Caimore Industrial GPRS/CDMA/WCDMA/
EVDO/TD-SCDMA/HSPA+/LTE-FDD/LTEL-TDD
WIFI Router User Manual

Copyright:
All contents in the files are protected by copyright law, and all copyrights are reserved by Xiamen Caimore Communication Technology Co., Ltd., without written permission, all commercial use of the files from Caimore are forbidden, such as copy, distribute, reproduce the files etc, but non-commercial purpose, downloaded or printed by individual (all files shall be not revised, and the copyright and other proprietorship notice shall be reserved) are welcome.

Trademarks:
Caimore are trademarks of Xiamen Caimore Communication Technology Co., Ltd. All other trademarks mentioned in this file are the property of their respective holders.

Notice:
The information in the file is subject to change without notice. Every effort has been made in the preparation of this file to ensure accuracy of the contents, but all statements, information, and recommendations in this file do not constitute the warranty of any kind, express or implied.

Suitable for:
This user manual is suitable for the following models:

<table>
<thead>
<tr>
<th>Product</th>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS WIFI Router</td>
<td>CM820-87G</td>
<td>GPRS+WIFI, 4xLAN</td>
</tr>
<tr>
<td>Device Type</td>
<td>Model</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>CDMA WIFI Router</td>
<td>CM820-87C</td>
<td>CDMA2000 1X+WIFI,4xLAN</td>
</tr>
<tr>
<td>WCDMA WIFI Router</td>
<td>CM820-87W</td>
<td>WCDMA+WIFI,4xLAN</td>
</tr>
<tr>
<td>TD-SCDMA WIFI Router</td>
<td>CM820-87S</td>
<td>TD-SCDMA+WIFI,4xLAN</td>
</tr>
<tr>
<td>EVDO WIFI Router</td>
<td>CM820-87E</td>
<td>CDMA2000 EVDO+WIFI,4xLAN</td>
</tr>
<tr>
<td>HSPA+ WIFI Router</td>
<td>CM820-87H</td>
<td>WCDMA HSPA+ +WIFI,4xLAN</td>
</tr>
<tr>
<td>LTE-TDD WIFI Router</td>
<td>CM820-87T</td>
<td>LTE-TDD +WIFI,4xLAN</td>
</tr>
<tr>
<td>LTE-FDD WIFI Router</td>
<td>CM820-87F</td>
<td>LTE-FDD +WIFI,4xLAN</td>
</tr>
</tbody>
</table>

**Revision History:**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Date</th>
<th>Author</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>Primarily Released</td>
<td>2008.10.17</td>
<td>linjh</td>
<td>Sundy</td>
</tr>
<tr>
<td>V2.0</td>
<td>Adjusted WEB configuration whole style Supported 3G gateway</td>
<td>2009-12-25</td>
<td>linjh</td>
<td>Sundy</td>
</tr>
<tr>
<td>V2.1</td>
<td>Updated, add new functions.</td>
<td>2011-11-18</td>
<td>linjh</td>
<td>Sundy</td>
</tr>
</tbody>
</table>
Table of Contents

Chapter 1 Brief Introduction of Product.................................................................5
  1.1 Produce Overview..........................................................................................5
  1.2 Product Appearance and Accessory Pictures...............................................6
  1.3 Product features..........................................................................................7
  1.4 software functions......................................................................................9
  1.5 Hardware Specification...............................................................................11
  1.6 Indicator Instruction..................................................................................17
Chapter 2 Installation Introduction....................................................................17
  2.1 Packing List..................................................................................................17
  2.2 Product Introduction Appearance...............................................................18
  2.3 SIM Card Installation................................................................................19
Warning: forbid to pull out or insert SIM card with electricity............................20
  2.4 Antenna Installation..................................................................................20
  2.5 RJ45-DB9F Instruction..............................................................................20
Chapter 3 Quick Start Guide..............................................................................21
  3.1 Inset SIM card into gateway SIM card socket（reference 2.3）...................22
  3.2 Connect antenna（reference 2.4）.................................................................22
  3.2 Connect gateway with PC hardware............................................................22
  3.3. Network Setting of PC side (Set IP address, Gateway, DNS)......................23
  3.4. Setup WAN Parameter...........................................................................25
  3.5 Setup DNS................................................................................................27
  3.6 SET Device Online...................................................................................30
Chapter 4 Detailed Parameter Configuration....................................................31
  4.1 Basic Configuration...................................................................................31
  4.1.1 WAN Configuration..............................................................................31
  4.1.2 PPPOE Configuration...........................................................................32
  4.1.3 LAN Configuration................................................................................33
  4.1.4 WIFI Configuration................................................................................34
  4.1.5 DHCPD Configuration...........................................................................39
  4.1.6 Dynamic Domain Name Server (DDNS) Configuration.........................40
  4.1.7 Keep Online (make sure to select one kind online maintenance solution)43
  4.2 Advance Configuration.............................................................................45
Appendix

Chapter 5 FAQ

1. Frequent on/off line. ................................................................. 79
2. Forgot password. ................................................................. 79
3. LAN indicator is off. ......................................................... 79
4. Can’t dial-up to be online. .................................................... 79
5. Dial-up to be online, but can’t visit website. ..................... 80

Appendix 1 Login gateway by Telnet ........................................ 80
Appendix 2 Login gateway by hypertrm ................................... 82
Appendix 3 Obtain debug information from syslogd server .... 85
Chapter 1 Brief Introduction of Product

1.1 Produce Overview

Caimore WIFI wireless router is an industrial designed wireless router with WIFI, 1 WAN port and 4 Ethernet RJ45 ports (4xLAN). The device is used by small, medium enterprises and home to access internet. Also it is used for data transmission. The device supports LAN WIFI function (802.11 a/b/g/n) and WAN 3G/4G/WIFI wireless network function. Meanwhile the system loads the wide area network communication VPN tunnel and security authentication of WIFI LAN to achieve seamless connection between wireless LAN and wireless WAN and provide users with high-speed, secure, reliable mobile broadband service.

The equipment adopts high-powered industrial MIPS communication processor and embedded with real-time operating system as software support platform. System integrates full range from the logical link layer to application layer communication protocol, support VPN (including PPTP, L2TP, MPPE, IPSEC and GRE), IPTABLE firewall, static and dynamic routing, PPPOE, PPP server and PPP client, DHCP server and DHCP client, DDNS, firewall, SNAT / DNAT, DMZ, WEB configuration, support APN / VPDN, supports auto-dialing after power on and automatic maintenance of communication links to ensure the link is always on-line, supports online and offline at a regular time functions, supports startup and shutdown at a regular time.

The product uses industrial design; system designed with watchdog( WDT) protection, meanwhile loaded System Watch Protection SWP (System Watch Protect); products passed 3000V power shock test; products possesses patented technology to maintain system stably, to ensure router always on-line; after 8 years of rigorous design,
testing and practical application, the products shows stable and reliable performance.

This product has been widely used in M2M fields, such as business Internet access, family on-line Internet access, financial transactions, post transactions, smart grid, intelligent transportation, environmental monitoring, fire monitoring, security monitoring, water monitoring, public safety, advertising, telemetry, industrial control, monitoring oil fields, coal mine monitoring, earthquake monitoring, weather monitoring, instrumentation monitoring, water meter reading, electrical meter reading, gas meter reading, thermal network monitoring, meter reading and other industries.

1.2 Product Appearance and Accessory Pictures

Product interface Pictures:

<table>
<thead>
<tr>
<th>Side View</th>
<th>Front View</th>
<th>Back View</th>
</tr>
</thead>
</table>

Product Accessory Picture:

<table>
<thead>
<tr>
<th>Power supply</th>
<th>Ethernet Cable</th>
<th>Serial line</th>
<th>Antenna</th>
</tr>
</thead>
</table>
1.3 Product features

Industrial Design

- Industrial CPU: Industrial high-performance embedded processing, 320MHz; with 16KB Dcache, high-speed cache data speed up data access speed; with 32KB Icache, high-speed instruction cache, enhanced instruction processing speed.
- Industrial wireless module: using industrial wireless module, the interference is strong, and transmission is stable.
- Real-time operating system: Adopting LINUX2.6 operation system with memory management unit, real-time, upgrades fast, stable system with improved TCP/IP protocol stack.
- Strengthened circuit board: PCB followed the principles of 3H and 3W, meanwhile all products of circuit boards used high-quality materials to ensure the plate material stable and reliable.
- Industrial components: machine components use strictly screened industrial-grade components.
- Industrial Power: Wide voltage power supply design, adaption range of power from DC5V to DC35V, built-in power supply for reverse current protection and over-voltage protection.
- Electromagnetic protection: built-in 1.5KV magnetic isolation protection at Ethernet interface.
- Anti-jamming design: metal shell, shield electromagnetic interference, the system protection grade IP30; antenna with lightning protection design; ultra-low and ultra-high temperature system design; particularly suitable for harsh industrial environments.

Stability and Reliability

- All products have acquired CE certificates of EU.
- Online maintenance patents: Intelligent anti-dropped, online testing, online.
maintenance, automatically re-dial when dropped, automatically reset when abnormal to ensure that equipment is always online.

- Three-tier system protection: based on the original two (software protection + CPU with built-in WDT protection) system protection increased level-one system VWM (Virtual Man Watch) detection to ensure system reliability.

- UIM / SIM card ESD protection: 1.8V/3V/5V standard putter user card interface,

- built-in 15KV ESD protection.

- Serial ports ESD protection: Serial port RS232 embedded 15KV ESD protection.

- Metal shell: metal case, anti-radiation, anti-interference; shell and system security isolation, lightning protection design; meet the power requirements of safety regulations; protection rating IP41; particularly suitable for harsh industrial control environments.

- All wireless modules are certified by the CGD, FCC or CE certification.

- High-speed processing CPU: Adopting industrial-grade high-speed CPU, can handle a variety of protocol data transfer fastly; solve the "fake online", "fake death", "crash" and other difficult problems.

- Memory management MMU: CPU with memory management MMU, can avoid system unstable situation caused by system memory abnormal problem.

- Large memory: FLASH 64Mb, SDRAM, 256Mb, a large memory to cache data sent by customer, meanwhile receiving large packages without data losing.

- Complete protocol stack: the new system loaded complete TCP / IP protocol stack, using comprehensive TCP / IP protocol stack; so that network traffic performance shows outstanding, the drop-line probability dramatically reduced.

- EMC performance outstanding: passed 3000V electrical shock test, especially suitable for use under harsh industrial environments; system EMC / EMI performs excellent, system stable and reliable; passed CE test;
Easy to use

- Product is set default parameters when leaving factory, customers can use device by modifying some parameters only or even without changing any parameter.
- Graphical configuration tool: improved graphical configuration tool that provides rapid deployment capabilities for customers to achieve rapid deployment; provides mass configuration
- Product manual supplies quick start guide for customers to use equipment quickly
- Software checking: Provides SYSLOG log output function, can be used as equipment work logs and help to analyze the reasons for exceptions; Provides the serial port debugging log, providing different levels of debugging output, enabling customers to view a variety of information, quickly locate the problem.
- After eight years of using, equipment with completed functions and easy to use.

1.4 software functions

- Support LAN WIFI (802.11 b/g/n) function and WAN 3G/4G wireless network function, the system loaded wide area network communication VPN tunnel, WIFI LAN transmission security authentication and other security features, to achieve seamless connectivity between wireless LAN and wireless WAN. Providing users with high-speed, secure, reliable mobile broadband services
- Provides a standard WAN port, supports PPPOE, can directly connect with ADSL equipment and other leased line.
- Support backup function of 3G wireless link and broadband link. When 3G can't communicate, it will change to PPPOE broadband network automatically.
- Support wireless video monitoring and dynamic image transmission
- Supports Ethernet data communication and packet forwarding, also supports
serial port TCP / UDP transparent data transmission or serial configuration

- Support VPN tunnel, including PPTP, MPPE, L2TP, GRE and IPSEC
- Intelligent anti-dropped, support online testing, online maintenance, automatic redial, router is always on-line
- Support IPTABLES firewall, packet filtering
- support Regular on-line offline functionality, can set the device on-line and offline in a certain period of time
- Support a variety of trigger and offline modes, including text messages, phone ringing, serial port data, network data trigger and offline mode
- Support dynamic routing and static routing, RIPv1, RIPv2, OSPF, BGP, NDSP, IRMP, SNSP, IGMP, DVMRP, PIM-SM/DM
- Support multiple protocols: TCP / IP, UDP, ICMP, SMTP, HTTP, POP3, OICQ, TELNET, FTP, etc.
- Support DHCP / DHCPD functionality
- Supports NAT port mapping function, such as SNAT, DNAT
- Support DDNS(Dynamic Domain Name Server): support ORAY, 88IP, and DYNDNS domain name service provider
- Support DMZ
- Support the APN / VPDN network
- Convenient WEB configuration, Remote WEB Management
- Support WEB configuration save and restore to achieve the rapid deployment parameters backup and batch of equipment
- Support telnet management, user-friendly console shell interactive environment
- Support multiple terminals sharing router ppp wan
- Support multiple wireless dial-up mode: automatically assigned, specify the IP, specify local and remote IP
- Support as a PPP server, multiple authentication methods, support mutual authentication
- Easy to use COM and SYSLOG System diagnostics, debugging
- Support Serial port local software upgrades
1.5 Hardware Specification

**Hardware system**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Industrial high-performance embedded ARM9 processing; 200MPS; with 16KB Dcache, high-speed cache data speed up high-speed data access with 16KB Icache, high-speed instruction cache enhanced instruction processing speed</td>
</tr>
<tr>
<td>MMU</td>
<td>CPU with MMU memory management unit, can prevent memory overflow exception</td>
</tr>
<tr>
<td>FLASH</td>
<td>64Mbits (expandable to 256Mbits) have enough memory to store programs and data</td>
</tr>
<tr>
<td>SDRAM</td>
<td>256Mbits (expandable to 2048Mbits), a large enough cache to improve system operation speed</td>
</tr>
</tbody>
</table>

**Operating System**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating</td>
<td>Using Real-time operating system with memory management unit, real-time, feature upgrades fast, system stable;</td>
</tr>
<tr>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>

**Interface Type:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet port</td>
<td>4xLAN(ONE 10/100 Base-T Ethernet ports), Ethernet IEEE 802-3, 802-2; built-in 1.5KV magnetic isolation protection</td>
</tr>
<tr>
<td>Serial ports</td>
<td>1 RS232 serial port or 1 RS485 interface (supports RS422/TTL) Bytesize: 7,8 bit Stopbits: 1, 2-bit Parity: no parity, odd parity, even parity, SPACE and MARK parity Baudrate: 110bps ~ 230400bps Flow Control: None flow control, RTS / CTS hardware flow control or XON / XOFF software flow control</td>
</tr>
<tr>
<td>Indicator LED</td>
<td>With “POWER”, connecting “Link / ACT”, communication “COMM” and “ONLINE” indicator LED</td>
</tr>
<tr>
<td>Antenna Interface</td>
<td>Standard SMA female interface, 50 ohm; optional 3M/5M/10M/15M antenna extension cable, meet the different needs of customers</td>
</tr>
<tr>
<td>UIM interface</td>
<td>1.8V/3V/5V standard putter user card interface, built-in 15KV ESD protection</td>
</tr>
<tr>
<td>Voice Interface</td>
<td>Standard headset interface (requires software)</td>
</tr>
<tr>
<td>Power Interface</td>
<td>Standard 3-pin power jack</td>
</tr>
</tbody>
</table>

**Power supply:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply voltage</td>
<td>Wide voltage design, DC 7V to the DC32V power supply directly to the device; and built-in power supply over-voltage protection and reverse current protection</td>
</tr>
<tr>
<td>Standard power supply</td>
<td>DC9V/1.5A</td>
</tr>
<tr>
<td>Current while Communicating</td>
<td>Average communication current: 390mA @ +9 VDC; instantaneous peak current: 1.0A @ +9 VDC</td>
</tr>
<tr>
<td>Standby current</td>
<td>Standby average current: &lt;56mA @ +9 VDC</td>
</tr>
</tbody>
</table>

**Physical features:**

Tel:+86 592 5901215  web:www.caimore.com/emain.asp
<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shell</td>
<td>Metal shell: metal case, anti-radiation, anti-interference; shell and system security isolation, lightning protection design; meet the power requirements of safety regulations; protection rating IP30; particularly suitable for harsh industrial control environments.</td>
</tr>
<tr>
<td>Product dimensions</td>
<td>195 * 121 * 30mm (not including the antenna and the fixed parts)</td>
</tr>
<tr>
<td>Packing Size</td>
<td>298x226x60mm</td>
</tr>
<tr>
<td>Weight</td>
<td>0.96kg</td>
</tr>
</tbody>
</table>

**Wireless parameters:**

**WIFI Wireless parameters**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIFI module</td>
<td>WIFI module chip-embedded, high integration, good stability</td>
</tr>
<tr>
<td>WIFI standard</td>
<td>Support 802.11 a/b/g/n standard, speed, support 6M/9M/12M/18M/24M/36/48/54Mbps, up to 108M</td>
</tr>
<tr>
<td>Encryption</td>
<td>Supports WAP encryption, built-in WAP and WAP 2.0, Built-in 64-bit and 128-bit WEP encryption, Support WEP encryption, built-in 802.11I 4.0 WEP (128-bit and 64-bit) TKIP, AES and CCMP and other hardware security engine</td>
</tr>
<tr>
<td>AP mode</td>
<td>Support AP mode</td>
</tr>
<tr>
<td>Transmission distance</td>
<td>Outdoor non-stop, outdoor coverage up to 150 meters</td>
</tr>
</tbody>
</table>

**HSPA+ 4G Gateway Parameters:**
### WCDMA 3G Gateway Parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless module</td>
<td>use industrial wireless module</td>
</tr>
<tr>
<td>Standards and frequency bands</td>
<td>Support HSPA+/UMTS/ WCDMA /HSDPA/HSUPA 850/900/1900/2100MHz</td>
</tr>
<tr>
<td></td>
<td>Support GSM/GPRS/EDGE 850/900/1800/1900MHz</td>
</tr>
<tr>
<td>Coding scheme</td>
<td>HSPA+/HSDPA/HSUPA/WCDMA/EDGE/GPRS/CSD mode</td>
</tr>
<tr>
<td>Communication bandwidth</td>
<td>HSPA+:</td>
</tr>
<tr>
<td></td>
<td>Downlink (up to 21Mbps)</td>
</tr>
<tr>
<td></td>
<td>Uplink (up to 5.76Mbps)</td>
</tr>
<tr>
<td></td>
<td>HSDPA/HSUPA</td>
</tr>
<tr>
<td></td>
<td>Downlink (up to 7.2Mbps)</td>
</tr>
<tr>
<td></td>
<td>Uplink (up to 5.76Mbps)</td>
</tr>
<tr>
<td></td>
<td>WCDMA</td>
</tr>
<tr>
<td></td>
<td>Downlink (up to 384Kbps)</td>
</tr>
<tr>
<td></td>
<td>Uplink (up to 384Kbps)</td>
</tr>
<tr>
<td>Transmit power</td>
<td>&lt;24dBm</td>
</tr>
<tr>
<td>Receiver sensitivity</td>
<td>&lt;-109dBm</td>
</tr>
<tr>
<td>Function support</td>
<td>Support data, SMS</td>
</tr>
</tbody>
</table>
**TD-SCDMA 3G Gateway Parameters:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless module</td>
<td>use industrial wireless module</td>
</tr>
<tr>
<td>Standards and frequency</td>
<td>Support UMTS / HSDPA / WCDMA 850/900/1900/2100MHz</td>
</tr>
<tr>
<td>bands</td>
<td>Dual Band EGSM 850/900/1800/1900MHz</td>
</tr>
<tr>
<td></td>
<td>Support GPRS / EDGE CLASS 12</td>
</tr>
<tr>
<td>Coding scheme</td>
<td>HSDPA/HSUPA/WCDMA/EDGE/GPRS/CSD mode</td>
</tr>
<tr>
<td>Communication bandwidth</td>
<td>HSDPA / HSUPA mode:</td>
</tr>
<tr>
<td></td>
<td>Download 7.2Mbps, Upload 5.76Mbps</td>
</tr>
<tr>
<td></td>
<td>WCDMA mode:</td>
</tr>
<tr>
<td></td>
<td>Download / Upload 384Kbps</td>
</tr>
<tr>
<td>Transmit power</td>
<td>&lt;24dBm</td>
</tr>
<tr>
<td>Receiver sensitivity</td>
<td>&lt;-109dBm</td>
</tr>
<tr>
<td>Function support</td>
<td>Support data, SMS</td>
</tr>
</tbody>
</table>

**CDMA2000 EV-DO 3G Gateway Parameters:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless module</td>
<td>use industrial wireless module</td>
</tr>
<tr>
<td>Standards and frequency</td>
<td>TD-SCDMA/HSDPA/HSUPA: 2010~2025MHz</td>
</tr>
<tr>
<td>bands</td>
<td>GSM/GPRS/EDGE: 850/900/1800/1900MHz</td>
</tr>
<tr>
<td>Coding scheme</td>
<td>TD-SCDMA/HSDPA/HSUPA/EDGE/GPRS mode</td>
</tr>
<tr>
<td>Communication bandwidth</td>
<td>Downlink (Max up to 2.8Mbps)</td>
</tr>
<tr>
<td></td>
<td>Uplink (Max up to 384Kbps)</td>
</tr>
<tr>
<td>Transmit power</td>
<td>&lt;24dBm</td>
</tr>
<tr>
<td>Receiver sensitivity</td>
<td>&lt;-108dBm</td>
</tr>
<tr>
<td>Function support</td>
<td>Support data, SMS</td>
</tr>
<tr>
<td>Item</td>
<td>Content</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wireless module</td>
<td>use industrial wireless module</td>
</tr>
<tr>
<td>Standards and frequency bands</td>
<td>Support IS-95 A/B, CDMA2000 1XrTT, and 1X EV-DO(Revision 0 and A) 800Mhz, Optional 800/1900Mhz or 450Mhz</td>
</tr>
<tr>
<td>Coding scheme</td>
<td>IS-95 A/B, CDMA2000 1XrTT, and 1X EV-DO mode</td>
</tr>
<tr>
<td>Communication bandwidth</td>
<td>Download 3.1Mbps, Upload 1.8Mbps</td>
</tr>
<tr>
<td>Transmit power</td>
<td>&lt;23dBm</td>
</tr>
<tr>
<td>Receiver sensitivity</td>
<td>&lt;-107dBm</td>
</tr>
<tr>
<td>Function support</td>
<td>Support data, SMS</td>
</tr>
</tbody>
</table>

**Other parameters:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>-25 °C ~+65°C</td>
</tr>
<tr>
<td>Extended operating temperature</td>
<td>-35 °C~+75°C</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40~+85°C</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>95%(No condensation)</td>
</tr>
</tbody>
</table>
### 1.6 Indicator Instruction

<table>
<thead>
<tr>
<th>Indicator</th>
<th>status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>ON</td>
<td>Device power is normal</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>Device hasn’t been powered</td>
</tr>
<tr>
<td>WAN</td>
<td>OFF</td>
<td>WAN Port hasn’t been connected.</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>WAN Port has been connected.</td>
</tr>
<tr>
<td></td>
<td>Blink</td>
<td>There is Data transmitting and receiving</td>
</tr>
<tr>
<td>WIFI</td>
<td>OFF</td>
<td>Not use WIFI</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>Use WIFI</td>
</tr>
<tr>
<td></td>
<td>Blink</td>
<td>There is data transmitting and receiving</td>
</tr>
<tr>
<td>COMM</td>
<td>Blink</td>
<td>There is data transmitting and receiving</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>There is no data transmitting and receiving</td>
</tr>
<tr>
<td>Online</td>
<td>ON</td>
<td>Device has attach the network</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>Device has no attach the network</td>
</tr>
</tbody>
</table>

## Chapter 2 Installation Introduction

### 2.1 Packing List

Thanks for using our communication products. When you open the product box, please check that the inside items are consistent with the packing list. Factory standard configuration in the box is as follows:

<table>
<thead>
<tr>
<th>Gateway Host</th>
<th>1 Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>Quantity</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>DC 9V Power Adapter</td>
<td>1 Unit</td>
</tr>
<tr>
<td>RJ45-DB9 Serial Line</td>
<td>1 Piece</td>
</tr>
<tr>
<td>Network Cable</td>
<td>1 Unit</td>
</tr>
<tr>
<td>3G Antenna</td>
<td>1 Piece</td>
</tr>
<tr>
<td>WIFI Antenna</td>
<td>1 Piece</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>1 Piece</td>
</tr>
</tbody>
</table>

2.2 Product Introduction Appearance

![Picture 2-2-1]

Front Panel Introduction

![Picture 2-2-2]

Indicator from left to right: Power, Link, Act, WIFI, Online

Rear Panel Introduction
2.3 SIM Card Installation

SIM cards store information of user’s ID, telephone directory, network settings, and additional services etc. Gateway supports 1.8V/3V/5V SIM card, SIM card interface socket uses a drawer-type SIM card connector, and users can easily install SIM card without open the chassis.

Installation method:

In the condition of without supplying power, Please use a needle-like object to press on the popup button of SIM card outlet, SIM card slot will flick out at once. Put the SIM card into the SIM card slot. But you must pay attention to keep the side which has metal point down, then insert card sheath back to SIM card outlet. See below of the picture:  

![Picture 2-3-1]
Warning: forbid pulling out or inserting SIM card with power supply.

2.4 Antenna Installation

Please turn SMA male connector clockwise to be tight. As the following picture:

![Picture 2-4-1]

2.5 RJ45-DB9F Instruction

This Router supports RS232 asynchronous communication serial interface and adopts RJ45. Serial interface mainly used to configure control or configure to be DTU.

Com/line: RS232 asynchronous communication serial interface

RJ45-DB9F Conversion line signal connection is as follow:

<table>
<thead>
<tr>
<th>RJ45</th>
<th>DB9F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
</tr>
</tbody>
</table>

The signal definition of DB9F Serial communication interface is as follow:

<table>
<thead>
<tr>
<th>PIN</th>
<th>RS232 Signal</th>
<th>Description</th>
<th>Direction relative to</th>
</tr>
</thead>
</table>

Tel:+86 592 5901215

web:www.caimore.com/emain.asp
### Chapter 3 Rapid Configuration

On the one hand, in order to make the customers detect rapidly the device and confirm whether it is in good condition and whether it can operate normally after receiving devices; on the other hand, for the customers who only need to modify the configuration parameters in the rapid configuration and other parameters adopts factory default parameter. So we specially make the instructions of rapid configuration to make it convenient for the customers to configure gateway rapidly. The following examples based on WINDOW XP explain the process of rapid configuration of Xiamen Caimore industrial wireless gateway.
Rapid configuration generally needs to configure the parameter of WAN and LAN and other parameters adopts the factory default parameters. If these parameters need to be modified, please read <chapter 4 Detailed Parameters Configuration>

3.1 Insert SIM card into Router SIM card socket (refer to 2.3)

3.2 Connect antenna (refer to 2.4)

3.2 Connect router with PC hardware

Method: router connects with PC directly. As the following picture:

![Picture 3-2-1]

Finish connecting LAN1, please kindly check whether Ethernet yellow indicator is on or not, if not, please check the connection between link and interface and make sure it is tight.
3.3. Network Setting of PC side (Configure IP address, Gateway, DNS)

Click “Start” of windows → “control panel”, click “network connection”, Picture as below:

![Network Setting Diagram]

**Picture 3-3-1**

**Method 1: Adopt obtaining IP addresses automatically**

Click “local connection”, select “properties (R)”, select “Internet Protocol (TCP/IP)”, click “properties (R)”, it will display the following window, select “Obtain an IP address automatically”, finish modifying, then click “OK”. In this way, wireless gateway assigns IP address to customer PC automatically. At this time, if DNS also adopts automatic assigning automatically, also can select “obtain DNS server address automatically”, then DNS setting is also ok. When you reach to “3.5 Set DNS”, customer can skip and doesn’t need to set DNS.
**Method 2: Adopt static IP**

Click Windows system “Control Panel” -> click “network connection” -> “local connection”, then select “properties(R)”, select “Internet protocol (TCP/IP)”, click “properties(R)”, it will show following window, then revise IP address according to below example (customer can configure his own IP address according to actual situation, but customer has to make sure IP address of PC side and gateway side are in the same network segment. Method of configure gateway IP address, please reference [4.1.3 LAN configuration](#), meanwhile please type LAN IP address of wireless gateway into TCP/IP properties “default gateway” on PC side and consider it as PC default gateway), after revising, please click “OK”.

This example parameter setting:

The Wireless gateway LAN1 port IP: 192.168.9.1 (factory default value)
PC side parameter setting:

IP address: 192.168.9.X (X is any one between 1-254, but can’t conflict with other
PC IP address, here X is 3 in this example)
Subnet mask: 255.255.255.0
Default gateway: 192.168.9.1(it is the wireless gateway LAN1 port IP address

![Internet Protocol (TCP/IP) Properties](image)

**Picture 3-3-3**

3.4. Setup WAN Parameter

Open “IE”, type 192.168.9.1 (gateway default LAN port default IP address)on the
address barb. Picture as below:
Type user name and password (default user name: admin, Password:admin).

Select WAN Configuration, please set and submit according to information offered by network operator.(read picture 3-4-3, it is the EVDO/CDMA login information). If you use APN/VPDN, please input these information (Center, APN, User, Password supplied by network operator) to the corresponding bar. It is to be default configuration (reference Appendix 5) according to network when leaving factory, then click “Apply” to save
Note: In normal situation, it is ok to use our factory default parameters, and does not need to revise, it only need to revise when using APN/VPDN special network.

3.5 Setup DNS

If in “method 1: adopt obtain IP automatically” of 3.3 Network Setting on PC Side customer selects “Obtain DNS server address automatically” and also save it, then can skip this step.

After finishing 3.4 SetupWAN Information, please re-power wireless gateway, then wait for gateway “online” indicator to be on, when it on, customer can set DNS of PC side.

DNS Configuration has two methods

Methods 1: adopt obtaining DNS automatically

Click “start”->“control panel”, click “network connection”:

![Change Windows Firewall settings](image)

Click “local connection”, select “properties(R)”, select “Internet protocol (TCP/IP)”, click “properties(R)”, it will display below window, select “Obtain DNS server address automatically”, then click “OK”. In this way, gateway will assign DNS server address automatic for PC.
**Method 2:** Set DNS of PC according to DNS obtained by gateway. According to ways of setting configure and connect well of PC and wireless gateway, then set well of related IP address, then login gateway by IE, when gateway login successfully, the online indicate is on, please click “system status” of gateway to check DNS assigned by carrier.
Picture 3-5-3

Record this DNS assigned by carrier, then type this DNS to “First DNS server” of PC. Process is to click “start” ->“control panel”, click “network connection”, picture as below:

![Image of network connection settings]

Picture 3-5-4

Click “local connection”, select “properties(R)”, select “Internet protocol (TCP/IP)”, click “properties(R)”, it will display below window, revise according to DNS of gateway system status, then click “OK”.

![Image of local connection settings]
3.6 SET Device Online

When finished 3.1-3.6 steps, please re-power wireless gateway, then wait of gateway “Online” indicator on (if indicator is not on more than 1 minute, please check above steps whether are right or not. If all are right, but indicator is still not on, please contact manufacturer to support), when “online” indicator is on, customer can use gateway to login network or operate wireless data transmission. Type website address on IE of PC, congratulations on you, you are online already and can go on wireless data transmission now.
Chapter 4 Detailed Parameter Configuration

4.1 Basic Configuration

4.1.1 WAN Configuration

Gateway dial-up configuration, it also called connecting wireless network basic parameter.

- Calling center number, Access Point Name, Username and Password: Usually these information are default setting (reference Appendix 5 before leaving factory, and don’t need to revise. If use APN/VPND, it needs to type these information supplied by ISP to the exact place.

- PIN code: If mobile UIM/SIM card set PIN code already, please input it here.

- Extra Initialization commands: it used in special situation, usually here is blank. If customer has any especial command, customer can input here.

- Way to obtain IP: Support obtaining IP automatically, Specify the local IP and Specify the Remote client’s IP. Default situation is obtain IP automatically, it is the IP address assigned by ISP when wireless dial-up. If select Specify IP address,
please input according to ISP supplied information. Otherwise, it can’t be online by dial-up. If ISP requires to specify one kind, and the other kind is obtaining automatically, Then the obtaining actually should be 0.0.0.0.

**Notice:**

1. PIN code can’t be input casually to avoid locking the card.
2. Please don’t input extra initialization command casually to avoid dial-up is unavailable.
3. Please don’t specify IP casually except ISP required to do so, otherwise, online is unavailable.

**4.1.2 PPPOE Configuration**

PPPOE is short name of point-to-point protocol over Ethernet, it can make Ethernet host connects with remote access Concentrator by a simple bridge equipment.

![Picture 4-1-2]

- **Working Mode:**
  - PPPOE Disable: only use 3G network, don’t use PPPOE
  - PPPOE Only: only use PPPOE, don’t use 3G
  - PPPOE Master: Mainly use PPPOE, when PPPOE can’t be used, then use 3G
PPPOE Backup: Mainly use 3G, when 3G can’t be used, use PPPoe.

- User Name: user name access to public network, supplied by ISP.
- Password: Password access to public network, supplied by ISP.

After dialing-up, system status displayed network type: PPPoE

**Picture 4-1-3**

## 4.1.3 LAN Configuration

Wireless Gateway Ethernet port configuration (local IP address and DHCP server)

**Picture 4-1-4**

Local interface 1 (LAN0): multiplex with WAN, it can be used to connect with LAN if without using PPPOE.

- Local IP: It is gateway LAN0 interface IP address, default setting IP address is 192.168.8.1.
- Local Subnet Mask: Set Subnet Mask corresponding local IP address.
- MAC: Set gateway ETH MAC address.

Local interface 2 (WIFI, LAN1-4): used to connect with WIFI and 4-port LAN.
- Local IP: It is gateway WIFI and LAN1-4 interface IP address, default setting IP address is 192.168.8.1.
- Local Subnet Mask: Set Subnet Mask corresponding local IP address. default setting Subnet Mask is 255.255.255.0
- MAC Address: Set gateway LAN1-4 MAC address.
- Primary DNS/Second DNS: It is the domain name decoding server address, default situation (blank) is obtain from ISP when gateway dial-up. If customer has stable DNS server, can input customer stable DNS server address, but we suggest that it is better to obtain from ISP when gateway dial-up.

Notice:
1. Make sure all connected equipment IP are in the same Subnet Mask with gateway.
2. When more units our company gateway work in the same LAN, MAC address will restore to default setting after “load default setting”, this is easy to make MAC address is conflict with other equipment. So please revise MAC address.
3. If customer inputs DNS server address, after dial-up, please check DNS gateway uses whether can decode domain name correctly or not.
4. Local interface 1 and Local interface 2 can’t be in the same subnet mask.

4.1.4 WIFI Configuration

Wi-Fi English full name is wireless fidelity, it is a like of wireless internet technology.
SSID: sign the wireless network name. Support 32 characters max, default is Caimore AP, we suggest revise it to avoid conflict with our company other products.

Region: select region this devices works.

Channel: select this device working channel. It doesn’t need to revise wireless channel except there are interference with other accessing points nearby. Priority Channel are 1, 6, and 11.

Mode: Select mode this device will work.

802.11B only: Only support 802.11B.
802.11 G only: Only support 802.11 G.
802.11 B/G only: Support B or G.

Safe Option:

None: No data encryption, it is the open network, device connect to AP without any password validates.

WEP: adopt WEP 64 or 128 bit data encryption

WPA-PSK: adopt WPA-PSK standard encryption, use pre-shared key protection access.
- WPA2-PSK: adopt WPA2-PSK standard encryption, use pre-shared key protection access. Encryption type is AES.
- WPA-PSK/WPA2-PSK: allow customer to access through WPA-PSK or WPA2-PSK.

Below is introduction of safe-option:

**WEP Encryption:**

![Diagram](Picture 4-1-6)

- Authentication: Default is Auto, if default can’t work normally, customer can choose Shared (Open system).
- Encryption: 64 bit or 128 bit.
- Passphase: WEP key. Customer can input by hand or adopt program creates encryption key automatically. Customer on wireless network has to input encryption key value correctly to make connection successfully.

**Notice:**

1. When more units our company gateway work in the same LAN, SSID will restore to default setting after “load default setting”, this is easy to make SSID conflict with other
equipment. So please revise SSID.

2. Encryption key can input by hand or created by system automatically. Input by hand, if select 64 bit, input 10 number HEX; if select 128 bit, input 26 numbers HEX (Note: number any combination between 0-9 and A-F). Creating encryption automatic, please input an word or a group of characters which can be printed in the “Password”, gateway can create WEP encryption key automatically and use it as wireless network Encryption key.

WPA-PSK Encryption:

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
<tr>
<td>WEP</td>
</tr>
<tr>
<td>WPA-PSK</td>
</tr>
<tr>
<td>WPA2-PSK</td>
</tr>
<tr>
<td>WPA-PSK/WPA2-PSK</td>
</tr>
</tbody>
</table>

Safe Option (WPA-PSK)

Encryption: AES
Passphrase

Picture 4-1-7

- Encryption Mode: Support TKIP, AES, TKIP/AES
- Passphrase: Encryption key, length is between 8 – 63 characters.

WPA2-PSK Encryption:
Encryption Mode: Support TKIP, AES, TKIP/AES.

Passphrase: Encryption key, length is between 8 ~ 63 characters.

WPA-PSK/WPA2-PSK Encryption:

- Encryption Mode: Support TKIP, AES, TKIP/AES
- Passphrase: Encryption key, length is between 8 ~ 63 characters.
- Hidden SSID: If use, customer can’t search device SSID. So only customer can connects by knowing device SSID to increase security.
4.1.5 DHCPD Configuration

DHCP is Dynamic Host Control Protocol. It can assign IP address to computers in the LAN automatically. For customers, it is not easy to set TCP/IP protocol parameters to all LAN computers, there are IP address, subnet mask, gateway, DNS server and so on. Problems can be solved easily by using DHCP. System default is open, if customer doesn’t use DHCPD service, please close this selection.

![DHCP Configuration Interface]

Picture 4-1-10

- Start IP, End IP: they are start and end address when DHCP server assigns IP automatically. After setting IP address internal computer received from this gateway is between these two addresses.

Notice:

1. DHCP start IP to end IP are must continuous, and in the same subnet with gateway, also can’t include gateway local IP, otherwise, DHCP server can’t work normally.
2. Two DHCP servers can’t be existed in the same LAN. If there are more device supply DHCP server function in the same LAN, it can cause IP address can’t assign normally in the system, then it needs to stop one DHCP server.
3. If use PPPOE, please don’t use “local interface 1” DHCPD.
4.1.6 Dynamic Domain Name Server (DDNS) Configuration

DDNS is to set dynamic IP that gateway obtained when dial-up to a certain domain name, is to bind the continuous IP obtained by wireless dial-up with the certain domain name. If wireless gateway opens DDNS, after wireless gateway obtaining new IP by dial-up successfully every time, it will send new obtained dynamic IP address to customer dynamic domain name server to realize binding updating between the setted domain name of dynamic domain name server and gateway IP address. Use DDNS function can solve the short-coming that gateway new obtained different IP address of every dial-up can’t be used as server. If customer needs to use wireless gateway as server, and communicate with equipment on customer side (such as DTU), it needs to open this DDNS function, meanwhile, it needs to input dynamic domain name to corresponding configuration option on customer side equipment, in this way, customer side equipment obtain wireless gateway IP address through DDNS from Domain name server before communicate with gateway every time, then communicate according to obtaining changing wireless gateway IP address.

This gateway supports Dyndns, 88IP and Oray dynamic domain name system. Default doesn’t use DDNS.
For example, if select Dyndns, please visit www.dyndns.com to finish registration of user name and domain name, then infill obtained domain name, user name and password information into corresponding places, then confirm “OK” to save.

- Services Provider: Dyndns (www.dyndns.com)
- Domain Name: domain name registrated from dyndns.
- User: User name to log in dyndns server.
- Password: password to log in dyndns server.

If select 88ip, please visit www.88ip.cn to finish registration of user name and domain name, then infill obtained domain name, user name and password information into corresponding places, then confirm “OK” to save.

- Service Provider: 88ip(www.88ip.cn)
- Server/Standby server: 88IP supply DNS server address, check http://www.88ip.cn/Info/list.asp?Unid=89
- Updating time interval (second): how long time to update one time
- Username: User name when log in 88ip server
- Password: password when log in 88ip server
If select Oray, please visit www.oray.com to finish registration of user name and domain name, this gateway supply user registration, user update, and using help shortcut button, user click corresponded button to enter into Oray website quickly, then infill obtained user name and password information into corresponding places, then confirm “OK” to save.

- Username: user when log in Oray server
- Password: password when login Oray server
- Registration: User registration page link to Oray website quickly
- Updating: User updating page link to Oray website quickly
- Help: User help page link to Oray website quickly.

If use DDNS function, gateway “system status”supplies DDNS updating situation, it is convenient for users to check DDNS whether work normally, if update successfully, it display Updated. As for Oray, there are 3 domain name updated successfully. Read picture below.

![Status](image)

**Picture 4-1-15**

**Notice:** Only when ISP assigned IP address is the whole central office IP address situation, wireless gateway can use as center server. Now in China, only telecom CDMA
4.1.7 Keep Online (make sure to select one kind online maintenance solution)

Keeping Online function is used to check wireless gateway online status, this function checks periodically and automatically data channel between gateway and wireless network whether normal or no, if finds off-line, software will re-dial automatically and intelligently, to realize device is online always without watcher, to make sure data channel smooth. Wireless gateway supplies 4 kinds online checking mode, customer can select one or more kinds, default use Rule2 and Rule3. Customer input stable “destination IP address” and “destination address port” to be reference of online maintenance. Please kindly noted, the input “destination IP address” and “destination address port” are must be stable, because wireless gate is reference of this server, if this server is not stable, it will cause wireless network off-line frequently. When more rules are used, only when all selected rules find communication line is obstructed, wireless gateway can judge device is off-line and restart connection automatically.
Rule 1: PING Mode

Wireless gateway checks destination IP address through PING (ICMP) packet periodic, when the referenced destination IP address device doesn’t respond PING (ICMP), wireless gateway considers communication line is disconnected already, wireless gateway will released the original link, then dial-up again automatically, till communication link is smooth. So please make sure the selected destination address IP server is stable and on, otherwise, gateway judge to be off-line, and make gateway on and off-line frequently. Notice: the selected destination IP address server is allowed PING, if not allowed, the destination IP address server doesn’t respond to PING, gateway judge to be off-line, and make gateway on and off-line frequently.

Rule 2: TCP mode

Wireless gateway checks destination IP address and port through TCP syn packet periodic, when the destination IP address device doesn’t respond, wireless gateway considers communication line is disconnected already, wireless gateway will released the original link, then dial-up again automatically, till communication link is smooth. So please make sure the selected destination address IP server is stable and on, otherwise, gateway judge to be off-line, and make gateway on and off-line frequently.
Notice: the selected destination IP address server is checking relevant port, if the selected destination IP address server is not stable or off or without checking relevant port, gateway judge it to be off-line, and make gateway on and off-line frequently.

Rule 3: Data Mode

In a certain period of time, if the gateway did not receive any data package, then it is believed that the communication link disconnected, and it will dial-up again till communication link is smooth.

Rule 4: LCP mode

Gateway checks online through LCP. In a certain period of time, if gateway did not receive package, it will restart.

Please kindly noted that the selected destination IP address server supports PAP/CHAP verification function in order to use LCP checking. If the selected destination IP address server is not stable or off or without supporting PAP/CHAP verification function, gateway will consider dropped, then it will be on and off-line frequently.

Notice:
1. Make sure to select one kind maintenance online mode, otherwise, gateway can’t restart after dropped.
2. The input destination address needs to be stable and supply corresponding services.
3. Keeping Online default is for public network, it needs to re-configure in special network to avoid dropped frequently.

4.2 Advance Configuration

4.2.1 IPTABLE Filter

It mainly used to filter wireless network data transmitting and receiving, to prevent illegal and invalid data from gateway. It admits and refuses computers of LAN
connected with gateway to get access to WAN, or admits and refuses WAN to get access to LAN connected with gateway.

![Image](picture4-2-1.png)

**Picture 4-2-1**

**Filter mode:** Client IP filtering and MAC address filtering, client can select according to their actual need.

- **Client IP filtering:** Filter data according to IP address base on appointed policy to admit or prevent corresponding IP address data.
- **MAC filtering:** Filter data according to MAC address base on appointed policy to admit or prevent corresponding MAC address data

**Running Rules:** This device has two kinds running rules.

- **Discard matching following rule data packets:** data packets comply to following rules are not allowed to go through, other data packets can go through
- **Receiving matching following rule data packets:** only receive data packets comply to following rule, others are discarded.

### 4.2.1.1 IP Filter Rule Configuration

To realize IP address filtering rules appointing, revising and deleting.

- **Rule name:** it is limited to use characters0-9,a-z,A-Z， also can’t repeat name
- **LAN IP:** Wireless gateway connected LAN IP address
LAN Ports: LAN IP address host corresponding ports scope. Valid value is 0~65535, please input from small to large

WAN IP: Data packet destination IP address

WAN Ports: Data packet destination ports scope. Valid value is 0~65535, please input from small to large

Protocol: data packet protocol, here are 3 types.

- ALL: All types data packet.
- TCP: All TCP packet.
- UDP: All UDP packet.

Direction: data packet direction, used to decide which is original address, there are 3 types.

- IN: From outside network to gateway.
- OUT: Transmit from gateway LAN.
- IN/OUT: Include IN and OUT

Interface: Data packet go through interface, such as br0, PPP0 and so on.

Example 1 of IP address filtering:

1. If select “start client IP address filtering”
2. Running rules select: “discard packets matching following rules”, click “Apply” to save running rule. Read Picture 4-2-2

Instruction: If select “discard packets matching following rules”, default rule is: wireless gateway allows all data to go through, but not allowed data packet to go through as 4-2-3 configure rules.

Example 1 of IP address filtering:

1. If select “start client IP address filtering”
2. Running rules select: “discard packets matching following rules”, click “Apply” to save running rule. Read Picture 4-2-2

Instruction: If select “discard packets matching following rules”, default rule is: wireless gateway allows all data to go through, but not allowed data packet to go through as 4-2-3 configure rules.

Picture 4-2-2

3. Input parameters in IP rule.
This example parameter is:

Name: enableipfilter01  
LAN IP: 192.168.1.23  
WAN IP: 121.204.201.13  
Protocol: all  
Direction: IN  
Interface: PPP0

Read picture 4-2-3, then click “submit” to save IP filtering rule.

4. Explanation and Introduction

After this rule built, gateway will start IP address filtering function. According to running rule “Discard packet matching following rule”, gateway discards all protocol data packets (select “ALL”) from WAN “121.204.201.13” (select “IN” direction) in PPP0 interface (select “PPP0” interface), but other IP address data packets don’t comply to this rule can come and go normally.

Example 2 of IP address filtering:

1. select “setup client IP filter”

Read picture 4-2-4.

Instruction: if running rule select “receive packet matches following rules”, default rule is: gateway forbids all data packet go through except data packet of picture 4-2-5 configured.

![Filter](image)

Picture 4-2-4

3. Input parameters in IP rule.

This example parameter:

- Name: enableipfilter02
- LAN IP: 192.168.1.23
- WAN IP: 121.204.201.13
- Protocol: all
- Direction: IN/OUT
- Interface: PPP0

Read picture 4-10-3, then click “Submit” to save.

4. Explanation and Instruction

After this rule built, gateway will start IP address filtering function. According to running rule “Receive packet matching following rule”, gateway forbid all data packet to go through, but only allow protocol data packets (select “ALL”) from WAN “121.204.201.13” (select “IN/OUT” direction) to go through PPPO interface (select PPP0 interface). Usually this rule shields invalid IP address to go through gateway, can reduce data flow, or as bank application, can shield other IP address access to bank IP address to realize filtering function and reduce data flow.

Tel:+86 592 5901215 49  web:www.caimore.com/emain.asp
4.2.1.2 MAC Filter Configuration

- **Rule name**: it is limited to use characters 0-9.a-z.A-Z, also can’t repeat name.
- **MAC**: Block or permit device MAC address, input format is: “00:12:23:34:45:56”

**Example 1:**

1. If select “setup MAC address filtering”
2. Running rule select: “discard packet matching following rule”
3. Input “00:00:23:34:45:56” in MAC.

So gateway will discard all data packet of MAC address “00:00:23:34:45:56”, meanwhile permit all data packet which MAC address is not “00:00:23:34:45:56” to go through.

**Example 2:**

1. If select “setup MAC address filtering”
2. Running rule select: “receive packet matching following rule”

3. Input “00:00:23:34:45:56” in MAC.

So gateway only receive data packet which MAC address is “00:00:23:34:45:56”, and discard all other data packet which MAC address is not “00:00:23:34:45:56”.

4.2.2 NAT/DMZ Configuration

NAT (Network Address Translation), it is a kind of technology which translate LAN IP address to legal network IP through different ports.

Mode 1: NAT According to appointed rule, it can translate data from WAN to appointed LAN IP address or port.

➢ **Rule name**: it is limited to use characters 0-9,a-z,A-Z, also can’t repeat name
➢ **WAN Start port**: WAN data packet TCP/UDP start port value.
➢ **LAN IP**: the translated LAN IP address
➢ **LAN start port**: LAN computer start port
➢ **Port number**: Several continuously ports from start port. For example, start port is 5001, and port number is 5, so translate WAN 5001,5002,5003,5004,5005
to LAN computer 192.168.1.9 port 5001,5002,5003,5004,5005

- **Protocol**: TCP/UDP, TCP, UDP

**Mode 2**: DMZ

Exposed one LAN computer to Internet completely, to realize bi-directional communication, and it needs to set this computer to be virtual server (DMZ host computer). When there is WAN user visit this virtual server translated public address, device will transmit data packet to this virtual server directly. If one PC of wireless gateway LAN wants to communicate with internet, this can be finished quickly by starting DMZ.

- **DMZ**: Set format is to select “Start DMZ” directly, then input virtual server IP in the IP address bar. Click “Apply” to save.

### 4.2.3 Router Configuration

Setup system static router setting and display system router information. System default router is to send all data to public internet, if user wants to visit appointed network, please add router by hand.

**Picture 4-2-7**

- **Name**: it is limited to use characters 0-9,a-z,A-Z, also can’t repeat name.

- **Destination IP address**: Router destination IP, can be host IP address, also can be IP segment.

- **Subnet mask**: the added subnet, if it is the host IP address, please input
255.255.255.255

- **Gateway IP address**: Next IP of the added router, if don’t need gateway, it can be “0.0.0.0”
- **Metric**: Default is 0
- **Interface**: System interface.

**Notice**: If router can’t add successfully (add rules successfully, but router information didn’t display), please confirm NSID whether comply to requirement or not.

Gateway router configuration example:

![Gateway router configuration example](image)

**Picture 4-2-8**

Introduction: There are 192.168.1.0/24, 192.168.3.0/24, 192.168.2.0/24 three network. 
192.168.1.2 is gateway Ethernet LAN1-4 IP address.
110.91.69.133 is ISP assigned PPP0 IP address when gateway dial-up.
192.168.2.8 is the occurred PPP1 tunnel IP address when gateway connects with server to build VPN tunnel.
172.16.0.1 is VPN server ETH0 IP.
121.204.199.230 is VPN server public IP.
192.168.2.6 is the occurred tunnel0 IP address when VPN server and wireless gateway built the VPN tunnel.

If computer with IP 172.16.0.2 wants to visit computer with IP 192.168.3.2, it needs to add one routing on VPN server to visit 192.168.3.0/24 network. As for this adding step, please read our routing configuration user manual or contact with our technical engineers. When after adding of server gateway, it needs to add two routing on wireless gateway at the same time. One routing is from WAN data packets to 192.168.3.0/24 computer, the other routing is from 192.168.3.0/24 LAN computer to W172.16.0.0/16. Following is the introduction of gateway adding configuration. Please add following rules from “routing” of gateway “advance configuration”:

Please add following rules from “routing” of gateway “advance configuration”:

<table>
<thead>
<tr>
<th>Name</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>test3</td>
<td>[0-9,a-zA-Z]</td>
</tr>
<tr>
<td>192.168.3.0</td>
<td></td>
</tr>
<tr>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>br0</td>
<td></td>
</tr>
</tbody>
</table>

Picture 4-2-9

192.168.3.0 connects with gateway LAN1-4, so interface needs to select br0. This function is to send data of gateway destination IP address 192.168.3.0/24 from outside to br0 interface, to realize send data packet to 192.168.3.0.
This routing function is: data packet sent to wireless gateway, if destination IP address is 172.16.0.0/24, it transmit this data packet to PPP1 interface, meanwhile, this data packet gateway IP is 192.168.2.6. So through this routing, wireless gateway sends data packet to PPP1 directly when receiving data packet of destination IP 172.16.0.0/24, then arrive server 192.168.2.6, then transmit data packet to 172.16.0.0/24 through server’s router, to finish all routing work of data packets.
4.3 VPN Configuration

4.3.1 GRE

GRE is VPN（Virtual Private Network） third tunnel protocol, that is to adopt Tunnel technology among protocols.

![GRE configuration screenshot](image)

Picture 4-3-1

- **Name**: it is limited to use characters 0-9,a-z,A-Z, also can’t repeat name.
- **Remote IP**: Remote public network IP
- **Remote Subnet**: format is 192.168.1.0/24
- **Interface IP address**: The appointed virtual interface IP address
- **Local WAN IP**: IP address used to create tunnel, if it is blank, it means to use WAN IP address
- **MTU**: the max data packets which can go through tunnel.

4.3.2 PPTP

PPTP, as a layer 2 protocol is to transmit the PPP data frames sealed in IP data package through IP network, such as the internet. PPTP can also be used as the connection between special LAN networks. It uses a TCP connection for tunnel maintenance, seals the data as PPP data frames and then transmits with GRE technology through tunnel. It...
can encrypt or compress loaded data sealed in data frames.

![PPTP Configuration Wizard](image)

**Picture 4-3-2**

- **Server IP**: Server IP or domain name.
- **Remote Subnet, Remote Subnet Mask**: Server LAN information
- **Username/Password**: User name and password connected to server.
- **Protocol**: pptp finishes ppp password validation format. There are following authentication way.
  - Pap: adopt Pap, username and password use Plain text Transmit Mode, safety level is low.
  - Chap: adopt Chap
  - MS-Chap: adopt MS-Chap.
  - MS-Chap-V2: adopt MS-Chap-V2
  - Any: Can adopt any one of above mentioned 4 kinds, if there is no special situation, please adopt this one.

- **MPPE**: Encryption way, types as following:
  - NoMppe: Don’t supply MPPE encryption.
  - Mppe(40/128): Supply MPPE function, support MPPE40 and MPPE128

**Encryption way**


- **Add default route**: If start this function, all data visiting this device will send to
PPTP tunnel. Under this situation, computer host of this device can only visit VPN network.

- **Other parameters**: Don’t need to input usually except service requested special negotiation parameters.

- **Specify Local IP /Specify Peer IP**: If server allows, this device requests from server to specify local IP when establish ppp link, if server doesnot assigns, it fails to establish tunnel.

- **Tunnel check interval (second)/Tunnel check times**: Once tunnel established, device can send interval LCP packets to check the link. If checking times fail, device will disconnect automatically and restart to connect.

- **Other parameters**: it will be used when need special parameters to establish link. It doesn’t need to input most time, except services with special negotiation parameters. Parameter format is: novj;novjcomp, use “;” to separate parameters.

**Notice**: If start “default route”, all data packet will be sent to VPN server, that means equipment under gateway can’t visit public network. Please revise “keeping online”parameters according to actual situation. Otherwise, it will off-line frequently.
### 4.3.3 IPSEC

- **Connection Mode:**
  - **Initiative Mode:** Initiate connection from this side.
  - **Passive Mode:** wait for remote side connection
- **Remote address:** Server IP or domain name (compulsive to input)
- **Remote address:**
- **Transport Mode:**
  - **Transport Mode:** usually used when wireless gateway connects server.
  - **Tunnel Mode:** usually used when establishing tunnel between two gateways
  - **Passthrough Mode:** allow IPSEC protocol passthrough.
- **Local endpoint type:**
  - **Network-To-Network:** used communication between equipment of gateway
  - **Road Warrior:** connect to server as mobile clients end.
- **Subnet:** When working mode is Network-To-Network, are network of both sides.
- **Nexthop IP:** When device is in LAN, then this IP is the IP address of devices pointed gateway.
Phase 1: Phase 1 establish IPsec SA, supply IPSec service for data communication.

- **IPsec port**: when start L2tp, L2tp monitor port. L2tp default port is 1701.
- **IPsec Identity**: Identity supplied to opposite side when connection negotiation.

**Work Mode**: Main and Aggressive mode.

- **PFS**: Precise transmit secrecy. Avoid when single key leaking to affect whole communication system.
- **Debug**: Enable debug information.
- **Enable NAT Traversal**: If this gateway doesn’t connect with public network, but transmit through IP original address, then please use “enable NAT Traversal”
- **Authentication**: Pre-shared Key mode and Certificates X509 mode.
- **Cipher**: DES, 3DES, AES and AES128
- **Hash**: SHA1 and MD5
- **DH group**: Group1, Group2, Group5, Group14, Group15, Group16, Group17 and Group18
- **SA lifetime (s)**: phase negotiation valid time
- **Key**: when Pre-shared Key, it is shared key.
- **Password**: when Certificate X509, key of the certificates.

Phase 2: Phase 2 is protected by phase 1, any message didn’t protect by phase 1 SA is refused. In phase 2, negotiate communication protocol fast, change key and establish communication.

- **DH group**: Group1, Group2, Group5, Group14, Group15, Group16, Group17 and Group18
- **Lifetime(S)**: Phase negotiation valid time.
- **Cipher**: DES, 3DES, AES and AES128
- **Hash**: SHA1 and MD5

Other

- **DPD Timeout(s)**: dpd timeout, default is 120s.
4.3.4 L2TP Configuration

L2TP （Layer Two Tunneling Protocol，the second layer channel protocol）is one kind VPDN technology, is used to transmit the send layer data channel, it also called the second data unit, such as point-to-point protocol (PPP) data unit, encapsulate into IP or UDP load, to go through switch network (such as internet) successfully, then arrive destination.

Server address: server IP or domain name.
Remote subnet, remote subnet mask: Subnet information of server side
Username/Password: LAC account and password
Tunnel ID/Tunnel password: LNS account and password.
4.4. System Manage

4.4.1 Time Manage

Manage this device real-time clock, support hand-setting and network time synchronization.

4.4.1.1. Set time by hand:

Select “Manually”, then choose the setting year, month, day, hour, minute and second. Then click “Apply” to finish set time system directly.
4.4.1.2. Use network time synchronization (SNTP)

Select “Sntp”, pre-setting are 3 international used time server.

Notice: Use SNTP, once start, it will update one time per hour. It needs device can visit internet, so it is not suitable for private special network.

4.4.2 User Management

Manage the user password of login web, and the user password of telnet and the user password of series port logging. Once forget, please restore to default setting (reference appendix 4).
User can revise password from here. When revise passport, please input “login username” at first, then input “old password”, then input “new password”, then input “confirm password”, then click “submit” to save new password.

### 4.4.3 System Status

In the web, it displays system current software version, WAN information, VPN information, DDNS (dynamic domain name status) after starting DDNS, login status and information. Read below picture:

![](image)

**Picture 4-4-4**

### 4.4.4 Configuration backup and Software Update

It manages system configuration, it can backup and restore the configuration parameters. And also can update system software, after updating, configuration parameter restores to default setting.
Picture 4-4-5

- **Save to local**: Backup configuration file to local PC
- **Restore**: Restore current configuration to default status
- **Configuration file**: Transmit saved configuration file to device
- **Update Image**: Update Image according to manufacturer supplied firmware

**Notice**: Please don’t power off when update firmware, till “Update successfully”, and to click “Confirm”, then system update success, and system will restart.

### 4.4.5 System Debug

It enable or disable debug function, and output the debug information (In order to check debug information clearly and solve problem quickly), system have 7 optional debug modules:
- **ROUTER**: Output System basic information, include dial-up information
- **DTU**: Output Gateway DTU module debug information
- **DDNS**: Output Gateway DDNS debug information.
- **PPTP**: Output Gateway PPTP debug information.
- **L2TP**: Output Gateway L2TP debug information.
- **SNTP**: Output Gateway SNTP debug information.
- **WEB**: Output Gateway WEB debug information.

Select corresponding debug modules and submit, system will restart. After system restart, click “refresh” to output and flash system current debug information.

### 4.5 Other Configuration

#### 4.5.1 Activation Mode

**Auto mode**

Device enters into auto dial-up status after power on. It is leaving-factory default setting

**Phone mode**
Wakeup by phone (the call mobile number is SIM card number inserted on gateway). Under this mode, gateway didn’t dial-up after power on, when there is calling phone in, gateway dial-up after checking the ringing.

![Picture 4-5-1](image)

**Free Mode:** When haven’t select “force offline”, Free Mode is a period of time value after wireless gateway transmit and receive data packet, if arrives this time value, gateway is offline automatically, release wireless communication link, eliminate communicate flow.

For example, Set Free Mode is 600s, and also select “force offline”, then after wireless gateway online, it transmit or receive data continuously, then after no data receiving or transmitting, 600s later, gateway will be offline automatically and close communication link.

**Force offline:** When system is online time till “free Mode” timeout, it offline immediately.

**Note:** If select “free” only, without “force offline”, please confirm “keeping online” rule whether no data transmit and receive within “Free mode” timeout, otherwise, if “keeping online” timer is less “free mode” timer, the device will offline.

**SMS Mode**

Gateway implements command after receiving SMS (receiving SMS time is only when gateway hasn’t dial-up to be online).
Picture 4-5-2

- **Free time**: When haven’t select “force offline”, Free time is a period of time value after wireless gateway transmit and receive data packet, if this time is timeout, gateway is offline automatically, release wireless communication link, eliminate communicate flow.

  For example, Set Free time is 600s, and also select “force offline”, then after wireless gateway online, it transmit or receive data continuously, then after no data receiving or transmitting, 600s later, gateway will be offline automatically and close communication link.

- **Force offline**: When system is online time till “free timeout”, it offline immediately.

- **Wakeup password**: Password used to validate command validity

**SMS wakeup command format:**

**SMSPASSWD: password: command: parameter**

Command and parameter:

- **REBOOT**
  - Function: Restart gateway
  - Command: REBOOT
  - Parameter: none
  - Format: SMSPASSWD:xxxxxx(password):REBOOT

- **CONNECT**
  - Function: gateway start dial-up, login
  - Command: CONNECT
Parameter: none
Format: SMSPASSWD:xxxxxx(Passord):CONNECT

DNA
Function: setup wireless gateway main DNS and backup DNS
Command: DNS
Parameter: none
Format:

Instruction:
set main DNS is 202.101.103.55, backup DNS is 202.101.107.55

DNS
Function: Eliminate DNS
Command: CLEAR
Parameter: none
Format: SMSPASSWD:xxxxxx(password):DNS:CLEAR

ACTMODE
Function: Device revised to be auto activation (default); wireless gateway dial-up automatically after adding power on.
Command: AUTO
Parameter: none
Format: SMSPASSWD:xxxxxx(password):ACTMODE:AUTO

Function: Device revised to be phone activation mode. Active gateway to be online by phone
Command: RING
Parameter: none
Format: SMSPASSWD:xxxxxx(password):ACTMODE:RING
Function: Device revised to be SMS activation mode. Active gateway to be online by SMS.
Command: SMS
Parameter: none
Format: SMSPASSWD:xxxxxx(password):ACTMODE:SMS

Function: Device revised to be DATA activation mode. Active gateway to be online by data, when gateway receives data, it is activated and be online.
Command: DATA
Parameter: none
Format: SMSPASSWD:xxxxxx(password):ACTMODE:DATA

Function: Device revised to be MIX activation mode. It is with all functions of SMS, PHONE and DATA. Once one function is meet, gateway is actived and can be online
Command: MIX
Parameter: none
Format: SMSPASSWD:xxxxxx(password):ACTMODE:MIX

Note:
1. “:” in command is English character.
2. If select “free” only, without “force offline”, please confirm “keeping online” rule whether no data transmit and receive within “Free” time.

DATA Mode
Device monitors local TCP pre-set port, to be waiting to connect status. When LAN host computer establishes TCP connection, LAN host computer sends command to control gateway to connect with network.
After connection, LAN host computer sends following commands to control device to connect with network. Command format is following:

**Function:** Device begins to connect network  
**Command:** CONNECT  
**Parameter:** none  
**Format:** SMSPASSWD:xxxxxx(password):CONNECT

**Function:** Disconnect current network connection.  
**Command:** CLOSE  
**Parameter:** none  
**Format:** SMSPASSWD:xxxxxx(password):CLOSE

**Function:** Restart gateway.  
**Command:** REBOOT  
**Parameter:** none  
**Format:** SMSPASSWD:xxxxxx(password):REBOOT

**Notice:**
1. Command without case-sensitive (including wakeup password), once device receives LAN host computer data, it disconnects TCP connection with LAN host computer immediately, enters into monitor status again.
2. If select “free” only, without “force offline”, please confirm “keeping online” rule.
whether no data transmit and receive within “Free” time.

**TIME Mode**

Gateway dial-up to be online or offline according to set timer, supports more rules, once there is one rule is met, it will be online.

![TIME Mode Diagram](image)

**Picture 4-5-4**

➢ **Support way:**

- **self define:** Set gateway online and offline time scope according to customer need
- **every year:** Set gateway online and offline time scope of the certain period every year.
- **every month:** Set gateway online and offline time scope of the certain period every month
- **every week:** Set gateway online and offline time scope of the certain period every week
- **every day:** Set gateway online and offline time scope of the certain period every day
- **every hour:** Set gateway online and offline time scope of the certain period every hour

**Notice:** need to confirm system time whether is correct or not

**MIX Mode**

With SMS, PHONE and DATA wakeup function. Once one is valid, it can wakeup
**Note:**

1. Command without case-sensitive (including wakeup password), once device receives LAN host computer data, it disconnects TCP connection with LAN host computer immediately, enters into monitor status again.

2. If select “free” only, without “force offline”, please confirm “keeping online” rule whether no data transmit and receive within “Free” time.

**4.5.2 Bandwidth Manage**

Limit device online bandwidth according to IP address.

- **Name:** it is limited to use characters 0-9,a-z,A-Z, also can’t repeat name
- **IP:** Limit IP address scope.
- **Upstream:** Max upstream bandwidth.
- **Downstream:** Max downstream bandwidth.
4.5.3 MAC address binding

Realize MAC address binding to the connected devices to avoid ARP cheating attack.

![Connected Devices](image)

Picture 4-5-7

4.5.4 Others

Set WEB visiting port and DNS re-direction

![OTHER](image)

Picture 4-5-8

- **Web port**: revise web port, default is 80. If revised to be 8080, it needs to log in gateway configuration way: http://gateway IP:8080

- **Advance DNS service**: If start and make LAN host computer DNS address points gateway, then all LAN host computer domain name requests of gateway are sent to device appointed DNS server forcibly (please check system status first DNS/standby DNS).

**Note**: At the same time, device DHCP service supply LAN network card address whose DNS is gateway to LAN dhcp clients.
4.5.5 Timing Restart

Specify device to restart device in the certain period

![Image](4-5-9)

- **Support way:**
  - **self define:** Set gateway online time according to customer need
  - **every year:** Set gateway online time of the certain period every year.
  - **every month:** Set gateway online time of the certain period every month
  - **every week:** Set gateway online time of the certain period every week
  - **every day:** Set gateway online time of the certain period every day
  - **every hour:** Set gateway online time of the certain period every hour

4.5.6 DTU Function Configuration

Wireless gateway series port (COM/LINE port), one is used to configure gateway parameters or restore to default leaving-factory setting, the other is used to configure to data channel to realize DTU data communication function. If use control port COM/LINE as DTU series port, it needs to enable “DTU”. Following is explanation of DTU parameter configuration to use COM/LINE port as DTU.
- Center Num: input number according to the number of center server, when there is only 1 center server, please input 1. When there are more center servers, please input the corresponding number.

- Center IP address and port: When there is only 1 center server, please input 1 in “center num”, at this time, it only needs to configure “Main center IP and port”, input center server IP and port into corresponding bars, read picture 4-5-10. If center server doesn’t use fixed IP address, but use domain name, please input domain name into corresponding IP address bar. Center 1 Address Port ~ Center 4 Address Port don’t need to input.

When there are several center servers (main number is more than 1), input corresponding center server number in “cent num”, at this time, it needs to configure “Center 1 Address Port” ~ “Center X Address Port”, X is number of center servers, input all center server IP address and port to corresponding bars, read picture 4-5-10. If center server doesn’t use fixed IP address, but use domain name, please input domain name into corresponding IP address bar. In this time, “Main center IP Address and Port” doesn’t need to input.

- Protocol: device adopted working protocol. Default is Caimore DTU protocol. If customers need their own protocol, please select CUSTOM option.
Work Mode: Set transmission mode. There are TCP work mode and UDP work mode. Default is TCP protocol.

Baudrate: Setup serial port working Baudrate, scope is 110~230400BPS. Please set baudrate is the same as user side equipment baudrate. Otherwise, series port can’t communicate.

Databits: Set serial port working databits, set value is 7 and 8. Please set databits is the same as user side equipment databits. Otherwise, series port can’t communicate.

Parity: Set serial port parity, set values are NONE, ODD or EVEN. Please set parity is the same as user side equipment parity. Otherwise, series port can’t communicate.

Stopbits: Set serial port stopbits, set values are 1 or 2. Please set stopbits is the same as user side equipment stopbits. Otherwise, series port can’t communicate.

Device ID: setup ID for DTU, supply center server to differentiate DTU. ID is fixed to be 8 numbers. If it is not full of 8 numbers, please add 0 in front to make it full of 8 numbers.

SIM Num: set mobile number which uses SIM card, the fixed is 11 numbers. This parameter doesn’t change SIM card mobile number, but a kind of way for center server to differentiate connected devices.

Frame interval: Default is 200ms.

Data that DTU receive packet rules as following:

1. When serial port receives data whose length is more than appointed buffer 2048 bytes, DTU will packet the receiving data and send to center server.

2. Within the configure “frame interval” time, DTU equipment hasn’t received any serial port data, DTU will packet the received data and send to center server.

Notice: “Frame interval” time set too small, it can result one data packet to be separated into more data packets. If set too large, it can result two or more data packet to be packed into one data packet and send to center server together. If adopt our default value, one packet will be separated into more or more packets will be packed into one. If customer
can’t calculate the suitable value, please contact our technical support engineer.

- **Times of reconnect:** Times of DTU to connect with center server, default is 3. If trial times is more than configure “times of reconnect”, gateway will auto power down and after a moment power on again, and dial-up, reconnect center server till connect server successfully.

- **Interval of reconnect:** Interval time of wireless gateway to reconnect with center server, unit is second. When DTU connects with center server fails, if reconnect time is less than configure times, it will reconnect center server within the appointed time.

- **Interval of keepalive:** Interval time of keepalive data sent timely to maintain link. Unit is second. Default is 60s. Interval of keepalive time can’t set too small, if so, it will cause flow increasing. It also can’t be too large, if so, device can be detected after long time offline. Suggested value is 10S<X<120S

- **Self register packet:** When DTU establish connection with center server, DTU will send registration information to center, if registration packet needs specific definition

- **Keepalive packet define:** After DTU connect with wireless network, if there is no data transmit within a certain time, wireless network will disconnect with DTU automatically. In order to keep DTU connection with wireless network, it will send packet to data center from time to time.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>don’t send packet</td>
</tr>
<tr>
<td>Use Default</td>
<td>use default 0xFE</td>
</tr>
<tr>
<td>Self Define</td>
<td>Customer define their own packet according to actual situation</td>
</tr>
</tbody>
</table>
Chapter 5 FAQ

1. Frequent on/off line

- Please enter system status to check network signal situation, to confirm whether network signal is too weak, please check antenna whether connect correctly.
- Please check corresponding parameters of keeping-online, whether rules are meet.
- If keeping-online destination IP uses domain name, please log in gateway command terminal (appendix 1) to confirm whether decode domain name and visiting destination address normally.

2. Forgot password

- Please restore to default setting, reference appendix 4.

3. LAN indicator is off

- Please check network cable whether connect with gateway closely.
- If gateway connects with PC directly, please change cross network cable.
- lease connect gateway with switch to check network link is normal or not.

4. Can’t dial-up to be online

- Please check WAN configuration information whether the same as information ISP supplied.
- Check signal by system status, if signal is weak, please check antenna whether connect correctly.
- Please check whether this place covered by network or not.
- Please check signal and card situation from system status, if card situation is
wrong, please re-insert or change new card.

5. Dial-up to be online, but can’t visit website

- Please check device gateway whether points Gateway.
- DNS is whether the same as gateway, if not, please revise (reference Appendix 6)
- If has input DNS information, please check whether are correct.
- If input DNS correct, please clear (use obtain DNS automatically), after dial-up
- successfully, please input according to system status supplied DNS.

Appendix 1   Login gateway by Telnet

1. Click window “start”->”run”, input:cmd<enter>

![Run Window](image)

Picture a1-1

2. Input telnet IP address:telnet 192.168.9.1  (gateway IP)<enter>
3. Login

4. Input username and password
5. It means login successfully when appear “#”, enter shell command.

Appendix 2  Login gateway by hypertrm

1. Click “start”->“run”, input: hypertrm <enter>
2. Input name: 1

3. Select serial port which PC connected with gateway COM/LINE:

4. Set serial port parameter: 57600, 8N1 and None flow control
5. After confirmation, input <enter>, below will display

```
localhost login: 
```

6. Input username and password, enter shell.
Appendix 3  Obtain debug information from syslog server

1. Run winSyslog, click “start logging”.

Picture a2-6
2. If your server access public network by ADSL ROUTER, please make Port mapping on your ADSL ROUTER, to Port mapping external UDP 514 port to your server 514 port.

**Appendix 4  Restore default setting**

1. Power on gateway
2. Pres RESET for 30 seconds.
3. Restart gateway

Appendix 5  Wireless network basic information(In China)

<table>
<thead>
<tr>
<th>Network</th>
<th>Cetner Num. (APN)</th>
<th>Access Point</th>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS</td>
<td><em>99</em>**1#</td>
<td>cmnet</td>
<td>blank</td>
<td>blank</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>uninet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDGE</td>
<td><em>99</em>**1#</td>
<td>cmnet</td>
<td>blank</td>
<td>blank</td>
</tr>
<tr>
<td>TD-SCDMA</td>
<td><em>98</em>1#</td>
<td>cmnet</td>
<td>blank</td>
<td>blank</td>
</tr>
<tr>
<td>CDMA</td>
<td>#777</td>
<td>blank</td>
<td>card</td>
<td>card</td>
</tr>
<tr>
<td>EV-DO</td>
<td>#777</td>
<td>blank</td>
<td>card</td>
<td>card</td>
</tr>
<tr>
<td>WCDMA</td>
<td>*99#</td>
<td>3gnet</td>
<td>blank</td>
<td>blank</td>
</tr>
</tbody>
</table>

Note: above supplied center number and access point information are only for reference in china, if there is difference with ISP supplied information, please use ISP supplied information. Usually it is ok to use our default setting parameter, it needs to revise when use APN/VPDN special network.
Appendix 6 Obtained DNS setting according to gateway

Please enter gateway system status to check DNS:

![Gateway System Status](image1)

**Picture a6-1**

Click “start”->“control panel”, click “network connect”, read picture below:

![Network Connection](image2)

**Picture a6-2**

Click “local connection”, select “properties (R)”, select “Internet protocol (TCP/IP)”, click “properties (R)”, then following configuration window will display, revise DNS according to gateway system status supplied, after revising, click “OK”.

---

Tel:+86 592 5901215 88  web:www.caimore.com/emain.asp
Input DNS according to system status supplies. Done.