Fanvil Product User Manual
IP-Gateway
Model: A1

Version：V1.0.60.16

Safety Notices

Please read the following safety notices before installing or using this gateway. They are crucial for the safe and reliable operation of the device.

- **Please use the external power supply that is included in the package. Other powers supplies may cause damage to the device, affect the behavior or induce noise.**
- **Before using the external power supply in the package, please check with home power voltage. Inaccurate power voltage may cause fire and damage.**
- **Please do not damage the power cord. If power cord or plug is impaired, do not use it, it may cause fire or electric shock.**
- **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.**
- **Do not drop, knock or shake it. Rough handling can break internal circuit boards.**
- **Do not install the device in places where there is direct sunlight. Also do not put the device on carpets or cushions. It may cause fire or breakdown.**
- **Avoid exposure the gateway to high temperature, below 0℃ or high humidity. Avoid wetting the unit with any liquid.**
- **Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.**
- **Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.**
- **When lightning, do not touch power plug or device line, it may cause an electric shock.**
- **Do not install this device in an ill-ventilated place.**
- **You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

Table of Content

1. Welcome to the A1 single port gateway

1.1. Package Contents

Please check your product packaging, it includes:
1. One A1 single port gateway
2. A group of cable
3. A power adapter
NOTE: if you use the non-A1 single port gateway comes with a power adapter, single port gateway A1 may cause damage or other injury. Specifications for the power adapter may difference between the different ship areas, If the power adapter provided with the product can not be used locally, please consult your local dealer.
4. User manua

2 Understanding of a single port gateway A1

A1 Single-port gateway IP-based voice media access device is designed for operators, enterprises, residential users, and residential VoIP solution to provide network equipment. A1 single port gateway into the analog voice information transmitted over IP networks, which use IP networks to transmit voice. It is full compliance with the SIP protocol standard, with the market most other SIP compliant devices and server-side.
The gateway will play Internet network (either public network or private network) connecting with the public telephone network bridge. It provides an FXS analog voice interface, used for ordinary small business PBX or gateway (PBX). Also provide an additional interface to a public telephone network PSTN (IE escape interface); power for the gateway, the call line will automatically go to PSTN lines from the VoIP line, the normal traffic for the user to provide the most effective protection.
Off this site using the most advanced voice processing technologies, such as advanced voice compression standards, echo cancellation, dynamic voice detection, silence detection, ensuring Quality of Service (QoS), voice quality comparable to regular PSTN phone.
In addition, A1 single port gateway also integrates a small router function. WEB comes through the gateway configuration page, simply configure the network parameters, can achieve multiple computers and network equipment, broadband access, ideal for small office and home users.
Because this site has a wealth of features and related detailed configuration options, in your call to enjoy a stress free before you know your A1 single port gateway.

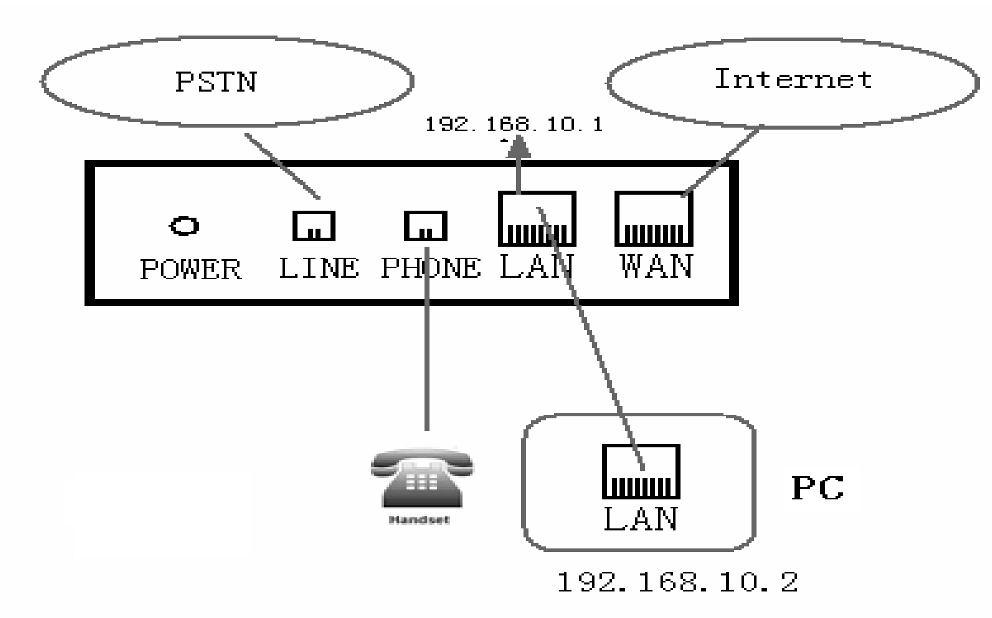
2.1. The positive of A1 single port gateway

2.2. Indicator signs

Name	Meaning	Description
POWER	Power LED	Always light, has power, you can start using the A1 single port gateway.
REG	Registration status indicator	Registered, the lights lit, the registration fails, the light flashes; do not use Notes Books, lights out.
PHONE	Phone work status lights	Show VoIP service is being used, or PSTN services, service, hang up: Death; pick up after the state if it is VoIP, Always; if you are in PSTN state: off.
WAN	WAN network interface lights	Indicator light, WAN port connected to the network. Flashing: Data transfer.
LAN	LAN network interface lights	Indicator light, LAN port connected to the network. Flashing: Data transfer.

2.3. Connector description

Name	Meaning	Description
POWER	Power switch	Output:12VDC， 500mA。
LINE	Lifeline	PSTN access lines.
PHONE	FXS Interface	Ordinary telephone connection, or switch into the line.
LAN	Network Interface	10/100M Adaptive connected PC.
WAN	Network Interface	10/100M Adaptive connected to the RJ45 port of Internet。



A1 single port gateway with two network interface itself: WAN port and LAN port, you can use the Internet connection into the WAN port or LAN port. Before inserting the power to read the manual carefully of “Safety."

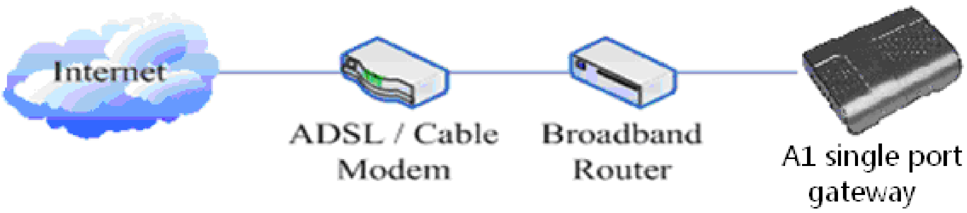
3. Getting Started

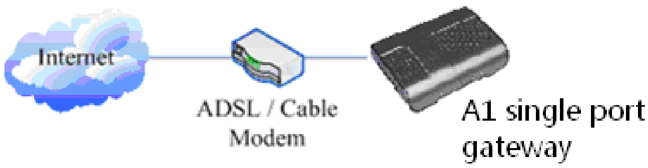
Before you start using the A1 single port gateway, please install the following:

3.1. Connect the power and network

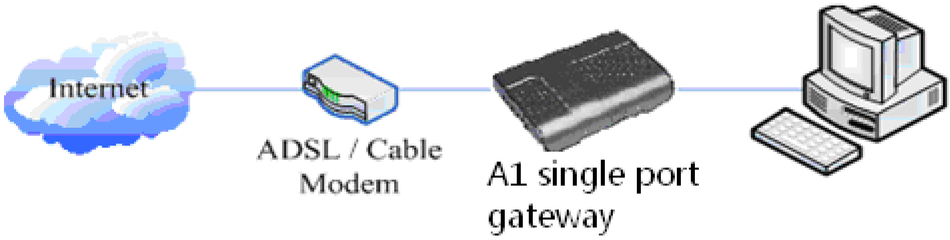
3.1.1. Connect the network

During this step, make sure your environment already have broadband Internet access capability.
1. Broadband Router
Direct network connection—by this method, you need at least one available Ethernet port in your workspace. Use the Ethernet cable in the package to connect WAN port on the back of your phone to the Ethernet port in your workspace. Since this VoIP Phone has router functionality, whether you have a broadband router or not, you can make direct network connect. The following two figures are for your reference.





2. as a broadband router
Use this method if you have a single Ethernet port in your workspace with your desktop computer already connected to it. First, disconnect the Ethernet cable from the computer and attach it to the WAN port on the back of your phone. Next, use the Ethernet cable in the package to connect LAN port on the back of your phone to your desktop computer. Your IP Phone now shares a network connection with your computer. The following figure is for your reference.



3.1.2. Connect the power

During this step, make sure your power supply connector and a single port gateway A1 outlet match, while A1 is also in line voltage and current required for a single port gateway.
1. The transformer connected to the DC port on the back of A1 single port gateway POWER jack
2. The AC adapter plug to an electrical outlet, A1 single port gateway boot.
3. At this point all of your lights (except the POWER indicator) will flash together. After booting, you will hear popping sounds, and then the indicator light is lit according to your current configuration corresponding light. (If your light is not normal, you need to further configure your network connection mode)
4. If you login on the gateway server, then you can start calling

4. A1 Basic operation of a single port gateway phone

4.1. Call transfer

- **Blind Transfer**

During a call, press FLASH (Flash) key, enter the number to be transferred * add and press 【#】 key to confirm, you can transfer the current call to third parties. (To use this feature, you must enable the gateway of the Call Waiting and Call Transfer function)

- **Attended Transfer**

During a call, press FLASH (Flash) key, enter the number waiting to be transferred connected, directly hang up, you can transfer successfully. (To use this feature, you must enable the gateway of the Call Waiting and Call Transfer function)
NOTE:1, Call Transfer must call in two cases all the way is free for operation;
2, Gateway (transfer side) and the establishment of phone A calls phone C gateway and then create a call, hang up the phone A, this time the gateway can also initiate the transfer.
3, your VoIP traffic services providers need to support (RFC3515), this feature to work correctly.

4.2. Call hold

- **Call Hold and set aside**

During a call you can press FLASH (FLASH) button and enter the number to dial and press 【#】 key to ensure
Recognition, can retain the current state of the call with third-party calls. If you press the FLASH (Flash) key, you can switch back. You also can send and receive on one side, then the party can not be retained to hear your conversation, the speaker you can not. During a call if you press 【*】 operation, will enter the three-way calling mode. (To use this feature, you must enable the gateway of the Call Waiting feature, you must achieve three-way calling mode to start the gateway Three Way Call function)

- **Call on hold and accept call waiting**

In normal conversation, a third party dial-in, the handset will beep ~ beep ~ tips coming, you can use FLASH (Flash) button to accept call waiting. If you press this button again, you can switch back. You also can send and receive on one side, then the party can not be retained to hear your conversation, the speaker you can not. (To use this feature, you must enable the gateway of the Call Waiting feature)

4.3. With the PSTN user calls

* T mapping shows that when the user connected to the PSTN line to the LINE port, then press * to switch to PSTN line, the user can call through the PSTN; if re-hook-hook dialing, the default line, or VoIP, need to press * to switch.

Of course you can also set the others, does not necessarily use the * T (Finally, the T end)

Dial-Peer Table

Number	Call Mode	Destination	Port	Alias	Suffix	Del length
*T	lifeline	0.0.0.0	0	no alias	no suffix	0

(See specific operations 5.3.3 Dial-peer)

Lifeline of the main functions is: to prevent blackouts, No Network Under such circumstances, the availability of telephone remains! Now, when introduced Notes on using the lifeline.

In two cases:

- Gateway is taking the lifeline, the user can use it as a regular phone
- Normal operating conditions, preferably up at the gateway before the PSTN line will be inserted into the escape port (LINE).

If you plug in the PSTN line up after the gateway, then you may hear pops or two, then you can not busy with a lifeline, but should wait a few seconds, pops, etc. to hear the same twice. At this point, you can rest assured that use.

5. Web configuration

5.1. Introduction of configuration

5.1.1. Ways to configure

A1 gateway has three different ways to different users.

- **Use phone keypad.**
- **Use web browser（recommendatory way）.**
- **Use telnet with CLI command.**

5.1.2. Password Configuration

There are two levels to access to phone: root level and general level. User with root level can browse and set all configuration parameters, while user with general level can set all configuration parameters except SIP (1-2) or IAX2's that some parameters can not be changed, such as server address and port. User will has different access level with different username and password.

- **Default user with general level：**
  - **username：guest**
  - **password：guest**
- **Default user with root level：**
  - **username：admin**
  - **password：admin**

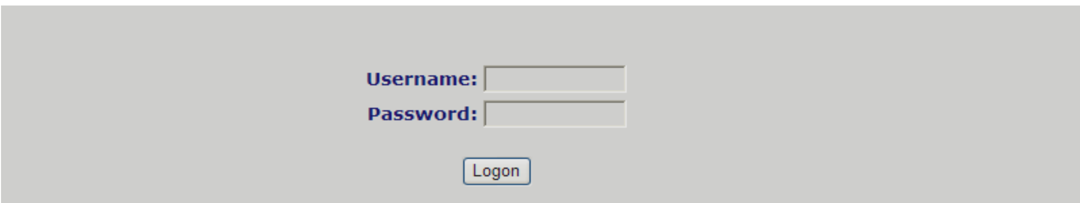
The default password of phone screen menu is 123.

5.2. Setting via web browser

When this phone and PC are connected to network, enter the IP address of the wan port in this phone as the URL (e.g. http://xxx.xxx.xxx.xxx/ or http://xxx.xxx.xxx.xxx:xxxx/).

Gateway IP address can be key by dialing # * 111 inquiries received

The login page is as below picture



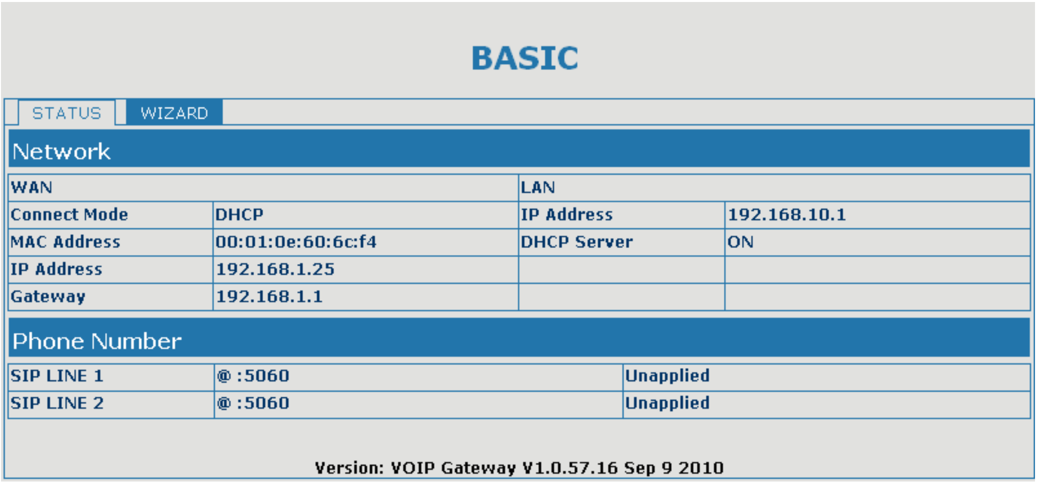
NOTE: After you configure the gateway, you need click save button in config under Maintenance in the left catalog to save your configuration. Otherwise the device will

lose your modification after power off and on.

5.3. Configuration via WEB

5.3.1. BASIC

5.3.1.1. Status



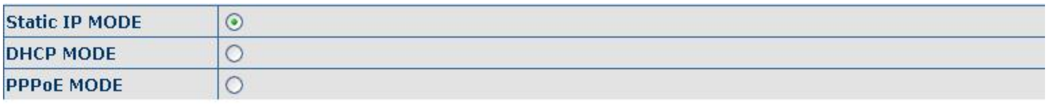
Status

Field name	Explanation
Network	Shows the configuration information on WAN and LAN port, including the connect mode of WAN port (Static, DHCP, PPPoE), MAC address, the IP address of WAN port and LAN port, ON or OFF of DHCP mode of LAN port.
Phone Number	Shows the phone numbers provided by the SIP LINE 1-3 servers and IAX2. The last line shows the version number and issued date.

5.3.1.2. Wizard

Wizard

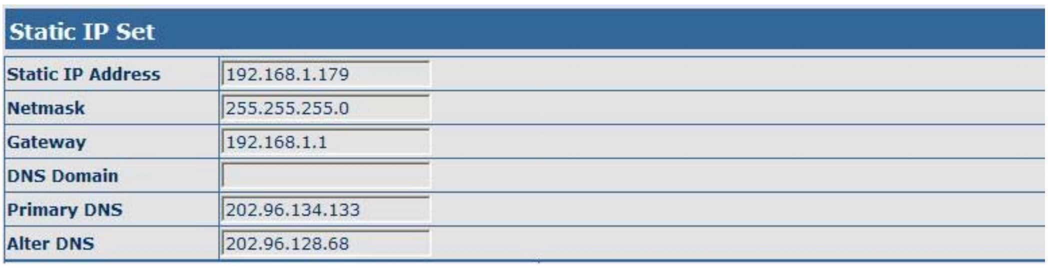
Field Name	Explanation



Please select the proper network mode according to the network condition. A1 gateway provide three different network settings:

- Static: If your ISP server provides you the static IP address, please select this mode, and then finish Static Mode setting. If you don't know about parameters of Static Mode setting, please ask your ISP for them.
- DHCP: In this mode, you will get the information from the DHCP server automatically; need not to input this information artificially.
- PPPoE: In this mode, your must input your ADSL account and password.

You can also refer to 3.2.1 Network setting to speed setting your network. Choose Static IP MODE, click【NEXT】can config the network and SIP(default SIP1)simply, also can browse too. Click【BACK】can return to the last page.



Static IP Address	Input the IP address distributed to you.
Netmask	Input the Netmask distributed to you.
Gateway	Input the Gateway address distributed to you.
DNS Domain	Set DNS domain postfix. When the domain which you input can not be parsed, gateway will automatically add this domain to the end of the domain which you input before and parse it again.
Primary DNS	Input your primary DNS server address.
Alter DNS	Input your standby DNS server address.

SIMPLE SIP SET	
Display Name	
Server Address	192.168.1.2
Server Port	5060
User Name	2113
Password	••••
Phone Number	2113
Enable Register	☑

Display Name	Set the display name.
Server Address	Input your SIP server address.
Server Port	Set your SIP server port.
User Name	Input your SIP register account name.
Password	Input your SIP register password.
Phone Number	Input the phone number assigned by your VOIP service provider.
Enable Register	Start to register or not by selecting it or not.

WAN	
Connect Mode	Static
Static IP Address	192.168.1.179
Gateway	192.168.1.1
SIP	
Register Server	192.168.1.2
Account/User Name	2113
PhoneNumber	2113
Register	ON
BACK	Finish

Display detailed information that you manual config.

Choose DHCP MODE，click【NEXT】can config SIP(default SIP1)simply, also can browse too. Click【BACK】can return to the last page. Like Static IP MODE。

Choose PPPoE MODE，click【NEXT】can config the PPPoE account/password and SIP(default SIP1)simply, also can browse too. Click【BACK】can return to the last page. Like Static IP MODE。

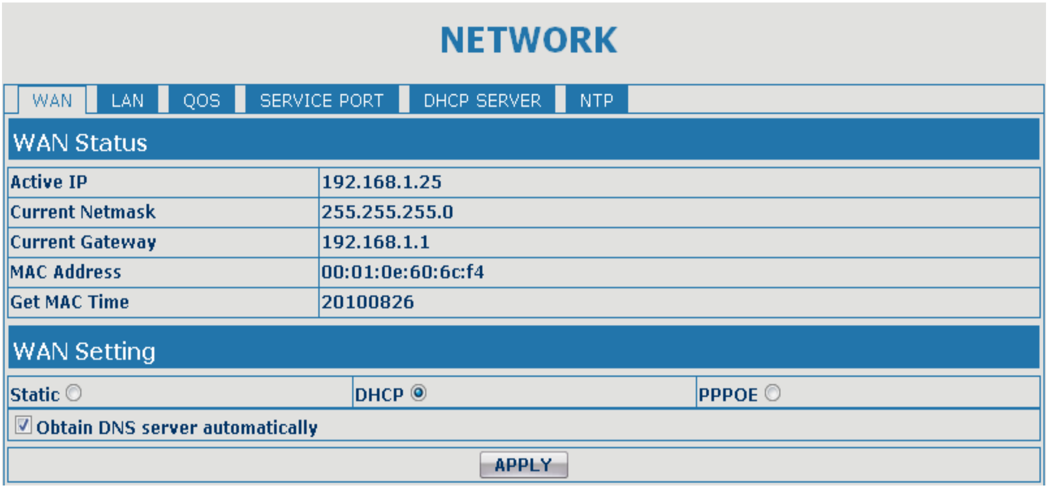
PPPOE Set	
PPPOE Server	ANY
Username	user123
Password	••••••••

PPPoE Server	It will be provided by ISP.
Username	Input your ADSL account.
Password	Input your ADSL password.

Notice: Click【Finish】button after finished your setting, gateway will save the setting automatically and reboot, After reboot, you can dial by the SIP account.

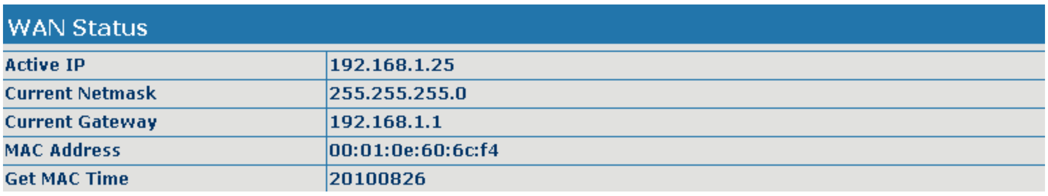
5.3.2. Network

5.3.2.1. WAN Config



WAN Config

Field Name	explanation



Active IP	The current IP address of the gateway.
Current Netmask	The current Netmask address.
MAC Address	The current MAC address of the gateway.
Current Gateway	The current Gateway IP address.
Get MAC Time	Shows the time of getting MAC address

Please select the proper network mode according to the network condition. A1 gateway provide three different network settings:

- Static: If your ISP server provides you the static IP address, please select this mode, and then finish Static Mode setting. If you don't know about parameters of Static Mode setting, please ask your ISP for them.
- DHCP: In this mode, you will get the information from the DHCP server automatically; need not to input this information artificially.
- PPPoE: In this mode, your must input your ADSL account and password. You can also refer to 3.2.1 Network setting to speed setting your network.

Obtain DNS server automatically	Select it to use DHCP mode to get DNS address, if you don't select it, you will use static DNS server. The default is selecting it.

Static IP Address	192.168.1.178
Netmask	255.255.255.0
Gateway	192.168.1.1
DNS Domain	
Primary DNS	202.106.195.68
Alter DNS	202.96.128.68
APPLY	

If you use static mode, you need set it.

IP Address	**Input the IP address distributed to you.**
Netmask	**Input the Netmask distributed to you.**
Gateway	**Input the Gateway address distributed to you.**
DNS Domain	**Set DNS domain postfix. When the domain which you input can not be parsed, gateway will automatically add this domain to the end of the domain which you input before and parse it again.**
Primary DNS	**Input your primary DNS server address.**
Alter DNS	**Input your standby DNS server address.**

PPPOE Server	ANY
Username	user123
Password	••••••••

If you uses PPPoE mode, you need to make the above setting.

PPPoE Server	**It will be provided by ISP.**
Username	**Input your ADSL account.**
Password	**Input your ADSL password.**

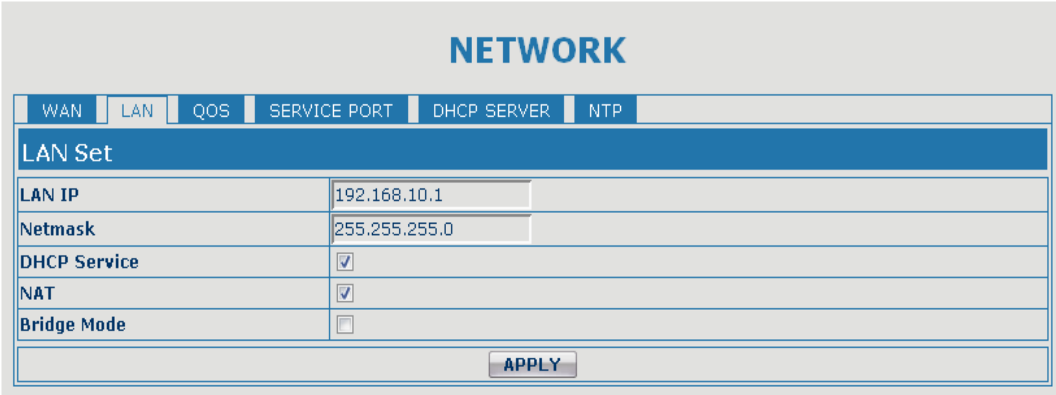
Notice:

1) **Click "Apply" button after finished your setting, IP gateway will save the setting automatically and new setting will take effect.**

2) **If you modify the IP address, the web will not response by the old IP address. Your need input new IP address in the address column to logon in the web.**

3) **If networks ID which is DHCP server distributed is same as network ID which is used by LAN of system, system will use the DHCP IP to set WAN, and modify LAN's networks ID(for example, system will change LAN IP from 192.168.10.1 to 192.168.11.1) when system uses DHCP client to get IP in startup; if system uses DHCP client to get IP in running status and network ID is also same as LAN's, system will refuse to accept the IP to configure WAN. So WAN's active IP will be 0.0.0.0**

5.3.2.2. LAN Config



LAN Config

Field name	explanation
LAN IP	Specify LAN static IP.
Netmask	Specify LAN Netmask.
DHCP Service	Select the DHCP server of LAN port or not. After you modify the LAN IP address, gateway will amend and adjust the DHCP Lease Table and save the result amended automatically according to the IP address and Netmask. You need restart the gateway and the DHCP server setting will take effect.
NAT	Select NAT or not.
Bridge Mode	Select Bridge Mode or not: If you select Bridge Mode, the gateway will no longer set IP address for LAN physical port, LAN and WAN will join in the same network. Click "Apply", the gateway will reboot.
Notice: If you choose the bridge mode, the LAN configuration will be disabled.	

5.3.2.3. Qos Config

The gateway support 802.1Q/P protocol and DiffServ configuration. VLAN functionality can use different VLAN IDs by setting signal/voice VLAN and data VLAN. The VLAN application of this device is very flexible.

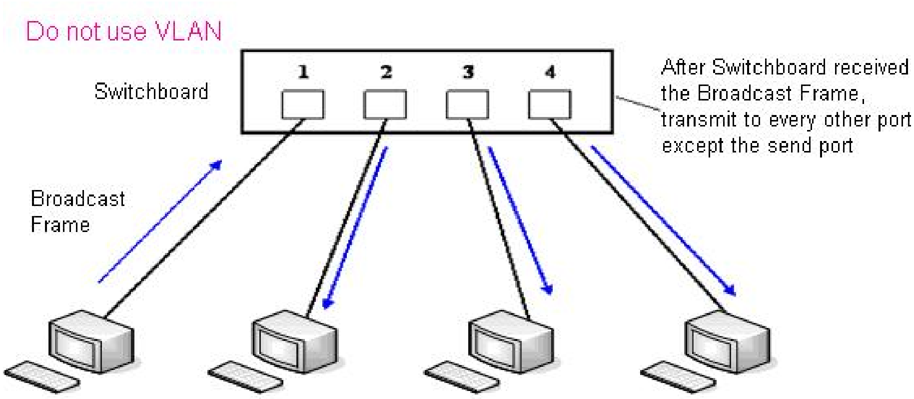
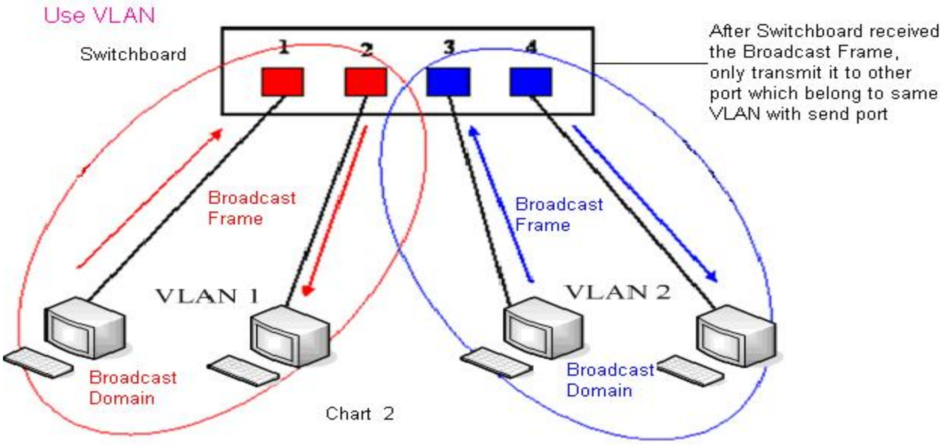


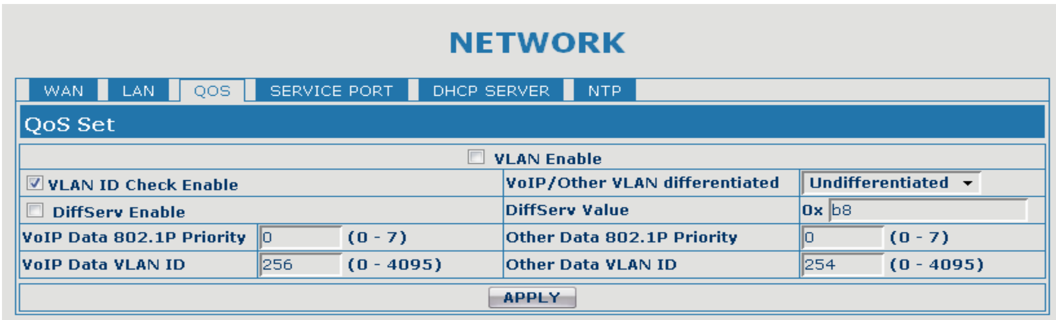
Chart 1



In chart 1, there is a layer 2 switch without setting VLAN. Any broadcast frame will be transmitted to the other ports except the send port. For example, a broadcast information is sent out from port 1 then transmitted to port 2,3and 4.

In chart 2, red and blue indicate two different VLANs in the switch, and port 1 and port 2 belong to red VLAN, port 3 and port 4 belong to blue VLAN. If a broadcast frame is sent out from port 1, switch will transmit it to port 2, the other port in the red VLAN and not transmit it to port3 and port 4 in blue VLAN. By this means, VLAN divide the broadcast domain via restricting the range of broadcast frame transmit ion.

Note: chart 2 use red and blue to identify the different VLAN, but in practice, VLAN uses different VLAN IDs to identify.



QoS Configuration

Field name	explanation
VLAN Enable	Before select it to enable VLAN, you need enable Bridge mode in LAN config.
VLAN ID Check Enable	Enable VLAN ID check by selecting it. After enable VLAN ID check, if VLAN ID of a data package is not the same with the gateway or a data package do not have VLAN ID, the data package will be discarded.
Voice/Data VLAN differentiated	After enable VLAN, system will set packets with different type of VLAN ID. Undifferentiated means after using VLAN, both VoIP packets and other data packets will use the voice VLAN ID; tag differentiated means after using VLAN, VoIP(signal and voice) packets will

	add voice VLAN ID, and other data packets will add data VLAN ID; data untagged means after using VLAN, only VoIP packets will add voice VLAN ID. Other data packets will not use VLAN.
DiffServ Enable	Select it or not to Enable or disable DiffServ.
DiffServ Value	Set DiffServ value, the common value is 0x00.
Voice 802.1P Priority	Specify 802.1P Priority of voice/signal data package.
Data 802.1P Priority	Set 802.1p of data VLAN. Non-VoIP data (such as http, telnet, ping etc) will use this value to set VLAN package.
Voice VLAN ID	Set VLAN ID of voice/signal data package.
Data VLAN ID	Set 802.1q of data VLAN ID. Non-VoIP data (such as http, telnet, ping etc) will use this value to set VLAN package.

NOTICE：

1） Startup VLAN, if set Voice/Data VLAN differentiated as Undifferentiated, all packets will use the Voice VLAN ID as the tag.

2) Startup VLAN, if set Voice/Data VLAN differentiated as tag differentiated and disables the DiffServ, then system will not distinguish the voice and data, all packets will use the Voice VLAN ID as the tag.

3) Startup VLAN, if set Voice/Data VLAN differentiated as tag differentiated and enables the DiffServ, then system will distinguish the voice and data and add the VLAN ID each other.

4) Startup VLAN, if set Voice/Data VLAN differentiated as data untagged, then the packet of the signal/voice will use the Voice VLAN ID as the tag, but the data packets will not take the VLAN tag.

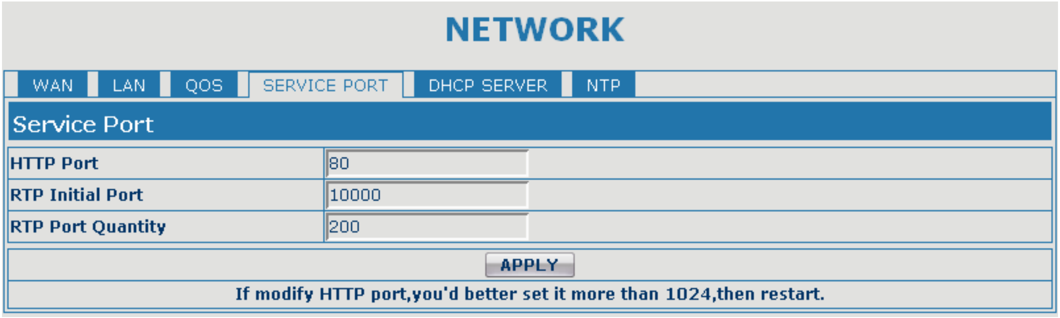
5) If Disable the VLAN, regardless to set the Voice/Data VLAN differentiated or not, all packets will not take the VLAN tag; If enable the DiffServ, all packets will only take the DiffServ value.

6) One must to notice, enable the VLAN ID Check Enable that is default, If enable it, the gateway will match the VLAN ID strictly. When others' VLAN ID not matches with us, the packets will discard. Contrarily, the gateway will accept the packets with the distinct VLAN ID.

7) You must gain the IP with the Static mode when you set VLAN, otherwise can't gain the IP in the VLAN and also can not dial with point to point.

5.3.2.4. Service Port

You can set the port of telnet/HTTP/RTP by this page.



SERVICE PORT

Field name	explanation
HTTP Port	set web browse port, the default is 80 port, if you want to enhance system safety, you'd better change it into non-80 standard port； Example: The IP address is 192.168.1.70. and the port value is 8090, the accessing address is http://192.168.1.70:8090
Telnet Port	Set Telnet Port, the default is 23. You can change the value into others. Example: The IP address is 192.168.1.70. the telnet port value is 8023, the accessing address is telnet 192.168.1.70 8023
RTP Initial Port	Set the RTP Initial Port. It is dynamic allocation.
RTP Port Quantity	Set the maximum quantity of RTP Port, the default is 200.

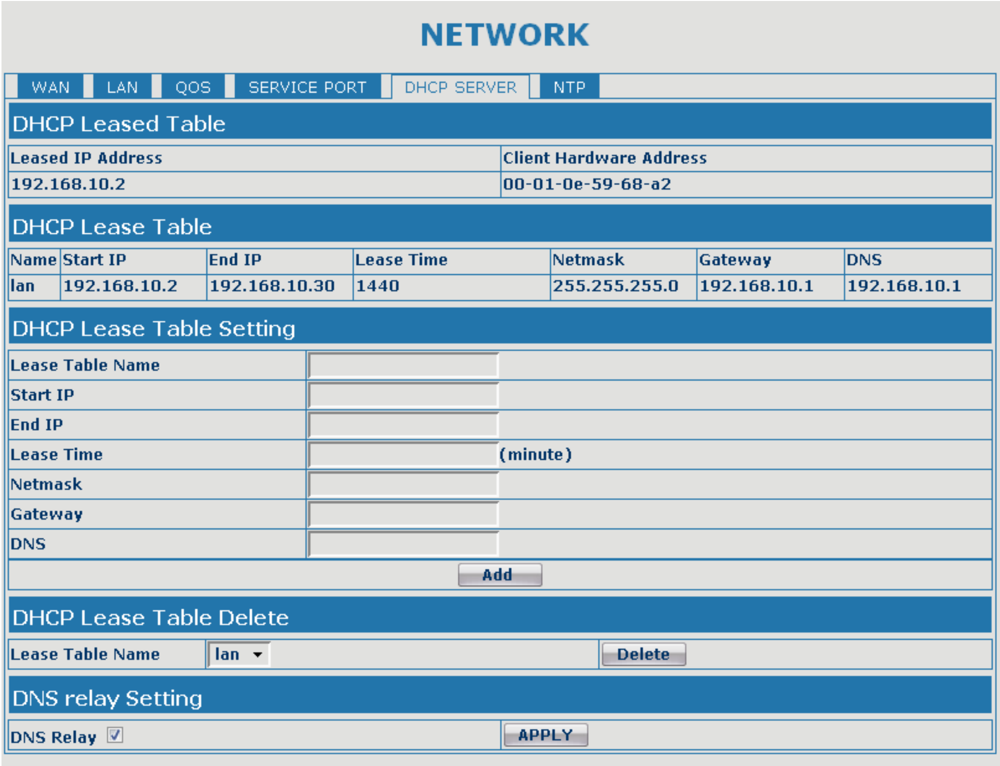
Notice:

1）You need save the configuration and reboot the gateway after set this page.

2） If you modify the port of Telnet and HTTP, you would better set the value more than 1024 because the port value less than 1024 is system port reserved.

3） if you set 0 for the HTTP port, it will disable HTTP service.

5.3.2.5. DHCP SERVER



DHCP SERVER

Field name	explanation
DHCP Leased Table	IP-MAC mapping table. If the LAN port of the gateway connects to a device, this table will show the IP and MAC address of this device.

Shows the DHCP Lease Table, the unit of Lease time is Minute.

Lease Table Name	Specify the name of the lease table
Start IP	Set the start IP address of the lease table
End IP	Set the end IP address of the lease table, the network device connected to LAN port will get IP address between Start IP and End IP by DHCP.
Netmask	Set the Netmask of the lease table
Gateway	Set the Gateway of the lease table
Lease Time	Set the Lease Time of the lease table
DNS	Set the default DNS server IP of the lease table; Click the Add button to submit and add this lease table

Select name of lease table, click the Delete button will delete the selected lease table from DHCP lease table.

DNS Relay	Select DNS Relay, the default is enabled. Click the Apply button to become effective.

Notice:

1） The size of lease table can not be larger than the quantity of C network IP address. We recommend you to use the default lease table and not modify it.

2）If you modifies the DHCP lease table, you need save the configuration and reboot.

5.3.2.6. NTP

Setting time zone and SNTP (Simple Network Time Protocol) server according to your location, you can also manually adjust date and time in this web page.

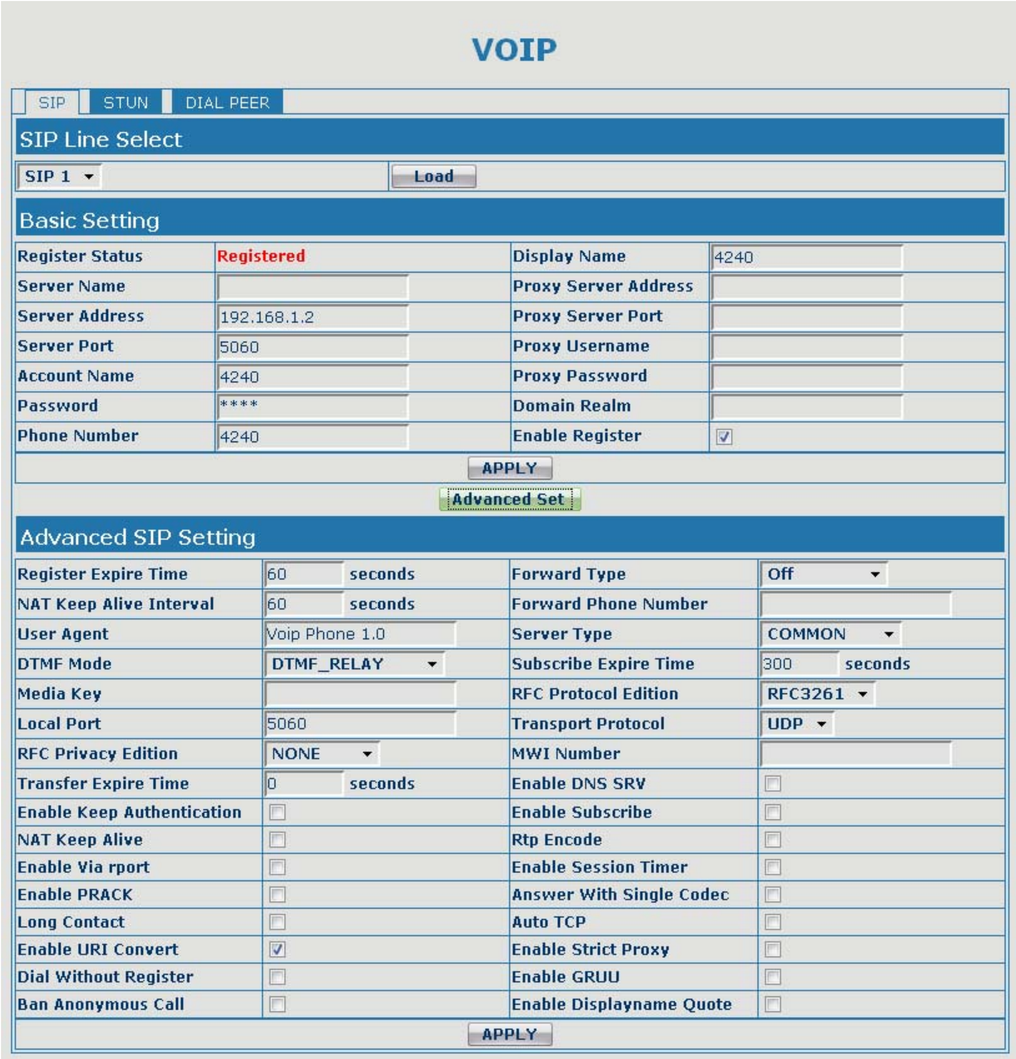
SNTP

Field name	explanation
Server	Set SNTP Server IP address.
Time Zone	Select the Time zone according to your location.
Time Out	Set the time out, the default is 60 seconds.
NTP	Select the NTP, and click Apply to make the SNTP Times effective.

5.3.3. VOIP

5.3.3.1. SIP Config

Set your SIP server in the following interface.



SIP Config

Field name	explanation

Choose line to set info about SIP, there are 3 lines to choose. You can switch by 【Load】 button.

Register Status	**Shows if the gateway has been registered the SIP server or not; or so, show Unapplied;**
Server Name	**Set the server name.**
Server Address	**Input your SIP server address.**
Server Port	**Set your SIP server port.**
Account Name	**Input your SIP register account name.**
Password	**Input your SIP register password.**
Phone Number	**Input the phone number assigned by your VoIP service provider. Phone will not register if there is no phone number configured.**
Display Name	**Set the display name.**

Proxy Server Address	Set proxy server IP address（Usually, Register SIP Server configuration is the same as Proxy SIP Server. But if your VoIP service provider give different configurations between Register SIP Server and Proxy SIP Server, you need make different settings.）
Proxy Server Port	Set your Proxy SIP server port.
Proxy Username	Input your Proxy SIP server account.
Proxy Password	Input your Proxy SIP server password.
Domain Realm	Set the sip domain if needed, otherwise this VoIP gateway will use the Register server address as sip domain automatically. (Usually it is same with registered server and proxy server IP address).
Enable Register	Start to register or not by selecting it or not.
Register Expire Time	Set expire time of SIP server register, default is 60 seconds. If the register time of the server requested is longer or shorter than the expire time set, the gateway will change automatically the time into the time recommended by the server, and register again.
NAT Keep Alive Interval	Set examining interval of the server, default is 60 seconds
User Agent	Set the user agent if have, the default is VoIP Phone 1.0
Signal Key	Set the key for signal encryption
Media Key	Set the key for RTP encryption
Local port	Set sip port of each line
Ring type	Set ring type of each line
Hot line Number	Set hot line number of each line
Conference Number	Configure conference number in server conference.
Transfer Expire Time	For the gateway supports the transfer of certain special features server, set interval time between sending “bye” and hanging up after the phone transfers a call.
Enable subscribe	Enable the option ,the gateway will receive the notify from the server.
Enable Keep Authentication	Enable/Disable Keep Authentication System will take the last authentication field which is passed the authentication by server to the request packet. It will decrease the server’s repeat authorization work, if it is enable.
NAT Keep Alive	Enable/Disable keeps NAT of SIP alive. If some server refuse to register with too short

	interval time, and has no packets sending to device in private network to keep NAT alive, user could set this function ON. It need set the keep alive interval time less than the NAT server's.
Enable Via report	**Enable/Disable system to support RFC3581. Via report is special way to realize SIP NAT.**
Enable PRACK	**Enable or disable SIP PRACK function, suggest use the default config.**
Long Contact	**Set more parameters in contact field; connection with SEM server**
Enable URI Convert	**Convert # to %23 when send the URI.**
Dial Without Register	**Set call out by proxy without registration;**
Ban Anonymous Call	**Set to ban Anonymous Call;**
Enable DNS SRV	**Support DNS looking up with _sip.udp mode**
Forward Type	**Select call forward mode, the default is Off** ● Off：Close down calling forward ● Busy：If the phone is busy, incoming calls will be forwarded to the appointed phone. ● No answer： If there is no answer, incoming calls will be forwarded to the appointed phone. ● Always：Incoming calls will be forwarded to the appoint phone directly. The phone will Prompt the incoming while doing forward.
Forward Phone Number	**Appoint your forward phone number.**
Server Type	**Select the special type of server which is encrypted, or has some unique requirements or call flows.**
DTMF Mode	**Select DTMF sending mode, there are three modes:** ● DTMF_RELAY ● DTMF_RFC2833 ● DTMF_SIP_INFO Different VoIP Service providers may provide different modes.
RFC Protocol Edition	**Select SIP protocol version to adapt for the SIP server which uses the same version as you select. For example, if the server is CISCO5300, you need to change to RFC2543; else phone may not cancel call normally. System uses RFC3261 as default.**
Transport Protocol	**Set transport protocols, TCP or UDP;**
RFC Privacy	**Set Anonymous call out safely; Support**

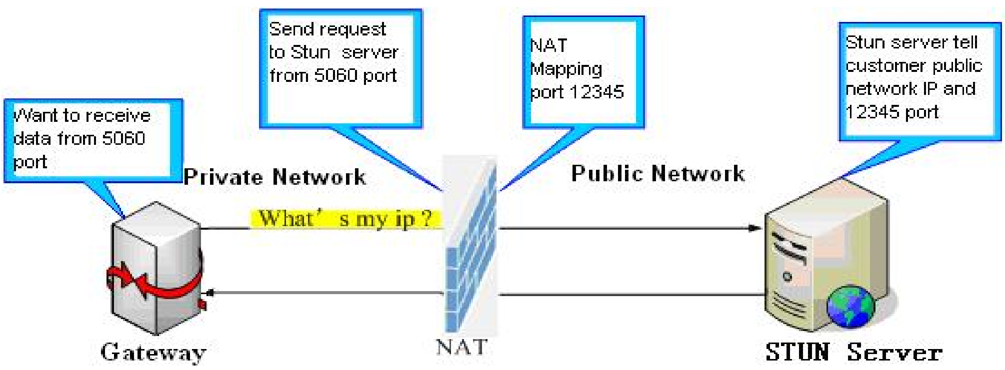
Edition	RFC3323and RFC3325;
Subscribe Expire Time	Overtime of resending subscribe packet. Suggest using the default config.
Enable Conference number	Set to use sever conference.
MWI Number	Input the number of the server's voice-mail box
Click to Talk	Set click to Talk (need practical software support).
Signal Encode	Enable/Disable Signal Encrypt.
RTP Encode	Enable/Disable RTP Encrypt.
Enable Session Timer	Set Enable/Disable Session Timer, whether support RFC4028.It will refresh the SIP sessions.
Answer With Single Codec	Enable/Disable the function when call is incoming, phone replies SIP message with just one codec which phone supports.
Auto TCP	Set to use automatically TCP protocol to guarantee usability of transport as message is above 1300 byte
Enable Strict Proxy	Support the special SIP server-when phone receives the packets sent from server, phone will use the source IP address, not the address in via field.
Enable GRUU	Set to support GRUU
Enable Display name Quote	Set to make quotation mark to display name as the phone sends out signal, in order to be compatible with server.

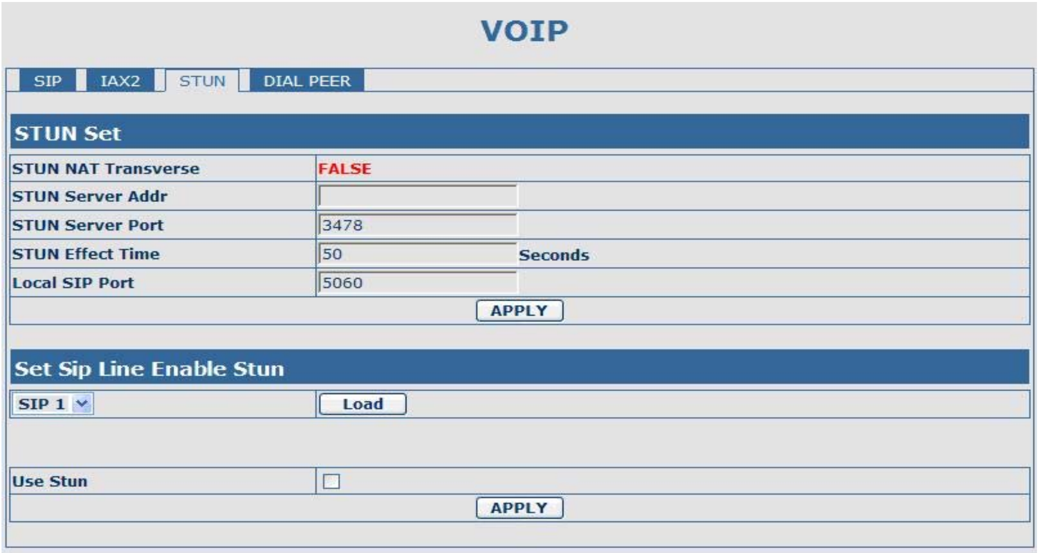
5.3.3.2. Stun Config

In this web page, you can config SIP STUN.

STUN:

By STUN server, the gateway in private network could know the type of NAT and the NAT mapping IP and port of SIP. The gateway might register itself to SIP server with global IP and port to realize the device both calling and being called in private network.





STUN

Field name	explanation
STUN NAT Transverse	**Shows STUN NAT Transverse estimation, true means STUN can penetrate NAT, while False means not.**
STUN Server Addr	**Set your SIP STUN Server IP address**
STUN Server Port	**Set your SIP STUN Server Port**
STUN Effect Time	**Set STUN Effective Time. If NAT server finds that a NAT mapping is idle after time out, it will release the mapping and the system need send a STUN packet to keep the mapping effective and alive.**
Local SIP Port	**Set the SIP port.**

Choose line to set info about SIP, There are 3 lines to choose. You can switch by 【Load】 button.

Use Stun	**Enable/Disable SIP STUN.**

Notice: SIP STUN is used to realize SIP penetration to NAT. If your phone configures STUN Server IP and Port (default is 3478), and enable SIP Stun, you can use the ordinary SIP Server to realize penetration to NAT.

5.3.3.3. DIAL PEER setting

This functionality offers you more flexible dial rule, you can refer to the following content to know how to use this dial rule. When you want to dial an IP address, the entry of IP addresses is very cumbersome, but by this functionality, you can set number 156 to replace 192.168.1.119 here.

Number	Destination	Port	Mode	Alias	Suffix	Del Length
156	192.168.1.119	5060	SIP	no alias	no suffix	0

When you want to dial a long distance call to Beijing, you need dial an area code 010 before local phone number, but you can also dial number 1 instead of 010

after we make a setting according to this dial rule. For example, you want to dial 01062213123, but you need dial only 162213123 to realize your long distance call after you make this setting.

Number	Destination	Port	Mode	Alias	Suffix	Del Length
1T	0.0.0.0	5060	SIP	rep:010	no suffix	1

To save the memory and avoid abundant input of user, add the follow functions:

Number	Destination	Port	Mode	Alias	Suffix	Del Length
13xxxxxxxxx	0.0.0.0	5060	SIP	add:0	no suffix	0
13[5-9]xxxxxxxx	0.0.0.0	5060	SIP	add:0	no suffix	0

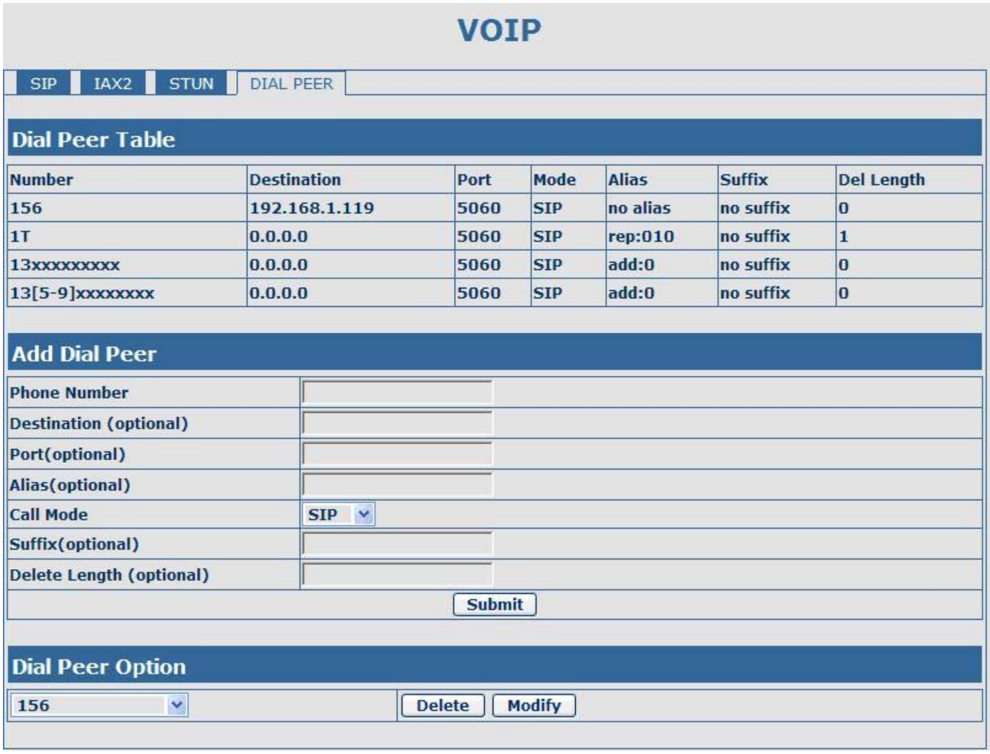
1、x Match any single digit that is dialed.

If user makes the above configuration, after user dials 11 digit numbers started with 13, the phone will send out 0 plus the dialed numbers automatically.

2、[] Specifies a range that will match digit. It may be a range, a list of ranges separated by commas, or a list of digits.

If user makes the above configuration, after user dials 11 digit numbers started with from 135 to 139, the phone will send out 0 plus the dialed numbers automatically.

Use this phone you can realize dialing out via different lines without switch in web interface.



DIAL PEER

Field name	explanation
Phone number	There are two types of matching conditions: one is full matching, the other is prefix matching. In the Full matching, you need input your desired phone number in this blank, and then you need dial the phone number to realize calling to what the phone number is mapped. In the prefix matching, you need input your

	desired prefix number and T; then dial the prefix and a phone number to realize calling to what your prefix number is mapped. The prefix number supports at most 30 digits
Destination	Set Destination address. This is optional config item. If you want to set peer to peer call, please input destination IP address or domain name. If you want to use this dial rule on SIP2 line, you need input 255.255.255.255 or 0.0.0.2 in it.SIP3 into 0.0.0.3
Port	Set the Signal port, the default is 5060 for SIP.
Alias	Set alias. This is optional config item. If you don't set Alias, it will show no alias.

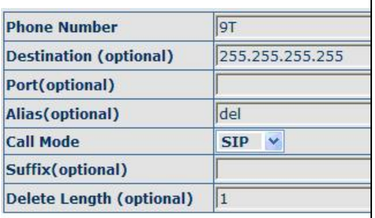
Note: There are four types of aliases.

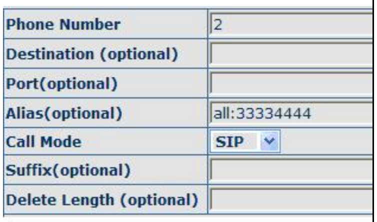
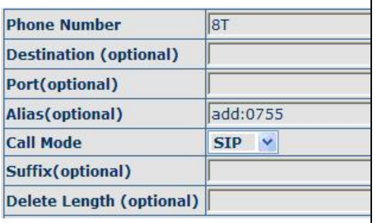
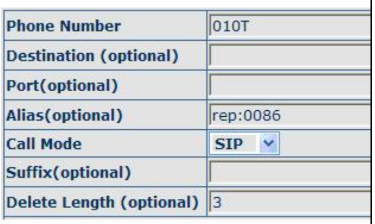
1) add: xxx, it means that you need dial xxx in front of phone number, which will reduce dialing number length.
2) all: xxx, it means that xxx will replace some phone number.
3) del: It means that phone will delete the number with length appointed.
4) Rep: It means that phone will replace the number with length and number appointed.

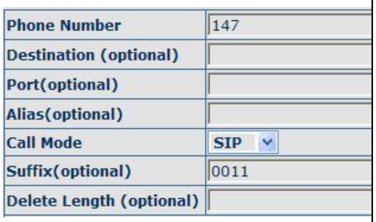
You can refer to the following examples of different alias application to know more how to use different aliases and this dial rule.

Call Mode	Select different signal protocol, SIP or IAX2
Suffix	Set suffix, this is optional config item. It will show no suffix if you don't set it.
Delete Length	Set delete length. This is optional config item. For example: if the delete length is 3, the phone will delete the first 3 digits then send out the rest digits. You can refer to examples of different alias application to know how to set delete length.

Examples of different alias application

Set by web	explanation	example
 Phone Number: 9T Destination (optional): 255.255.255.255 Port(optional): Alias(optional): del Call Mode: SIP Suffix(optional): Delete Length (optional): 1	You need set phone number, Destination, Alias and Delete Length. Phone number is XXXT; Destination is 255.255.255.255 (0.0.0.2) and Alias is del. This means any phone No. that starts with your set phone number will be sent via SIP2 line after the first	If you dial "93333", the SIP2 server will receive "3333"

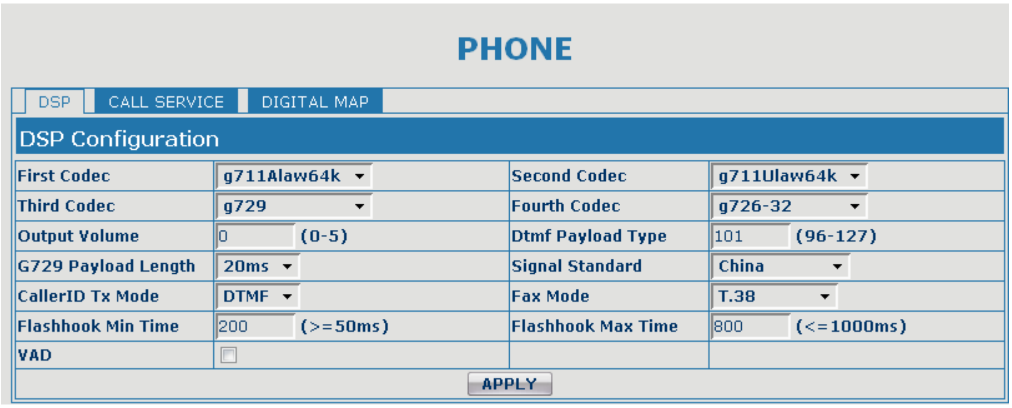
	several digits of your dialed phone number are deleted according to delete length.	
	This setting will realize speed dial function, after you dialing the numeric key “2”, the number after all will be sent out.	When you dial “2”, the SIP1 server will receive 33334444
	The phone will automatically send out alias number adding your dialed number, if your dialed number starts with your set phone number.	When you dial “8309“, the SIP1 server will receive “07558309”
	You need set Phone Number, Alias and Delete Length. Phone number is XXXT and Alias is rep:xxx If your dialed phone number starts with your set phone number, the first digits same as your set phone number will be replaced by the alias number specified and New phone number will be send out.	When you dial “0106228”, the SIP1 server will receive “86106228”

	If your dialed phone number starts with your set phone number. The phone will send out your dialed phone number adding suffix number.	When you dial “147”, the SIP1 server will receive “1470011”

5.3.4. Phone

5.3.4.1. DSP Config

In this page, you can configure voice codec, input/output volume and so on.



DSP Configuration

Field name	explanation
First Codec	The fist preferential DSP codec: G.711A/u, G.722, G.723, G.729
Second Codec	The second preferential DSP codec: G.711A/u, G.722, G.723, G.729
Third Codec	The third preferential DSP codec: G.711A/u, G.722, G.723, G.729
Forth Codec	The forth preferential DSP codec: G.711A/u, G.722, G.723, G.729
Fifth Codec	The fifth preferential DSP codec: G.711A/u, G.722, G.723, G.729
Input Volume	Specify Input (MIC) Volume grade.；
Hands-free Volume	Specify Hands-free Volume grade
G729 Payload Length	Set G729 Payload Length
Handdown Time	Specify the least reflection time of Handdown, the default is 200ms.
Ring Type	Select Ring Type
Output Volume	Specify Output (receiver) Volume grade.

Ring Volume	Specify Ring Volume grade
G722 Timestamps	160/20ms or 320/20ms is available
G723 Bit Rate	5.3kb/s or 6.3kb/s is available
Default Ring Type	Set up the ring by default
Signal Standard	Select Signal Standard.
VAD	Select it or not to enable or disable VAD. If enable VAD, G729 Payload length could not be set over 20ms.

5.3.4.2. Call Service

In this web page, you can configure Hotline, Call Transfer, Call Waiting, 3 Ways Call, Black List, white list Limit List and so on.

Call Service

Field name	explanation
Hotline	Specify Hotline number. If you set the number, you can not dial any other numbers.
Warm line time	Automatically after configuration hooks time to call the hotline number. If configured to 0, the hook immediately after the call the hotline number
No Answer Time	Specify No Answer Time
P2P IP Prefix	Set Prefix in peer to peer IP call. For example: what you want to dial is 192.168.1.119, If you define P2P IP Prefix as 192.168.1., you dial only #119 to reach 192.168.1.119. Default is “.”. If there is no “.” Set, it means to disable dialing IP.
Do Not Disturb	Select NO Disturb, the phone will reject any incoming call, the callers will be reminded by busy, but any outgoing call from the phone will work well.
Ban Outgoing	If you select Ban Outgoing to enable it, and you can not dial out any number.
Enable Call	Enable Call Transfer by selecting it.

Transfer	
Enable Call Waiting	Enable Call Waiting by selecting it.
Enable Three Way Call	Enable Three Way Call
Accept Any Call	If select it, the phone will accept the call even if the called number is not belong to the phone.
Black List	Set Add/Delete Black list. If user does not want to answer some phone calls, add these phone numbers to the Black List, and these calls will be rejected. X and. Are wildcard. x means matching any single digit. for example, 4xxx expresses any number with prefix 4 which length is 4 will be forbidden to dialed out DOT (.) means matching any arbitrary number digit. for example, 6. Expresses any number with prefix 6 will be forbidden to dial out. If user wants to allow a number or a series of number incoming, he may add the number(s) to the list as the white list rule. the configuration rule is -number, for example, -123456, or -1234xx Black List -4119 . Means any incoming number is forbidden except for 4119 Note: End with DOT (.) when set up the white list
Limit List	Set Add/Delete Limit List. Please input the prefix of those phone numbers which you forbid the phone to dial out. For example, if you want to forbid those phones of 001 as prefix to be dialed out, you need input 001 in the blank of limit list, and then you can not dial out any phone number whose prefix is 001. X and. Are wildcard. X means matching any single digit. for example, 4xxx expresses any number with prefix 4 which length is 4 will be forbidden to dialed out . Means matching any arbitrary number digit. For example, 6. Expresses any number with prefix 6 will be forbidden to dial out.
Notice: Black List and Limit List can record at most10 items respectively.	

5.3.4.3. Digital Map Configuration

This system supports 4 dial modes:

1). End with “#”: dial your desired number, and then press #.

2). Fixed Length: the phone will intersect the number according to your specified length.

3). Time Out: After you stop dialing and waiting time out, system will send the number collected.

4). User defined: you can customize digital map rules to make dialing more flexible. It is realized by defining the prefix of phone number and number length of dialing.

In order to keep some users' secondary dialing manner when dialing the external line with PBX, phone can be added a special rule to realize it. So user can dial a number as external line prefix and get the secondary dial tone to keep dial the external number. After finishing dialing, phone will send the prefix and external number totally to the server.

For example, there is a rule 9, xxxxxxxx in the digital map table. After dialing 9, phone will send the secondary dial tone, user may keep going dialing. After finished, phone will call the number which starts with 9; actually the number sent out is 9-digit with 9.

Digital Map Configuration

Field name	explanation
End with "#"	Set Enable/Disable the phone ended with “#” dial.
Fixed Length	Specify the Fixed Length of phone ending with.
Time out	Set the timeout of the last dial digit. The call will be sent after timeout.

Below is user-defined digital map rule:

[] Specifies a range that will match digit. May be a range, a list of ranges separated by commas, or a list of digits.

x Match any single digit that is dialed.

. Match any arbitrary number of digits including none.

Tn Indicates an additional time out period before digits are sent of n seconds in length. n is mandatory and can have a value of 0 to 9 seconds. Tn must be the last 2 characters of a dial plan. If Tn is not specified it is assumed to be T0 by default on all dial plans.

RULE
"[1-8]xxx"
"9xxxxxxx"
"911"
"99T4"
"9911x.T4"

Cause extensions 1000-8999 to be dialed immediately

Cause 8 digit numbers started with 9 to be dialed immediately

Cause 911 to be dialed immediately after it is entered.

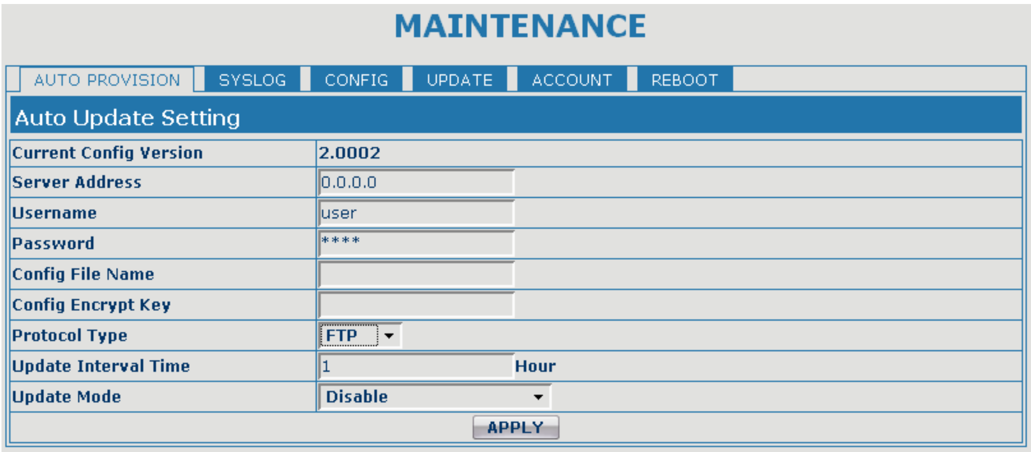
Cause 99 to be dialed after 4 seconds.

Cause any number started with 9911 to be dialed 4 seconds after dialing ceases.

Notice: End with "#", Fixed Length, Time out and Digital Map Table can be used simultaneously, System will stop dialing and send number according to your set rules.

5.3.5. Maintenance

5.3.5.1. Auto Provision



Auto Provision

Field name	explanation
Current Config Version	Show the current config file's version.
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be IP address or Domain name with subdirectory.
Username	Set FTP server Username. System will use anonymous if username keep blank.
Password	Set FTP server Password.
Config File Name	Set configuration file's name which need to update. System will use MAC as config file name if config file name keep blank. For example, 000102030405。
Config Encrypt	Input the Encrypt Key, if the configuration file is

Key	encrypted.
Protocol Type	Select the Protocol type FTP、TFTP or HTTP.
Update Interval Time	Set update interval time, unit is hour.
Update Mode	Different update modes: 1. Disable: means no update 2. Update after reboot: means update after reboot. 3. Update at time interval: means periodic update.

5.3.5.2. Syslog Config

Syslog is a protocol which is used to record the log messages with client/server mechanism. Syslog server receives the messages from clients, and classifies them based on priority and type. Then these messages will be written into log by some rules which administrator can configure. This is a better way for log management.

8 levels in debug information:

Level 0---emergency: This is highest default debug info level. You system can not work.

Level 1---alert: Your system has deadly problem.

Level 2---critical: Your system has serious problem.

Level 3---error: The error will affect your system working.

Level 4---warning: There are some potential dangers. But your system can work.

Level 5---notice: Your system works well in special condition, but you need to check its working environment and parameter.

Level 6---info: the daily debugging info.

Level 7---debug: the lowest debug info. Professional debugging info from R&D person.

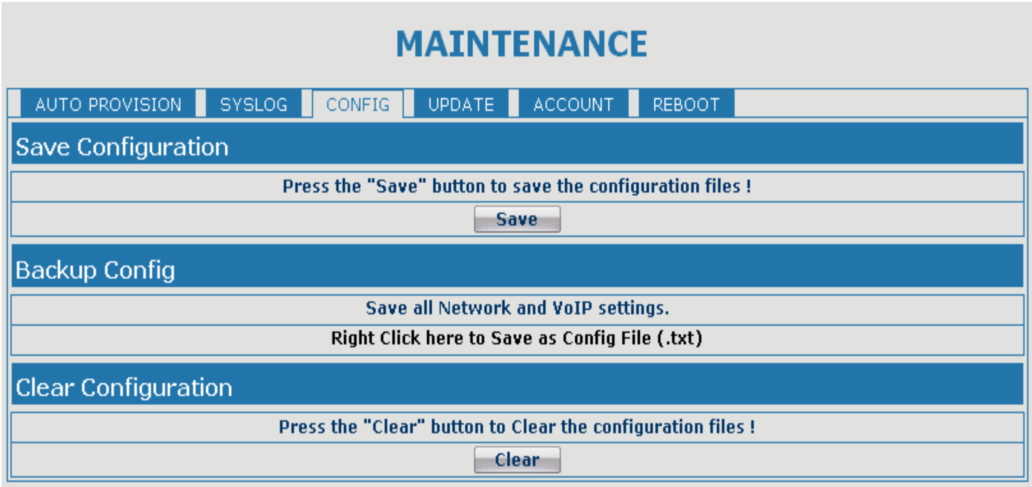
At present, the lowest level of debug information send to Syslog is info; debug level only can be displayed on telnet.

Syslog Configuration

Field name	explanation
Server IP	Set Syslog server IP address.
Server Port	Set Syslog server port.
MGR Log Level	Set the level of MGR log.

SIP Log Level	Set the level of SIP log.
IAX2 Log Level	Set the level of IAX2 log.
Enable Syslog	Select it or not to enable or disable syslog.

5.3.5.3. Config Setting

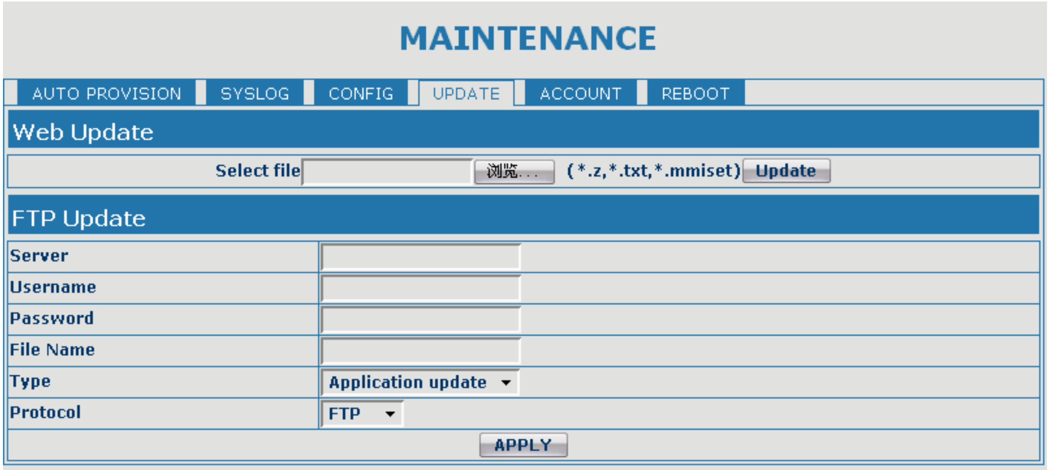


Config Setting

Field name	explanation
Save Config	you can save all changes of configurations. Click the Save button, all changes of configuration will be saved, and be effective immediately. .
Backup Config	Right clicks on “Right click here…” and select “Save Target As.…” then you will save the config file in .txt format
Clear Config	user can restore factory default configuration and reboot the gateway. If you login as Admin, the gateway will reset all configurations and restore factory default; if you login as Guest, the gateway will reset all configurations except for VoIP accounts (SIP1-2 and IAX2) and version number.

5.3.5.4. Update

You can update your configuration with your config file in this web page.

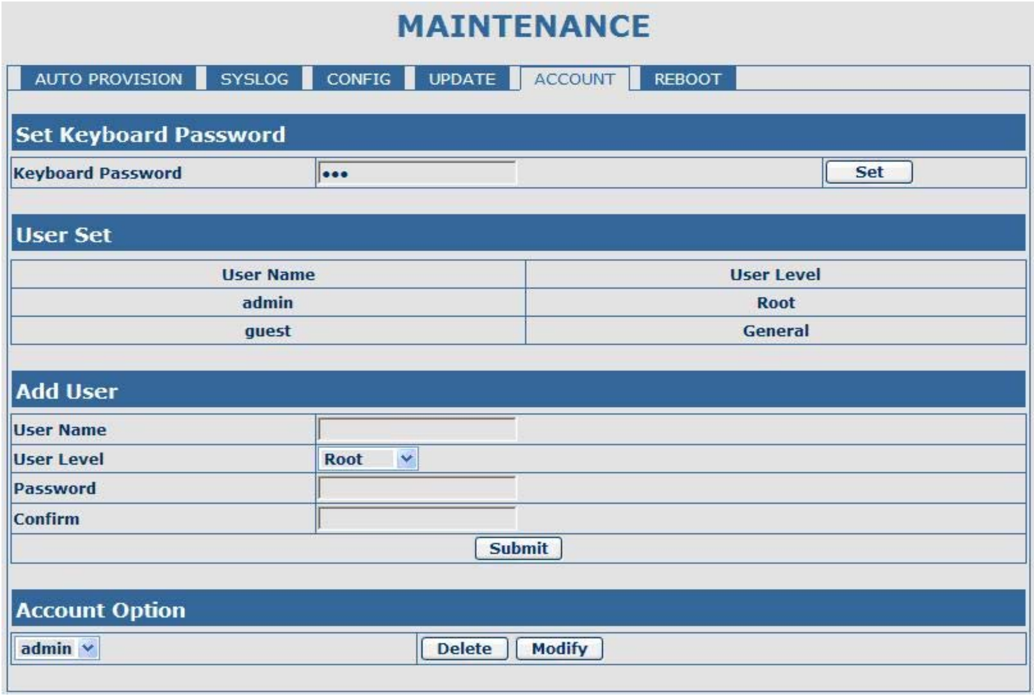


Update

Field name	explanation
Web Update	Click the browse button, find out the config file saved before or provided by manufacturer, download it to the gateway directly, press "Update" to save. You can also update downloaded update file, logo picture, ring, mmiset file by web.
Server	Set the FTP/TFTP server address for download/upload. The address can be IP address or Domain name with subdirectory.
Username	Set the FTP server Username for download/upload.
Password	Set the FTP server password for download/upload.
File name	Set the name of update file or config file. The default name is the MAC of the gateway, such as 000102030405.
Notice: You can modify the exported config file. And you can also download config file which includes several modules that need to be imported. For example, you can download a config file just keep with SIP module. After reboot, other modules of system still use previous setting and are not lost.	
Type	Action type that system want to execute： 1. Application update: download system update file 2. Config file export: Upload the config file to FTP/TFTP server, name and save it. 3. Config fie import: Download the config file to gateway from FTP/TFTP server. The configuration will be effective after the gateway is reset.
Protocol	Select FTP/TFTP server

5.3.5.5. Account Config

You can add or delete user account, and change the authority of each user account in this web page



Account Configuration

Field name	explanation
Keyboard Password	Set the password for entering the setting menu of the gateway by the phone key board. The password is digit.

User Name	User Level
admin	Root
guest	General

This table shows the current user existed.

User Name	Set account user name.
User Level	Set user level, Root user has the right to modify configuration, General can only read.
Password	Set the password.
Confirm	Confirm the password.

Select the account and click the Modify to modify the selected account, and click the Delete to delete the selected account.

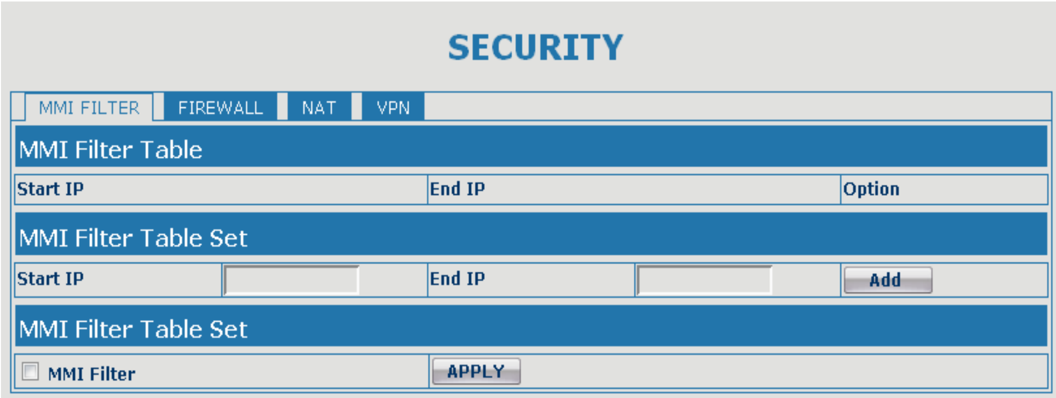
General user only can add the user whose level is General.

5.3.5.6. Reboot

If you modified some configurations which need the gateway's reboot to be effective, you need click the Reboot, then the gateway will reboot immediately. Notice: Before reboot, you need confirm that you have saved all configurations..

5.3.6. Security

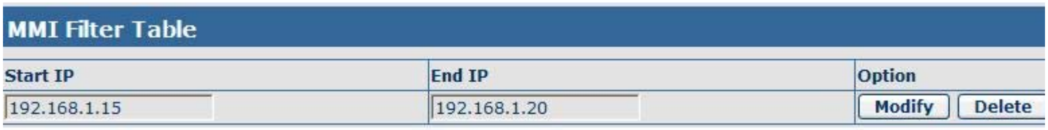
5.3.6.1. MMI Filter



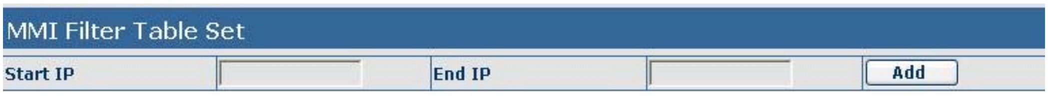
MMI Filter

User could make some device own IP, which is pre-specified, access to the MMI of the gateway to config and manage the gateway.

Field name	explanation



MMI Filter IP Table list:



Add or delete the IP address segments that access to the phone.
Set initial IP address in the Start IP column, Set end IP address in the End IP column, and click Add to add this IP segment. You can also click Delete to delete the selected IP segment.

MMI Filter	Select it or not to enable or disable MMI Filter. Click Apply to make it effective.

Notice: Do not set your visiting IP outside the MMI filter range, otherwise, you can not logon through the web.

5.3.6.2. Firewall

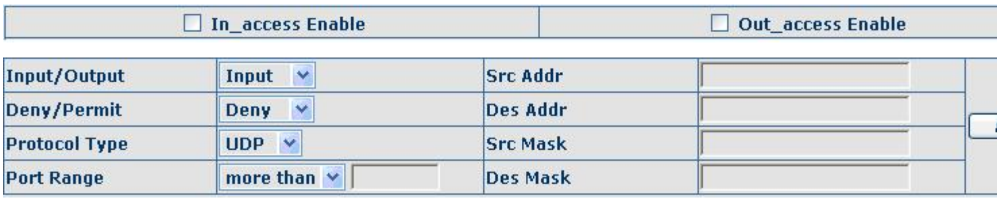
Firewall Configuration

In this web interface, you can set up firewall to prevent unauthorized Internet users from accessing private networks connected to the Internet (input rule), or prevent unauthorized private network devices from accessing the Internet (output rule).

Firewall supports two types of rules: input access rule and output access rule. Each type supports at most 10 items.

Through this web page, you could set up and enable/disable firewall with input/output rules. System could prevent unauthorized access, or access other networks set in rules for security. Firewall, is also called access list, is a simple implementation of a Cisco-like access list (firewall). It supports two access lists: one for filtering input packets, and the other for filtering output packets. Each kind of list could be added 10 items.

We will give you an instance for your reference.



Field name	explanation
In access enable	Select it to Enable in_ access rule
out access enable	Select it to Enable out_ access rule
Input/Output	Specify current adding rule by selecting input rule or output rule.
Deny/Permit	Specify current adding rule by selecting Deny rule or Permit rule.

Protocol Type	Filter protocol type. You can select TCP, UDP, ICMP, or IP.
Port Range	Set the filter Port range
Src Addr	Set source address. It can be single IP address, network address, complete address 0.0.0.0, or network address similar to *.*.*.0
Des Addr	Set the destination address. It can be IP address, network address, complete address 0.0.0.0, or network address similar to *.*.*.*
Src Mask	Set the source address' mask. For example, 255.255.255.255 means just point to one host; 255.255.255.0 means point to a network which network ID is C type.
Des Mask	Set the destination address' mask. For example, 255.255.255.255 means just point to one host; 255.255.255.0 means point to a network which network ID is C type.

Click the Add button if you want to add a new output rule.

Firewall Output Rule Table

Index	Deny/Permit	Protocol	Src Addr	Src Mask	Des Addr	Des Mask	Range
0	deny	ICMP	192.168.1.14	255.255.255.0	192.168.1.118	255.255.255.0	more than

Then enable out access, and click the Apply button.

So when devices execute to ping 192.168.1.118, system will deny the request to send ICMP request to 192.168.1.118 for the out access rule. But if devices ping other devices which network ID is 192.168.1.0, it will be normal.

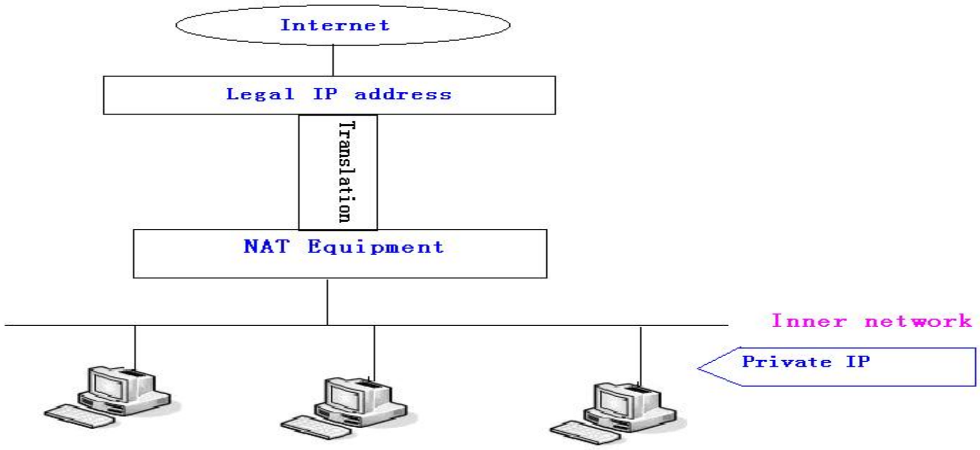
Rule Delete

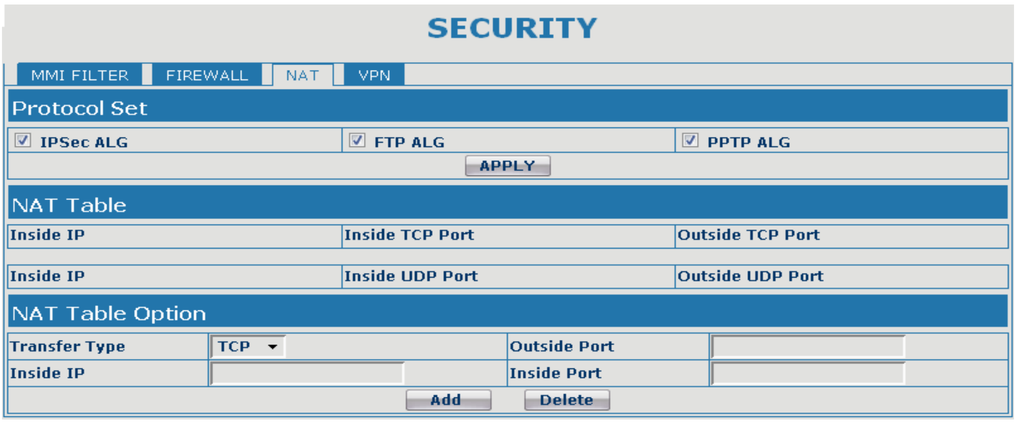
Input/Output	Input	Index To Be Deleted		D

Click the Delete button to delete the selected rule.

5.3.6.3. NAT Config

NAT is abbreviated from Net Address Translation; it's a protocol responsible for IP address translation. In other word, it is responsible for transforming IP and port of private network to public, also is the IP address mapping which we usually say.





NAT Configuration

Field name	explanation
IPSec ALG	It is an encryption technology. Select it to enable IPSec ALG, the default is enable
FTP ALG	FTP is a service of connection layer which can transform intranet IP into extranet IP when intranet IP is sending out packet. Select it to enable FTP ALG, the default is enable
PPTP ALG	Select it enable PPTP ALG, the default is enable

Shows the NAT TCP mapping table

Shows the NAT UDP mapping table

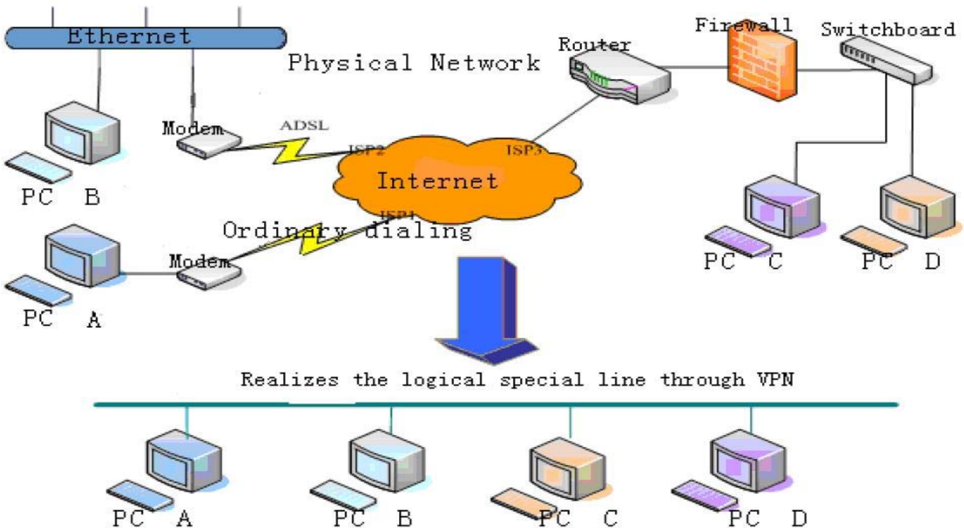
Transfer Type	Select the NAT mapping protocol style, TCP or UDP
Inside IP	Set the IP address of device which is connected to LAN interface to do NAT mapping.
Inside Port	Set the LAN port of the NAT mapping
Outside Port	Set the WAN port of the NAT mapping

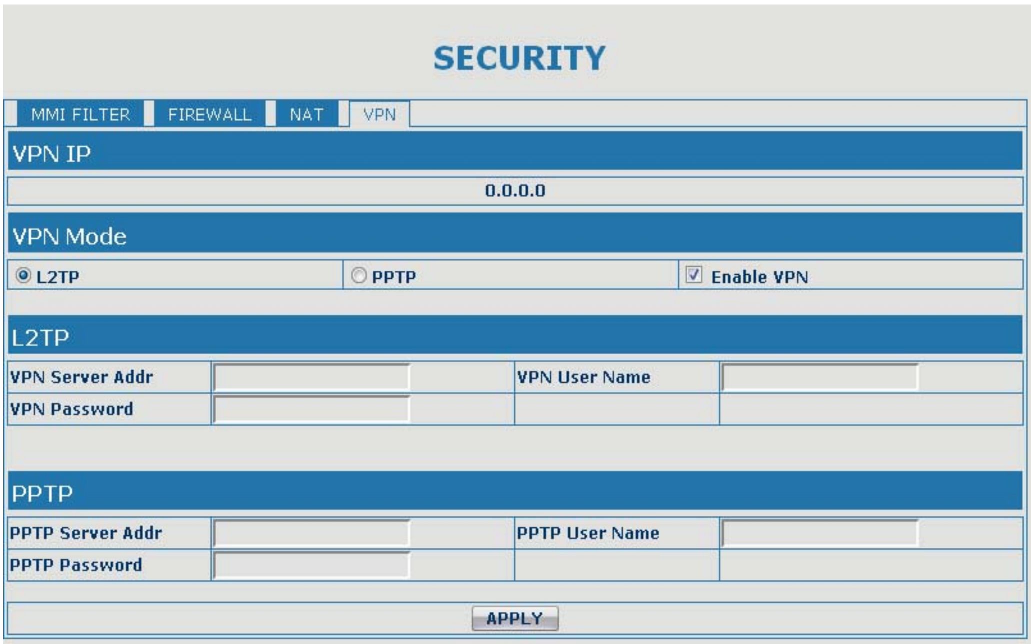
Notice: After finish setting, click the Add button to add new mapping table;

click the Delete button to delete the selected mapping table.

5.3.6.4. VPN Config

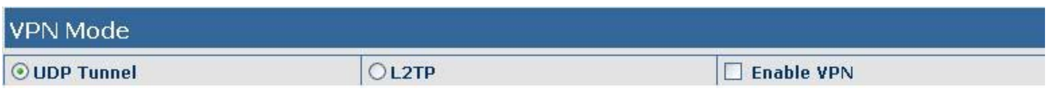
This web page provides us a safe connect mode by which we can make remote access to enterprise inner network from public network. That is to say, you can set it to connect public networks in different areas into inner network via a special tunnel.





VPN Configuration

Field name	explanation
VPN IP	Shows the current VPN IP address



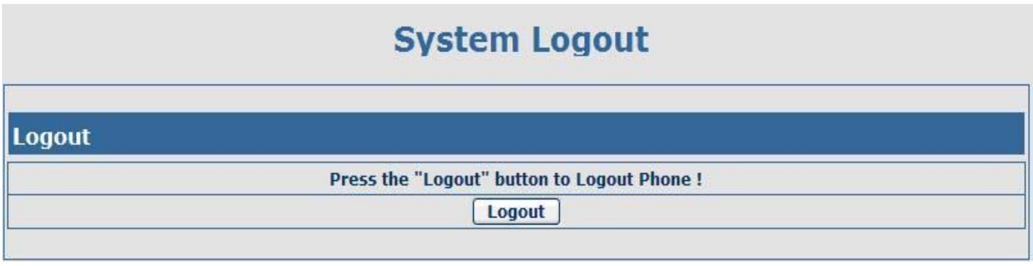
Select UDP Tunnel (VPN Tunnel) or VPN L2TP. You can choose only one for current state. After you select it, you'd better save configuration and reboot your device.

Enable VPN **Select it or not to enable or disable VPN；**

VPN Server Addr	**Set VPN L2TP Server IP address**
VPN User Name	**Set User Name access to VPN L2TP Server**
VPN Password	**Set Password access to VPN L2TP Server**

VPN Server Addr	**Set VPN PPTP Server IP address**
VPN User Name	**Set User Name access to VPN PPTP Server**
VPN Password	**Set Password access to VPN PPTP Server**

5.3.7. Logout



Click Logout， and you will exit web page. If you want to enter it next time, you need input user name and password again.

6. Appendix

6.1. Specification

6.1.1. Hardware

Item		A1 GATEWAY
Adapter (Input/Output)		Input: 100-240V Output: 12V 1A
port	WAN	10/100Base- T RJ-45 for LAN
	LAN	10/100Base- T RJ-45 for PC
Operation Temperature		0 ~ 40℃
Relative Humidity		10 ~ 65%
main chip		Ralink MIPS 24KEC (320MHz)
SDRAM		16M
Flash		4M

6.1.2. Voice features

- Support SIP 2.0 (RFC3261) and correlative RFCs
- Codec: G.711A/u, G.729a/b，G.726-32k，ilbc
- Echo cancellation: G.168 Compliance in LEC, additional acoustic echo cancellation(AEC) can reach 96ms max filter length in hands-free mode
- Support Voice Gain Setting, VAD, CNG
- NAT penetration, Support for STUN way through
- SIP support SIP domain, SIP authentication(none basic, MD5), DNS name of server, Peer to Peer/ IP call
- SIP can register two SIP accounts, through the Pubic Server / Private server, users can either account for inbound and outbound
- Support call line automatically selected, when the public can not connect the server when the server can automatically switch to the private call
- DTMF Relay: support SIP info，DTMF Relay，RFC2833
- SIP application: SIP Call forward/transfer（blind/attended）/hold/waiting/3 way talking/
- Call control features: Flexible dial map, hotline, empty calling No. reject service, black list for reject authenticated call, limit call, no disturb, caller ID, Flexible deer peer rule.
- Support T.38 Fax
- With the escape port (lifeline), can support power to answer and make phone calls through the exit port can also be the system starts the call by dialing rules lifeline
- Add voip unavailable features to automatically connect to the lifeline routes
- Add busy when N / A lines of the 4 modes
- Support IAX2

6.1.3. Network features

- WAN/LAN: support bridge and router model
- Support PPPoE for XDSL

- Support DHCP server in the LAN port
- Gateway ping test through keyboard commands
- Support DHCP client in the WAN port
- Support basic NAT and NAPT
- Support VLAN (optional: voice vlan/ data vlan),support NTP
- Support DMZ
- Support VPN (L2TP) function
- WAN Port supports main DNS and secondary DNS server can select dynamically to get DNS in DHCP mode or statically set DNS address.
- QoS with DiffServ
- Support DNS relay, supports SNTP Client, Firewall support the simple
- Network tools in telnet server: including ping, trace route, telnet client

6.1.4. Maintenance and management

- Support Safe Mode
- Can be updated by safe Mode
- Web ,telnet and keypad management
- Management with different account right
- Upgrade firmware through HTTP, FTP or TFTP Telnet remote management/ upload/download setting file
- Support Syslog
- Support Auto Provisioning (upgrade firmware or configuration file)

6.2. Particularly suitable for A1 single port gateway

- Service Provider of telecom operators and (ITSP) Internet Telephony
- Large companies (for international and domestic long distance and / or internal communications, mainly in the way free sparring)
- Import and export business of small or medium enterprises, such as foreign travel, study intermediary agents, immigration agents and other intermediaries
- Foreign / joint ventures, foreign enterprises in China, offices, representatives and agents, etc.
- Foreign hotel (which can be placed in the rooms and business center or leased)
- All levels of government in dealing with foreigners more departments, such as foreign trade sector, the CPAFFC, sports units, cultural units, Foreign Experts Affairs, the foreign affairs department, etc.
- Schools and research institutes, such as the joint venture school, school or Foreign Affairs Department of the research unit.
- IP supermarkets, IP telephone booth (mostly set in the migrant workers, students focus on areas such as low-income people)
- Personal and home users, such as immigrant families, host families, student hostels, separation of individual family members due to long working relationship, often with family or friends living abroad keep in touch with the individuals.

6.3. Common Problems

Symptom	Solution
POWER light does not shine	1、Check the power connection is correct. 2、Check the power adapter is used.
	1、Check the cable connection is valid, check the PC card indicator light is on.

WAN/LAN link light does not shine	**2、Check the card is working properly, the specific approach is seen in the PC, there with "?" Or "!" Device under "Network Adapter". If so, remove the device and reinstall. Otherwise, the NIC in another slot, if not enough, replace the card.**
	Access modes commonly used example (already installed on your computer dial-up software) **Description:**
Can not access the internet	**1、Make sure the front of the problem does not exist.** **2、Make sure that dial-up software is properly installed and set.** **3、Sure to enter the correct user name and password.** **4、If it does not work after the success dial up, make sure the IE browser's proxy server is set correctly.** **5、Please try to log multiple pages to confirm a Web server failure is not due.**

EPCOM

1630 Paisano Dr.
El Paso. Tx 79901.   Ph (915)533-5119
www.epcom.net

SYSCOM

Ave 20 de Noviembre No. 805   Col. Centro
Chihuahua, Chih. 31000   Tel 052 (614) 415 – 2525
www.syscom.mx