Caimore
Wireless Router
User Manual

Copyright:

All information in this user manual is protected by copyright law. Whereby, no organization or individual shall copy or reprinted the whole or part of this user manual by any means without written authorization from Xiamen Caimore Communication Technology Co.,Ltd.

Trademarks :

Caimore, , & CAIMORE are all registered trademarks of Xiamen Caimore Communication Technology Co.,Ltd. Other trademarks mentioned in this manual belong to other organizations related. Xaimen Caimore Communication Technology Co.,Ltd does not own the right of other trademarks and logos.

Notice:

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

Revision History:

Version	Description	Date	Author	Issue
V1.0	Primarily Released	2008.10.17	linjh	
V2.0	Adjusted WEB configuration whole style Supported 4G gateway	2009-12-25	Lenev	
V2.1	Updated, add new functions.	2011-11-18	linjh	
V3.0	Updated, directions of the support and snmp functions for 4G	2013-9-17	lijh	

Contents

Chapter 1 Product Introduction

1.1 Product Overview：

CM520-8AX series WIFI router is cellular terminal devices that support WIFI (802.11 a/b/g/n) and 4G wireless network.

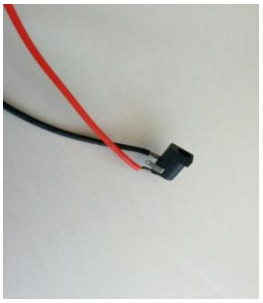
Meanwhile it loads WAN VPN secure tunnel and WIFI LAN authentication of transmission and other security features of wide area network VPN secure tunnel and WIFI LAN transmission. It has realized the function of QOS, SNMP remote management, support QQ, wechat, microblog, a key certification and variety of authentication access, local media watch, remote multimedia batch update, reports statistics advertisement push, broadband management, WIFI backstage management, online behavior management, GPS positioning, GPS accurate advertisement push. Of course, they also have achieve seamless connection between LAN and wireless WAN, providing users with a high-speed, secure, reliable mobile broadband service.

Currently, it has been widely used in vehicle, small and medium-sized enterprise, home wireless networking, and kinds of public facilities. Such as city bus, coach, tour bus, shopping malls, exhibition halls, hotels, etc.

This user manual is suitable for the following models:

CM520-8AF,CM520-87F,CM520-86F,CM520-89F,CM520-91F,CM520-8VF ,CM520-8BF,CM520-8CF， , CM520-61F, CM520

1.2. WIFI vehicle products Appearance and Accessory

			
Power	Optional DC	Ethernet Cable	Optional adaptor

(Note: The power accessories for WIFI Vehicle device are using three vehicle power supply cables---red, yellow and black. The red is positive and connect the ACC,the black is negative, and the yellow is positive and connect the battery with the voltage range of 7V-33V.If you want to have other indoor tests, please use the power adapter and connect to the DC with vehicle cable.**)**

1.3 Product features：

Industrial Design

- **Industrial CPU: Industrial CPU:** industrial high-performance embedded processor, 533MHZ, with 16KB Dcache, high-speed cache data speed up data access , with 32KB Icache, high-speed instruction cache, enhanced instruction processing speed.
- **Industrial wireless module:** using industrial wireless module, strong interference rejection, and stable transmission.
- Real-time operating system: using LINUX2.6 operating 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 of 3H and 3W,, meanwhile the circuit boards of all products used high-quality materials to ensure the board materials stable and reliable.
- Industrial components: the machine adopts strictly screened industrial components.
- Industrial Power: Wide voltage power supply design, adaptive range of power is from DC5V to DC35V, built-in power reverse supply protection and over-voltage and over-current 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

Stable and reliable

- **Online maintenance patents:** Intelligent anti-dropped, online testing, online maintenance, automatically reset to ensure that equipment is always online.
- **Three-tier system protection:** based on the original two protection functions (software protection +WDT + CPU built-in protection), the system increased a detection and protection function of VWM (Virtual Man Watch), if it appears that the network is abnormal or system receives Strong interference anomaly, the system will auto reset, which thoroughly solve the problem that it needs maintainer to pull out electric when the system appears abnormally in the industry, and ensure that the system is stable and reliable.
- **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, built-in 15KV ESD protection.
- Metal shell: Strong anti-interference ability, meanwhile has shielding effect and radiation protection, protection grade is IP31.
- All wireless modules are certified by the CGD or FCC certification or CE certification.
- High-speed processing CPU: ARM9 industrial-grade high-speed CPU, can handle a variety of protocol data conversions at higher speed; solve the difficult problems ,such as, "fake online", "fake death", "crash" etc
- **MMU：** New type CPU with MMU， to prevent the system unstable when it appears abnormally.
- Large memory: FLASH 128Mbits, SDRAM 1Gbits, a large memory to cache data sent by customer, meanwhile receiving large packets, no data lose.
- **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, and the drop-line probability dramatically reduced.
- **EMC performance outstanding:** Obtained CE Certification ; passed China detection department test , EMC test and 3000V electrical shock test, especially suitable for use under harsh industrial environments; system EMC

/ EMI performance excellent, system stable and reliable.

Easy to use

- **Using Factory default configuration parameters,** customers only need to modify some parameters, even no need to change any parameter, you can quickly use the equipment
- **Graphical configuration tool:** improved graphical configuration tool that provides rapid deployment capabilities for customers to achieve rapid deployment; provides mass configuration.
- **Product manual offers** quick configuration instructions, you can quickly use the equipment
- **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 sedimentation**, the function of equipment is very completed and easy to use.

1.4 Software Functions： ：

- **Support WIFI** (802.11 b/g/n) and 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**, supports PPPOE, can directly connect to ADSL equipment and other leased line
- **Support backup function** for 4G wireless link and broadband link, if cannot communicate in 4G, it will auto switch to PPPOE broadband and vice versa.
- **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, ensure the equipment 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 timer switch function**
- **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 WIFI WAP encryption ,**built in WAP and WAP2.0,and 64 bits and 128bits wep encryption, support WEP encryption and built in the hardware security engine ,such as 802.11I 4.0 WEP(64 bits and 128bits) TKIP,AES and CCMP etc.

- **Mppe supports encryption** of MPPE40 and MPPE128 and encryption mode of stateful, IPSEC supports encryption algorithm of DES、3DES、AES and AES128.
- **Support QOS bandwidth** management.
- **Support Dynamic and static route**
- **Support DHCP/DHCPD**
- **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**, support 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**
- **IP 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**
- **Supports TFTP remote software upgrade**
- **Support real-time clock**
- **Support both LINUX and WINDOWS operating systems**
- **Support local multimedia access, remote batch update**
- **Support shadowing**
- **support for SNMP remote management**
- **support QQ, wechat, microblog, a key certification and variety of authentication access.**
- **support bandwidth management, down the line speed, total bandwidth speed, user sharing mode**
- **Support Bus Power Management**

1.5 Specification： ：

Cellular Parameters

Cellular Network	Standard and frequency bnads	Communication bandwidth	Transmit power	Receiver sensitivity
LTE-TDD/ HSPA+ /UMTS//HSDPA/ HSUPA/WCDMA/ EDGE/GSM	LTE TDD: 2600/2300MHz UMTS: 2100/900MHz GSM: 850/900/1800/1900M	LET TDD:DL 68Mbps/UL 17Mbps DC_HSPA+:DL 42Mb/s(Category 24) HSPA+:DL 28Mb/s(Category 18)	WCDMA/HSDPA:24dBm LET:23 dBm	<-109dBm

	Hz RxDiv Band:UMTS 2100/900MHz LTE TDD 2600/2300MHz	HSdPA:DL 14.4Mb/s(Category 8) HSUPA+:DL 5.76Mb/s(Category 6) WCDMA CS:UL 64kbps/DL 64kbps WCDMA PS:UL384kbps/DL384kbps		
LTE-FDD/ HSPA+ /UMTS//HSDPA/ HSUPA/WCDMA/ EDGE/GSM	LTE FDD: 2600/2100/1800/DD800MHz UMTS: 2100/900MHz RxDiv Band: UMTS 2100/900MHz LTE FDD	LET FDD:DL 100Mbps/UL 50Mbps DC_HSPA+:DL 42Mb/s HSPA+:DL 28Mb/s HSDPA: DL 14.4Mb/s HSUPA+:DL 5.76Mb/s WCDMA CS:UL 64kbps/DL 64kbps WCDMA PS:UL384kbps/DL384kbps	WCDMA/HSDPA:24dBm LET:23 dBm	<-109dBm

WIFI parameters:

Item	Content
WIFI module	WIFI module chip-embedded, high integration, good stability
WIFI standard	Support 802.11 b/g/n standard, speed， Support 6M/9M/12M/18M/24M/36/48/54Mbps,up to 108M
Encryption	Supports WAP encryption, built-in WAP and WAP 2.0, Built-in 64-bit an 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
AP mode	Support AP mode
Transmission distance	Outdoor non-stop, outdoor coverage up to 150 meters

GPS Parameters

ITEM	CONTENT
GPS Module	Use industrial GPS wireless module
Receiver type	Receive GPS,48 channels, Frequency L1 ,chip speed 1575.42MHZ,C/A code,chip speed 1.023MHZ.
Positioning accuracy	Positioning:2.5m CEP SBAS:2.0m CEP

Speed accuracy	Speed accuracy < 0.01m/s（high speed）<0.01 °(heading)，（ 50 % @ 30 m/s
Capture time	Cold start: 35S,Auxiliar start <3S；Hot start：1S
Output information	NMEA,UBX BIN：GGA GSA GSV RMC VTG GLL
navigation data update rate	1Hz
sensitivity	Track:-163dBm;Navigation:-160dBm;Acquisition：-147dBm
Operating limit	Speed：500m/s Height：50000m

Hardware System：

Item	Content
CPU	industrial high-performance embedded processor, 320MHZ
MMU	CPU with MMU memory management unit, can prevent memory overflow
FLASH	128Mbits
SDRAM	1GMbits
Dual TF Card	2*128G TF card

Operating System：

Item	Content
Operating system	Using LINUX2.6 operating system with memory management unit and real-time featur upgrades is very fast and system is stable；

Interface Type：

Item	Content
WAN port	One 10/100M self-adaption WAN port, built-in isolation, support Auto MDI/MDIX support PPPOE.
Ethernet port	Four 10/100 Base-T Ethernet port(LAN1-LAN4),support Auto MDI/MDIX; built-in 1.5KV magnetic isolation protection
Serial Port	1 RS485 interface 1 or RS232 serial port (support RS422/TTL) Data bit: 7,8 bit Stop bits: 1, 2-bit Parity: no parity, odd parity, even parity, SPACE and MARK parity Baud rate: 300bps - 115200bps

	Flow Control: None flow control
USB interface	one USB interface, USB2.0, HOST interface, speed at 12Mbps
I/O interface	Support 3 channel I/O interface, can apply to vehicle detection and control; this function is optional and customized.
Indicator LED	Power indicator SYS indicator WIFI-2.4G indicator; WIFI-5G indicator; 4G online indicator
Antenna Interface	Standard SMA female interface, 50 ohm; optional 3M/5M/10M/15M antenna extension cable, meet the different needs of customers
WIFI antenna	Parity: no parity, odd parity, even parity, SPACE and MARK parity
UIM interface	1.8V/3V/5V standard putter user card interface, built-in 15KV ESD protection
Power Interface	Standard 3-pin power jack
RESET button	Reset button to restore factory settings

Power supply:

Item	Content
Supply voltage	Wide voltage design, DC 6V to the DC32V power supply directly to the device; an built-in power supply has the over-voltage protection and reverse current protection
Standard power	DC9V/1.5A
Communication Current	Average communication current : 390mA @ +9 VDC; Communicating instantaneous peak current: 1.0A @ +9 VDC
Standby current	Standby average current: <56mA @ +9 VDC

Physical features:

Item	Content
Housing	Metal housing, anti-radiation, anti-interference; lightning protection design;protection rating IP30; particularly suit for harsh industrial control environments.

Product dimensions	167 * 104 * 26mm（not including the antenna and the fixed parts）
Packing Size	350*215*88mm
Weight	

Other Parameters:

Item	Content
Operating Temperature	-25 ℃ ~+65 ℃
Extended operating temperature	-35 ℃~+75 ℃
Storage Temperature	-40~+85 ℃
Relative Humidity	95%(No condensation)

1.6Indicator：

Indicator：

Indicator	State	Description
Power	On	Power is Normal
	Off	Power off
WAN	Off	WAN unconnected
	On	WAN connected
	Flash	Data transmitting and receiving
WIFI	Off	Disable WIFI
	On	Enable WIFI
	Flash	Data transmitting and receiving
COMM	Flash	Data transmitting and receiving
	Off	No Data transmitting and receiving
Online	On	On line
	Off	Off line

Chapter 2 Installation

2.1 Packing List

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

Gateway Host	1 Unit
RJ45-DB9 Serial Line	1PC
DC 9V Power Adapter	1 Unit
Network Cable	1PC
4G Antenna	1PC
WIFI Antenna	1PC
CD of User Manual	1PC

2.2 Product Introduction

Product Appearance：

Picture 2-2-1

Front of Device：

图 2-2-2

① Power Indicator ② WIFI Indicator ③ COMM Communication Indicator(not use now) ④ALARM Indicator(not use now) ⑤Online

Indicator(4G/WAN Indicator)

Back of Device:

图 2-2-3

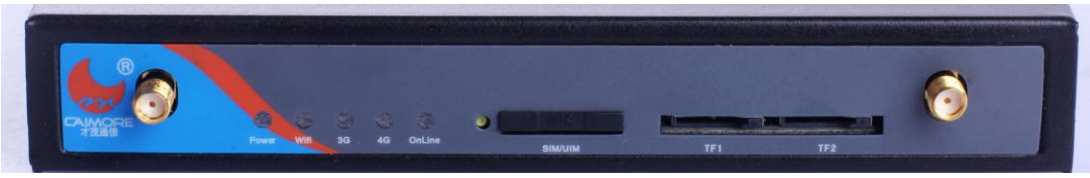
① Restore to Default Setting Button ②Power Port ③ USB(NOT USE NOW)
④ Port for test or debug ⑤Ethernet Port ⑥ WAN Port

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: :

Without electrifying device, please use a needle object to press on the out button of SIM card outlet, SIM card sheath will flick out at once. Cover SIM card with SIM card sheath. But you must pay attention to put the side which has metal point of SIM card outside, and insert card sheath back to SIM card outlet. See below of the picture:



Picture 2-3-1

Warning: forbid to pull out or insert SIM card with electricity.

2.4 Antenna Installation

Please turn SMA male connector clockwisely to be tight. Read below picture:
Left is 4G antenna, Right is WIFI antenna.

Picture 2-4-1

2.5 RJ45-DB9F Instruction

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

Com/line: RS232 asynchronous communication serial interface

RJ45-DB9F Conversion line signal connection as below mentioned: The signal definition of DB9F Serial communication interface shows as below mentioned:：

RJ45	DB9F
1	8
2	6
3	2
4	1
5	5
6	3
7	4
8	7

The signal definition of DB9F Serial communication interface shows as below mentioned:

PIN	RS232 Signal Name	Description	Direction relative to DTU

1	DCD	carrier wave signal check	Output
2	RXD	receive data	Output
3	TXD	send data	Input
4	DTR	data terminal ready	Input
5	GND	Power reference ground	
6	DSR	data device ready	Output
7	RTS	Request to send	Input
8	CTS	Data device get ready to receive data	Output

Chapter 3 Rapid Configuration

We release this setting instruction in order to realize below mentioned two points. First, When customer receives our device, they can check fast whether the device is good or not, whether it can work normally or not. Second, Most customer can use device fast by only changing setting parameters of this setting instruction (other parameters are default setting). Take Window XP as an example, let us explain our wireless industrial fast setting process.

Fast setting usually need to configure WAN parameter and LAN parameter and keep other parameters as leaving-factory default setting. If need to change other parameters, please read < chapter 4 Detailed Parameters Configuration >

3.1、Inset SIM card into gateway SIM card socket（refer 2.3）.

3.2、Connect antenna（refer 2.4）

3.2、Connect gateway with PC hardware

Method1:Gateway connect with Switch(OR HUB) by Ethernet cable. PC connected with LAN 1, please kindly check whether Ethernet yellow indicator is on or not,if not,please check the link and interface if connect tightly or not.

3.3、PC Network settings（(Set IP address, Gateway, DNS）

Click “ Start” 

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

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 below window, select “Obtain an IP address automatically ”, after that, then click “OK” . In this way, wireless gateway assigns IP address to customer PC automatically. At this time, if DNS also adopt assigning automatically, also can select “obtain DNS server address automatically ”, then DNS setting is also ok. When arrive <3.5 Set DNS>, customer can skip and no need to set DNS.

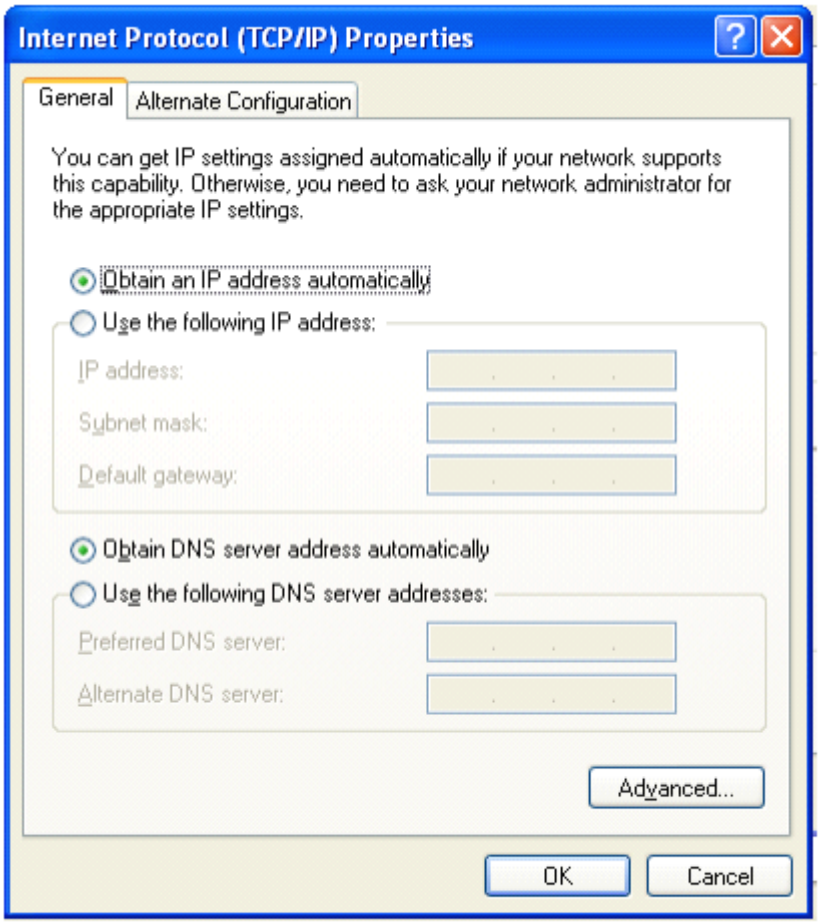


图 3-3-2

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:

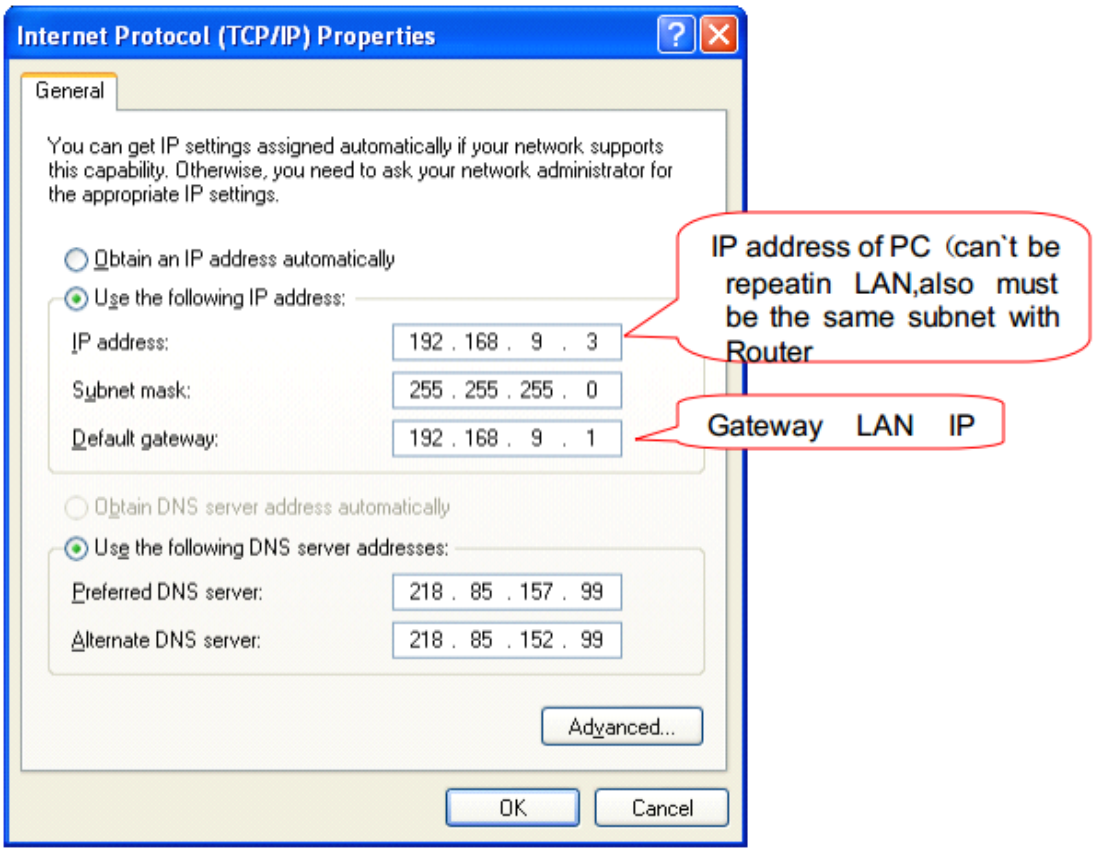
The Wireless gateway LAN1 port IP: 192.168.9.1 (leaving-factory default value)

PC side parameter setting:

IP address: 192.168.9.X (X is any one between 1-254, but can't confilict with other PC IP address, here X is 3 in this example)

Subnet mask: 255.255.255.0

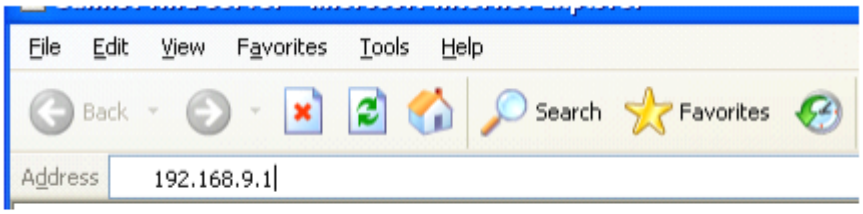
Default gateway: 192.168.9.1(it is the wireless gateway LAN1 port IP address 192.168.9.1) Ways of obtain and revise DNS, please reference Appendix 6.



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 bar. Picture as below:

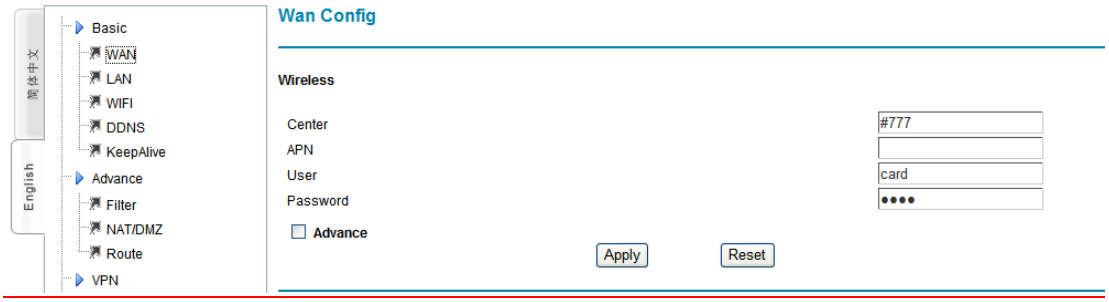


Picture 3-4-1

Type user name and password (default user name: admin, Password: admin).

Select WAN Configuration, please set and submit according to information ISP supplied (read picture 3-4-3, it is the EVDO/CDMA lonin information).

If use APN/VPDN, please type these information (Center, APN, User, Password supplied by ISP) to the related correct bar is ok. It is to be default configuration (refer Appendix 5) according to network when leaving factory, then click "Apply " to save



Picture 3-4-3

Note: In normal situation, it is ok to use our leaving-factory default parameters are ok,and doesn' t need to revise, it only need to revise when using APN/VPDN special network.

3.5 Setup DNS

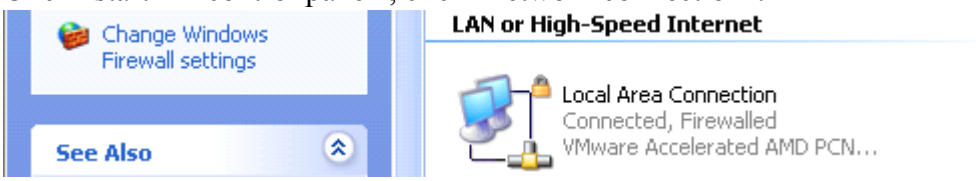
If **"method 1:** adopt obtain IP automatically "of "3.3 Network Setting on PC Side" has selected "Obtain DNS server address automatically" and also save it, then can skip this step.

After finishing 3.4 Setup WAN 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:

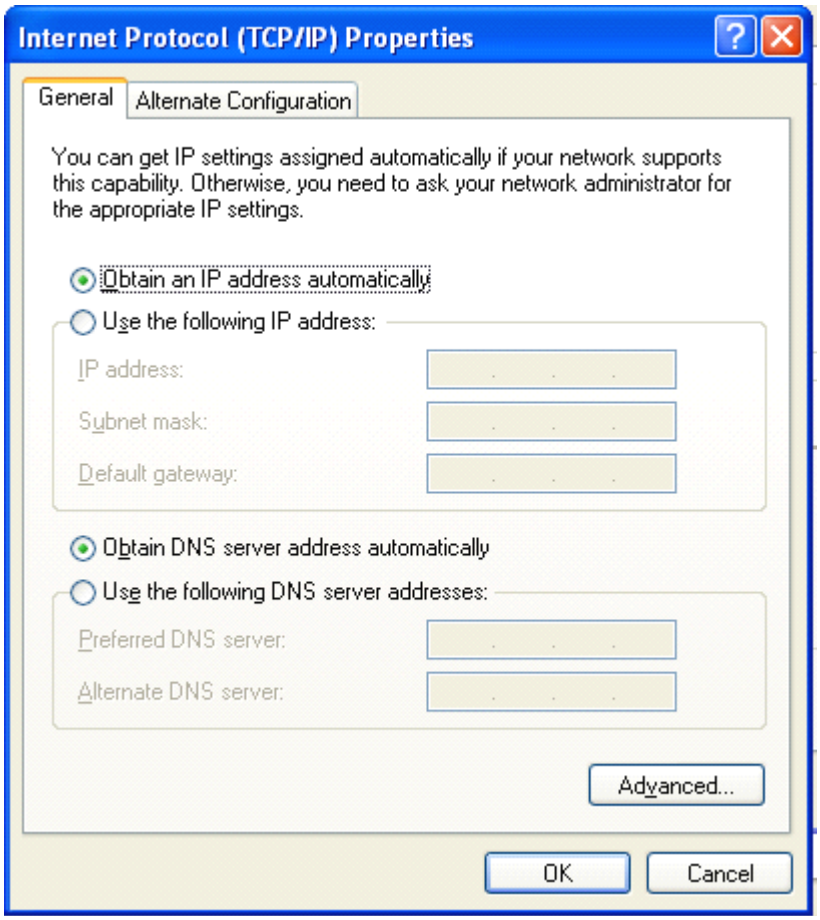
Methods 1: adopt obtaining DNS automatically

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



Picture 3-5-1

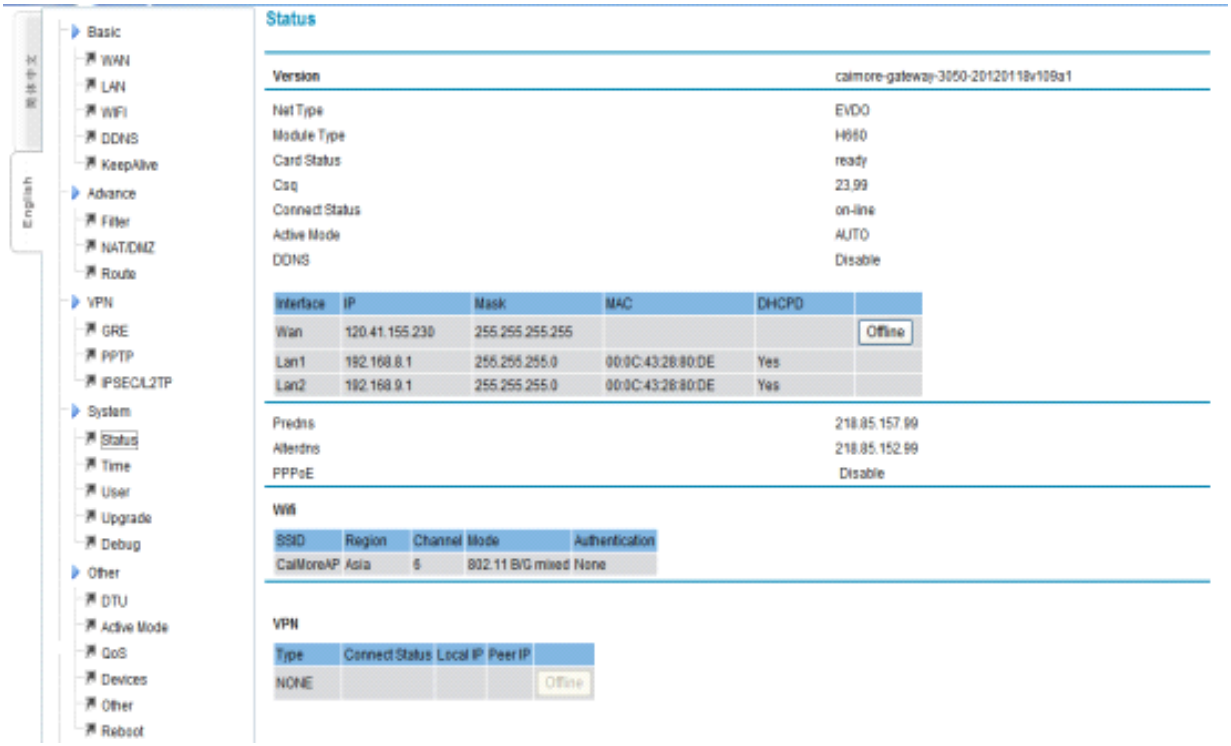
Click“local connection”, select “properties(R)”, select“Internet protocol (TCP/IP)”, click “properties(R)”, it will display below window, select“Obtain DNS server address automatically”, then click“OK”. In this way, gateway will assign DNS server address automatically for PC.



Picture 3-5-2

Method 2: Set DNS of PC according to DNS obtained by gateway

According to the third chapter, the method of rapid configuration, configurate and connect PC with wireless gateway, and then set the IP address of each other. Finally, login gateway by IE; when login on network successfully, namely online indicator is on, please click “system status”of gateway to check DNS assigned by carrier.



Picture 3-5-3

Record this DNS assigned by carrier, and then type this DNS to"First DNS server" of PC. The process is to click "start" ->"control panel"; click "network connection", and picture as below:

Picture 3-5-4

Click "local connection"; select "properties(R)"; select"Internet protocol (TCP/IP)"; click "properties(R)"; and it will display below window; revise it according to DNS of gateway system status; after that, click"OK".

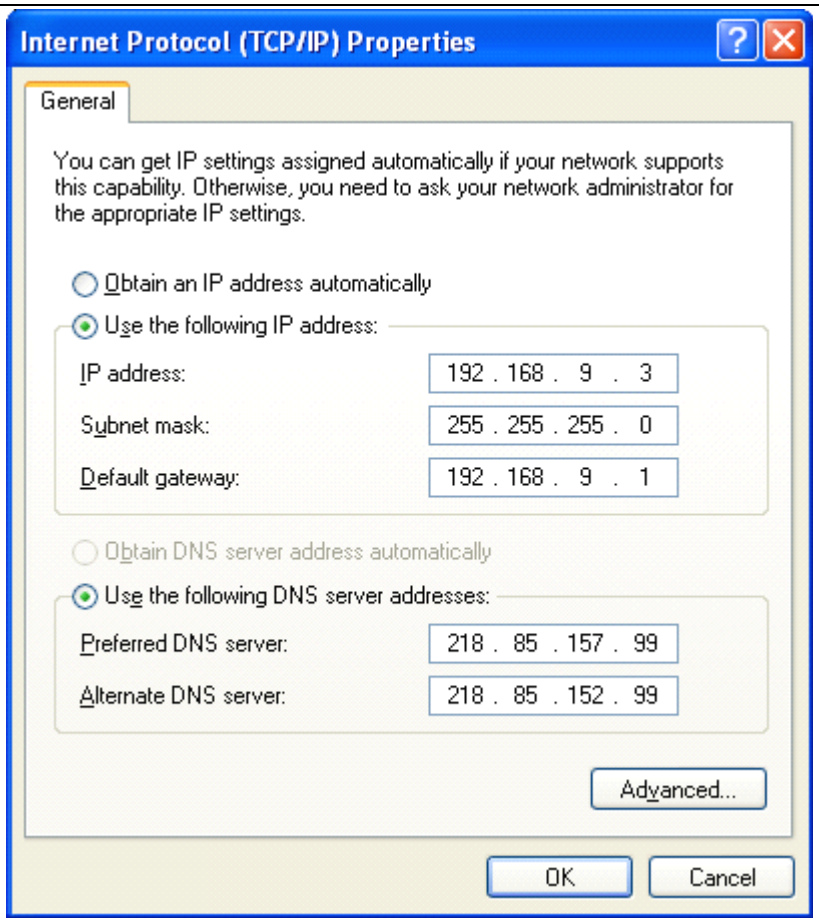


图 3-5-5

3.6. Device Online Testing

When finishing 3.1-3.6 steps, please re-power wireless gateway, and then wait gateway“Online ” indicator on (if indicator is not on after more than 1 minture, please check above steps and configuration information are right or not. If all are right, but indicator is still not on, please feel free to contact us for technical help). when online indicator is on, users can use gateway to login network or operate wireless data transmission. Type website address on IE of PC, like www..com, and then congratulations on you, you are online already and can transfer wireless data now.

Chapter 4 Detailed Parameter Configuration

4.1 Basic Configuration

4.1.1 WAN Configuration

Gateway dial-up configuration, that is the basic parameter of connecting wireless network.

Picture 4-1-1

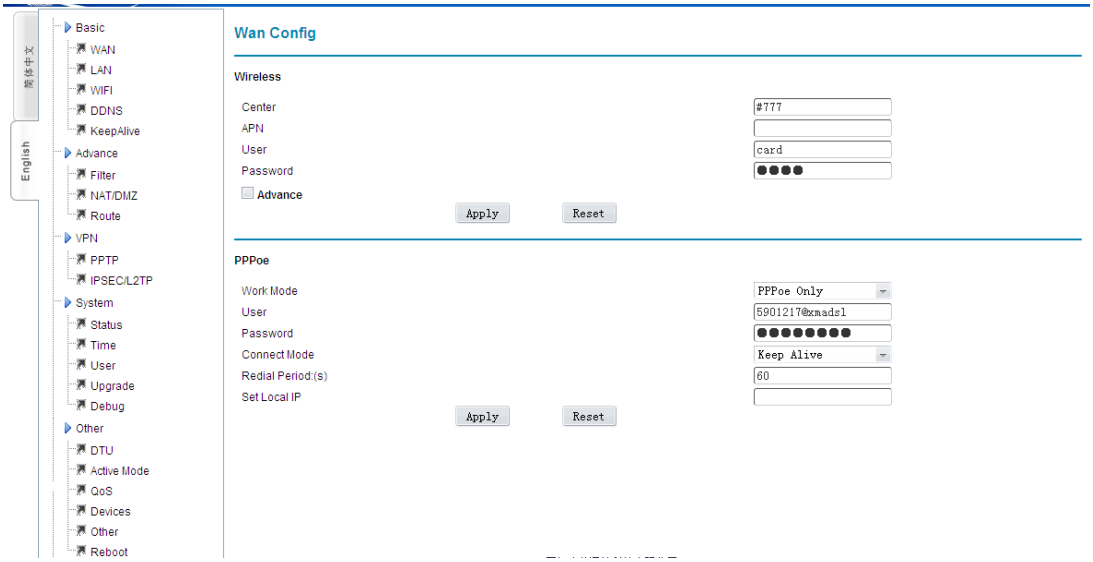
- Calling center number, Access Point Name, Username and Password: Usually the information is default setting (refer to Appendix 5). Usually it doesn't need to revise. If use APN/VPND, it needs to type these information supplied by ISP to the exact place.
- PIN code: If mobile UIM/SIM card set PIN code 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.
- The 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 one is obtaining automatically, please input 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 the short name of point-to-point protocol over Ethernet, and it can make Ethernet host connect with remote access concentrator by a simple bridge equipment



Picture 4-1-2

➢ **Working Mode:**

PPPOE Disable: only use 4G network, do not use PPPoe

PPPOE Only: only use PPPoe, do not use 4G

PPPOE Master: Mainly use PPPoe. When PPPoe is unable to used, then use 4G

PPPOE Backup: Mainly use 4G. When 4G can't be used, then 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

As picture 4-1-3

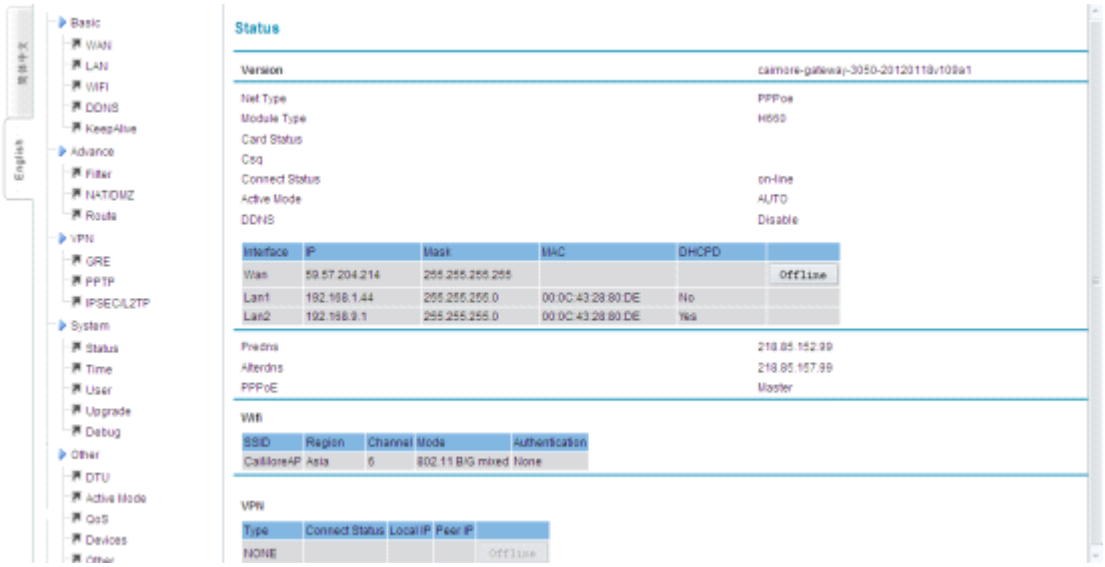
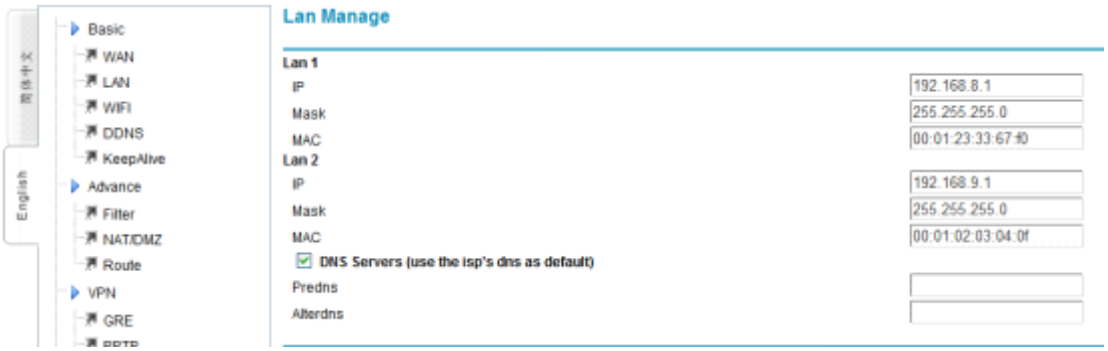


图 4-1-3

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 Address: 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, and default situation (blank) is obtained 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 IP connected to equipment are in the same Subnet Mask with gateway.
2. When multi units work in the same LAN, MAC address will restore to default setting after "load default setting". It is easy to make MAC address conflict with other equipment. So please revise MAC address.
3. If users input DNS server address, after dialing, please check whether DNS

used by gateway can decode domain name.

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, and it is a kind of internet technology.

Picture 4-1-5

- **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:

Picture 4-1-6

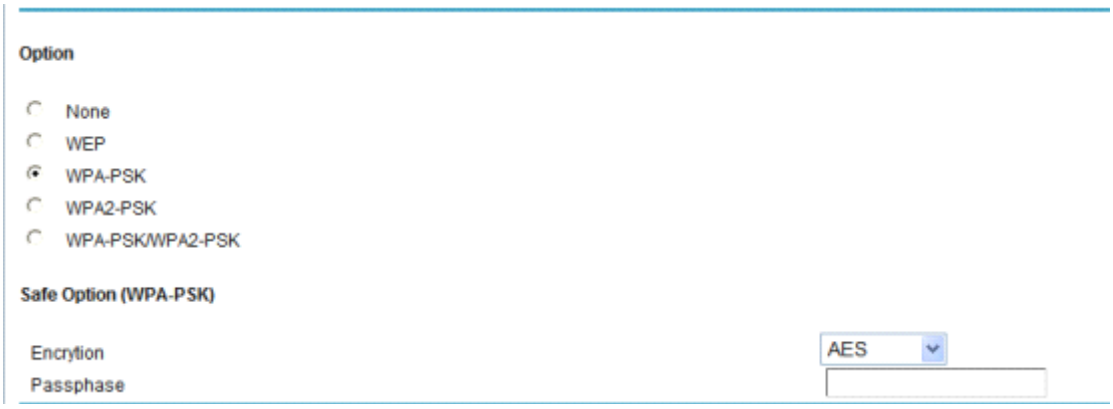
- **Authentication:** Default is Auto, if default can't work normally, customer can choose Shared (Open system).
- **Encryption:** 64 bit or 128 bit.
- **Passphase:** WEP key. Customer can input by hand or adopt program creats encryption key automatically. Customer on wireless network has to input encryption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

Notice：

1. When multi units of 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 secret key automatically, please input a word or a group of printable characters in the "Password", and then click CREAT button. Gateway can create WEP secret key automatically and use it as wireless network Encryption key.

WPA-PSKEncryption:



Picture 4-1-7

- **Encryption Mode:** Support TKIP,AES,TKIP/AES.
- **Passphase:** Encryption key, length is between 8 ~ 63 characters.

WPA2-PSK Encryption:

Picture 4-1-8

- **Encryption Mode:** Support TKIP, AES, TKIP/AES.
- **Passphase：**Encryption key, length is between 8 ~ 63 characters.

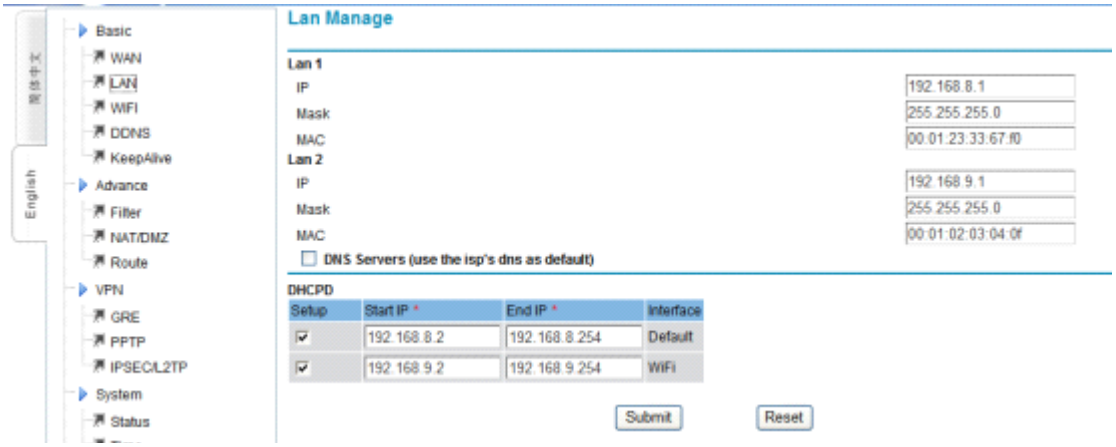
WPA-PSK/WPA2-PSK Encryption:

Picture 4-1-9

- **Encryption Mode:** Support TKIP,AES,TKIP/AES
- **Passphase:** 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. The system default is open. If customer doesn't use DHCPD service, please close this selection.



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. Lapped DHCP servers can't be existed in the same LAN. If there are multi devices supply DHCP server function in the same LAN, it can cause IP address can't assign normally in the system. 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 obtained by gateway when dialing up to a certain domain name to bind the continuous IP obtained by wireless dial-up with the certain domain name.

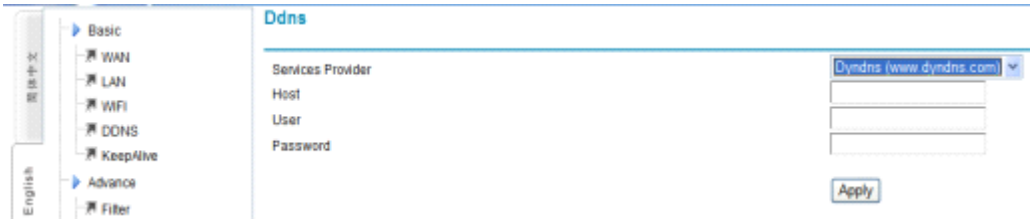
If wireless gateway opens DDNS, after wireless gateway obtaining a new IP by dialing up successfully every time, it will send new obtained dynamic IP address to customer dynamic domain name server to realize binding updating between the settled domain name of dynamic domain name server and gateway IP 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.

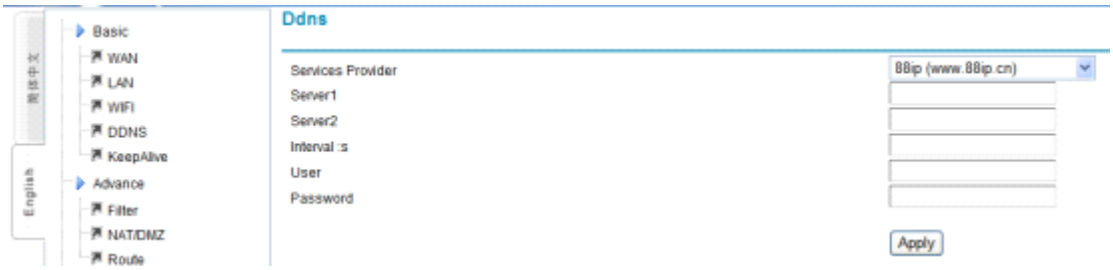
Picture 4-1-11



Picture 4-1-12

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 "SUBMIT" 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.



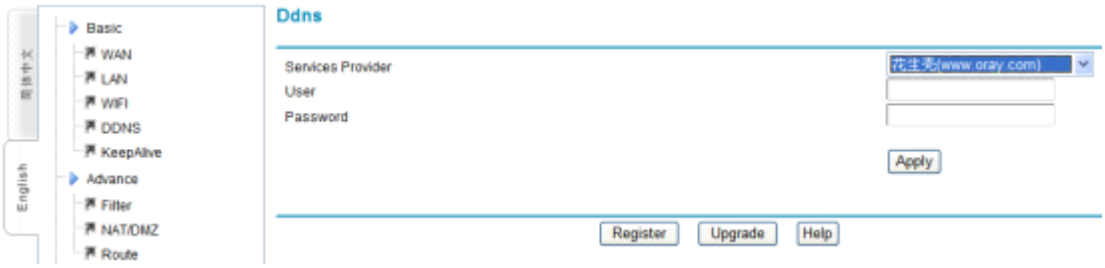
Picture 4-1-13

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 "SUBMIT" 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 to update one time
- **Username:** User name when log in 88ip server
- **Password:** password when log in 88ip server

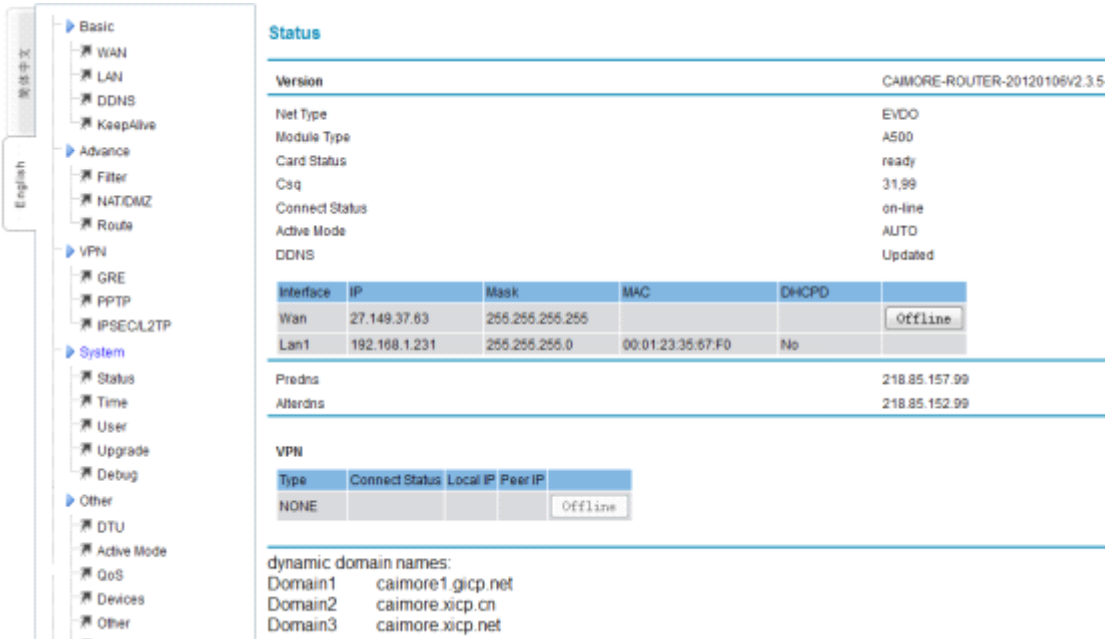


Picture 4-1-14

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 "SUBMIT" 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, and it is convenient for users to check DDNS whether it works normally. If update successfully, it will display Updated. As for Oray, there are 3 domain name updated successfully. Picture as follows:



Picture 4-1-15

Notice: Only when the IP address assigned by ISP is global address, wireless gateway can use as center server. Now in China, only telecom CDMA 20001X and CDMA2000 EVDO 4G network have the global IP address.

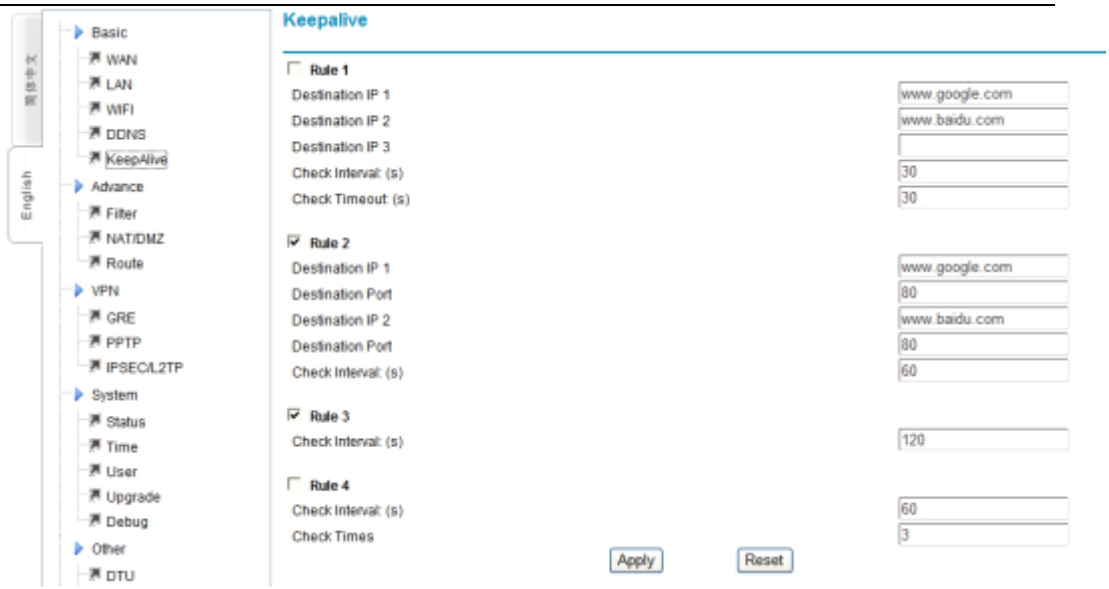
4.1.7 Keep Online (make sure to select one kind online maintenance solution)

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 ”and regard them as the 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 multi 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.



Picture 4-1-16

➢ **Rule 1: PING Mode**

Wireless gateway checks destination IP address through PING (ICMP) packet periodically. When the referenced destination IP address device doesn't respond PING (ICMP), wireless gateway considers communication line is disconnected already, and it 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 will judge to be off-line, and make gateway on-line 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 will 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 periodically, 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：DataMode

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-line and off-line frequently.

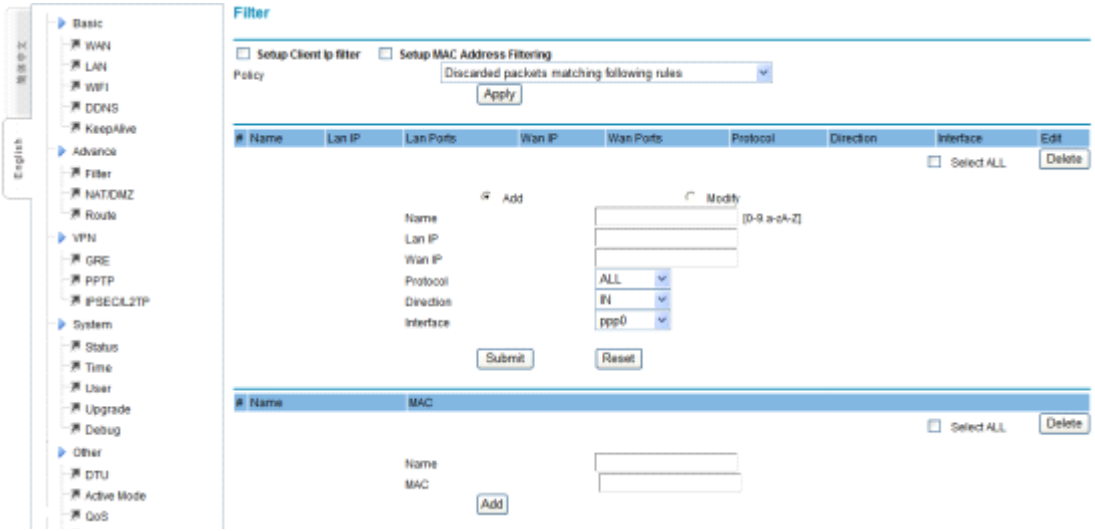
Notice:

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.



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.

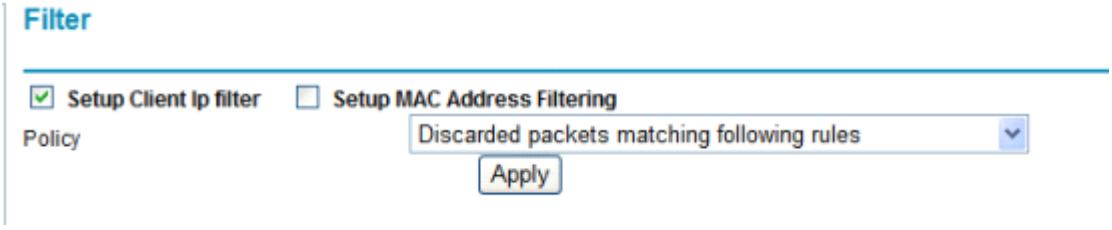
  IN/OUT: Include IN and OUT
- **Interface:** Data packet go through interface, such as br0，PPP0 and so on.

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 configured rules.



3. 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

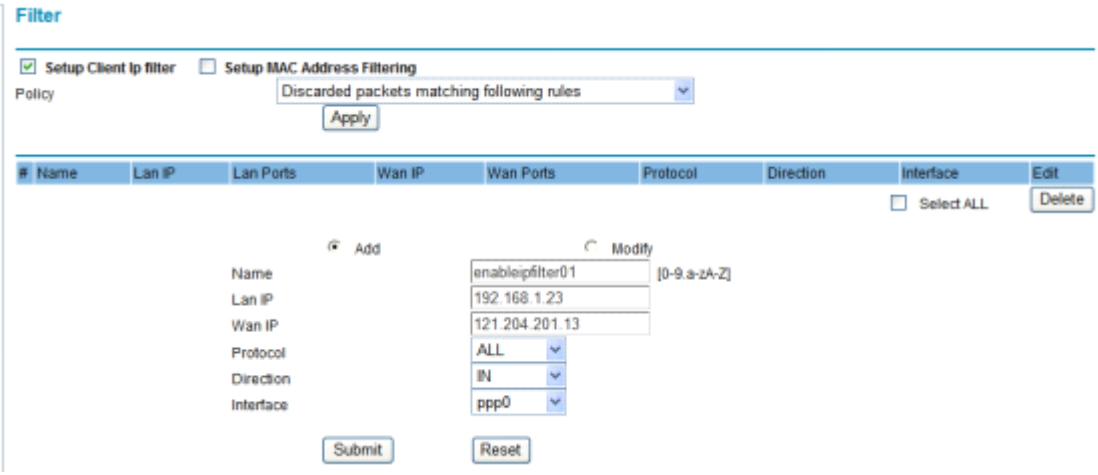
Direction：IN

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.



Picture 4-2-3

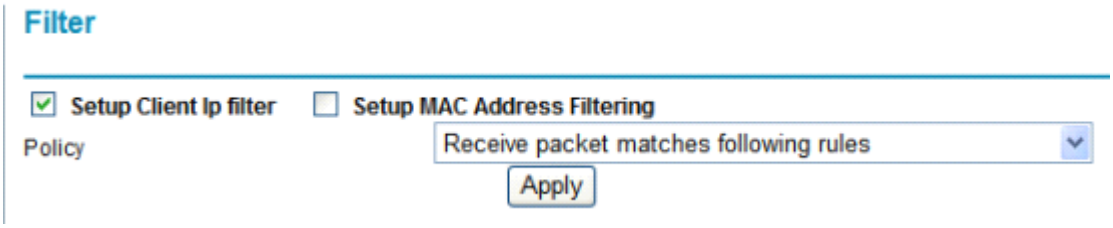
Example 2 of IP address filtering:

1、select "setup client IP filter"

2、Running rule: "receive packet matches following rules", click "Apply" to save.

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.



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

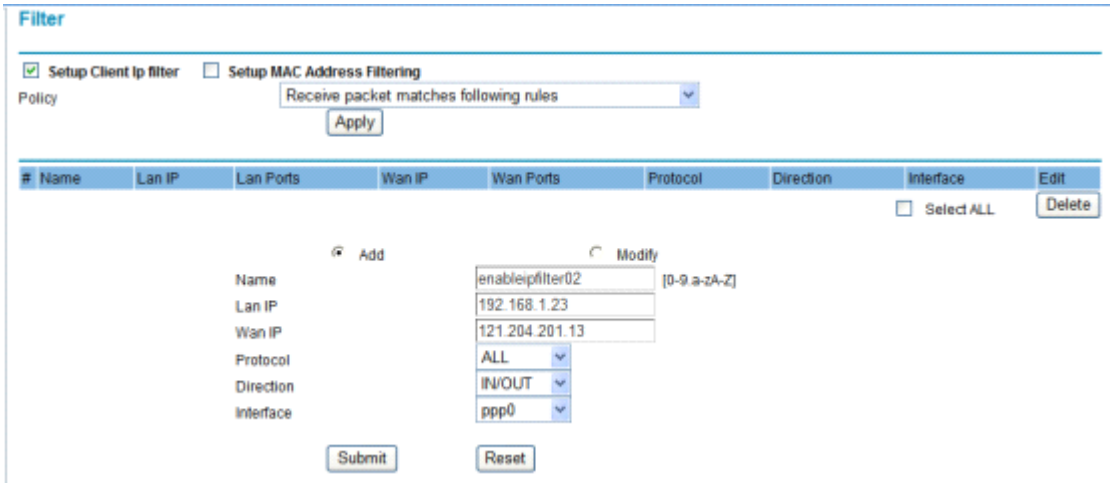
Direction：IN/OUT

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 functional and reduce data flow.



Picture 4-2-5

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 fule "

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 fule"

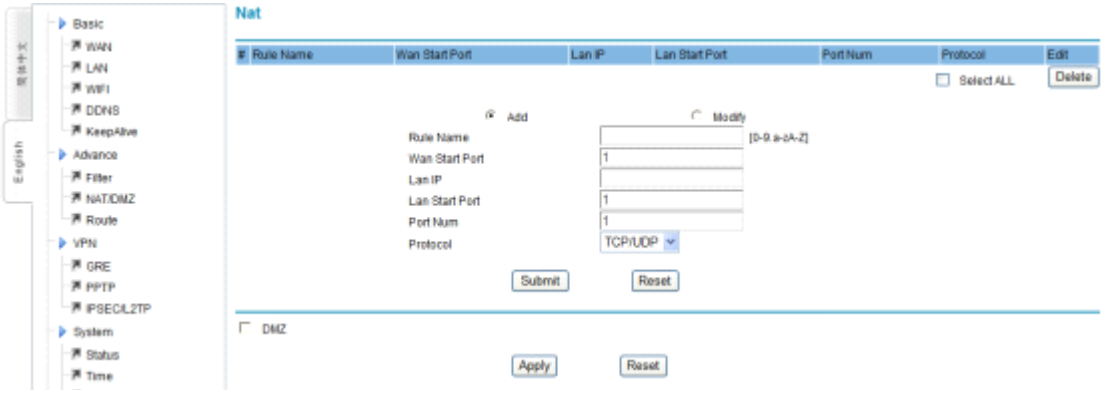
3、Input"00:00:23:34:45:56"in MAC.

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.



Picture 4-2-6

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 continuous ports from start port. For example, start port is5001, 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

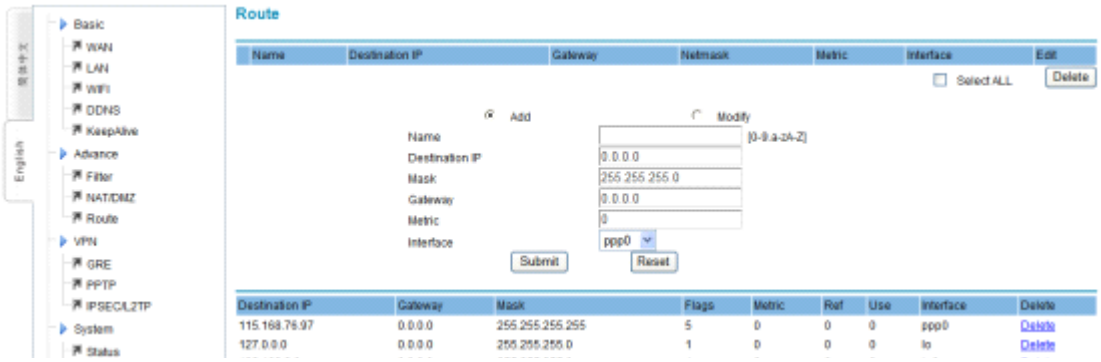
Exposed one LAN computer to Inernet completely, to realize bi-directional communication, and it needs to set this computer to be virtual server (DMZ host computer). When there is WAN user visit this virtual server translated public address, device will transmit data packet to this virtual server directly.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

- **DMZ：** Set form 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

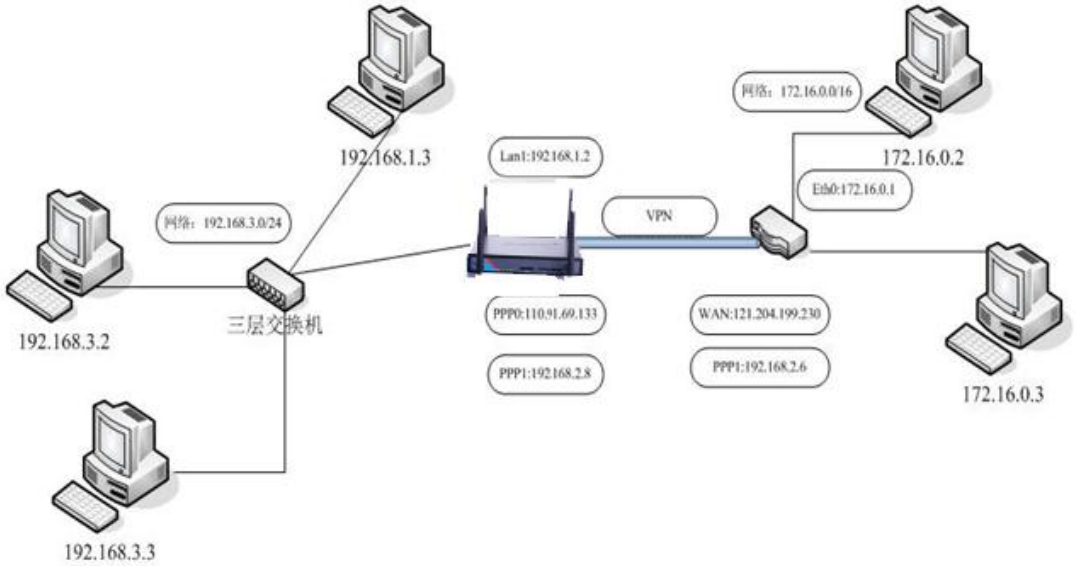
Gateway IP address： Next IP of the added router, if don't need gateway, it can be"0.0.0.0"

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:



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.

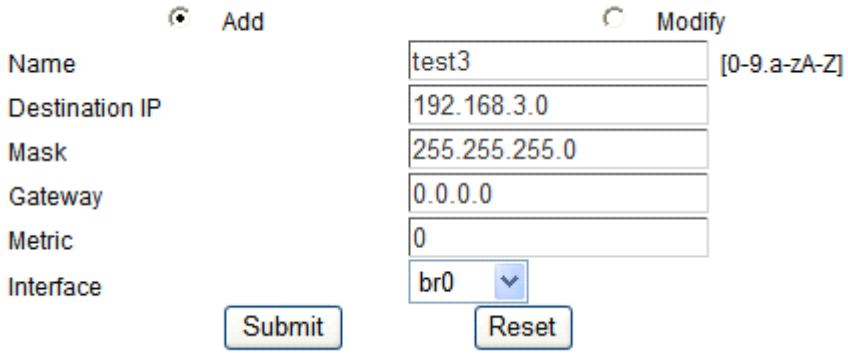
172.16.0.1 is VPN server ETH0 IP.

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.

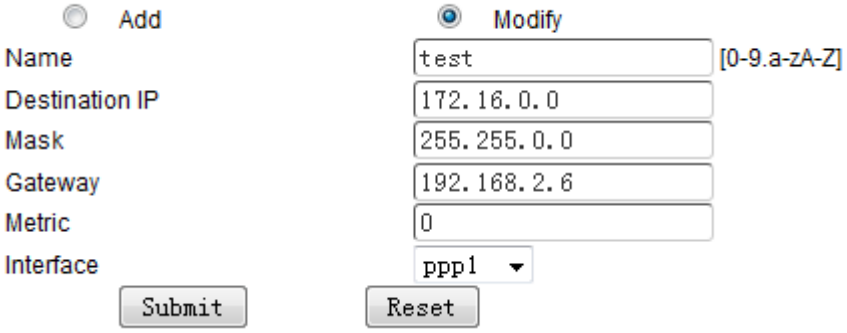
If computer with IP 172.16.0.2 wants to visit computer with IP 192.168.3.2, it needs to add one routing on VPN server to visit 192.168.3.0/24 network. As for this adding step, please read our routing configuration user manual or contact with our technical engineers. When after adding of server gateway, 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”:



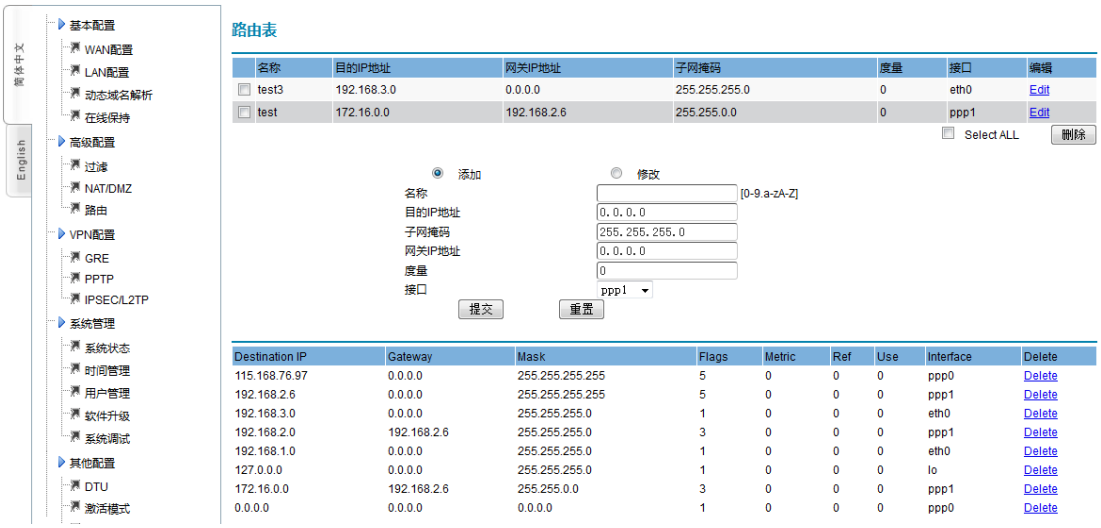
Picture 4-2-9

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.。



Picture 4-2-10

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.。

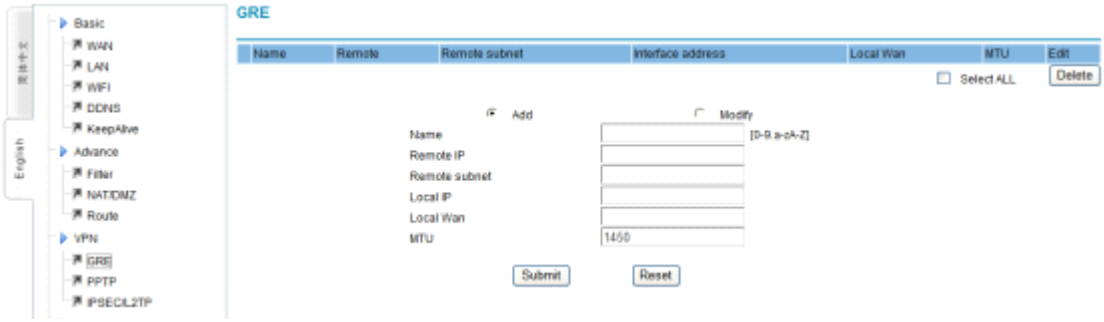


Picture 4-2-11

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.



Picture 4-3-1

（Note: firstly to ensure that the two both ends of the established GRE can obtain the public IP address by dialing.）

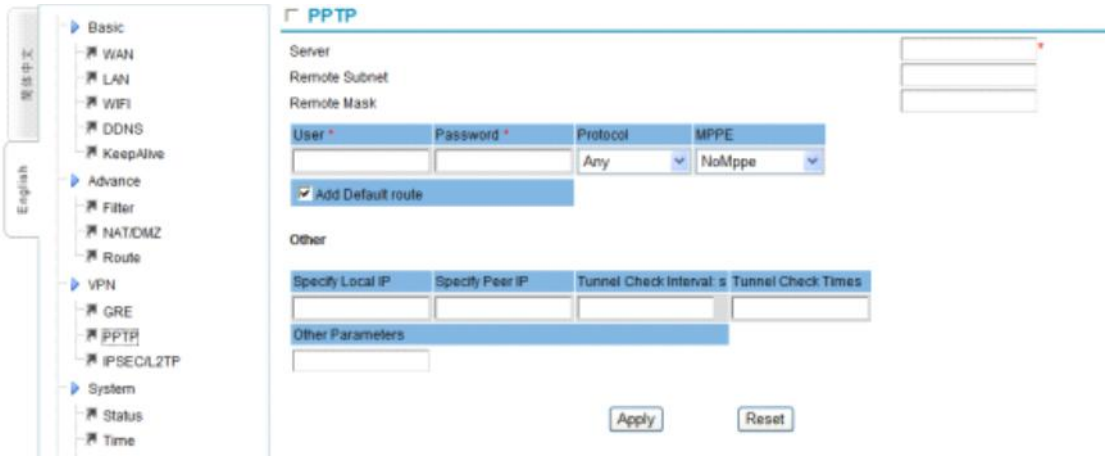
- **Name**：it is limited to use characters 0-9.a-z.A-Z，also can't repeat name.
- **Remote IP** ：Remote public network IP
- **Remote Subnet**：format is 192.168.1.0/24.
- Interface IP address：The appointed virtual interface IP address.
- **Local WAN IP**：IP address used to create tunnel, if it is blank, 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 transmission. 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.



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, which user name and password are plain text transmitted, and the 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

Mppe-StateFul: Supply MPPE stateful Encryption.

Add default route： If start this function, all data visited 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.

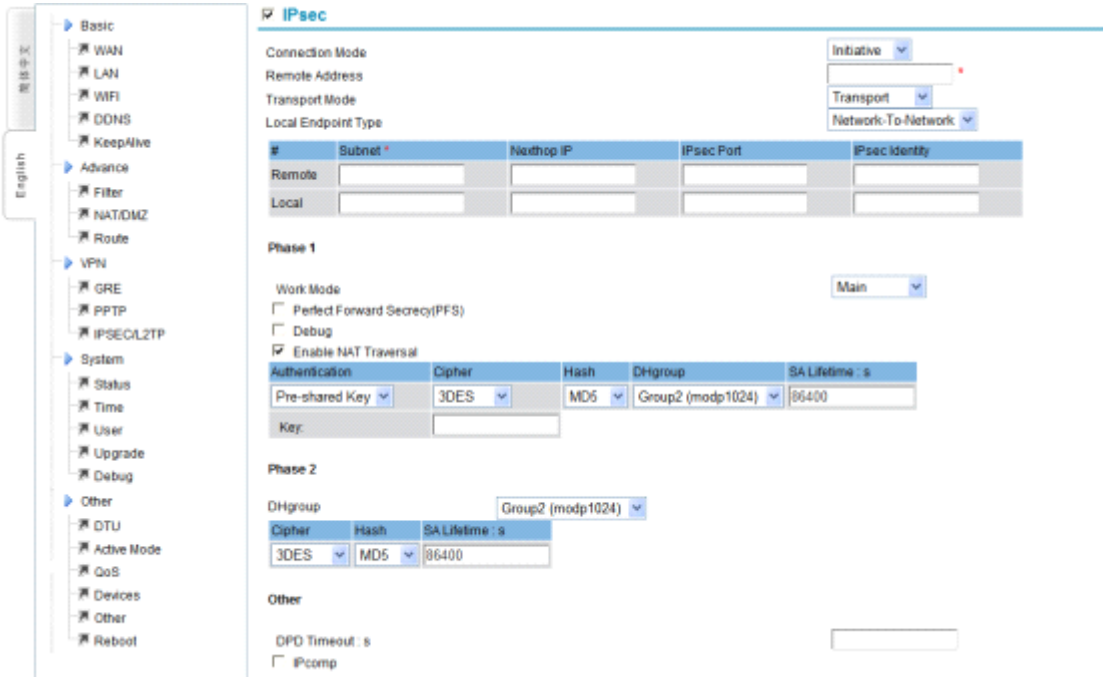
Specify Local IP /Specify Peer IP: If server allows, this device requests from server to specify local IP when establish ppp link, if server assigns, it fails to establish tunnel.

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.

O**ther parameters:** it will be used when special parameters are needed to establish link. It doesn't need to input usually, except for the 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 can't visit public network. Please revise "keeping online" parameters according to actual situation. Otherwise, it will be off-line frequently.

4.3.3 IPSEC



Picture 4-3-4

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)

Transport Mode:

- **Transport Mode:** usually used when wireless gateway connects server.
- **Tunnel Mode**: usually used when establishing tunnel between two gateways
- **Pass-through Mode**: allow IPSEC protocol pass through.

Local endpoint type:

- **Network-To-Network**: used communication between equipment of gateway and equipment of server
- **Road Warrior**: connect to server as mobile clients end.
  - **Subnet**: It is subnet of both sides when working mode is Network-To-Network
  - **Next-hop IP**: When device is in LAN, then this IP is the IP address of gateway that the device points to
  - **IPsec port**: when start L2tp at the same time, L2tp monitor port and L2tp default port is 1701.
  - **IPsec Identity**: the identification supplied to the opposite side when connects negotiation

Phase 1 : establish IPsec SA through consultation in the first stage, and supply IPSec service for data communication.

- **Work Mode**: Main and Aggressive mode.
- **PFS**: Precise forwarding secrecy. Avoid affecting the whole communication system when single key leaks

  Debug: Enable debug information
- **NAT Traversal**: If this gateway doesn't connect with public network directly, but transmit through IP original address, please use "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：** the secret key is the one of certification when the authentication mode is Certificate X509

Phase 2： Phase 2 is protected by phase 1, any message that was not protected by phase 1 SA will be refused. In phase 2, negotiate the communication protocol fast, changing secret key and establish communication.

DH group： Group1 、Group2 、Group5 、Group14 、Group15 、Group16 、Group17 and Group18

Lifetime(S): Phase negotiation valid time.

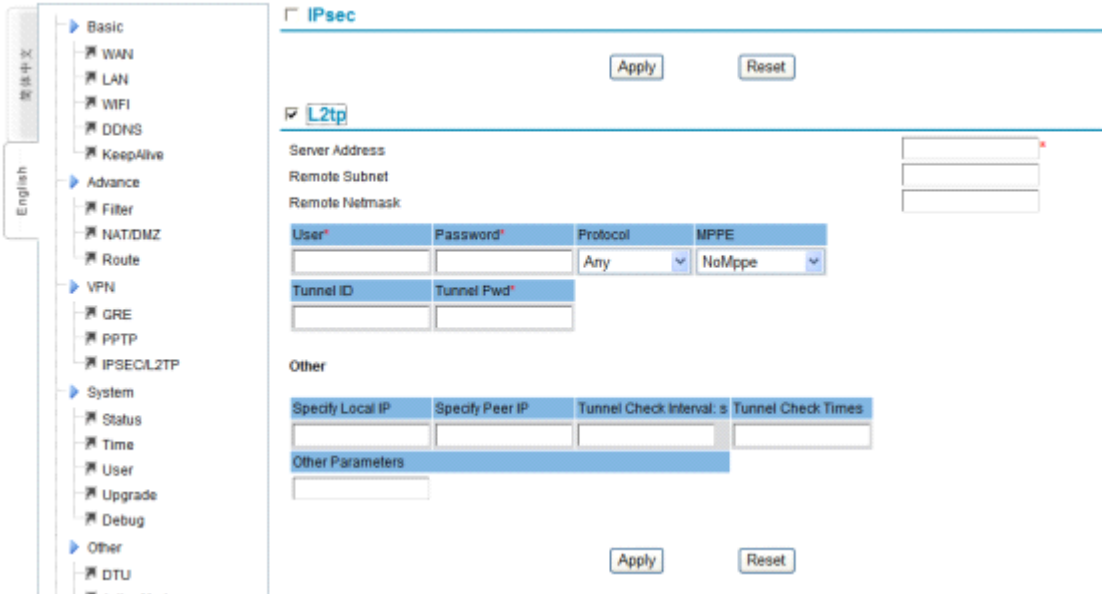
- **Cipher：** DES, 3DES, AES and AES128
- **Hash：** SHA1 and MD5

Other

- **DPD Timeout(s)：** the default time of dps timeout is 120s.
- **IPComp:** IP Payload Compression Protocol

4.3.4 L2TP

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



Picture 4-3-5

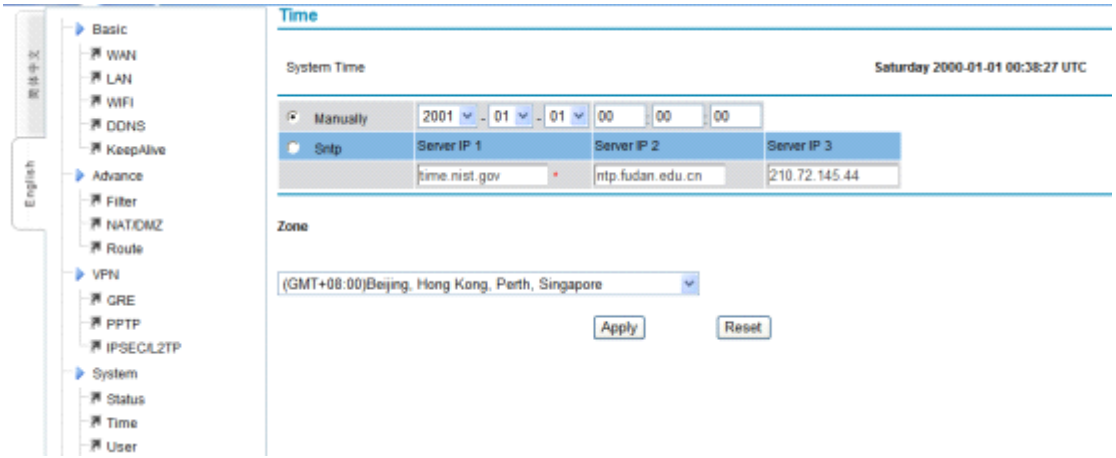
- **Server address**: server IP or domain name.
- **Remote subnet, remote subnet mask**: Subnet information of server side
- **Username/Password**: LAC account and password
- **Tunnel ID/Tunnel password**: LNS account and password.

4.4 System Management

4.4.1 Time management

Manage the real-time clock of this device, supporting hand-setting and network time synchronization.

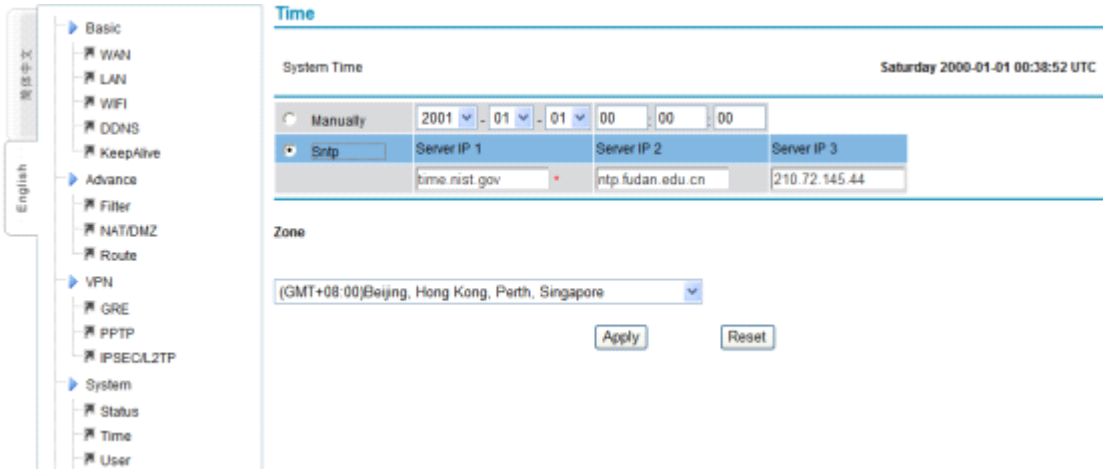
- **Set time by hand**



Picture 4-4-1

Select "Manually", then choose the year, month, day, hour, minute and second to set. Click "Apply" to finish set time system directly.

- **（SNTP）Use network time synchronization（SNTP）**



Picture 4-4-2

Select “SNTP”, the pre-settings are 3 international common time servers.

Notice: The device needs to be able to access the Internet if it synchronizes with network time, so it cannot be applied in the 4G private network. And if once starts, it will update every other hour.

4.4.2 User Management

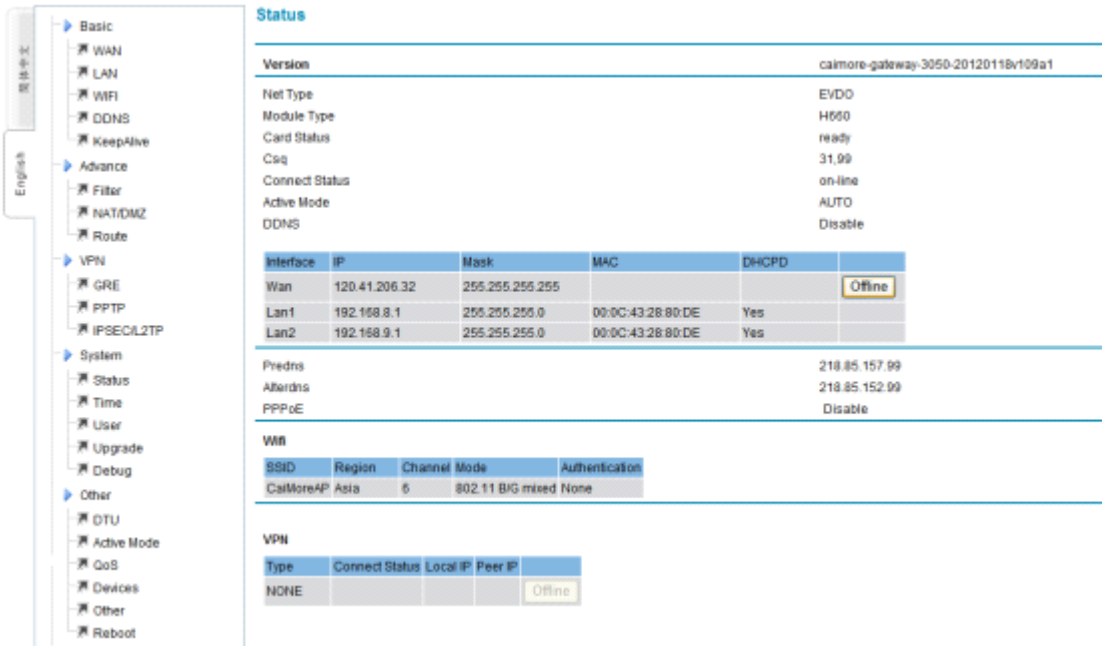
Manage the user password of login web, telnet and the serial port logging. Once forgot, please restore to default setting (refer to appendix 4).

Picture 4-4-3

User can revise the password from here. When revise the password, please input “login Username “at first, then input “old password”, after that, input “new password”, and next, input “confirm password”, clicking “submit” to save new password in the last.

4.4.3 System Status

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



Picture 4-4-4

4.4.4 Software Upgrade

Configure, manage and update the system, and after that the system will be reset to defaults.

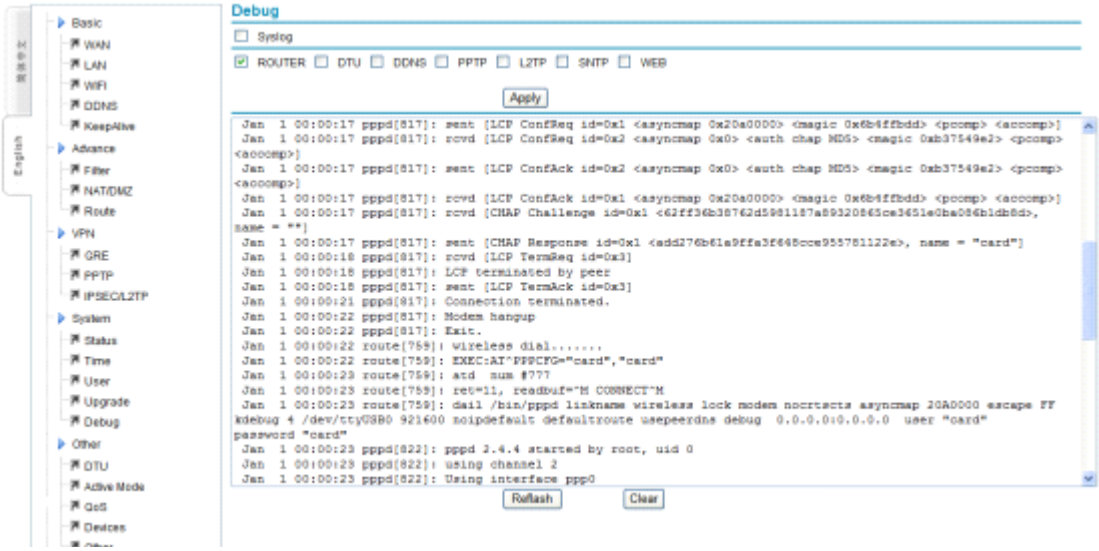
Picture 4-4-5

- **Save to local**: Backup the configuration file to the local PC
- **Restore**: Restore current configuration to default status
- **Configuration file**: Import the configuration to the device
- **Update file:** Update the device according to the firmware supplied from the manufacturer

Notice: Please don't power off when update firmware, till "Update successfully", and click "Confirm" when system updates successfully, and then, restart the system.

4.4.5 System Debug

It enables or disables the debug information of the main functions. In order to check debug information clearly and solve problem quickly, system have 7 optional debug modules:



Picture 4-4-6

- ROUTER: Output the basic information of system, including dial-up information
- DTU：Output DTU debugging of gateway
- DDNS：Output DDNS debugging of gateway.
- PPTP：Output PPTP debugging of gateway.
- L2TP：Output L2TP debugging of gateway.
- SNTP：Output Internet Time debugging of gateway.
- WEB：Output WEB debugging of gateway.

Select the corresponding function debugging and submit it, system will be restarted. After that, clicking “reflesh” to update current debug information of system.

4.5 Internet Access Management

4.5.1 Captive Portal

Local push function is mainly used for pushing advertisement page link when using gateways access to the Internet, the users can define the advertising pages link, advertising push polling time and the time-frequency. Turn on this feature, when users are in a networked process, the system will push "the first ad pages", then according to the ads URL list and frequency,when there are users clicking in an Internet,ad pages will be pushed, when to reach the polling time ad , it will push the "ended advertising pages", the system starts to count polling time again, and do the cycles to push ads.

Picture 4-5-1

Ads push Port: Port number listened by push program.

Ads polling time: The interval between the first pushed ad to the final pushed ads (min).

The first ad pages:used for first received the ad page after access the Internet, it is pushed just once under push polling time.

The Ended ad pages: used for pushed ad page when polling time ends

Advertising Name: user-defined ad name.

URL: User-defined ad link.

Push Frequency: The repeat interval (min) for ad pushed to the client terminal.

4.5.2 WIFIDOG Configure

Wifidog function is used for web authentication, when users connects to a wireless hotspot, requesting to send the data, it will first open the authentication page under the path of configured authentication server address to allows users to authenticate,after the authentication succeed ,the users can access to Internet.

Picture 4-5-2

Gateway ID: Gateway mark which wifidog upload messages to the server

WEB server name: The user-defined server name.
External port: total data interface of device.
Internal port: The user data interface.
Wifidog port: The wifidog port number.
The maximum number of concurrent users: the largest number of users simultaneously request.
Detecting interval: detecting user traffic information and device status interval (s).
User Timeout detection times: determining user timeout detection times.
Authentication Server Address: The authentication server address .
Enable SSL: Docking whether the server uses SSL decryption.
Authentication Server Port: The port number used by the server.
Authentication server path: the server authentication path ,the two path sides to be add with '/'.
Domain whitelist: wifidog unshielded domain address, rule format is FirewallRule allow tcp to XXX, generally used for server using some tool such as QQ, wechat and other third-party to authenticate,it requires that the corresponding domain add into white list.
Internet management rules and server synchronization: if the server's "Internet management" configuration synchronize to a local.
Whether upload browsing history: Choose whether to upload the user's URL browsing record.
Timing report: report browsing history Interval,unit is sec.
Given byte report: it will be reported when it reaches set accumulated bytes' browsing record.Unit is bytes.
Note: For the timing report and given bytes report, if one of them complied with the then records has to be reported

4.5.3 Application Filtering

Set up certain users' application filtering,such as video,music,download and URL ect.

Picture 4-5-3

Rule name: Mark restricted rules' namei

IP range: Limit IP segment

Protocol Type: Select the type of protocol to be filtered. (video, music, download, etc.)

Direction of the packet: Select the data source to be filtered, IN, OUT, IN / OUT

Strategy: The strategy for data processing of matched rule, accept or prohibit

4.5.4 Followed Ads

Enable: Enable the followed ads function.

Rules configure: Configure replaced page content is that page inserted with advertising content, the rules of the first row FILTER: block-weeds, Second row:regular expression rules, such as s | page content | replaced contents $ 0 | g.

After enabling it and the device connected, the ads can be viewed on the top of page when browsing the page.

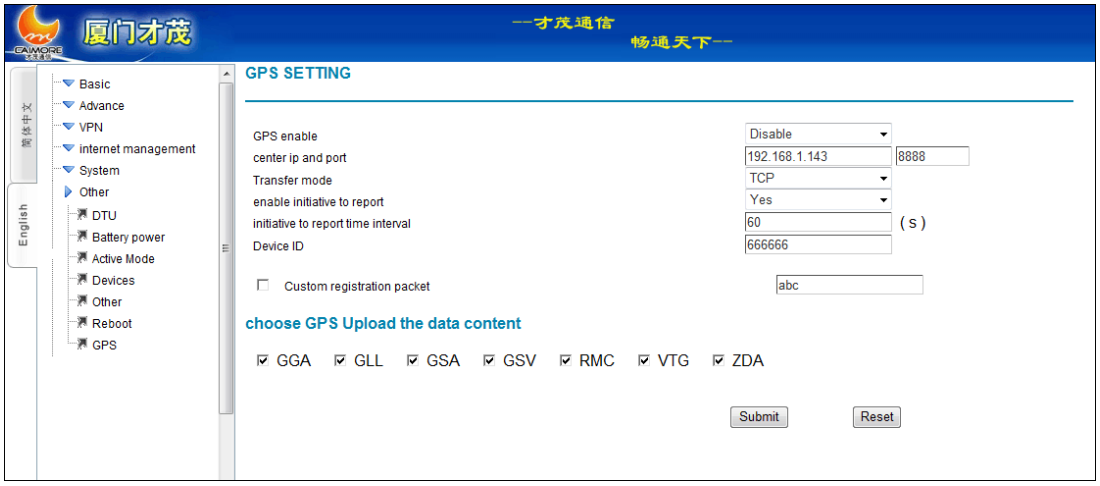
4.5.5 Battery Power Feature configure

This function is used to set the time of using battery supply when ACC power is cut off.Using battery power supply is to achieve that when the ACC power is cut off,it can continue to use battery power to make sure that the device can operate.

Battery backup time: The power supply duration after ACC is cut off.
Note: The battery supply voltage must be less than ACC power supply voltage.

4.5.6 GPS Function

GPS function is to configure GPS data center address and port, enabling snmp function, GPS data will be sent to the snmp server. When initiative report is unable,center address terminals can send AT command to the device which captures the specified GPS data,when initiative report is enabled, the device can GPS data content to center address during the set reported interval.



Picture 4-5-6

Enable GPS:
Enable: Enable GPS function.
Disable: Disable GPS function.
Center address and port : set center address and port.
Agreement:
TCP: TCP protocol which interact with data center
UDP: UDP protocol which interact with data center.
Whether the initiative to report:
Yes: Initiative to report GPS data to a central address.

No: Not initiative to report the GPS data to a central address.
Device ID: The user-defined gateway's mark.
Custom registration package: the user-defined registration package .
The uploaded GPS data options: Open the initiative to report, choose GPS data content uploaded to the central address.
GGA, GLL, GSA, GSV, RMC, VTG, ZDA the data contents, see Appendix 7.

Note: Not the initiative to report then,to receive AT command description.
Get Coordinates: AT + LOCATE: Re: Lon = 118.176565; Lat = 24.493771; (Lon = Longitude (ddmm.mmmm); Lat = Latitude (ddmm.mmmm)).
Get Time: AT + TIME: Re: Time = 125959; (12 H 59 M 59 S; Note: GPS reception time is world time, users need to convert it into local time according to their own time zone, such as China in the East eight zone, world time +8 hours).
Get Data Status: AT + STATUS: Re: Status = A; (A positioning data valid, V position data is invalid).
Get relative speed: AT + SPEED: Re: Speed = 1.13; (rate is 1.13 nm / hr).
Get altitude : AT + ALTITUDE: Re: Altitude = 58.2; (Altitude is 58.2m).

4.6 Other configurations

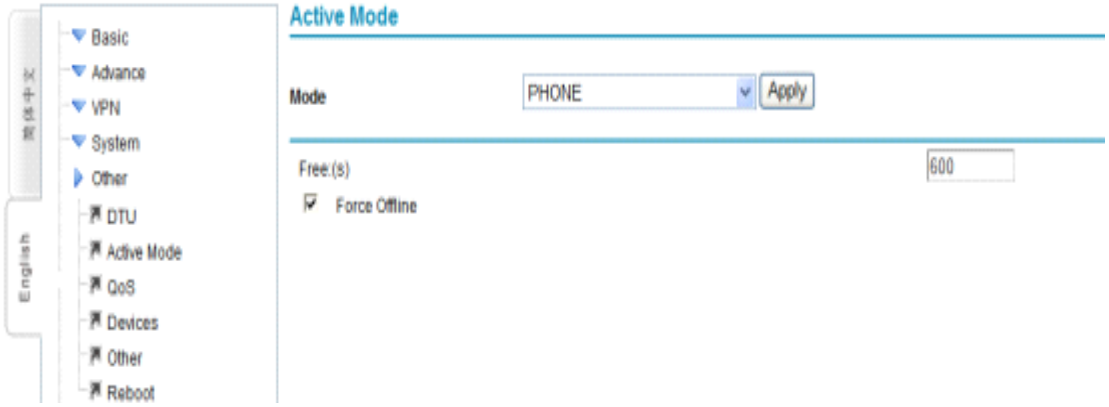
4.6.1 Activation Mode

Automatic modem

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

Phone mode

Wake up by phone (the mobile number is SIM card number that is inserted on gateway). Under this mode, gateway didn't dial-up after power on, when there is calling, gateway dial-up after checking the ringing



Picture 4-5-1

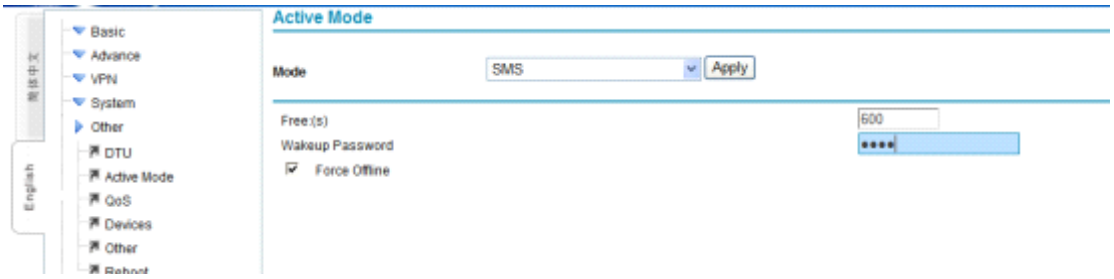
- **Idle Time:** When "force offline" wasn't chosen, Idle Time is a period of time value after wireless gateway transmits and receives data packet. If arrives this time value, gateway will be offline automatically, releasing wireless communication link, and eliminate communicate flow.

  For example, idle time is 600s, and in the meanwhile, selecting "force offline", then after wireless gateway is online, it transmits or receives data continuously. And 600s later, after finishing the data receiving or transmitting, wireless gateway will be offline automatically and close the communication link.
- **Force offline:** When system is online and till it reaches the specified value of idle time, it will be offline immediately. That is also fixed communication time. The specified time is up, the system will be offline immediately.

Note: If select "Idle Time" only, without "force offline", please confirm whether "keeping online" rule has no data transmitting and receiving within "Idle Time"

SMS Mode

Gateway executes command after receiving SMS (it will receive SMS only when gateway hasn't dial-up to be online).



Picture 4-5-2

- **Idle Time:** When "force offline" wasn't chosen, Idle Time is a period of time value after wireless gateway transmits and receives data packet. If arrives this time value, gateway will be offline automatically, releasing wireless communication link, and eliminate communicate flow.

For example, idle time is 600s, and in the meanwhile, selecting "force offline", then after wireless gateway is online, it transmits or receives data continuously. And 600s later, after finishing the data receiving or transmitting, wireless gateway will be offline automatically and close the communication link.

- **Force offline**: When system is online and till it reaches the specified value of idle time, it will be offline immediately. That is also fixed communication time. The specified time is up, the system will be offline immediately.
- Wakeup password: user for the password of validating 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 dial-up at the same time, log in and start to transmit the data

Command: CONNECT

Parameter: none

Format: SMSPASSWD: xxxxxx (Password): CONNECT

DNS

Function: set the main DNS and backup DNS of wireless gateway

Command: CONNECT

Parameter: none

Format: SMSPASSWD: xxxxxx (password): DNS:201.101.103.55:201101.107.55

Instruction: set the main DNS as 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：The device revised to be auto activation (default)；wireless gateway dial-up automatically after 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. Activate 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 met, gateway is activated and can be online

Command：MIX

Parameter：none

Format：SMSPASSWD: xxxxxx (password):ACTMODE:MIX

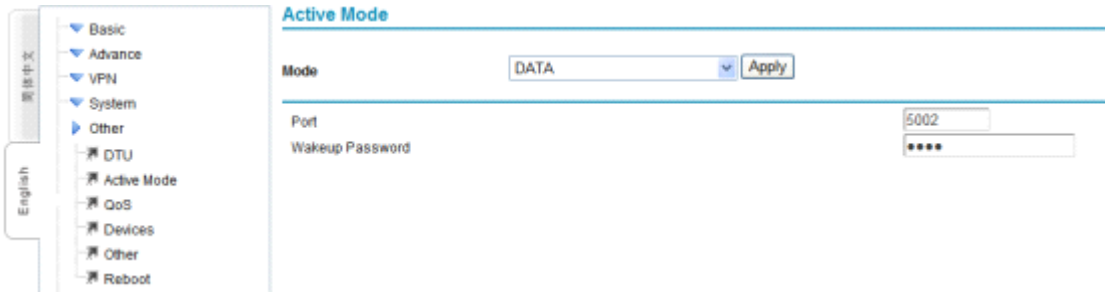
Note:

1. “:” in command is English character.
2. If select “Idle Time” only, without “force offline”, please confirm whether “keeping

online" rule has no data transmitting and receiving within "Idle Time"

Data Mode

Device monitors local TCP pre-set port, to be the status of waiting for connection. When LAN host computer establishes TCP connection, LAN host computer sends command to control gateway to connect with network.



Picture 4-5-3

After connected, LAN host computer sends following commands to control device to connect with network. Command format is following:

SMSPASSWD: password: CONNECT the device starts to connect with network
SMSPASSWD: password: CLOSE turn off the Internet connection
SMSPASSWD: password: REBOOT restarts the gateway

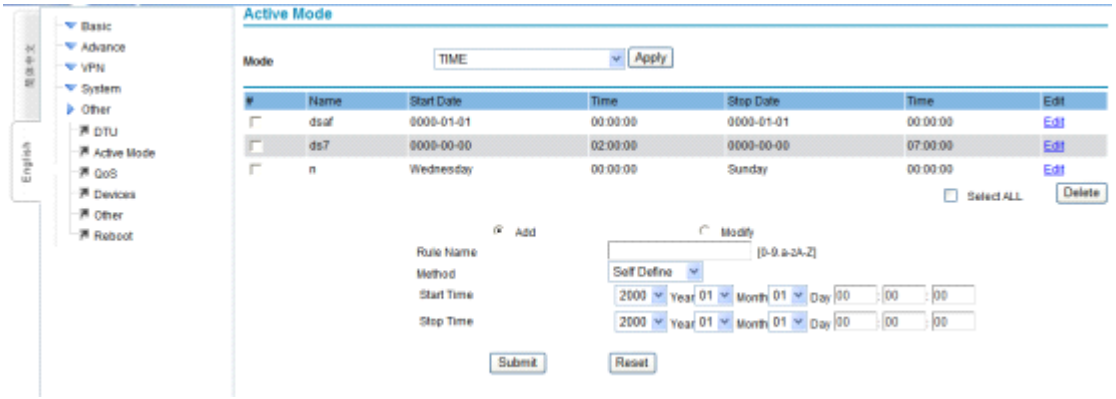
Note:

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

2. If select "Idle Time" only, without "force offline", please confirm whether "keeping online" rule has no data transmitting and receiving within "Idle 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.



Picture 4-5-4

Support way:

self define：Set gateway online and offline time scope according to customers' 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 whether system time is correct or not

MIX Mode

It is with the functions of SMS, PHONE and DATA wakeup. Once one is valid, it can wake up the gateway

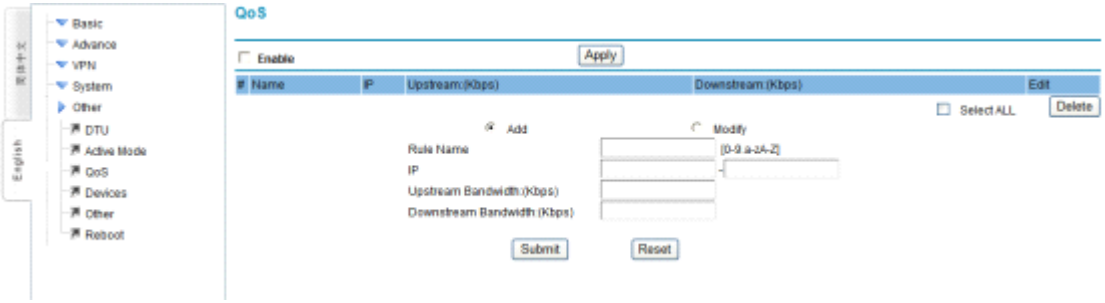
Picture 4-5-5

Note:

1. Command is without case-sensitive (including wakeup password), so once device receives LAN host computer data, it disconnects TCP connection with LAN host computer immediately, enters into monitor status again.
2. If select "Idle Time" only, without "force offline", please confirm whether "keeping online" rule has no data transmitting and receiving within "Idle Time"

4.6.2 Bandwidth Management

Limit bandwidth of device according to IP address

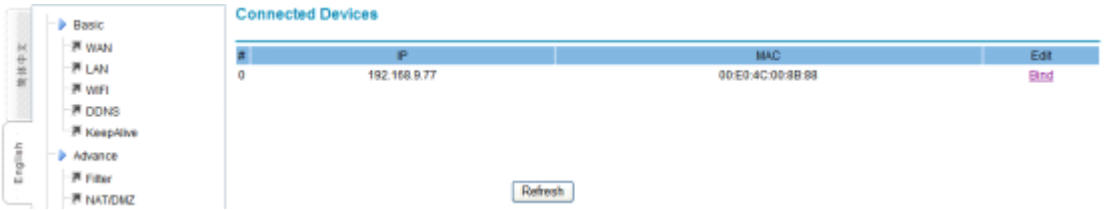


Picture 4-5-6

- **Name**：it is limited to use characters 0-9.a-z.A-Z, and tautonymy is not allowed, as the identification of distinguishing the multi-rules.
- **IP**：Limit IP address scope.
- **Upstream**： Max upstream bandwidth.
- **Downstream**：Max downstream bandwidth.

4.6.3 connecting device（MAC address binding）

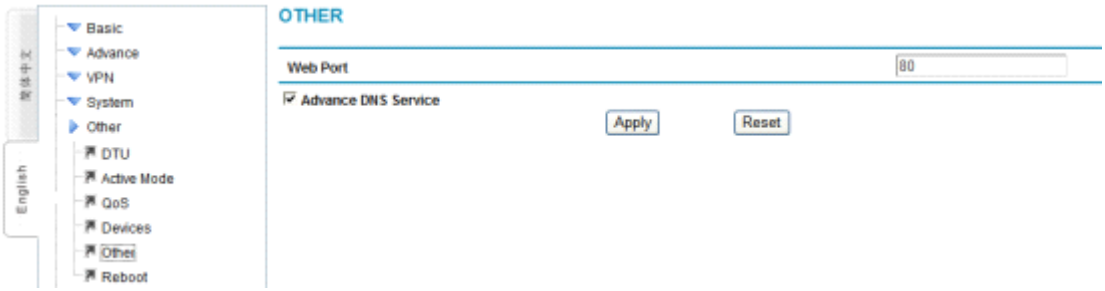
Realize MAC address binding to the connected devices to avoid ARP cheating and attack.



Picture 4-5-7

4.6.4 Other configurations

Set WEB visiting port and DNS re-direction



Picture 4-5-8

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

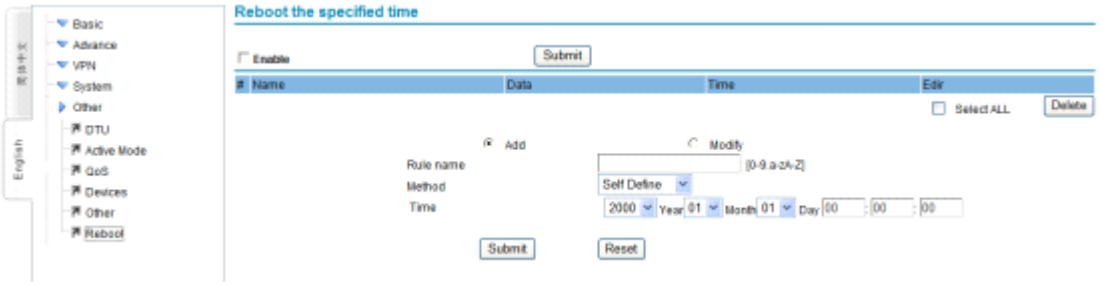
Advance DNS service: If start and make LAN host computer DNS address points gateway, then all LAN host computer domain name requests of gateway are sent to DNS server appointed by the device by force (please check system status “first DNS/standby

DNS”).

Note: At the same time, DHCP service will supply the LAN network card address that gateway is DNS to LAN dhcp clients

4.6.5 Timing Restart

Specify device to restart in a certain period



Picture 4-5-9

Support way:

self define： Set gateway online time according to customers’ 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

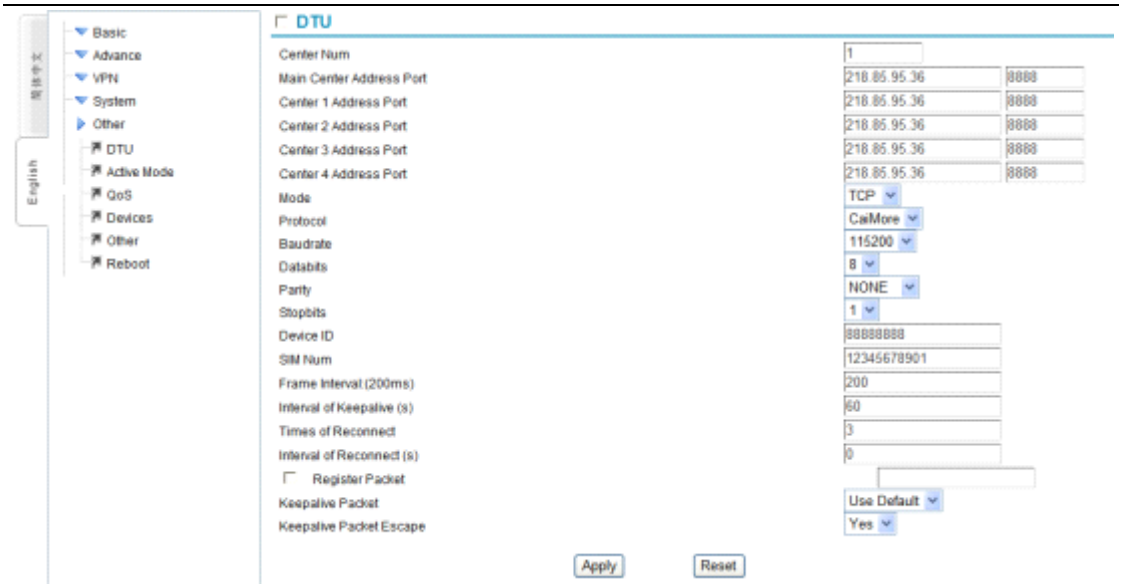
every week： Set gateway online time of the certain period every week

every day： Set gateway online time of the certain period every day

every hour： Set gateway online time of the certain period every hour

4.6.6 DTU configuration

The series port of wireless gateway (COM/LINE port), is used to configure gateway parameters or restore to default leaving-factory setting, on the other hand, it is used to configure to data channel to realize DTU data communication. 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.



Picture 4-5-10

- **Center Number**: 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 number", at this time, it only needs to configure "Main center IP and port", inputting center server IP and port into corresponding bars, read picture 4-5-10. If center server doesn't use fixed IP address, but 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 "center number", 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 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**: set the 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.
- **Baud rate**: Setup working Baud rate of serial port, scope is 110~230400BPS. Please set that baud rate is the same as that of user side equipment. Otherwise,

series port can't communicate.

- **Data bits**: Set working data bits of serial port, and the value can be 7 and 8. Please set that data bits are the same as that of user side equipment. Otherwise, series port can't communicate.
- **Parity**: Set the parity of serial port, and the values can be NONE, ODD or EVEN. Please set that parity is the same as that of user side equipment. Otherwise, series port can't communicate.
- **Stop bits**: Set stop bits of serial port, and the values can be 1 or 2. Please set that stop bits are the same as that of user side equipment. Otherwise, series port can't communicate.
- **Device ID**: number DTU, supplying one way of differentiating DTU for center server. 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 Number**: set mobile number which uses SIM card, and it is fixed to be 11 numbers. This parameter cannot 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 configured "frame interval" time, DTU equipment hasn't received any serial port data, DTU will packet the received data and send to center server.

"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 or it will be packed into one. If customer can't calculate the suitable value, please contact our technical support engineer.

- **Times of reconnection**: Times of DTU to connect with center server, and the default is 3. If trial times are more than configured "times of reconnection", gateway will automatically power down and after a moment power on again, and dail-up, reconnecting center server till connect server successfully.
- **Interval of reconnection**: Interval time of wireless gateway to reconnect with

center server, the unit is second. When the connection with center server fails, if reconnect time is less than configured times, it will reconnect center server within the appointed time.

- **Interval of keeping alive：** Interval time of keeping alive data sent periodically to maintain link. Unit is second. Default is 60s. Interval of keeping alive 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-registered packet：** When DTU establish connection with center server, DTU will send registration information to center; if registration packet needs specific definition, please install the specific definition here
- **Keep alive packet define：** After DTU connect with wireless network, if there is no data transmission 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

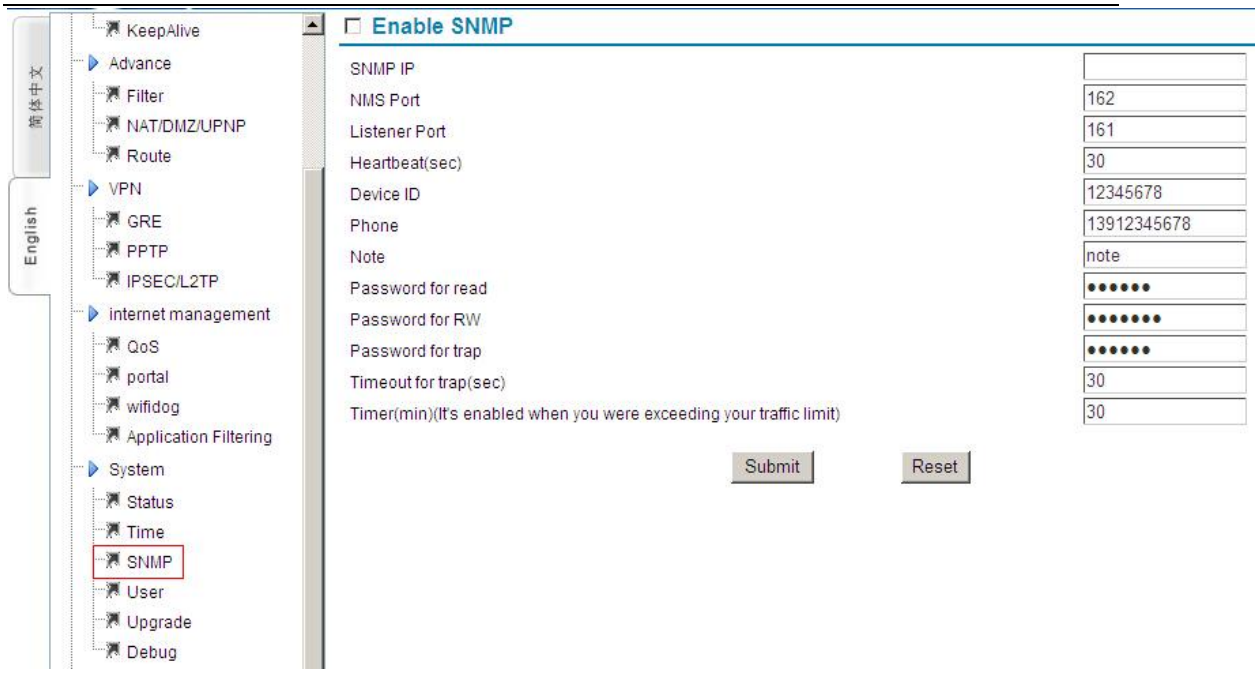
  Option：None Function introduction: don't send packet

  Option：Use Default Function introduction: use default 0xFE

  Option：Self Define Function introduction: Customer define their own packet according to actual situation

4.6.7 SNMP Configuration

SNMP is Simple Network Management Protocol. If enable this function, the device can connect with SNMP server, and users can manage and configure the multi devices with SNMP client, including parameter configuration of one or more device, upgrading remotely and querying GPS location information(if GPS is supported), flow information, real-time signal information, etc.



- **Address of NMS(network management system):** the address of NMS
- **NMS port:** the port of NMS server (the default can be used)
- **Monitor port:** the monitor port of SNMP of NMS (the default can be used)
- **Time of Heartbeat Packet(Second):** the interval time of heartbeat packet sent to the NMS server
- **Device ID:** the ID of device
- **Number:** the number of device (usually default)
- **Remarks:** remark information
- **Reading permission passwords:** to set the permission passwords for reading, the default is public
- **Writing permission passwords:** to set the permission passwords for writing, the default is private
- **TRAP packet permission**
- **Time of TRAP packet timeout (second):**
- **Timing online(second) (use when the flow exceeds)**

Chapter 5 FAQ

1、 Frequent on/offline

- Please enter system status to check network signal situation, to confirm

whether network signal is too weak.

- Please check corresponding parameters of keeping-online, whether rules are met.
- If keeping-online destination IP uses domain name, please log in gateway command terminal (appendix 1) to confirm whether decode domain name and visit destination address normally.

2、 Forget passwords

- Please restore to default setting, reference appendix 4.

3、 LAN indicator is off

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

4、 Can’t dial-up to be online

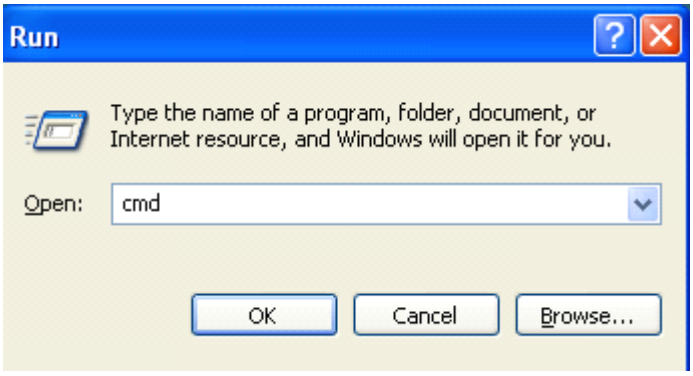
- Please check WAN configuration information whether it is the same as information ISP supplied.
- Check signal by system status, if signal is weak, please check whether the antenna connects correctly.
- Please check whether this place is covered by network.
- Please check signal and card situation from 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 it points Gateway.
- Whether DNS is the same as gateway, if not, please revise (reference Appendix 6)
- If DNS information is input, please check whether they are correct.
- If DNS is correct, please clear (use obtain DNS automatically), after dial-up successfully, please input according to system status supplied DNS.

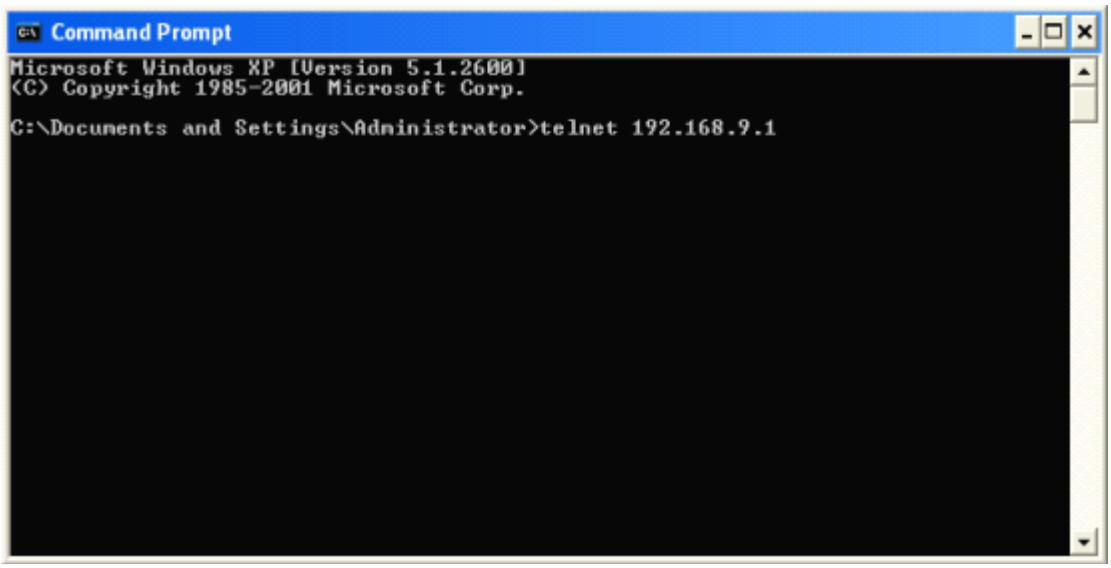
Appendix 1 Login gateway by Telnet

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



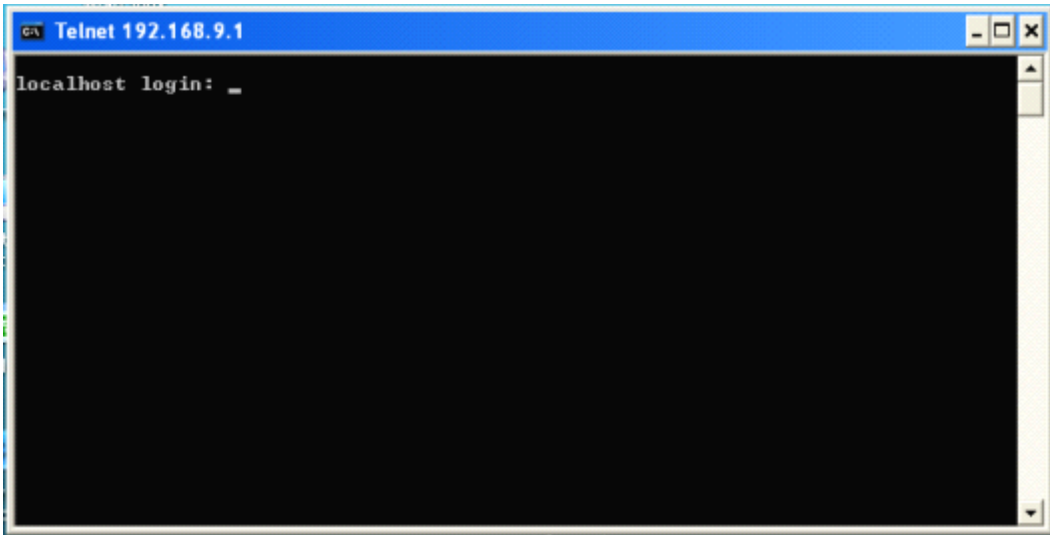
Picture a1-1

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



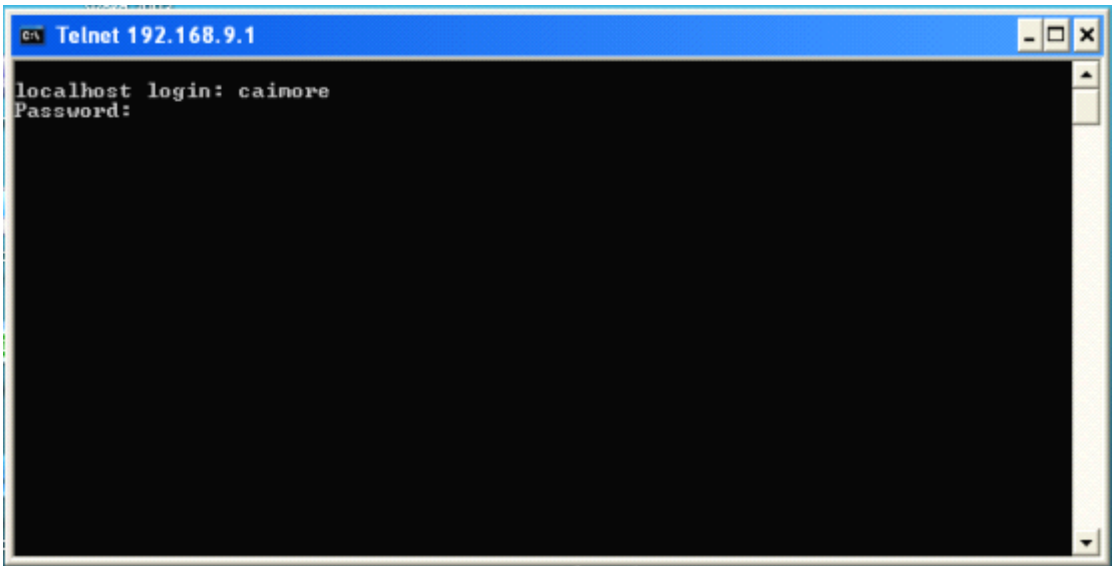
Picture a1-2

3、Login



Picture a1-3

4、Input username and password

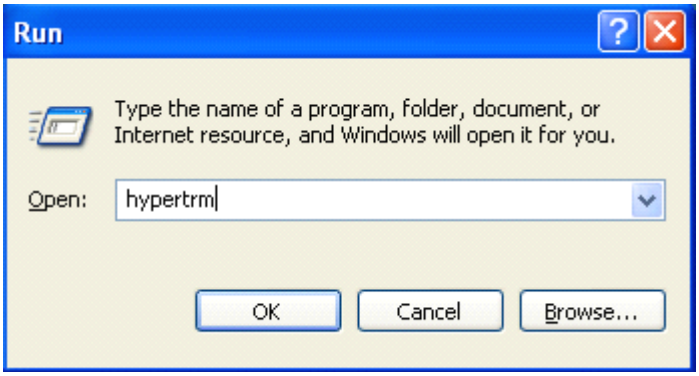


Picture a1-4

5、It means login successfully when appear “#”,enter shell command.

Appendix 2 Login gateway by hypertrm

1、Click “start”->“run” ,input: hypertrm <enter>



Picture a2-1

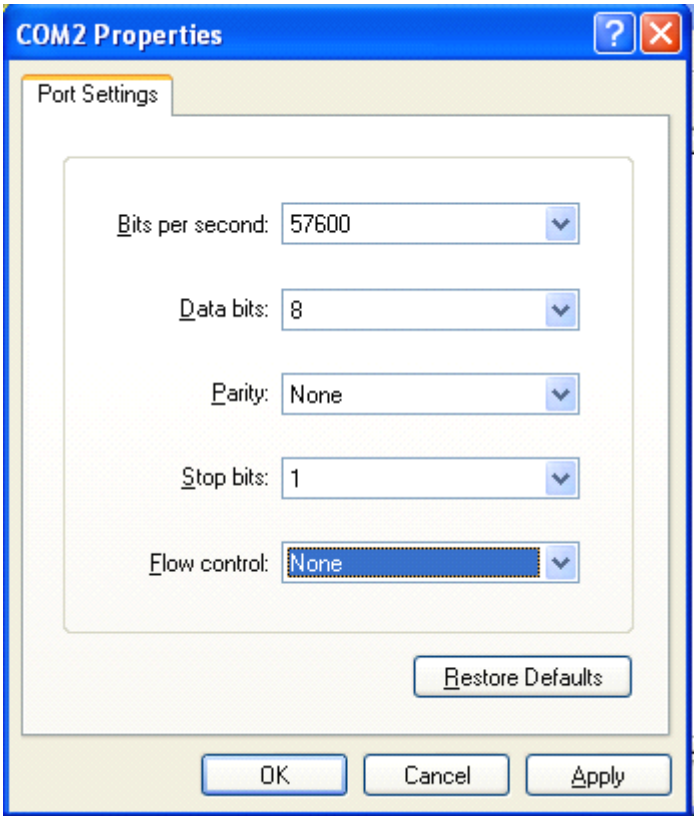
2、Input name:1

Picture a2-2

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

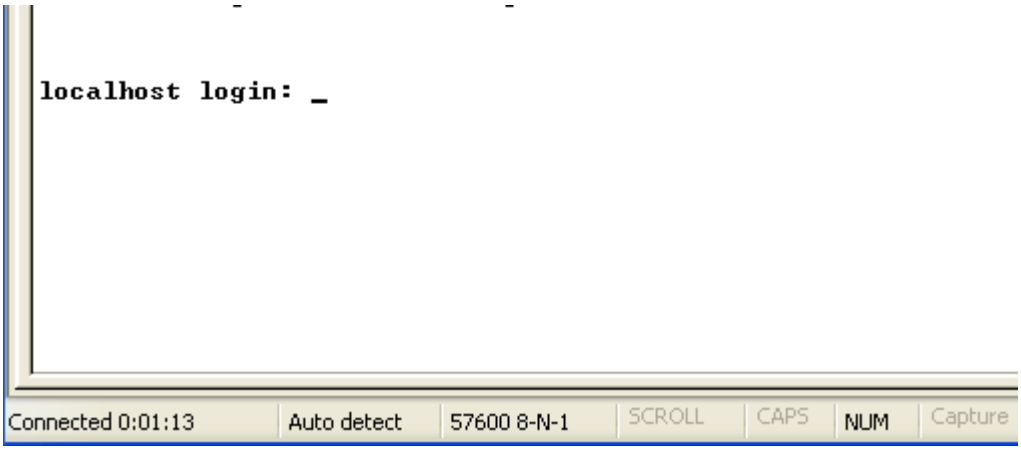
Picture a2-3

4、Set serial port parameter:57600,8N1 and None flow control



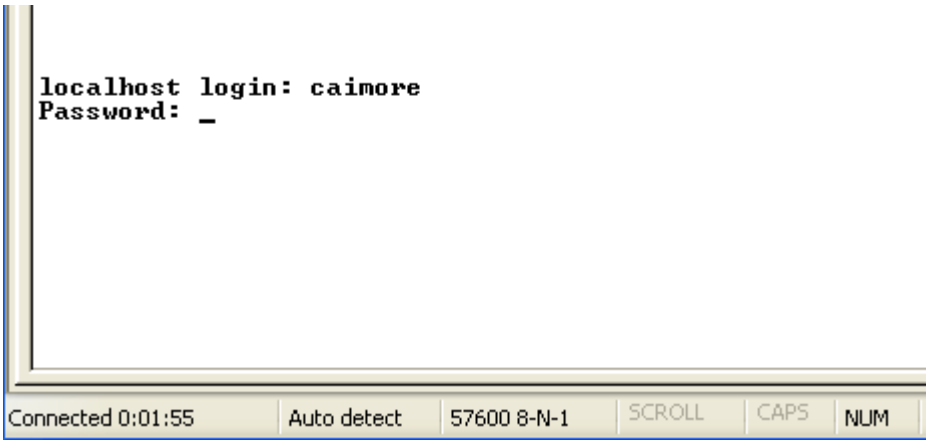
Picture a2-4

5、After confirmation, input <enter>,below will display



Picture a2-5

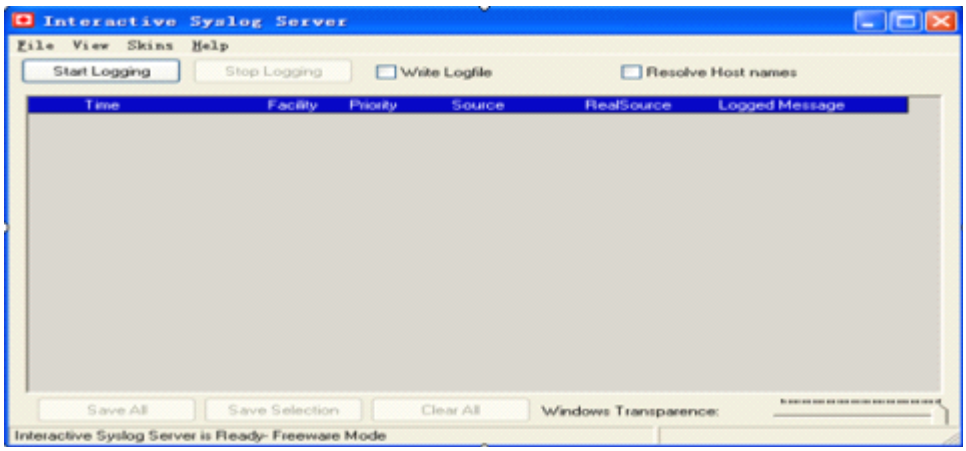
6、Input username and password, enter shell.



Picture a2-6

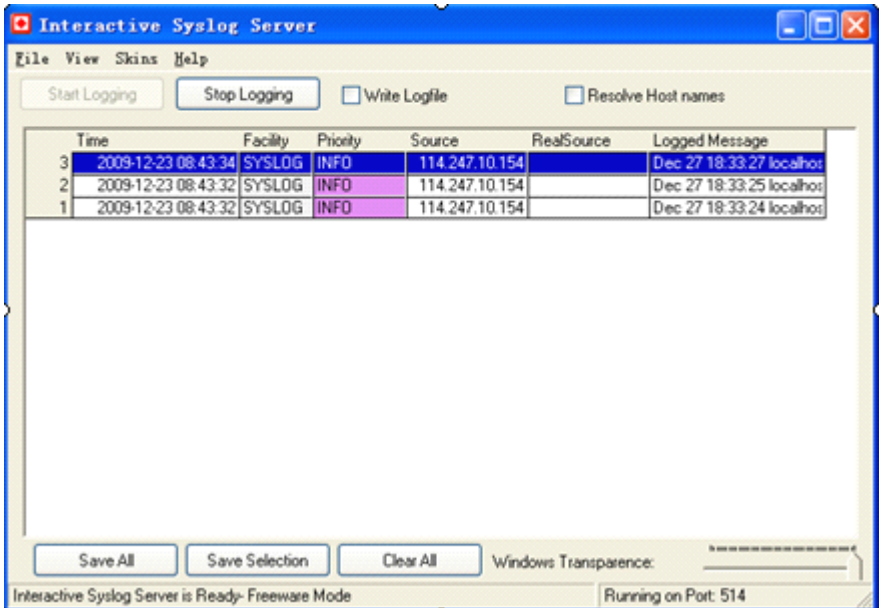
Appendix 3 Obtain debug information from syslogd server

Run winSyslog, clicking "start logging".



Picture a3-1

2、If your server access public network by ADSL ROUTER, please make Port mapping on your ADSL ROUTER, to Port mappingt external UDP 514 port to your server 514 port.



Picture a3-2

Appendix 4 Restore default setting

1、Power on gateway

2、Press RESET for 30 seconds.

Picture a4-1

3、Restart gateway

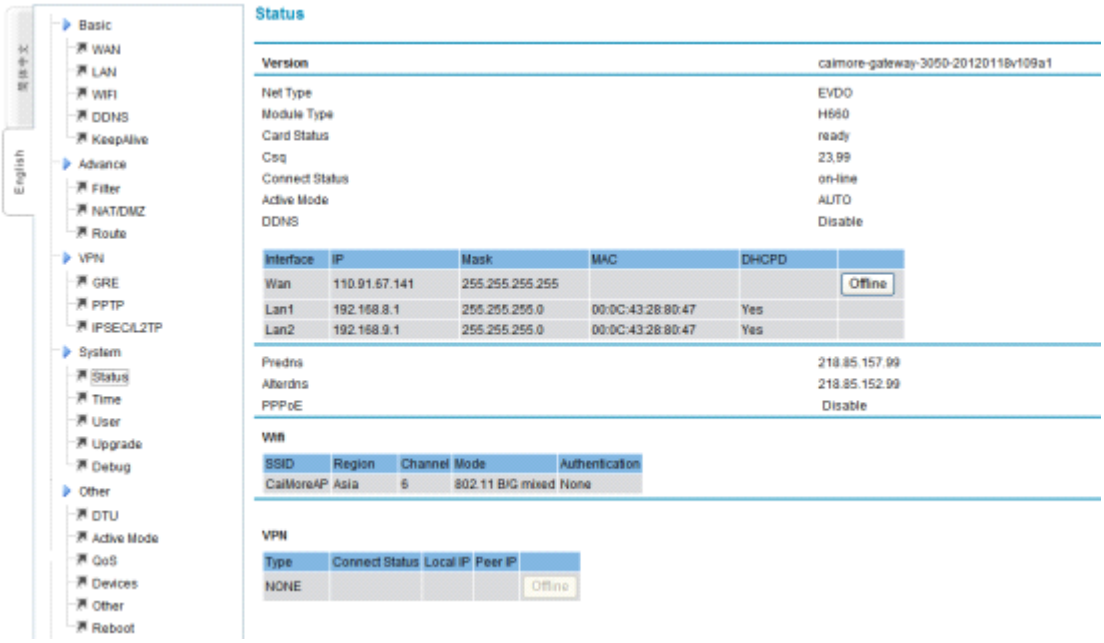
Appendix 5 Wireless network basic information

Network	Center Num.（APN）	Access point	User name	password
GPRS	*99***1#	Cmnet (mobile) Uninet (netcom)	blank	blank
EDGE	*99***1#	cmnet	blank	blank
TD-SCDMA	*98*1#	cmnet	blank	blank
CDMA	#777	blank	card	card
EV-DO	#777	blank	card	card
WCDMA	*99#	4Gnet	blank	blank

Note: above 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:



Picture a6-1

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

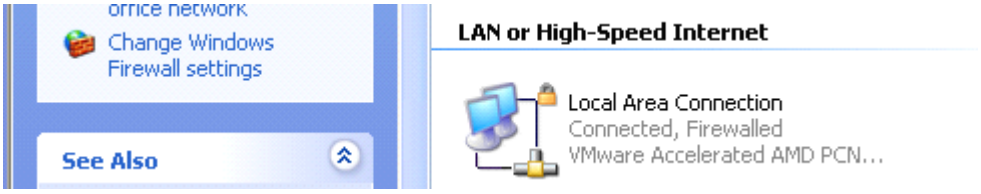
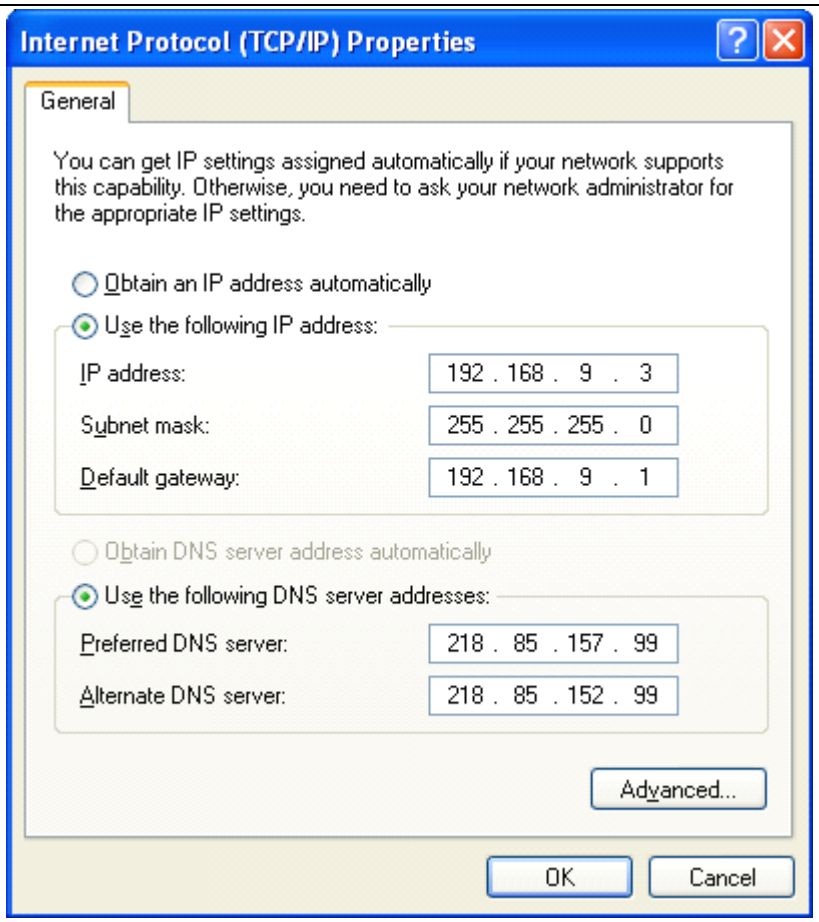


图 a6-2

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


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 9 . 3
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 9 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 218 . 85 . 157 . 99
Alternate DNS server: 218 . 85 . 152 . 99
Advanced...
OK
Cancel

Picture a6-3

FCC statement

This device complies with Part 15 of the FCC Rules: Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference that is received, including any interfer ence that may cause undesired operation.

RF exposure warning :
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment shall be installed and operated with minimum distance 20cm between the radiator & body.

This device is acting as host and operating in the 2.4 GHz (2412 ~2462 MHz) band.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.