type: none"> phone/data phone
Offline method	Support "timeout" and "idle". "timeout" means router will get offline once time reaches the configured time commencing from online time. "idle" means if idle (no data transmission) time is as long as the configured time, the router will get offline.	Dropdown List options <ul style="list-style-type: none"> timeout idle
Online time	Online time of router, for "idle", online time will recalculated if there is data transmission.	Value area : 0~86400 Unit: second
Data trigger	Configured as wakeup by data. When router receives data from external network, the modem will be triggered to be online, LAN data and broadcast data will not trigger actions. If configured as "phone&data", either phone or data can trigger actions	Dropdown List options <ul style="list-style-type: none"> modem-up modem2-up modem-all-up

Step 4 Click "ADD" to add a new wake up rule.

After add a new rule, the rule will be shown on the bottom, click "Del" to delete the rule.



One phone number be set for actions of different modems, but cannot be set as different actions of one modem.

It's OK for either SIM of the two SIMs of H8922S 3G/4G router to open SMS or voice function, no matter which slot to be installed.

"Data" will trigger only actions: modem-up/modem2-up/modem-all-up

If "online time" is set as 0, it means router will be always online. To get the router offline, pls choose actions to trigger offline.

"Online time" in "wake up" will affect other functions like SIM switch, network backup, task management.

So when users set wakeup parameter, please note whether there is conflict with other functions.

Voice trigger: router will begin the action after 5 seconds of the sound "du".

5.3.7 DTU configuration (Optional)

DTU (Data transfer Unit) is to transfer data for meters with RS232 interface from site to center through 3G/4G network. It supports TCP/UDP Client/Server mode.

Step 1 Log-on WEB GUI of H8922S 3G/4G routers.

Step 2 Click "Applications > DTU" to open "DTU" tab.

Figure 5-24 DTU configuration

DTU Service: ☒ Enable ☐ Disable

Basic Settings

Work Mode:

Local Port:

Protocol: ☒ TCP ☐ UDP

Received Timeout: * 1-65535 ms

RS232 Data Timeout: * 1-65535 ms

Data Center Configure

Server IP or Domain: * Max length is 64

Server Port: * 1-65535

Connect Interval: 1-65535 s

Retry Times: 1-65535

Heartbeat Settings

Heartbeat Data Max length is 64

Heartbeat Interval 1-65535 s

Rs232 Setting

Rate

Parity

Databits

Stopbits

Step 3 Configure “DTU” parameter.

Table 5-15 DTU Parameter instruction

Parameter	Details	Operation
DTU Service	Enable or Disable DTU Service	DTU Service options <ul style="list-style-type: none"> • Enable • Disable
• Basic Settings		
Work Mode	Work mode: <ul style="list-style-type: none"> • Server: 3G/4G router act as TCP/UDP server • Client: 3G/4G router act as TCP/UDP client • DDPClient: 3G/4G router act as UDP client with Hongdian protocol 	Select from Dropdown List <ul style="list-style-type: none"> • Server • Client • DDPClient
Local Port	DTU service port	Specify the port number:1-65535
Protocol	Protocol of TCP/UDP connection <ul style="list-style-type: none"> • TCP protocol is a connection-oriented reliable • transport protocol for high reliability requirements and for communication efficiency which is not • high degree of sensitivity of the occasion 	Select protocol: TCP or UDP Note: When the work mode is "DDP clients," only support "UDP protocols used in conjunction with the DDP protocol."

Parameter	Details	Operation
	UDP protocol is a connectionless unreliable transport protocol, suitable for relatively high efficiency requirements, and the occasion of relatively low reliability	
Received Timeout	DTU port timeout which receive from the data center, within the received packet does not exceed the maximum packet length range, the data is reading at this time, if the data is been reading, and will display all data during this time; If no data, when it is greater than the timeout, it will consider reading data completely, displays DTU serial terminal	Specify time according to your need data:1-65535ms Default value:500 Units:ms
RS232 Data Timeout	DTU waiting time to send the serial data to the data center side. Within waiting time, the data sent over UDP / TCP packets received maximum packet length, then sent immediately; if not more than UDP / TCP packets received maximum packet length, then wait for data until it reaches the last packet idle time , and then to send	Specify time according to your need data:1-65535ms Default value:500 Units:ms
Data Center Configure		
Server IP or Domain	DataServerCenter(DSC) ip or domain	Format: A.B.C.D/Mask or Word Type
Server Port	DataServerCenter(DSC) port number	Port number:1-65535
Connect Interval	The reconnect interval is DTU client fail to connect to DSC server	Manually input:1-65535 Units: second
Retry Times	The retry times is DTU client fail to connect to DSC server	Manually input:1-65535
Heartbeat Settings		

Parameter	Details	Operation
Heartbeat Data	customize heartbeat data content	Manually input, max length is 64
Heartbeat Interval	Set heartbeat interval(when there is no data transfer, the router send the heartbeat data content every heartbeat interval)	Manually input:1-65535 Units: second
RS232 settings		
Rate	Set the serial port transfer rate	Select from the dropdown list, according to the practical settings of DTU serial port Default: 115200
Parity	Set the data parity	Select from the dropdown list, according to the practical settings of DTU serial port Value: None, Old, Even Default: None
Databit	Set the data transfer bit	Select from the dropdown list, according to the practical settings of DTU serial port Value: 5,6,7,8 Default: 8
Stopbit	Set the data stop bit	Select from the dropdown list, according to the practical settings of DTU serial port Value: 1,2 Default: 1

Step 4

Step 5 Single click “save” icon to finish “DTU” configuration,
DTU will start to work when modem is online if it is enabled.

---END

5.3.8 GPS configuration (Optional)

GPS is to transfer GPS data the device gets from satellite. It uses UDP protocol.

Step 1 Log-on WEB GUI of H8922S 3G/4G routers.

Step 2 Click “Applications > GPS” to open “GPS” tab.

Figure 5-25 GPS configuration

Table 5-16 GPS Parameter instruction

Parameter	Details	Operation
GPS Service	Enable or Disable GPS Service	GPS Service options <ul style="list-style-type: none"> • Enable • Disable
• Basic Settings		
Work Mode	Set the work mode of the GPS	Select from the dropdown list, Default: Client
Product Mark	The identification of the router GPS, used for identifying the device	Word Type, max length is 64
Local Port	The router port for reporting the GPS data	Value: 1-65535
Server IP or Domain	Server IP or domain for getting the GPS data	Format: A.B.C.D/Mask or Word Type
Server Port	Server port for getting the GPS data	Value:1-65535

Step 3**Step 4** Single click “save” icon to finish “GPS” configuration

GPS will start to work when server IP or domain is reachable from router.

---END

5.4 Security

5.4.1 Overview

“Security” will control where the data can pass through by analyzing IP address and port of ICMP, TCP/IP package from the destination end or source end. H8922S 3G/4G router supports IP filter, domain filter and MAC filter.

5.4.2 Configuration

IP Filter

IP filter refers to judgment whether to allow router to forward the data according to filter rules, thus to manage internet surfing of PC in LAN. IP filter is used to allow part of PCs in LAN to visit external WAN network or forbiden some PCs from visiting specific website.

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “Security > IP Filter” to open “IP Filter” tab.

Figure 5-26 IP Filter tab

The screenshot displays the IP Filter configuration page. At the top, there are three tabs: 'IP Filter', 'Domain Filter', and 'MAC Filter'. The 'IP Filter' tab is selected. Below the tabs, there are two main sections: 'INPUT Filter' and 'FORWARD Filter'. Each section contains a table with the following columns: 'Action', 'Protocol', 'SRC Address', 'Source Port', 'Destination IP', 'Destination Port', and 'Operation'. The 'FORWARD Filter' section also includes a 'Filter mode' dropdown menu with 'Black List' and 'White List' options. At the bottom of the page, there are 'Add' and 'Refresh' buttons.

- Step 3** In the forwarding filtering rules.
- Black List: The default allows packet forwarding, in line with the list of "discarded" rules packet cannot be forwarded through the router.
 - White List: The default refuses packet forwarding, in line with the list of "accept" rules packet can go through router forwarding.
- Step 4** Click “Add” to add a new IP filter rule and configure IP filter parameter. There are two types of IP filter: “Input” and “Forward”, as show in Figure 5-28 and Figure 5-29

Figure 5-27 IP filter “Input” type

Basic Settings	
Type	<input checked="" type="radio"/> Input <input type="radio"/> Forward
Default Action	<input checked="" type="radio"/> Accept <input type="radio"/> Drop
Protocol	all ▼
Source IP	<input type="text"/> * 192.168.8.1 or 192.168.8.0/24
Source Port	<input type="text"/> 1-65535 or [1-65535]
Destination Type	interface ▼
Interface	br0 ▼
Destination Port	<input type="text"/> 1-65535 or [1-65535]

Figure 5-28 IP Filter “Forward” type

Basic Settings	
Type	<input type="radio"/> Input <input checked="" type="radio"/> Forward
Default Action	<input checked="" type="radio"/> Accept <input type="radio"/> Drop
Mirror Rule	<input type="radio"/> En <input checked="" type="radio"/> Dis
Protocol	all ▼
Source IP	<input type="text"/> * 192.168.8.1 or 192.168.8.0/24
Source Port	<input type="text"/> 1-65535 or [1-65535]
Destination IP	<input type="text"/> * 192.168.0.1, 192.168.0.1/24
Destination Port	<input type="text"/> 1-65535 or [1-65535]

Table 5-17 IP filter parameter instruction

Parameter	Details	Operation
Type	<p>Select a filter type, you can choose according to their needs, "Input" or "Forward"</p> <p>Input: whether to allow access to the router</p> <p>Forward: whether to allow the router forwarding</p>	Dropdown List options
Default Action	<p>The default action rule. You can select "Accept" or "Drop "</p> <p>Accept: firewall to accept the package, which can be passed</p> <p>Drop: firewall discards the packet directly</p>	Dropdown List options
Mirror Rule	<p>When the filter type selects "Forward", it needs to be configured</p> <p>Enable: Base on the configured rules, system auto adds totally opposite rules in addition. Opposite rules mean all the source address/port and destination address/port are reverse in the rules</p> <p>Disabled: no treatment</p>	Dropdown List options
Protocol	Protocol used by IP packets	<ul style="list-style-type: none"> • Dropdown List options • all • tcp • udp • icmp
Source IP	<ul style="list-style-type: none"> • The source IP address of the packet 	<p>Manual input</p> <p>Format: A.B.C.D/Mask</p>
Source Port	The source Port of the packet, when the protocol choose "icmp", it don't need to configure	Value area: 1-65535 or [1-65535], it can be a range, or a single port
When the IP Filter type select "Input"		
Destination Type	Design an IP packet access router interface	<p>Dropdown List options</p> <ul style="list-style-type: none"> • interface • any

Parameter	Details	Operation
Interface	Configure when Destination Type select "Interface", means the IP packet access the router interface	Dropdown List options <ul style="list-style-type: none"> • br0 • modem • modem2 • eth0 • eth1
Destination Port	IP packet access router ports (when the protocol select "icmp", requires no configuration)	Value area: 1-65535 or [1-65535], it can be a range, or a single port
When the IP Filter type select "Forward"		
Destination IP	IP packet destination IP	Manual input Format: A.B.C.D/Mask
Destination Port	IP packet destination port	Value area: 1-65535 or [1-65535], it can be a range, or a single port

Step 5 Single click "save" to finish.

--END

Domain Filter

Domain filter support black list and white list. It is used to forbid PCs in LAN from visit some websites or allows them to visit specific websites.

Step 6 Log-on WEB GUI of H8922S 3G/4G router.

Step 7 Click "Security> Domain Filter" to open "Domain Filter" tab.

Figure 5-29 Domain filter tab

The screenshot displays the 'Domain Filter' configuration page. At the top, there's a navigation bar with tabs: Network, Applications, VPN, Forward, Security (selected), System, and Status. Below this, there's a sub-navigation bar with IP Filter, Domain Filter (selected), and MAC Filter. The main content area has a section for 'Action' with two radio buttons: 'Black List' and 'White List'. Below the radio buttons is a table with three columns: 'Domain Address', 'Action', and 'Operation'. At the bottom of the page, there are two buttons: 'Add' and 'Refresh'.

- Black list: websites in the blacklist cannot be visited. Click "black list" to forbid visiting the websites in the list.

- White list: only the websites in the white list can be visited, while other websites cannot be visited. Click “White list” to activate it.

Step 8 Click “ADD” to add a new domain filter rule and configure domain filtering parameter.

Figure 5-30 Domain filter tab

Table 5-18 Domain Filter parameter instruction

Parameter	Details	Operation
Domain keyword	Keyword of domain for filter	WORD type, max 64 digits. E.g. www.google.com, the keyword is “google”.
Default action	Actions to filter the keyword	<ul style="list-style-type: none"> • Accept. • Drop

Step 9 Single click “Save” to finish configuring a rule.

---END

MAC Filter

Step 10 Log-on WEB GUI of H8922S 3G/4G router.

Step 11 Click “Security> MAC Filter” to open “MAC Filter” tab.

Figure 5-31 MAC Filter tab

The screenshot shows the MAC Filter configuration page. The top navigation bar includes tabs for Network, Applications, VPN, Forward, Security, System, and Status. The Security tab is active, and within it, the MAC Filter sub-tab is selected. The page is divided into two main sections: INPUT Configure and FORWARD Configure. Each section contains an 'Action' dropdown menu with 'Black List' and 'White List' options. Below the dropdown is a table with three columns: MAC Address, Action, and Operation. At the bottom of the page, there are 'Add' and 'Refresh' buttons.

Table 5-19 MAC Filter explanation

Parameter	Details	Operation
Input configuration		
Action	To activate MAC input filtering black list / white list.	<ul style="list-style-type: none"> • Blacklist: rules in blacklist cannot visit router, other MACs can visit router. • White list: rules in white list can visit router, other MACs cannot visit router.
Forward configuration		
Action	To activate MAC forward filtering black list / white list.	<ul style="list-style-type: none"> • Blacklist: rules in blacklist cannot visit external network, other MACs can visit external network through router. • White list: rules in white list can visit external network, other MACs cannot visit external network through router.

Step 12 Click “Add” to add a new MAC filter rule and configure MAC filtering parameter.

Figure 5-32 MAC Filter configuration

Table 5-20 MAC Filter Parameter instruction

Parameter	Details	Operation
Basic Settings		
MAC	MAC to be filtered	WORD type MAC format: XX:XX:XX:XX:XX:XX
Default Action	Default actions of the rule. Can be "accept" or "Drop": <ul style="list-style-type: none"> Accept: to accept all packages from this MAC. Drop: to drop all packages from this MAC. 	To choose "accept" or "Drop"
Filter mode	To choose "Input", "Forward" or "Both". <ul style="list-style-type: none"> Input: all packages visiting router. Forward: all packages forwarded by router. Both: both Input and forward. 	To choose "Input", "Forward" or "Both".

Step 13 Single click "save" icon to finish.

---END

5.5 Forward configuration

5.5.1 Overview

Forward function of H8922S 3G/4G router includes NAT, Routing, dynamic routing (RIP, OSPF) (optional) and QoS (optional).

5.5.2 NAT

DNAT configuration rule

DNAT is used to replace the destination address of packets accessing external network, router will replace the destination address of packet accessing external network into the user custom settings.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Forward > NAT” to open “NAT” tab.

Figure 5-33 NAT tab

Network	Applications	VPN	Forward	Security	System	Status
NAT	Routing					

MASQ

Interface	Operation

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

DNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

Add Refresh

Step 3 Click “Add” to add a new NAT rule.

Figure 5-34 DNAT rule configuration

The screenshot shows the 'NAT' configuration page with the 'Routing' sub-tab active. Under 'Basic Settings', the 'NAT Type' is set to 'DNAT'. The 'Protocol' is set to 'all'. The 'Original Address Type' is set to 'interface'. The 'Interface' is set to 'br0'. The 'Original Port' is empty, with a hint '1-65535 or [1-65535]'. The 'Mapping Address' is empty, with a hint '* eg. 192.168.0.1'. The 'Mapping Port' is empty, with a hint '1-65535 or [1-65535]'. At the bottom, there are 'Save' and 'Return' buttons.

Step 4 Select “DNAT” in NAT Type, to configure DNAT rule parameter.

Table 5-21 DNAT Parameter instruction

Parameter	Details	Operation
Basic Settings		
Protocol	Supports “TCP”, “UDP”, “ICMP” or “ALL”	Select from Dropdown List
Original Address Type	The external address, the address needs to be converted	Dropdown List <ul style="list-style-type: none"> • interface • static
Interface (when the initial address type select “interface”, needs to be configured)	Indicates the external address of IP packets to an interface of the router	Dropdown List <ul style="list-style-type: none"> • br0 • modem • modem2 • eth0 • eth1
Original Address (when the initial address type select “static”, needs to be configured)	The external address, the address needs to be converted	Manual input Format1: A.B.C.D Format2: A.B.C.D/Mask

Parameter	Details	Operation
Original port	The port of external IP, the port need to be replaced	Value area: 1~65535
Mapping address	Internal IP address	e.g. 192.168.8.1
Mapping port	The port of Internal IP address	Value area :1~65535

Step 5 Single click “save” icon to finish.

---END

SNAT configuration rule

SNAT is the source address translation, and its role is to translate source address of IP packets into a another address.

Step 6 Log-on WEB GUI of H8922S 3G/4G router.

Step 7 Click “Forward > NAT” to open “NAT” tab.

Step 8 NAT Type select “SNAT”, Configuration interface as shown in Figure 5-47.

Figure 5-35 SNAT rule configuration

The screenshot displays the SNAT rule configuration page. At the top, there are tabs for 'NAT' and 'Routing'. Below this is a 'Basic Settings' section. The 'NAT Type' is set to 'SNAT' (selected with a radio button). The 'Protocol' is set to 'all'. The 'Original Address' field is empty, with a red asterisk and the text '* 192.168.8.1 or 192.168.8.0/24' next to it. The 'Original Port' field is empty, with the text '1-65535 or [1-65535]' next to it. The 'Mapping Address Type' is set to 'interface'. The 'Interface' is set to 'br0'. The 'Mapping Port' field is empty, with the text '1-65535 or [1-65535]' next to it. At the bottom, there are 'Save' and 'Return' buttons.

Step 9 Configure SNAT rule parameter.

Parameter instruction as Table 5-22

Table 5-22 SNAT rule instruction

Parameter	Details	Operation
Protocol	Convert some kind of protocol packets into address	<ul style="list-style-type: none"> • Dropdown List • all • tcp • udp • icmp
Original Address	The source address need to be replaced	Manual input Format1: A.B.C.D Format2: A.B.C.D/Mask
Original Port	The port of external IP, the port need to be replaced	Value area: 1-65535 or [1-65535], it can be a range, or a single port
Mapping Address Type	Internal IP address	<ul style="list-style-type: none"> • Dropdown List • interface • static
Interface	Select the interface of the router as source address after replacement	<ul style="list-style-type: none"> • Dropdown List • br0 • modem • modem2 • eth0 • eth1
Mapping Port	The new port which replaces the original port of source address.	Value area: 1-65535 or [1-65535], it can be a range, or a single port

Step 10 Single click “save” icon to finish.



NOTE

When a SNAT rule is configured with port specified, selecting “all” in protocol means selecting two protocols contain "tcp", "udp"; when a SNAT rule is configured with no port specified, selecting “all” in protocol means selecting three protocols contains "tcp", "udp", "icmp".

---END

MASQ rule configuration

MASQ is MASQUREADE.

Step 11 Log-on WEB GUI of H8922S 3G/4G router.

Step 12 Click “Forward > NAT” to open “NAT” tab.

Step 13 Select “SNAT” in NAT Type. The configuration page is shown in Figure 5-48.

Figure 5-36 MASQ configuration

The screenshot shows the MASQ configuration page. At the top, there are two tabs: 'NAT' and 'Routing', with 'Routing' being the active tab. Below the tabs is a 'Basic Settings' section. Inside this section, there are two rows of configuration options. The first row is 'NAT Type', which has three radio button options: 'DNAT', 'SNAT', and 'MASQ'. The 'MASQ' option is selected. The second row is 'Interface', which has a dropdown menu currently showing 'br0'. At the bottom of the configuration area, there are two buttons: 'Save' and 'Return'.

Step 14 Configure MASQ rule parameter.

Table 5-23 MASQ rule Parameter instruction

Parameter	Details	Operation
NAT Type	To select “MASQ”	Select “MASQ”
Interface	Interface includes: <ul style="list-style-type: none"> • br0: use br0 interface as commutation address between router & LAN and external network • Modem: use modem interface as commutation address between router & LAN and external network • modem2: use modem2 interface as commutation address between router & LAN and external network • eth0: use eth0 interface as commutation address between router & LAN and external network 	Select from Dropdown List

Step 15 Single click “save” icon to finish.



MASQ rule: the source address of all packets in the LAN need to be transferred into the specific ip address of the router, so the PC from the LAN can send packets out; If MASQ rule in the router will be deleted, the router LAN of the PC cannot communicate with external network.

---END

5.5.3 Static Routing

Static routing can forward packets according that the user configured specific forwarding path manually. Static Routing form is divided into static routing and policy routing, static routing is based on the destination address as an alternative route; while policy route is

based on the source address that match with the policy to forward the packets (forwarding router detects the received packet's source address, and then forward packages according to the source which matches policy route) and policy routing priority, use numbers 3 to 252 to differentiate, the smaller number with higher priority. And there are priorities between static routing and policy routing: policy routing higher priority than static routing.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Forward > Routing” to open “NAT” tab, as Figure 5-49.

Figure 5-37 Static Routing Interface

Route Type	Network	Gateway	Priority	Operation
Static Route	0.0.0.0/0	modem		Delete
Static Route	192.168.8.0/24	192.168.8.1		Delete

Add Refresh

Step 3 Click “Add” to add a new static route, configure interface as Figure 5-50 and Figure 5-51.

Figure 5-38 Static Routing Interface

Basic Settings

Route Type ☒ Static Route ☐ Policy Route

Network * eg. 192.168.8.0/24

Gateway Type static ip

Gateway * eg. 192.168.8.1

Save Return

Figure 5-39 Policy Routing Interface

The screenshot shows the 'Policy Routing Interface' configuration page. It features a top navigation bar with tabs for 'NAT', 'Routing', 'RIP', and 'OSPF'. Below this is a 'Basic Settings' section with the following fields:

- Route Type:** Radio buttons for 'Static Route' and 'Policy Route' (selected).
- Source Type:** A dropdown menu currently showing 'static ip'.
- Network:** A text input field with a red asterisk and a hint '* eg. 192.168.8.0/24'.
- Gateway Type:** A dropdown menu currently showing 'static ip'.
- Gateway:** A text input field with a red asterisk and a hint '* eg. 192.168.8.1'.
- Priority:** A text input field with a red asterisk and a hint '* 3-252'.

At the bottom of the form are two buttons: 'Save' and 'Return'.

Parameter Instruction as Table 5-24.

Table 5-24 Static Routing Parameter Instruction

Parameter	Details	Operation
Basic Setting		
Routing Type	To select “Static Route” or “Policy Route”	<ul style="list-style-type: none"> • Dropdown List
When Routing Type is “Static Route”		
Network	Set the destination IP address and subnet mask of static route	Manual input Format1: A.B.C.D/Mask
Gateway Type	Specify gateway type of static routing, includes: <ul style="list-style-type: none"> • interface • static IP 	Dropdown List
Gateway	Set a next hop IP address of static route, IP address of the adjacent router interface	Dropdown List <ul style="list-style-type: none"> • If the gateway type selects static IP, gateway need to manually input, format: A.B.C.D • If the gateway type select interface, the gateway needs to select from dropdown list
When Routing Type is “Policy Route”		
Source Type	Set source type of policy route <ul style="list-style-type: none"> • Static IP 	Dropdown List

Parameter	Details	Operation
	<ul style="list-style-type: none"> Interface 	
Network	It can be configured when "static IP" is selected in source type, by adding IP address or subnet manually.	Manual input Format1: A.B.C.D/Mask
Source Interface	When source type is policy route, need to manually set source network address of policy router <ul style="list-style-type: none"> modem modem2 	Dropdown List
Gateway Type	Set the next hop IP of policy route <ul style="list-style-type: none"> static ip interface 	Dropdown List
Gateway	When the gateway type select "Static IP" to fill in the IP address, when gateway type is "interface", it will use the selected interfaces as gateway	Manual input Format1: A.B.C.D/Mask
Priority	Set policy routing priority, the priority lower the number, the higher the priority	Value area: [3,252]

Step 4 Single click "save" icon to finish the static routing setting.



NOTE

Static routing will forward according to the destination address of the packet, if the router received the packet (e.g. source address is 1.1.1.1 destination address is 2.2.2.2), it will forward the packet to next hop according to the route which meets with the destination address (2.2.2.2).

It will forward the packet to next hop according to the route which meets with the destination address (2.2.2.2).

Policy routing will forward according to the source address of the packet, if the router received the packet (e.g. source address is 1.1.1.1 destination address is 2.2.2.2), it will forward the packet to next hop according to the route which meet with the source address (1.1.1.1).

Policy routing has higher priority than static routing, policy-based routing priority regardless of how much.

---END

5.5.4 QoS (Optional)

QoS (Quality of Service) quality of service, is a security mechanism for the network, is a technique to solve the network bandwidth allocation and network priority and other issues. When the network is overloaded or congested, QoS to ensure that critical traffic is

not delayed or dropped, while ensuring the efficient operation of the network, our H8922S 3G/4G Router supports custom QoS services.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Forward > QoS” to open “QoS” tab, as Figure 5-52.

Figure 5-40 QoS interface

Step 3 QOS configuration parameter, configuration parameter instruction as Table 5-25.

Table 5-25 QoS parameter instruction

Parameter	Details	Option
Status	Enable or disable QoS feature	Click the button to select
Basic Setting		
Rule Name	QoS rule name	<p>The max to 12 characters</p> <p>Only set when adds a new rule and the follow-up can not be modified</p> <p>The rule name can not be repeated, otherwise the rule will be covered after the rule is added in front of the cover</p>
Control Interface	The interface type of QOS, include:	Dropdown List

Parameter	Details	Option
	<ul style="list-style-type: none"> • br0: QOS interface is LAN • modem: QOS interface is modem • modem2: QOS interface is modem2 	
Network	The network address that flow in and out via the QOS interface, is the object of speed limit.	Full in destination address and subnet mask Manual input Format1: A.B.C.D/Mask
Port	The network interface of QOS	Value area: 1-65535 You can not configure the port, if not the configuration represents all ports
Rate	Transmission rate of the network address settings	Value area: 1~65535 Units: Kbps
Ceil Rate	In ensuring the basic rate and the spare bandwidth, the maximum bandwidth of the network address of the communication can be obtained with higher priority will be given priority redundant bandwidth	Value area: 1~65535 Units: Kbps
Priority	Set the precedence of the rules	Value area: [1,30]

Step 4 Single click “save” icon to QOS setting.



NOTE

QoS is mainly used to allocate the average bandwidth for the users which access Internet through the router, or assigned specific users with more bandwidth. If the router is connected with two subnets: 192.168.8.1/24 and 192.168.9.1/24, the router QoS can control the rate of these two subnets; If the router's bandwidth is relatively well-off, the router can adjust the bandwidth based on priority and redundancy of two subnets, that is, the router meets the high priority redundancy bandwidth firstly, then meets the low priority subnet redundancy bandwidth.

---END

5.5.5 Dynamic Routing (Optional)

RIP configuration

RIP protocol (Routing Information Protocol) is the most widely IGP (Interior Gateway Protocol), it was designed for the same technology used in small networks, and therefore adapt to most of the campus network and used in a continuous regional networks that the rate change is not big, H8922S 3G/4G Router supports RIP v2 protocol. For more complex environments, generally do not use the RIP protocol.

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “Forward > RIP” to open “RIP” tab, as Figure 5-53.

Figure 5-41 RIP interface

Parameter Instruction as Table 5-26.

Table 5-26 RIP Parameter Instruction

Parameter	Details	Operation
RIP Service	Enable or disable RIP Service	Click the button to select. • Enable • Disable
Redistribute Connected	Enable or disable Redistribute Connected	Click the button to select. • Enable • Disable
Redistribute Static	Enable or disable Redistribute Static	Click the button to select. • Enable • Disable
Redistribute Kernel	Enable or disable Redistribute Kernel	Click the button to select. • Enable • Disable

- Step 3** Click “Add” to add a new RIP route, configuration interface as Figure 5-54.

Figure 5-42 RIP route configuration interface

Step 4 Configure RIP route parameter instruction, as Table 5-27.

Table 5-27 RIP parameter instruction

Parameter	Details	Operation
Basic Setting		
Add Type	Add the type of RIP route	Click the button to select Add Type <ul style="list-style-type: none"> When it is "Network", need to configure destination network address. When it is "Neighbor", need to configure neighbor's IP address
Network(directly connect to the router)	Add the destination network of RIP route	Add the destination network of RIP route Format: A.B.C.D/Mask
Neighbor(directly connect to the router)	Add the neighbor's IP address of RIP route	Add the neighbor's IP address of RIP route Format: A.B.C.D

Step 5 Single click "save" icon to RIP route setting.



- RIP is an interior gateway protocol. If the communications between the two routers do not go through another router, the two routers are adjacent. The RIP protocol specifies that no information exchange between non-adjacent routers.
- Routers exchanging information is all the information currently known to the router. That is its own routing table. At a fixed time to exchange routing information (such as every 30 seconds), then the router receives the routing information to update the routing table.
- RIP protocol "distance" also known as "hops" (hop count), because each through a router hop count is incremented. The RIP judges a better router according to the less routing hops, as the "shorter distance". RIP allows a path can contain up to 15 routers. Therefore, when the distance reach to 16 hops, it means the destination unreachable. RIP visible only for small Internet.

---END

OSPF configuration

OSPF (Open Shortest Path First) protocol is one of the (Interior Gateway Protocol), the most widely used IGP, for a single AS (autonomous system) in the routing decisions for large networks. OSPF business can be based whether the user needs to be configured at the factory H8922S 3G/4G Router.

Step 6 Log-on WEB GUI of H8922S 3G/4G router.

Step 7 Click “Forward > OSPF” to open “OSPF” tab, as Figure 5-55.

Figure 5-43 OSPF Interface

OSPF parameter instruction as Table 5-28

Table 5-28 OSPF parameter instruction

Parameter	Details	Operation
OSPF Service	Enable or disable OSPF Service	Click the button to select <ul style="list-style-type: none"> • Enable • Disable
Redistribute Connected	Enable or disable Redistribute Connected	Click the button to select <ul style="list-style-type: none"> • Enable • Disable

Parameter	Details	Operation
Redistribute Static	Enable or disable Redistribute Static	Click the button to select <ul style="list-style-type: none"> • Enable • Disable
Redistribute Kernel	Enable or disable Redistribute Kernel	Click the button to select <ul style="list-style-type: none"> • Enable • Disable

Step 8 Click “Add” to add a new OSPF route, configuration interface as Figure 5-56.

Figure 5-44 OSPF route configuration interface

Step 9 Configure RIP route parameter instruction, as Table 5-29.

Table 5-29 OSPF route parameter instruction

Parameter	Details	Option
Add Type	Add the type of OSPF route	Click the button to select Add Type <ul style="list-style-type: none"> • Network • Neighbor • Interface
• When Add Type is “Network”,		
Network	Set the network address as ospf sending address	Manual input Format1: A.B.C.D/Mask
AS Number	Used to identify the network (only the routers with the same domain address can exchange routing information)	Manual input Value area:[0,65535]
When Add Type is “Neighbor”,		

Neighbor	The router can reach in the next hop	Manual input Format1: A.B.C.D/Mask
When Add Type is "Interface",		
Interface Name	The interface of the router	<ul style="list-style-type: none"> • Dropdown List • br0 • modem • modem2 • eth1 • eth0
Interface Attribute	Configure the router interface attribute, include cost and network	<ul style="list-style-type: none"> • Click the button to select • cost • network
Cost	Configure the cost of the router interface, used to learn routing table	Manual input Value area:1-65535
Network Type (when the interface attribute is network)	Configure the network type of the router interface	<ul style="list-style-type: none"> • Dropdown List • broadcast • non-broad • point-to-multipoint • point-to-point

Step 10 Single click "save" icon to OSPF route setting.

Step 11 Single click "save" icon to finish.



NOTE

OSPF is a link-state (Link-state) routing protocol, commonly used for the same routing domain. Here, the routing domain is an autonomous system, which refers to the routers can switch routing information through a unified network switching or routing protocol routing policy in the AS, all OSPF routers maintains an identical description of the database structure AS, which is stored in the database link status information corresponding routing domain, OSPF router is through this database to calculate its OSPF routing table.

As a link-state routing protocol, OSPF link state broadcast data LSA (Link State Advertisement) sent to all routers in an area, which is different from the distance vector routing protocols. Distance vector routing protocol passed some or all routing information of the routing table to the adjacent routers.

---END

5.6 VPN configuration

5.6.1 Overview

H8922S 3G/4G router supports VPN (Virtual Private Network) including L2TP/PPTP/GRE/IPIP/IPSEC. What's more, it supports VPN OVER VPN, e.g. GRE over IPsec, IPsec over PPTP/L2TP/GRE/IPIP.

5.6.2 VPDN configuration

VPDN stands for Virtual Private Dial-up Networks. Now VPDN supports L2TP and PPTP

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 See “4.3.1 Login WEB GUI

Step 3 Click “VPN > VPDN” to open “VPDN” tab.

Figure 5-45 VPDN configuration

Step 4 Click “Add” to add a new VPDN rule.

Figure 5-46 VPDN rule configuration

Step 5 Configure VPDN rule parameter.

Table 5-30 VPDN rule parameter instruction

Parameter	Details	Operation
VPDN service	To enable or disable the VPDN rule	Click “Enable”
Basic Settings		
Interface name	Name of this VPDN rule	Cannot be modified after save.
protocol	VPDN protocol includes <ul style="list-style-type: none"> • L2TP • PPTP 	Select from Dropdown List, cannot be modified after save.
Service IP or Domain	IP or domain of server to be visited	To input the IP or domain of server to be visited.
Username	Username of server to be visited	To input the username.
Password	Password of server to be visited	To input password.
Advanced settings	Advanced parameter of PPP link	Click “Display”

Step 6 Single click “save” icon to finish.

After a VPDN rule is added, router will build VPN communication with service address automatically. To see the tunnel status, click “View” in “Tunnel” tab.

Figure 5-47 L2TP tunnel status

Network	Applications	VPN	Forward	Security	System	Status
VPDN	Tunnel	IPSec				

Interface Name: hongdian

Status: disconnected

Protocol: l2tp

Local IP Address:

Remote IP:

Refresh Return

---END

5.6.3 Tunnel configuration

Tunnel technology transfers data between the networks through the Internet infrastructure. In the whole process of transmission, when the encapsulated data package delivered on a public Internet, the logic path which the packet passes through is called tunnel. GRE and IPIP Tunnel configuration supports two modes.

GRE (Generic Routing Encapsulation, Generic Routing protocol encapsulation) specifies how to use a network protocol to another network protocol encapsulation method. The main purpose of the GRE protocol, there are two: internal protocol encapsulation and private address encapsulation.

IPIP tunnel is a simple agreement between two routers for IP packet encapsulation, IPIP tunnel interface will be like a physical interface in the interface list, many routers including Cisco, basically support the agreement. This agreement enables multiple network distribution possible.

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “VPN > Tunnel” to open “Tunnel” tab.
- Step 3** Click “Add” to add a new tunnel.

Figure 5-48 Tunnel configuration

The screenshot shows the 'Tunnel' configuration page in the router's web interface. At the top, there are three tabs: 'VPN', 'Tunnel', and 'IPsec'. The 'Tunnel' tab is selected. Below the tabs, there is a section for 'IP Tunnel Service' with two buttons: 'Enable' and 'Disable'. Below this, there is a 'Basic Settings' section with the following fields:

- Tunnel Name:** A text input field with a red asterisk and the hint '* Max length is 8'.
- Tunnel Mode:** A dropdown menu with 'ipip' selected.
- Local Virtual IP:** A text input field with a red asterisk and the hint '* eg. 10.1.1.1'.
- Peer Virtual IP:** A text input field with a red asterisk and the hint '* eg. 10.1.1.2'.
- Interface Type:** A dropdown menu with 'static ip' selected.
- Local Extern IP:** A text input field with a red asterisk and the hint '* eg. 192.168.8.1'.
- Peer Extern IP:** A text input field with a red asterisk and the hint '* eg. 192.168.0.1'.

At the bottom of the form, there are two buttons: 'Save' and 'Return'.

- Step 4**
- Step 5** Configure Tunnel rule parameter

Table 5-31 Tunnel rule parameter instruction

Parameter	Details	Operation
IP Tunnel Service	To enable or disable IP tunnel service	Click “Enable”
Basic Settings		
Tunnel name	Name of the tunnel, cannot be modified after save	Input the name of tunnel
Tunnel Mode	Tunnel mode: <ul style="list-style-type: none"> • gre • ipip 	Select from Dropdown List
Local virtual IP	Virtual IP address of local tunnel	Format: interface type A.B.C.D/M.
Peer virtual IP	Virtual IP address of peer tunnel	Format: interface type A.B.C.D/M.
Interface type	To choose “interface” or “static IP”	Select from Dropdown List.
Local Extern interface	This parameter will need to be set if “interface” is selected in “interface type”. Choose any connected interface as external interface	Select from Dropdown List.
Local extern IP	This parameter need to be set if “static IP” is selected for “interface type”. It is to set IP address to external network	Format: interface type A.B.C.D/M.
Peer extern IP	External interface IP of counterpart network tunnel. Usually a public IP address, also can be a LAN IP	Format: interface type A.B.C.D/M.

Step 6 Single click “save” icon to finish.

---END

5.6.4 IPSec configuration

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “VPN > IPSec” to open “IPSec” tab.

Figure 5-49 IPSec tab

Network	Applications	VPN	Forward	Security	System	Status
VPN	Tunnel	IPSec				

Phase1

Policy Name	Encrypt	Hash	Authentication	Operation

Phase2

Policy Name	Encrypt	Hash	Remote Subnet	Operation

IPSec Interface

Interface Name	Encrypt Interface	Destination IP or Domain	Operation

[Add](#)
[Refresh](#)

Step 3 Click “Add” to add a new IPSec rule.

There are 3 phases for IPSec configuration:

1. Phase 1 parameter

Figure 5-50 IPSec phase 1 configuration

Basic Settings

Select ☒ Phase1 ☐ Phase2 ☐ Ipsec

Policy Name * Max length is 12

Initiate Mode

Encrypt

Hash

Authentication

Pre Share Key * Max length is 24

Self Identify Max length is 64

Match identify Max length is 64

IKE Lifetime * 120-86400 s

Group Name

DPD Service ☐ Enable ☒ Disable

DPD Delay 1-512 s

DPD Retry Times 1-512 times

Table 5-32 IPSec Phase 1 Parameter instruction

Parameter	Details	Operation
Basic Settings		
Select	To select which phase of IPSec, phase 1, phase 1 or phase IPSec	Select "Phase 1"
Policy Name	Name of phase 1, mainly to match phase "IPSec"	To input the name of phase 1. Cannot be changed after save.
Initial Mode	To choose "main" or "aggr"	Select from Dropdown List, "aggr" is recommended
Encrypt	Supports 3des and aes	Select from Dropdown List
Hash	Supports md5 and sha1	Select from Dropdown List

Parameter	Details	Operation
Authentication	To select authentication	Select from Dropdown List, presently only "PSK" supported
Pre Share Key	To set pre share key	Max 24 letters
Self Identify	To set the self ID of IPSec	To input the ID, need to match the ID of other side
Match Identify	To input the match ID of IPSec	To input match ID, need to match ID of other side
IKE Lifetime	Life time of IKE key	Value area: 120~86400 Unit: second
Group Name	Select group	Select from Dropdown List
DPD Service	To enable DPD service	To click "Enable"
DPD Delay	To set DPD check interval time	Manual input Value area : 1~512 Unit: second
DPD Retry Times	Max times to continuous DPD check failure.	Manual input Value area: 1~512

Single click "save" icon to finish phase 1 configuration.

2. Phase 2 parameter.



In above parameters, "Initial Mode", "Encrypt", "Hash", "Authentication" "Pre Share Key", "IKE Lifetime", "Group Name" need to match parameter of IPSec server. "Self Identify" and "Match Identify" needs to match "match Identify" and "Self Identify" of IPSec sever respectively.

Figure 5-51 IPSec phase 2 configuration

Basic Settings

Select ☐ Phase1 ☒ Phase2 ☐ Ipsec

Policy Name * Max length is 12

Encryption Protocol

Encrypt

Hash

PFS

Group Name

Lifetime * 120-86400 s

Transport Mode

Local Subnet * eg. 192.168.8.0/24

Remote Subnet * eg. 192.168.88.0/24

Table 5-33 IPSec Parameter instruction

Parameter	Details	Operation
Basic Settings		
Select	To select which phase of IPSec, phase 1, phase 1 or phase IPSec	Select "Phase 2"
Policy Name	Name of phase 2, mainly to match phase "IPSec"	To input the name of phase 2. Cannot be changed after save
Encryption Protocol	Supports esp, ah, ah+esp	Select from Dropdown List
Encrypt	Supports des, 3des, aes	Select from Dropdown List
Hash	Supports md5 and sha1	Select from Dropdown List
Group Name	Need to configured when PFS is "open", to set the key length of SA initial of phase 2	Select from Dropdown List

Parameter	Details	Operation
PFS	To open or close PFS	Select from Dropdown List
Lifetime	IPSec SA key life time	Value area: 120~86400 Unit: second
Transport Mode	Supports tunnel, transport and auto.	Select from Dropdown List
Local Subnet	Set local subnet	No need to set for “transport” mode, only for “auto” and “tunnel”. Format: A.B.C.D/M
Remote Subnet	To set local subnet	No need to set for “transport” mode, only for “auto” and “tunnel”. Format: A.B.C.D/M

Single click “save” icon to finish phase 2 setting.

3. “IPSec” parameter configuration

Figure 5-52 IPSec configuration tab

To configure “IPSec” parameters, then click “Save”.

Table 5-34 IPSec Parameter instruction

Parameter	Details	Operation
Basic Settings		

Parameter	Details	Operation
Select	To select which phase of IPSec, phase 1, phase 1 or phase IPSec	Select "IPSec"
Interface Name	Name of this phase	Input name
Match Phase1	To select a matching name of "phase1"	Select from Dropdown List.
Match Phase2	To select a matching name of "phase2"	Select from Dropdown List
Destination IP or Domain	counterpart IPSec server IP or domain	Input counterpart IPSec server IP or domain
Encryption Interface	To select binding interface of IPSec. to bind VPDN/modem/br0 as local interface of IPSec initial can support IPSec OVER VPDN. In addition, after binding, IPSec rule will change as per the charge of binding interface. Thus can resume link of IPSec dialing interface and keep IPSec linked as soon as possible	Select from Dropdown List

---END

5.6.5 OpenVPN Configuration

OpenVPN is the VPN achievement based on the OpenSSL library's application layer. Compared with the traditional VPN, it is simple and easy to use. OpenVPN all the communications are based on a signal IP port, and it use the UDP protocol transports default and recommended. It can also support the TCP protocol. OpenVPN connection can through most of the proxy servers and work well in the NAT environment. Its server side has the function of pushing some network configuration information (including IP address, route configuration and so on) to the client side. OpenVPN offers two types of interfaces for networking via the universal TUN/TAP driver. It can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. Port 1194 is the official IANA (Internet Assigned Numbers Authority) assigned port number for OpenVPN.

Step 1 Login WEB GUI.

Step 2 See "4.3.1 Login WEB GUI".

Step 3 Click "VPN > OpenVPN".

Step 4 Enter "OpenVPN" page, as shown in Figure 2-4.

Figure 5-53 OpenVPN configuration page

Step 5 Configure OpenVPN parameter.

Step 6 The parameter instruction is shown in Table 2-1.

Table 5-35 OpenVPN parameter instruction

Parameter	Detail	Operation
OPENVPN Service	Enable OPENVPN Service.	Click button options: <ul style="list-style-type: none"> • Enable • Disable
Basic Setting		
Working Modem	Supports two working modes: <ul style="list-style-type: none"> • Client mode: client type mode • Multi mode: peer to peer working mode (peer is non-server) 	Dropdown list options: <p>Select the required working mode from dropdown list.</p>

Parameter	Detail	Operation
Dev	<p>Dev represents the network interface type, and supports two types:</p> <ul style="list-style-type: none"> • Tun(OSI Layer 3):Simulates network layer device to operate the third layer data packets, such as IP packets • Tap(OSI Layer 2):Equates to an Ethernet device to operate the second layer data packets, such as Ethernet data frame. 	<p>Dropdown list options:</p> <p>Select the required working mode from dropdown list.</p> <p>Demand consistent with peer.</p>
Protocol	<ul style="list-style-type: none"> • Data transfer protocol type settings: ●TCP protocol: A kind of connection oriented reliable transmission protocol, which is suitable for the occasions where the reliability requirement is high and the communication efficiency is not high. ●UDP protocol: A kind of non - connection unreliable transmission protocol, which is suitable for the scene with relatively high efficiency and relatively low reliability. 	<p>Dropdown list options:</p> <p>Select the required working mode from dropdown list.</p> <p>Demand consistent with peer.</p>
Destination address or domain	Specifies connected server address	<p>WORD type , max 32 bytes.</p> <p>Demand consistent with peer.</p>
Port	Specifies connected server port	<p>Value range: 1~65535</p> <ul style="list-style-type: none"> • Default: 1194 <p>Demand consistent with peer.</p> <ul style="list-style-type: none"> •
Compress	<p>Compression protocol: configure whether VPN connection compression is opened.</p> <p>If the server is open, the client must open.</p>	<p>Click button options:</p> <ul style="list-style-type: none"> • Enable • Disable

Parameter	Detail	Operation
Nobind	Configure whether to bind to the specific local port.	Click button options: <ul style="list-style-type: none"> • Enable • Disable
Authentication	Configuring the VPN data transfer mode: <ul style="list-style-type: none"> • SSL: encrypt the network connection in transport layer, high safety factor. • Text: transport with text form during transmission, low safety factor 	Dropdown list options: Select the required data transfer type from dropdown list.
Ca	Specifies the file path for the client CA certificate	WORD type, max 32 bytes.
Key	Specifies the private key path for the current client	WORD type, max 32 bytes.
Cert	Specifies the certificate file path for the current client	WORD type, max 32 bytes.”。
Tls	Open TLS, if the server is open, the client must also open. TLS: secure transport layer protocol (TLS) to provide confidentiality and data integrity between two communication applications. The protocol consists of two layers: the TLS record protocol (TLS Record) and the TLS handshake protocol (TLS Handshake)	WORD type, max 32 bytes.
Cipher	SSL's encryption algorithm system.	Drop box options: <ul style="list-style-type: none"> • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC

Step 7 Click “Save” to finish OpenVPN configuration.

---END

5.7 System configuration

5.7.1 Overview

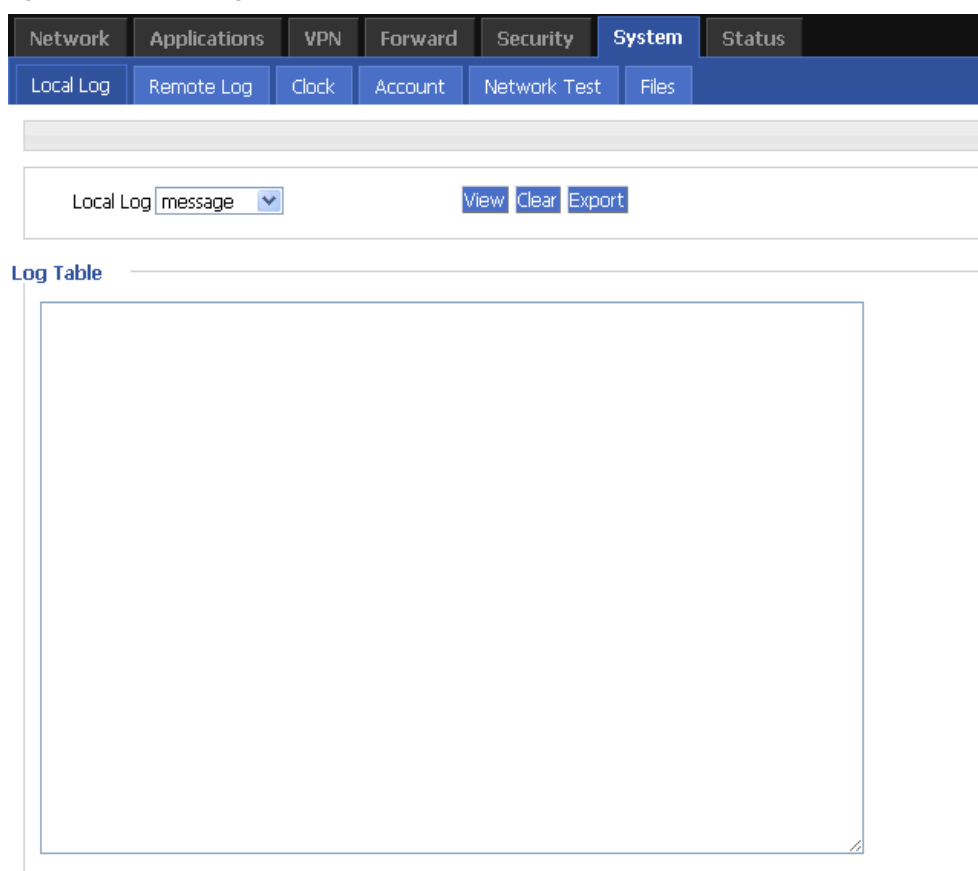
“System” can let you know the status of router, firmware upgrading and other maintenance.

5.7.2 Local Log

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “System > Local Log” to open “Local Log” tab.

Figure 5-54 Local Log tab



Step 3 Select type of “Local Log” and then click “View” to see log.

Click “Clear” to clear the log info in the “Log Table”, and click “Export” to export log in your local PC.

There are 3 types log:

- Message: system log, to record the running log of router, usually for most of users.
- Application: application program log, to record the Open or close of some application programs.
- Kernel: kernel log of router, usually for R&D engineers.



To see “local log”, “remote log” must be enabled.

---END

5.7.3 Remote Log

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “System > Remote Log” to open “Local Log” tab.

Figure 5-55 Remote Log tab

Step 3 Configure “Remote Log” parameter.

Table 5-36 Remote log parameter instruction

Parameter	Details	Operation
Log Status	To enable or disable remote log	Click “Enable”
Remote IP or Domain	IP address or Domain of remote log server	To input the IP address or domain to receive log
Remote Port	Port of remote log serve	Default port: 514

Step 4 Single click “save” icon to finish “Remote Log” parameter configuration.



A software tool Syslog is use to receive remote log in server. Syslog can be downloaded at website of <http://www.hongdian.com>.

---END

5.7.4 Clock

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “System > Clock” to open “Clock” tab.

Figure 5-56 “NTP” Time Synch.

Network Applications VPN Forward Security **System** Status

Local Log Remote Log **Clock** Account Network Test Files

Status

Time Synch. Type

NTP Server IP or Domain

NTP Server BackUp Max length is 64

NTP Synch. Interval * 1-65535 s

Time Zone

Figure 5-57 Manual Time Synch. Type

Network Applications VPN Forward Security **System** Status

Local Log Remote Log **Clock** Account Network Test Files

Status

Time Synch. Type

Set Date - - eg. 1970-01-01

Set Time - - eg. 07:01:01

- Step 3** Set “clock” parameters.

Table 5-37 Clock Parameter instruction

Parameter	Details	Operation
Status	To enable to disable Time Synchronization service	<ul style="list-style-type: none"> To click “Enable” or “Disable”

Time Synch. Type	Type to synchronize system time	• Select “NTP” or “Manual”
When select “NTP” in “Time Synch. Type”		
NTP Server IP or Domain	IP or domain of NTP server	Select from Dropdown List
NTP Server Backup	Backup NTP server	Manual input server domain or IP address
NTP Synch. Interval	Interval for NTP client to check time with NTP Server. E.g. every 10 minutes	Value area: 1~65535 Unit: second Default: 600 s
Time Zone	Time Zone	Select from Dropdown List
Time Zone Number	For “Custom” option in “Time Zone”. E.g. +8 or -4	WORD type
When select “Manual” in “Time Synch. Type”		
Set Date	To set date	YYYY-MM-DD e.g. 1970-01-01
Set Time	To set time	HH:MM:mm E.g. 07:01:01

Step 4 Single click “save” icon to finish.

---END

5.7.5 Account

“Account” is to change username/password, change web port and forbid other users to visiting the router.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “System > Account” to open “Account” tab.

Figure 5-58 Account tab

Account Type: WEB

Account Level: admin

Current Username: admin

Old Password: * Max length is 64

New Username:

New Password:

New Password Again:

Port: 1-65535

Save

Step 3 Set account parameters.**Table 5-38** Account parameter instruction

Parameter	Details	Operation
Account Type	Visit the router on web	<ul style="list-style-type: none"> Select from Dropdown List
Account Level	Level of account to login router	Select from Dropdown List <ul style="list-style-type: none"> Admin: can view and change the parameter. Guest: can view parameter and export log and use "Network Test".
Current Username	Current username	Showing user name
Old password	Current password	To input current PW
New Username	New username	Manual input, max 64 word type.
New Password	New password	Manual input, max 64 word type.
New password again	To confirm the new password	Manual input, max 64 word type.
Port	Web port to login router	Manual input Value area 1~65535

Parameter	Details	Operation
		Default: 80

Step 4 Click “Save” to finish configuration. After saving, user needs to login again.

---END

5.7.6 Network Test

Network Test

This function includes Ping function and Trace router function.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “System > Network Test” to open “Network Test” tab.

Figure 5-59 Network Test Tab

The screenshot displays the 'Network Test' tab in the router's web interface. The top navigation bar includes 'Network', 'Applications', 'VPN', 'Forward', 'Security', 'System' (selected), and 'Status'. The 'System' sub-menu shows 'Local Log', 'Remote Log', 'Clock', 'Account', 'Network Test' (selected), and 'Files'. The main content area features a 'Destination' input field with a red asterisk, and 'Ping' and 'Trace' buttons. Below this is a 'Result' section with a large empty box for test results. At the bottom, there is a 'Refresh' button.

Step 3 Input IP address or domain to be tested in “Destination”, click “Ping”, to check whether the router can be linked with destination.

Table 5-39 Network Test Parameter instruction

Parameter	Details	Operation
Destination	To input IP address or domain to be	Input IP address or

Parameter	Details	Operation
	tested	domain to be tested
Ping	To use Ping to test link	Click “Ping”
Trace	To use Trace command to test hops from the router to destination	Click “Trace”
Result	Test result	

---END

5.7.7 Files

Firmware Setting

H8922S 3G/4G router supports upgrade firmware locally.

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “System > Files” to open “Files” tab.

Figure 5-60 Files tab



NOTE

If “reset” is selected, all parameters will be reset to factory setting.

In upgrading, don’t close the page.

Upgrading files is suggested not to exceed 6MB. If larger than 6MB please use “CFE MINI WEB update”.

Step 3 Click “Browse” to select upgrading file and then click “Upgrade”.

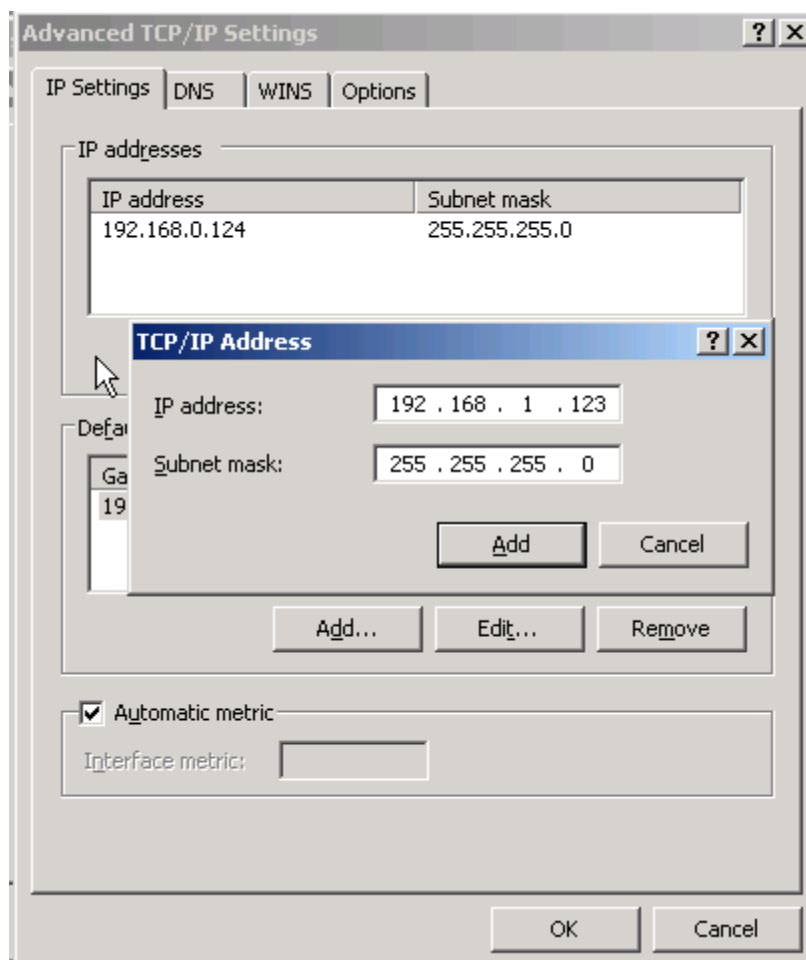
---END

CFE mode upgrading

If upgrading file is larger than 6MB, CFE mode upgrading shall be used to upgrade.

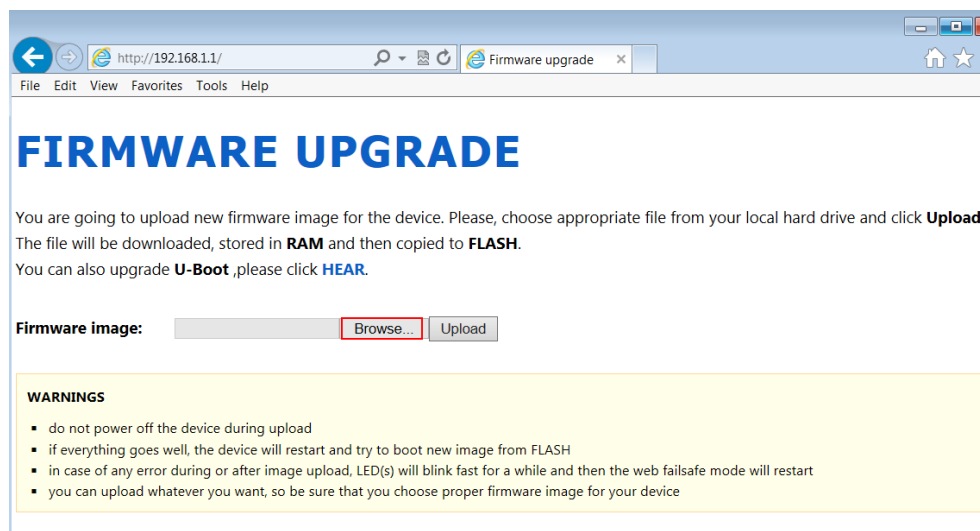
Step 4 Add an IP address 192.168.1.

Figure 5-61 Add an IP address

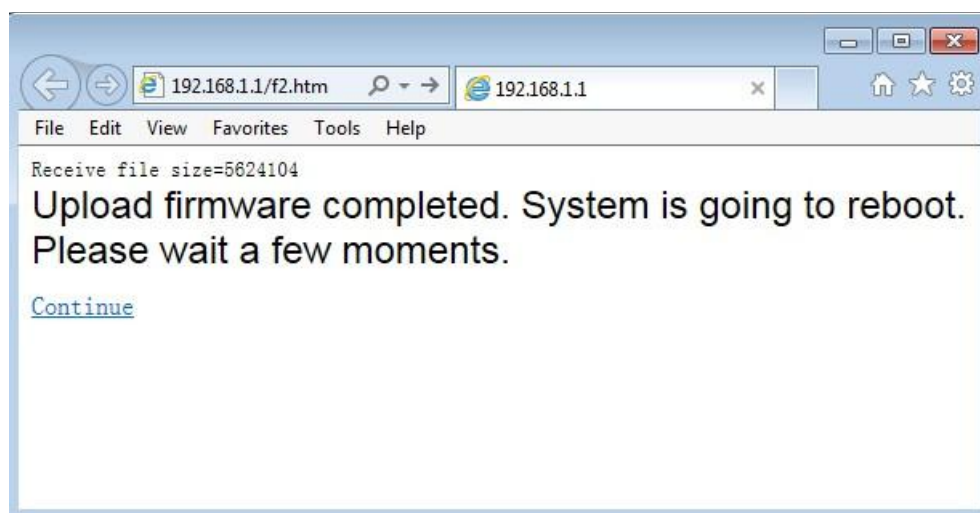


Step 5 Press the RESET/DEF interface. Do not release it. Hold it, meanwhile power on router, till 30 seconds, and connection to PC is built properly. Then release RESET/DEF interface.

Step 6 Input 192.168.1.1 in your browser, click “enter” you will see following page. If not, start over again from step 1.

Figure 5-62 CFE mode upgrading

Step 7 Click “Browse” to select upgrading file, and then click “Upload” to begin upgrading.

Figure 5-63 CFE upgrading page

Upgrading will need 4-6 minutes, if RUN light is on, upgrading is OK.



TIP

You can also PING br0 address on your PC (**ping 192.168.8.1 -t**). if Ping ok, upgrading is OK.

---END

Backup setting

H8922S 3G/4G router supports to backup and to recover configuration file.

- Click “Browse” to select a configuration file to be imported. And then click “Import” to resume the configuration as the configuration file.
- Click “Export” to export configuration file and save it in local PC.

Figure 5-64 Backup setting page

**NOTE**

After import, router will reboot automatically.

“Key”: if key is input when export configuration file, this key need to be input in import. Not more than 8 digits for key.

Factory setting

H8922S 3G/4G router has function to resume factory configuration. Users can set the configuration to factory mode, and also can set the current configuration into default configuration and generate a default factory configuration file in router. To resume this default factory setting, users can click “Load” in “factory setting”. If the default factory configuration file is deleted, the router will be resumed back to initial factory setting.

Figure 5-65 Factory setting page

The screenshot shows the 'Factory setting' page of the H8922S 3G/4G Router. The page has a top navigation bar with tabs: Network, Applications, VPN, Forward, Security, System (selected), and Status. Below this is a sub-navigation bar with tabs: Local Log, Remote Log, Clock, Account, Network Test, and Files. The main content area contains several sections: 'Firmware Setting' with 'Choose File' and 'No file chosen' buttons, and 'Upgrade' and 'Reset' buttons; 'Backup setting' with 'Choose File' and 'No file chosen' buttons, and 'Import', 'Export', and 'Key' buttons; 'Factory setting' with 'Save' and 'Load' buttons (highlighted with a red rectangle); and 'Patch Operation' with a 'Delete' button. At the bottom, there is a table with columns 'Patch Name', 'Patch Version', and 'Operation', and 'Reboot' and 'Refresh' buttons.

- Save: to save the current setting as default factory configuration setting.
- Load: to resume default factory setting.

Patch operation function

H8922S 3G/4G router supports to delete patch.

Figure 5-66 Patch operation

The screenshot displays the router's web interface with the 'System' tab selected. The interface includes a top navigation bar with tabs: Network, Applications, VPN, Forward, Security, System (active), and Status. Below this is a secondary navigation bar with links: Local Log, Remote Log, Clock, Account, Network Test, and Files. The main content area contains several sections: 'Firmware Setting' with a 'Choose File' button, 'No file chosen' text, and 'Upgrade' and 'Reset' buttons; 'Backup setting' with a 'Choose File' button, 'No file chosen' text, and 'Import', 'Export', and 'Key' buttons; 'Factory setting' with 'Save' and 'Load' buttons; and 'Patch Operation' which is highlighted with a red box. The 'Patch Operation' section includes a 'Delete' button, a table with columns 'Patch Name', 'Patch Version', and 'Operation', and 'Reboot' and 'Refresh' buttons at the bottom.

- Delete: to delete patch.

Reboot/Refresh

Click “Reboot” to restart the router, or click “Refresh” to refresh the page.

Figure 5-67 Reboot /Refresh

The screenshot shows the 'System' tab in the router's WEB GUI. The top navigation bar includes 'Network', 'Applications', 'VPN', 'Forward', 'Security', 'System' (selected), and 'Status'. Below this, a sub-menu bar contains 'Local Log', 'Remote Log', 'Clock', 'Account', 'Network Test', and 'Files'. The main content area has several sections: 'Firmware Setting' with 'Choose File' and 'No file chosen' buttons, and 'Upgrade' and 'Reset' buttons; 'Backup setting' with 'Choose File' and 'No file chosen' buttons, and 'Import', 'Export', and 'Key' buttons; 'Factory setting' with 'Save' and 'Load' buttons; and 'Patch Operation' with a 'Delete' button. At the bottom, there is a table with columns 'Patch Name', 'Patch Version', and 'Operation'. Below the table are 'Reboot' and 'Refresh' buttons, which are highlighted with a red rectangle.

5.8 Status

5.8.1 Overview

Status provides the basic info, network status info, router info of H8922S 3G/4G Router.

5.8.2 Base Information

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click "Status > Base information" to open "Base Information" tab.

Figure 5-68 Base Information tab

The screenshot shows the 'Status' tab in the router's WEB GUI. The top navigation bar includes 'Network', 'Applications', 'VPN', 'Forward', 'Security', 'System', and 'Status' (selected). Below this, a sub-menu bar contains 'Base Information' (selected), 'LAN', 'WAN', 'Modem', and 'Routing Table'. The main content area displays a table with router information:

Router Model	H7932-RHH
Router SN	7932R201209HH21001
Hardware Version	V13-S205E
Software Version	3.0.0

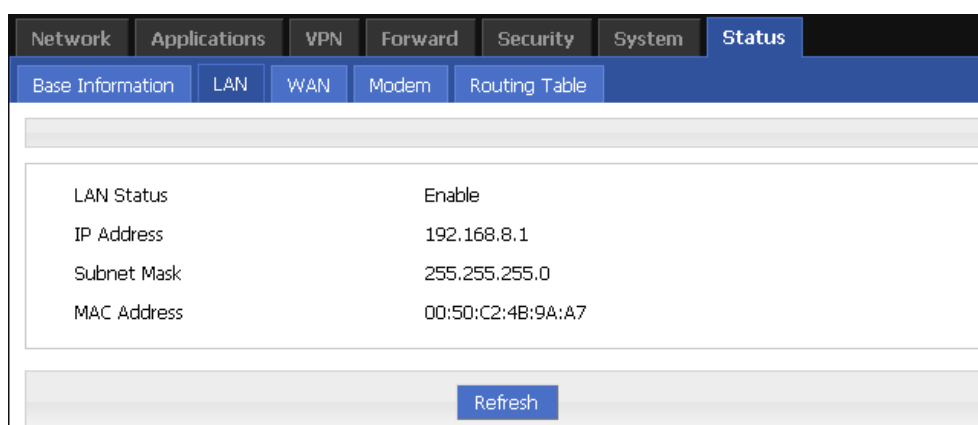
At the bottom of the content area is a 'Refresh' button.

Table 5-40 Base information Parameter instruction

Parameter	Details	Operation
Router Model	Router model info	
Router SN	Router Serial No info	
Hardware version	Router hardware version info	
Software version	OS and application software info.	

5.8.3 LAN

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “Status > LAN” to open “LAN” tab.

Figure 5-69 “LAN” info**Table 5-41** LAN Parameter instruction

Parameter	Details	Operation
LAN status	To show current LAN interfaces status.	
IP address	To show the LAN IP address.	
Subnet Mask	Subnet mask of LAN interface.	
MAC address	To show the MAC address of the router.	

5.8.4 WAN

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “Status > WAN” to open “WAN” tab. There are three types of WAN status: static IP/DHCP/PPPOE.

Figure 5-70 Static IP WAN status

Network	Applications	VPN	Forward	Security	System	Status
Base Information	LAN	WAN	Modem	Routing Table		
WAN Status		Enable				
Wan Type		static IP				
Local IP Address		192.168.10.1				
Mask		255.255.255.0				
MAC Address		00:50:C2:4B:9A:A9				
<div>Refresh</div>						

Figure 5-71 DHCP WAN status

Network	Applications	VPN	Forward	Security	System	Status
Base Information	LAN	WAN	Modem	Routing Table		
WAN Status	Enable					
Wan Type	dhcp					
Local IP Address	192.168.10.1					
Mask	255.255.255.0					
MAC Address	00:50:C2:4B:9A:A9					
<div>Refresh</div>						

Figure 5-72 PPPoE WAN status

Parameter	Value
WAN Status	Enable
Wan Type	pppoe
Local IP	192.168.100.247
Remote IP	192.168.100.1

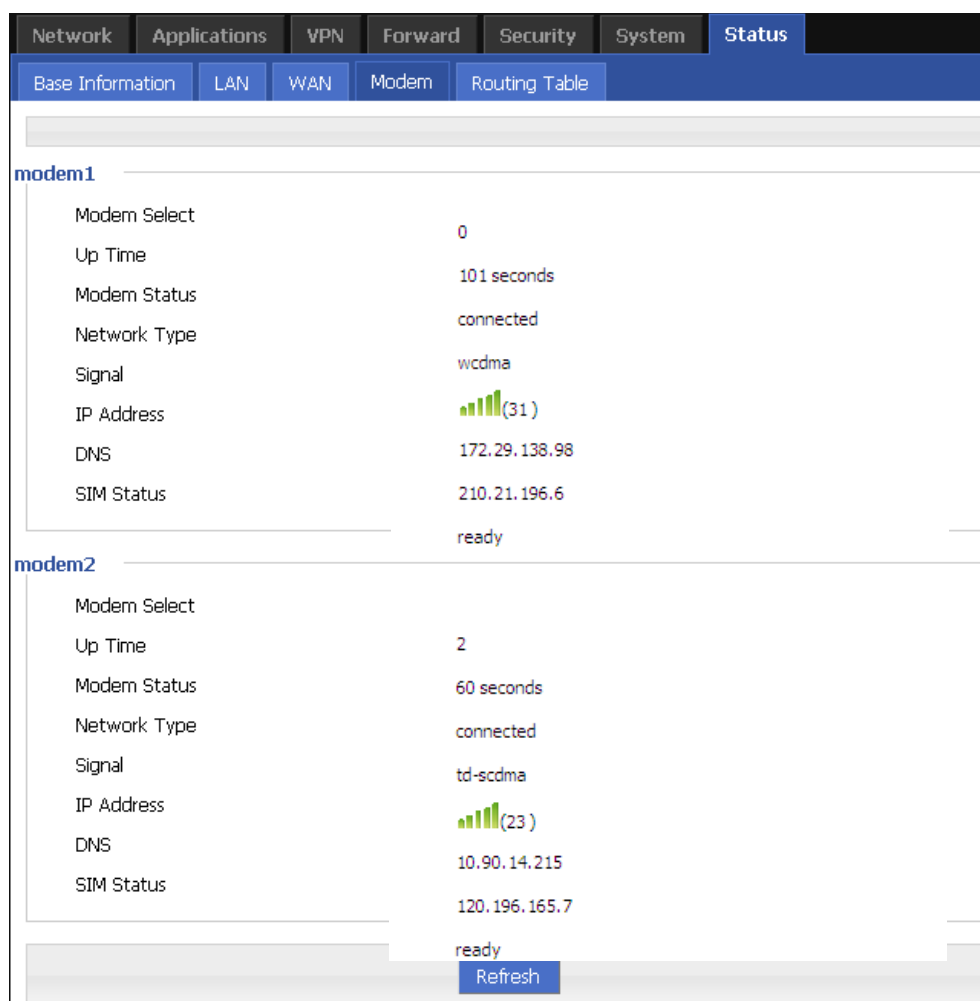
Refresh

Table 5-42 WAN Parameter instruction

Parameter	Details	Operation
WAN status	To show the current WAN is used or not	
WAN Type	To show the current WAN type	
Local IP	To show the local IP of WAN interface	
Subnet mask	To show the subnet mask	
MAC address	To show the MAC address of the router	
PPPoE for WAN type		
Status	To show the link status of WAN interface PPPoE	
Local IP	To show the router IP distributed by PPPoE	
Remote IP	To show IP of PPPoE server	

5.8.5 Modem

- Step 1** Log-on WEB GUI of H8922S 3G/4G router.
- Step 2** Click “Status > Modem” to open “Modem” tab.

Figure 5-73 Modem Status page**Table 5-43** Modem Parameter instruction

Parameter	Details	Operation
Modem Select	To show the current modem name	
Up tome	To show the current on line time of the modem Unit: second	
Modem Status	To show the Router's status to link to the mobile network	
Network type	Current network type of the SIM in use	
signal	Signal of mobile network Value area: 1-31	

Parameter	Details	Operation
IP Address	To show the external network IP address which the router links	
DNS	To show which DNS router is using	
SIM Status	Status of current SIM	

5.8.6 Routing Table

Step 1 Log-on WEB GUI of H8922S 3G/4G router.

Step 2 Click “Status > Routing Table” to open “Routing Table” tab.

Figure 5-74 Routing table page

Table 5-44 Routing table Parameter instruction

Parameter	Details	Operation
Static route		
Network	IP address the router can reach	
Subnet Mask	IP network the router can reach. It is used together with “Network”	
Gateway	Next hop IP address which the router will reach	
interface	Interface from router to gateway	
metric	Route No which the router reaches destination IP	

Parameter	Details	Operation
Static route		
Policy route		
Priority	Priority the router select route	

---END

5.9 RESET button function

“RESET” button is on the rear panel and next to power interface. This button can be used when the router is in use or when the router is turned on. There are 3 functions to press “RESET” button when the router is in use:

- Press “RESET” for about 2 seconds, router will reboot.
- Press “RESET” 5-10 seconds, the router will reboot, meanwhile, the router will be resumed to default factory setting configuration.
- Press “RESET” over 20 seconds, the router will reboot, and get into CFE upgrading. The router is resumed to default factory setting configuration.
- Press button when the router is turned on:
- Press “RESET” button and turn on the router, and keep pressing “RESET” for 2 seconds. The router will get into CFE upgrading mode.

---END

6 Typical application

About this chapter

Chapter	Content
6.1 Overview	Summary some typical application of H8922S 3G/4G router
6.2 Awake function	How to awake H8922S 3G/4G Router if not auto-dial
6.3 Parameter select	Parameter switch to achieve SIM backup function
6.4 VPN	H8922S 3G/4G Router VPN setting
6.5 Timing Task	Set Timing task on H8922S 3G/4G Router

6.1 Overview

H8922S 3G/4G Router commonly used function includes wake up, parameter switch, VPN, etc.

6.2 Awake function

Typical case

H8922S 3G/4G router support wake up function, means router will not auto-dial after power on, but dial triggered by data or call or SMS. Then router auto in offline by idle or timeout. This function could save your data traffic fee.

For example, after setting phone trigger number, a call to router by that number could trigger the router dial online; one phone number could control both modem & modem2.

parameter setting

Let us check an example:

Figure 6-1 Wake up/trigger setting example

Wake Up Service

Basic Settings

Wake Up Method

Offline Method

Online Time * 0-86400 s

Data Trigger

Add Phone Number

Phone Number * Max length is 32

Task Type

Phone Number	Task Type	Operation
861888888888	modem2-up	<input type="button" value="Del"/>
861222222222	modem-down	<input type="button" value="Del"/>
861222222222	modem2-down	<input type="button" value="Del"/>
861888888888	modem-up	<input type="button" value="Del"/>

Effect

By this setting, after router power on, if there are data trigger or you could call/SMS SIM1 or SIM2 number from 861888888888 to trigger corresponding SIM online, modem will dial online, After 3600s, router will offline. Or you could use 861222222222 to call SIM, make the router offline. Please notice, to enable this function, the SIM must support phone and/or SMS function.

6.3 Parameter select

Typical case

H8922S 3G/4G Router provide parameter select function, when working modem disconnect or works abnormal, router will switch to another SIM swiftly according to the rule you set. And ensure the network availability.

Parameter Select

Let us check an example:



Please set the "Parameter select" of modem and modem2 separately

Set rules as below

Figure 6-2 Rules setting

Rule Name	Interval	Retry Times	Running Timeout	Operation			
2	60	3	----	Mod	Del	En	Dis
1	60	3	----	Mod	Del	En	Dis

Figure 6-3 Parameter select setting 1

Rule Name	Name	Check Method	Operation
1	modem 0	check 8.8.8.8	Delete

Status [Enable](#) [Disable](#)

Basic Settings

Rule Name * 0-9

Interval * 1-512 s

Retry Times * 1-512

Running Timeout 1-65535 s

[Save](#)

select an interface to check

Interface Name

Check Method

Destination IP * eg. 192.168.8.1

[Add](#)

[Refresh](#) [Return](#)

Figure 6-4 Parameter select setting 2

Rule Name	Name	Check Method	Operation
2	modem2 2	check 8.8.8.8	Delete

Status [Enable](#) [Disable](#)

Basic Settings

Rule Name * 0-9

Interval * 1-512 s

Retry Times * 1-512

Running Timeout 1-65535 s

[Save](#)

select an interface to check

Interface Name

Check Method

Destination IP * eg. 192.168.8.1

[Add](#)

[Refresh](#) [Return](#)

When a working modem is offline, router will run parameter select rule: “check icmp”, check the IP you set by ping, in this case, 8.8.8.8. After 3 times failure, router will switch to modem2, and dial online works again.

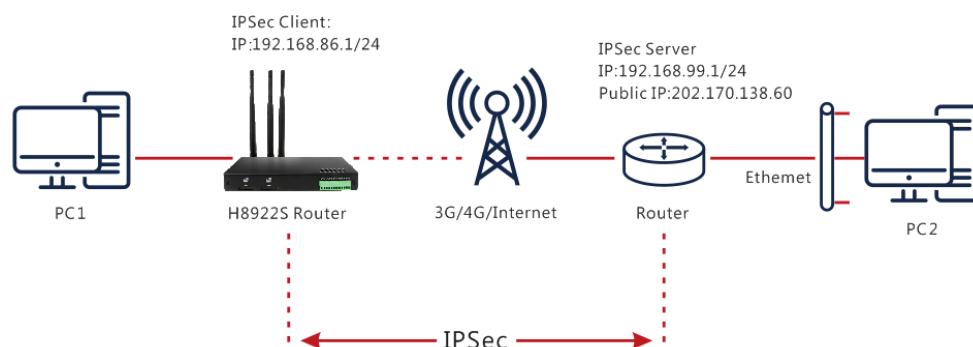
6.4 VPN

Introduction

VPN, virtual private network, a technology based on Internet, now H8922S 3G/4G router supports L2TP/PPTP/GRE/IPIP/IPSec of VPN.

L2TP used to build a virtual private network, after H8922S 3G/4G Router connect to company NAS server, PC under H8922S could visit company network like visiting the local area network.

Let us check a setting example:

Figure 6-5 Build IPsec

PC1 connect H8922S then build IPSEC link by VPN function of H8922S with company router. I assume using IPsec tunnel mode, H8922S end local network 192.168.86.1/24, company server end 192.168.99.1/24, by IPSEC, two LAN could communicate.

Parameter Setting

Figure 6-6 IPsec Phase 1

Basic Settings	
Select	<input checked="" type="radio"/> Phase1 <input type="radio"/> Phase2 <input type="radio"/> Ipsec
Policy Name	<input type="text"/> * Max length is 12
Initiate Mode	<input type="text" value="main"/>
Encrypt	<input type="text" value="des"/>
Hash	<input type="text" value="md5"/>
Authentication	<input type="text" value="psk"/>
Pre Share Key	<input type="text" value="...."/> * Max length is 24
Self Identify	<input type="text" value="xxx@xxx"/> Max length is 64
Match identify	<input type="text" value="yyy@yyy"/> Max length is 64
IKE Lifetime	<input type="text" value="28800"/> * 120-86400 s
Group Name	<input type="text" value="group768"/>
DPD Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DPD Delay	<input type="text" value="30"/> 1-512 s
DPD Retry Times	<input type="text" value="4"/> 1-512 times

Figure 6-7 IPSec Phase 2

Basic Settings

Select ☐ Phase1 ☒ Phase2 ☐ Ipsec

Policy Name * Max length is 12

Encryption Protocol

Encrypt

Hash

PFS

Group Name

Lifetime * 120-86400 s

Transport Mode

Local Subnet * eg. 192.168.8.0/24

Remote Subnet * eg. 192.168.88.0/24

Figure 6-8 IPSec

Basic Settings

Select ☐ Phase1 ☐ Phase2 ☒ Ipsec

Interface Name * Max length is 12

Match Phase1

Match Phase2

Destination IP or Domain * Max length is 64

Encrypt Interface

Company router server should have same setting but the identity and subnet setting for the company router server should be the opposite of those for H8922S 3G/4G Router.

Result

After setting H8922S 3G/4G Router and company router parameter, they can connect each other by IPSEC, and ping peer subnet, you could check status by click “view” button.

Figure 6-9 IPSec status

Interface Name	1
Status	connected
Local Subnet	192.168.86.0/24
Remote Subnet	192.168.99.0/24

```

~ #ping192.168.99.1 -I 192.168.86.1
PING 192.168.99.1 (192.168.99.1) from 192.168.86.1: 56 data bytes
64 bytes from 192.168.99.1: seq=0 ttl=255 time=1569.360 ms
64 bytes from 192.168.99.1: seq=1 ttl=255 time=769.937 ms

--- 192.168.99.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 769.937/1169.648/1569.360 ms

```

6.5 Timing Task

Typical Application

H8922S 3G/4G Router support timing task, by setting timing task, at certain time, router will operate reboot, online command. Etc. Easier the customer operation. I assume set the router online at certain time and keep a moment, then reboot every 24 hours. You could set like below.

Figure 6-10 Timing

Task Name	Operating Time	Task Type	Operation			
2	interval:1440	reboot	Mod	Del	En	Dis
1	date:1005-1008	modem-online	Mod	Del	En	Dis

Result

Router will be online at 10:05 AM and keep online until 10:08, then offline at 10:09.
And router will reboot every 24 hours count began last reboot.

Figure 6-11 router online

```

10:04:57 time[912]: ntpclient -h clock.via.net -s return 1{time.c->109}
10:04:57 time[912]: open the file(/tmp/ntp_first.mark) success!{time.c->254}
10:04:57 time[912]: NTP failed!{time.c->274}
10:04:59 pppd[345]: sent [LCP EchoReq id=0xf magic=0x5511fa91]
10:05:00 pppd[345]: rcvd [LCP EchoRep id=0xf magic=0xc1caf26e]
10:05:05 modem[969]: got SIG_TERM signal{modem.c->605}
10:05:05 modem[969]: argument error{hp_chat.c->533}
10:05:05 modem[1019]: modem_parameter_init :: boot!{modem.c->702}
10:05:05 modem[1019]: modem name is (0, 0){modem.c->294}
10:05:05 modem[1020]: find the modem(ZTE-AD3812:10){modemcheck.c->185}
10:05:06 modem_mg[229]: search usb device{modem_mg.c->1489}
10:05:06 modem[1020]: open the device(/dev/ttyUSB2) succeed{hp_chat.c->326}

```

Figure 6-12 router off line

```

10:09:02 pppd[1067]: Terminating on signal 15
10:09:02 pppd[1067]: Connect time 3.0 minutes
10:09:02 pppd[1067]: Sent 445 bytes, received 2660 bytes.
10:09:03 netdown[1336]: ppp interface modem down{netdown.c->37}
10:09:03 netdown[1336]: killall -SIGUSR2 modem{netdown.c->47}
10:09:03 pppd[1067]: Script /usr/sbin/pppdown-run started (pid 1335)
10:09:03 pppd[1067]: sent [LCP TermReq id=0x2 "User request"]
10:09:03 pppd[1067]: rcvd [LCP TermAck id=0x2]
10:09:03 pppd[1067]: Connection terminated.

```

Figure 6-13 router reboot

```

10:12:01 timing[1484]: timing: Reboot the system{hp_misc.c->984}

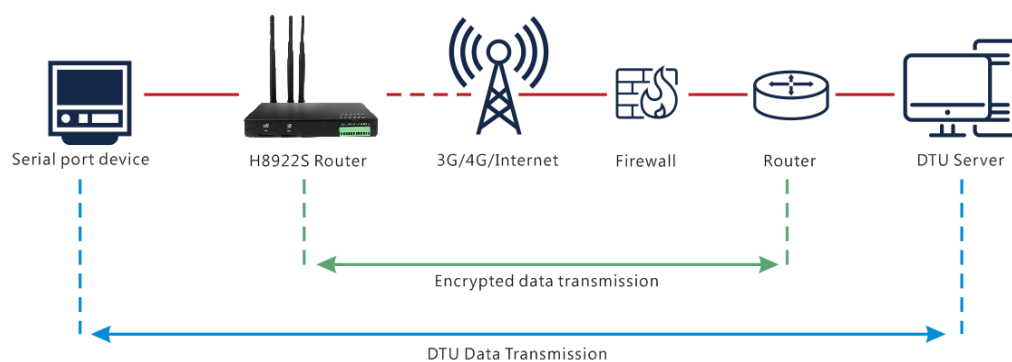
```

6.6 DTU function application

Scene presentation

H8922S router fully takes into account the DTU access function requirements, the system built-in and registration center and data center communication function, can provide similar DTU data terminal unit transparent data transmission function.

This scene is the DTU transmission of Wan, the transmission protocol is TCP, and the serial device in the scene is simulated by SSCOM serial interface software. In reality, the serial devices can be RTU, PLC and so on. The implementation of the DTU transport is shown in the figure below.

Figure 6-14 DTU Application

Parameter configuration

This scenario requires the "DTU" configuration, and the configuration step is referred to as "DTU configuration" section.

The parameter configuration is shown in the figures below.

Figure 6-15 TCP mode configuration

DTU Service Enable Disable

Basic Settings

Work Mode Client

Local Port 1234 1-65535

Protocol ☒ TCP ☐ UDP

Channel Type ☒ TREBLE ☐ BACKUP

Received Timeout 500 * 1-65535 ms

RS232 Data Timeout 500 * 1-65535 ms

Encryption NONE

Data Center Configure

Server IP or Domain 210.75.17.180 Max length is 64

Server Port 30076 1-65535

Server IP or Domain 2 Max length is 64

Server Port 2 1-65535

Server IP or Domain 3 Max length is 64

Server Port 3 1-65535

Connect Interval 5 1-65535 s

Retry Times 3 1-65535

Figure 6-16 Add text data

Login packets Settings

Login Data: Max length is 64

Heartbeat Settings

Heartbeat Data: Max length is 64

Heartbeat Interval: 1-65535 s

Rs232 Setting

Rate:

Parity:

Databits:

Stopbits:

Open the Socket tool (TCP&UDP testing tool) in the server or PC which IP is the “Server IP” in the router’s DTU configuration, start a TCP server listening the port which is the same with “Server Port” in the router’s DTU configuration .

Figure 6-17 TCP server tool

Hercules SETUP utility by HW-group.com

UDP Setup | Serial | TCP Client | **TCP Server** | UDP | Test Mode | About

Received data

```
myLoginData..myHeartbeat ..myHeartbeat ..myHeartbeat
..myHeartbeat ..myHeartbeat ..myHeartbeat ..myHeartbeat
..myHeartbeat ..myHeartbeat ..
```

Sent data

☐ HEX

Server status

Port:

TEA authorization

TEA key

1: 01020304 3: 090A0B0C

2: 05060708 4: 0D0E0F10

☐ Client authorization

Client connection status

```
19:26:14: All connections
19:27:08: All connections
8:38:24: All connections
9:03:50: 192.168.8.1 Clie
9:05:25: All connections
9:05:43: 192.168.8.1 Clie
9:06:08: All connections
```

Clients count: 0

Cursor decode

HEX: Decimal: Decoder Input:

Server settings

☐ Server echo

☐ Redirect to UDP

HWgroup
www.HW-group.com
Hercules SETUP utility
Version 3.2.8

Application result

The Client mode of H8922S is to make the router work as a normal TCP/UDP client, which can connect to a TCP/UDP server via the server's IP and port. After socket connection is setup, the message received on socket will be forward to RS232 serial port; conversely, the message of RS232 port can be forward to the socket connection.

7

FAQ

About this chapter

Chapter	Content
7.1 Hardware failure	Possible hardware failure during using H8922S 3G/4G Router and how to handle them
7.2 Dial online problem	Possible problem during dialing and how to handle them
7.3 VPN	Possible problem when connecting VPN
7.4 Web configuration	Possible WEB configuration problem and how to handle them

7.1 Hardware Failure

7.1.1 All LED dark

Phenomenon

Router LED all dark

Possible Reason

- Power supply does not match, it should be 9-36VDC
- No power supply

Solution

- Make sure the power supply is 9~36VDC
- Check the power adapter and cable connection

7.1.2 SIM Slot

Phenomenon

Cannot insert SIM card

Possible Reason

- SIM slot damaged
- SIM card wrong direction

Solution

- SIM slot damaged, please contact us to repair
- Check the SIM card direction, please make sure the SIM gold finger is up

7.1.3 Ethernet Connection

Phenomenon

LAN LED dark, cannot visit router WEB GUI

Possible Reason

- Ethernet cable connection problem
- Ethernet cable damage
- PC end network card abnormal

Solution

- Re-connect Ethernet cable
- Change a Ethernet cable
- Check network card setting on PC end

7.1.4 Antenna Connection

Phenomenon

Cannot connect antenna

Possible Reason

- Antenna type do not match
- Wrong connection

Solution

- Please check antenna interface, should be SMA-J
- Please check antenna type, there are 3G/4G and WIFI, GPS antenna, do not mix them

7.2 Dial Online Problem

7.2.1 Dial discontinue

Phenomenon

H8922S 3G/4G Router discontinue during dialing, dial failure

Possible Reason

- SIM card network type do not match
- SIM charges owed
- Power supply do not match
- Modem setting wrong

Solution

- Change to a suitable SIM card
- Recharge SIM card
- Change to suitable power supply
- Change Modem setting, please check related chapter

7.2.2 No Signal

Phenomenon

H8922S 3G/4G Router modem status show no signal

Possible Reason

- Antenna connect wrong
- Modem cannot online
- Modem offline

Solution

- Connect suitable antenna
- Modem cannot online, check SIM and modem setting
- Modem offline, check router setting, like wake up setting, ICMP setting, check if there are any setting make router offline

7.2.3 Cannot find SIM/UIM card

Phenomenon

H8922S 3G/4G Router cannot find SIM/UIM card

Possible Reason

- SIM card damage
- SIM bad contact

Solution

- Replace SIM card
- Re-install SIM card

7.2.4 Poor Signal

Phenomenon

H8922S 3G/4G Router no signal or poor signal

Possible Reason

- Antenna connect wrong
- Area signal weak

Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm signal problem
- Change to high-gain antenna

7.2.5 Compress Protocol not match

Phenomenon

H8922S 3G/4G Router dial failure, log shows compress protocol not match

Possible Reason

Modem compress protocol do not match with server end

Solution

Change compress protocol setting

7.3 VPN Problem

7.3.1 VPDN cannot connect

Phenomenon

VPDN cannot connect

Possible Reason

- VPDN port work abnormal
- VPDN parameter wrong
- VPDN peer server abnormal

Solution

- Make sure Modem is online
- Set the correct port to VPDN
- VPDN parameter wrong
- Check VPDN peer server

7.3.2 VPN cannot communicate

Phenomenon

VPN already connect, but cannot communicate

Possible Reason

- Router table configuration wrong
- VPN peer server configuration wrong

Solution

- Add related Router table
- Check VPN peer server setting

7.3.3 Router can communicate but subnet cannot

Phenomenon

Router can communicate but subnet can not communicate

Possible Reason

- VPN peer server configuration wrong
- Local Router has no MASQ
- Wrong local route table

Solution

- Check VPN peer server setting
- Local Router has no MASQ, please manual add VPN port MASQ
- Wrong local route table, set right route table

7.4 WEB configuration

7.4.1 Updating firmware failure

Phenomenon

Updating firmware failure

Possible Reason

- Auto reboot during updating H8922S 3G/4G Router

- Power supply problem
- Wrong firmware
- Power off during updating router

Solution

- Check setting, disable the function which may cause reboot
- Change to a suitable power supply
- Ask technical support for suitable firmware
- Power off during updating router, please make sure power supply normal

7.4.2 Backup setting problem

Phenomenon

Router import backup setting failure

Possible Reason

- Backup setting file format wrong
- No reboot after backup setting

Solution

- Choose a right file to import
- Must reboot after import setting, then parameters available

7.4.3 Updating patch failure

Phenomenon

Updating fix patch failure, after updating, view fix patch and found no fix patch

Possible Reason

- Patch format wrong
- Patch name too complicated

Solution

- Check patch format, change to a right one
- Change the patch name to a simple one

7.4.4 CFE Updating failure

Phenomenon

CFE updating failure, firmware edition no change

Possible Reason

- Power supply do not match
- Firmware version or format do not match
- Power off during updating process

Solution

- If power supply does not match, please change then update again
- If firmware version, format do not match, please change then update again
- If power off during updating, please update again

7.4.5 Update failure in WEB GUI

Phenomenon

Updating by WEB GUI, failed and cannot visit WEB GUI again

Possible Reason

Firmware oversize cause updating failure

Solution

Using CFE mode to update again, and router will restore to factory mode. If after CFE updating, still cannot visit WEB GUI, please contact us for repairing

7.4.6 Forget Router Password

Phenomenon

Forget router login password

Possible Reason

User has changed the password

Solution


After router power on, push and hold RESET button over 10 seconds then release, then re-power on router, router will back to factory mode (Username/Password both admin), but patch will reserve


**CAUTION**

When router is power on, press and hold RESET button around 1s, router will reboot and kept all setting.




Create smart things


 F14 - F16, Tower A, Building 14, No.12, Ganli 6th Road, Longgang District, Shenzhen 518112, China.

 +86-755-88864288-5

www.hongdian.com

 +86-755-83404677

 sales@hongdian.com

 [hongdianchina](#)

 [Hongdian_China](#)