User Manual

FV8010 Series

Gateway

Version2.0

CONTENT

1 Welcome

FV8010 series of gateways are innovative gateways that offer a rich set of functionality and superb sound quality. They are fully compatible with SIP industry standard and can interoperate with many other SIP compliant devices and software on the market.

2 Installation

2.1 Package List

The FV8010 gateway package contains:
1) One FV8010 gateway
2) One universal power adapter
3) One Straight Ethernet cable

2.2 Safety Compliances

The gateway should only be operated with the universal power adapter provided with the package. Damages to the gateway caused by using other unsupported power adapters would not be covered by the manufacturer's warranty.

3 Product Overview

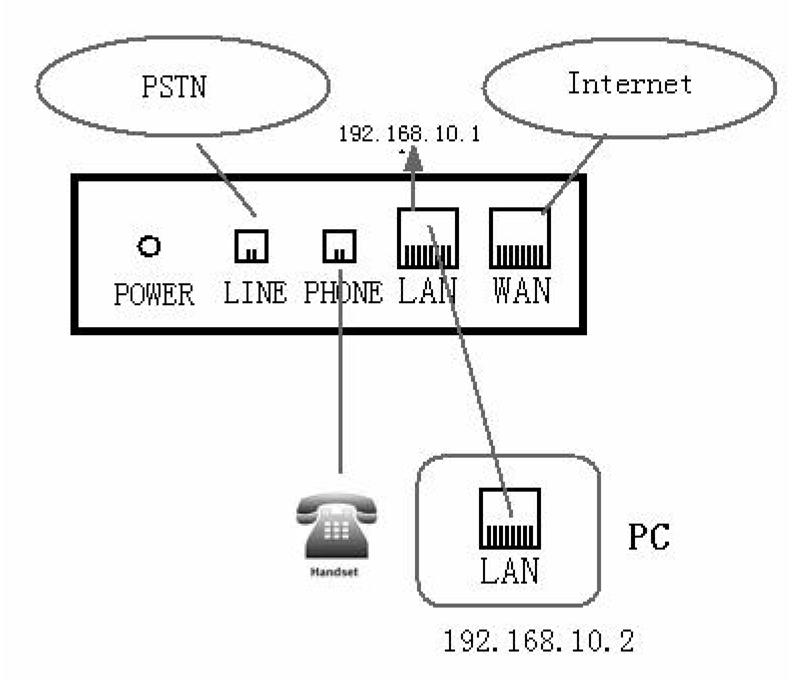
FV8010 IP Gateway is a next generation IP network facility based on industry open standard SIP (Session Initiation Protocol) . Built on innovative technology, FV8010 IP Gateway features market leading superb sound quality and rich functionalities.

Power: **Output Power:12VDC,500mA.**
Line: **RJ11 port. Lifeline . Connect to PSTN line**
Phone: **RJ11 port, FXS . Connect to normal phone or PABX**
WAN: **RJ45 port.for Internet**
LAN: **RJ45 port.for PC**

Power: **Power indicator.**
REG: **Server indicator. Registered: ON; Registering: Blinking; Do not register: OFF.**
Phone: **Indicate the calling status.**
Hook-on: OFF.
Hook-off and in VoIP state: ON.
Hook-off and in PSTN state: OFF.

4.0 Web configuration

4.1 Physical connection

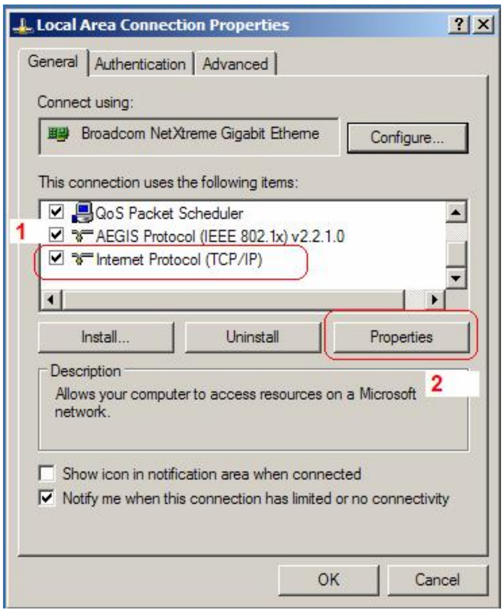


4.2 Preparation for Web configuration

The IP Gateway Web Configuration Menu can be accessed by the following URL: http://Gateway-IP-Address. The default LAN IP address is "192.168.10.1" and WAN IP address is "192.168.1.179". If the web login port of the gateway is configured as non-80 standard port, then user need to input http://xxx.xxx.xxx.xxx: xxxx/, otherwise the web will show that no server has been found.

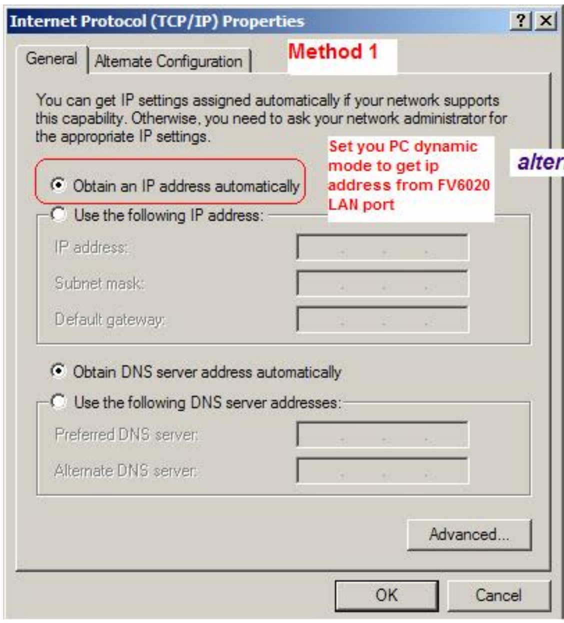
If connect PC with FV8010 LAN port and config to obtain IP address automatically, you could check the default gateway IP which is LAN IP address. The procedure as below

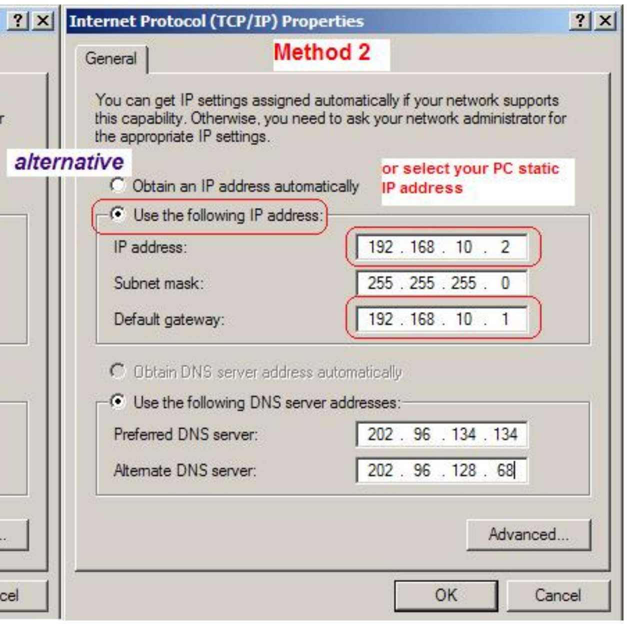
a) Access to "Property of local area connection" dialog box



b) Select "Internet Protocol (TCP/IP)",click "Property" button

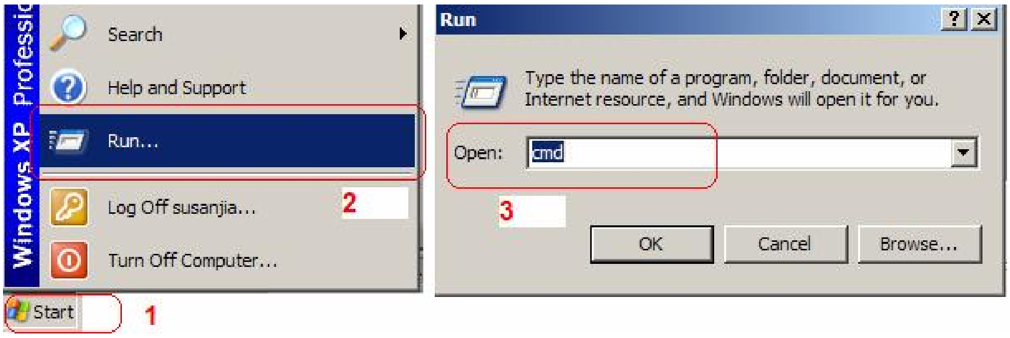
c) Setting refers to below dialog box, and then click "OK" button, PC will obtain IP address automatically.（or set your pc static ip 192.168.10.2）

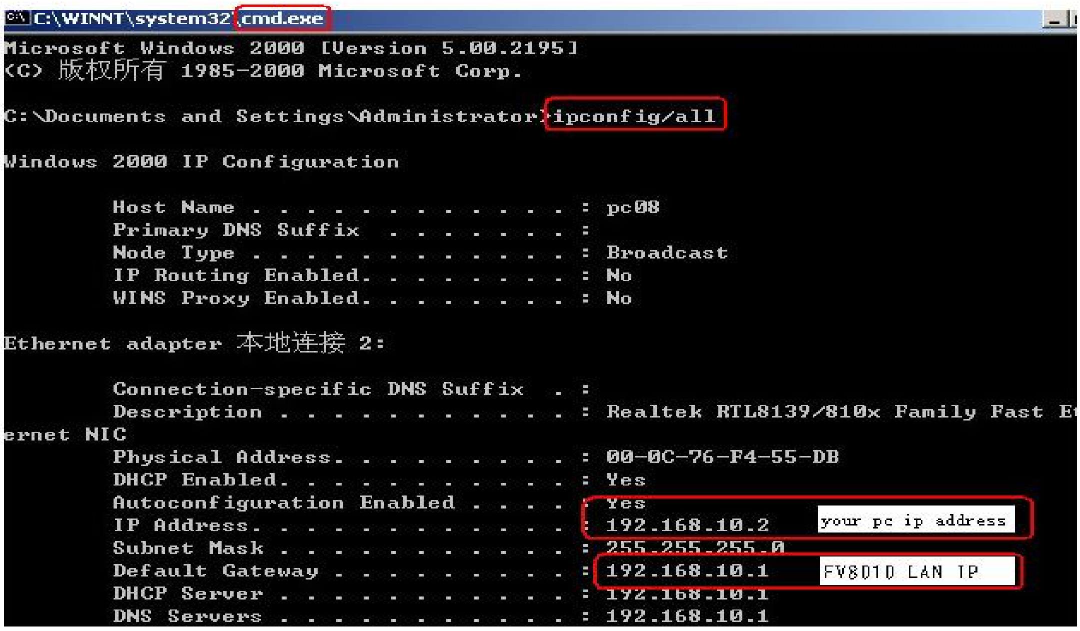




Method 1 Method2

d) Input “cmd” command on the RUN submenu under PC START, key in “ipconfig/all on the command lines dialog box to find the default gateway IP address, which is FV8010 LAN IP address



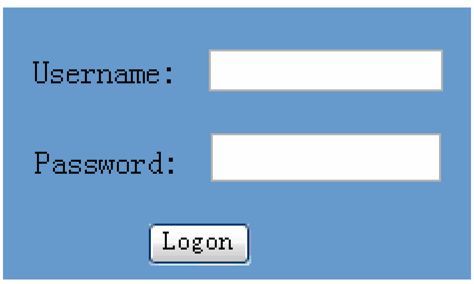


4.3 User verification

Users are requested to make verification when config or browse the IP phone thru web pages, users can direct login the config menu by inputting username and password as below ,

Default username and password is:

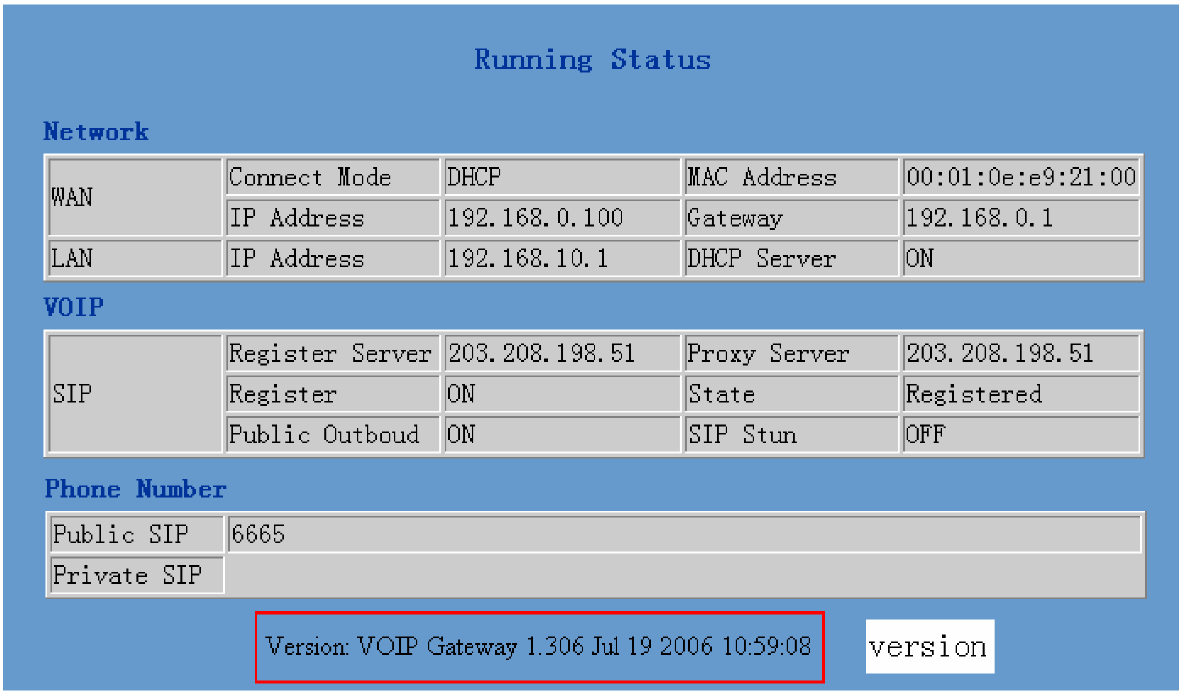
Administrator:	Username: admin	password: admin	low level user interface
User:	Username: guest	Username: guest	high level user interface



4.4 Current State

On this page user can gather information of each commonly-used parameter of the phone, it is shown as the following figure:

- **Network section: Display the current WAN, LAN configurations of the phone**
- **VoIP section: Display the current default signaling protocol in use， and server parameter in use of each protocol**
- **Phone Number section: Display the phone number against each protocol**


Running Status

Network

WAN	Connect Mode	DHCP	MAC Address	00:01:0e:e9:21:00
	IP Address	192.168.0.100	Gateway	192.168.0.1
LAN	IP Address	192.168.10.1	DHCP Server	ON

VOIP

SIP	Register Server	203.208.198.51	Proxy Server	203.208.198.51
	Register	ON	State	Registered
	Public Outboud	ON	SIP Stun	OFF

Phone Number

Public SIP	6665
Private SIP	

- **The version number and date of issue have been shown at the end of this page**

4.5 Network configuration

Network configuration includes WAN Config and LAN Config.

4.5.1 WAN Configuration

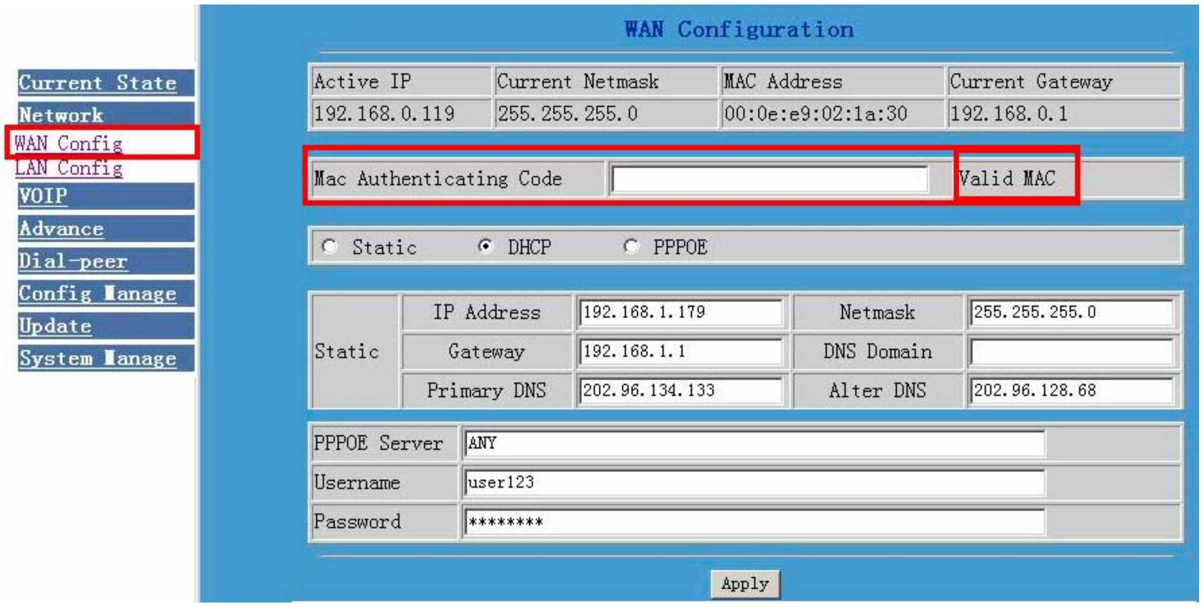
This web page displays the WAN parameter configuration.

User can view the current network IP linking mode of the system on this page.

User will be authorized to set the network IP, Gateway and DNS if the system adopts the static linking mode. If the system selects DHCP service in the network which is using DHCP service, IP address will be gained dynamically.

If the system selects PPPOE service in the network which is using the PPPOE service, then the IP address will be gained by the set PPPOE ISP internet and password of the account.

Note: if IP address has been modified, the web page will no longer respond owing to the modification, so new IP address should be input in the address field now.

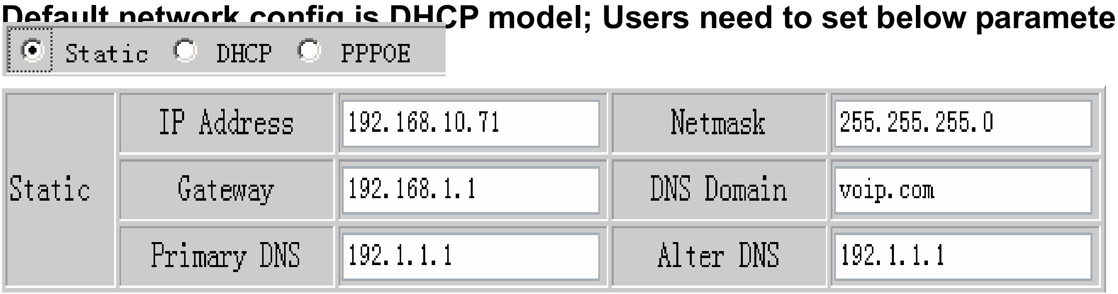


Display <valid MAC > , that means the FV8010 had been certificated.
Display <invalid MAC> , that means the phone need a MAC Authenticating Code .(get it from Favil or your provider)
Display <invalid MAC >,that means the FV8010 can not work normally.

Three models (Static /DHCP/PPPoE) are paratactic. Users can set the right model base on actual requirements.

● WAN Port static mode configuration

Default network config is DHCP model; Users need to set below parameters



IP Address	WAN IP address
Netmask	Network mask

Gateway	Default gateway IP address
DNS Domain	Option configuration
Primary DNS	IP address for primary Domain Name Server
Alter DNS	Option configuration

Click "Apply" button after finished above setting, IP Phone will save the setting automatically with immediate effect.

If users visit FV8010 thru WAN, user need to know the FV8010 WAN port ip address . (on normal phone operation : #*111# for hear FV8010 saying IP)

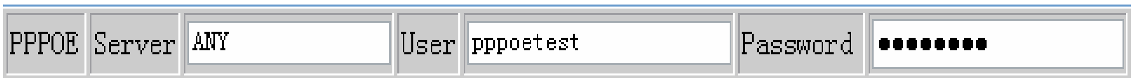
- **WAN port DHCP mode configuration**

Select "DHCP" on below single option, IP Phone will auto-config the WAN parameter with immediate effect.

- **WAN port PPPoE mode configuration**

Select "PPPOE" on below single option,

Set below parameter of PPPOE mode

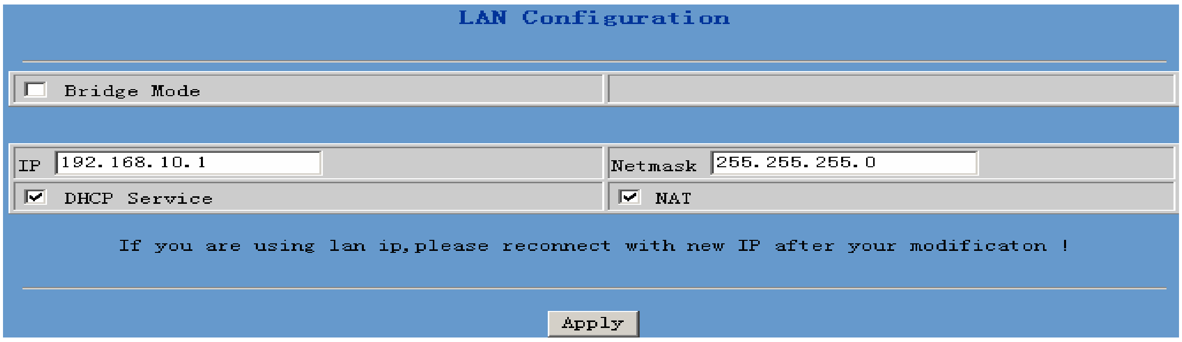


Server	**If ISP no special requirements, remains default setting**
User	Provided by ADSL ISP
Password	Provided by ADSL ISP

Click "Apply" button after finished above setting, IP Phone will auto-config the WAN parameter with immediate effect. The setting of WAN is still effective and enables IP Phone to connect to internet.

4.5.2 LAN Configuration

This web page displays the LAN parameter configuration. Please note once the bridging mode is selected, the LAN configuration will be no longer effective.



Configuration Example

- **Config LAN: generally config one private IP address**

IP	LAN IP address
Netmask	Network Mask

- **Start LAN DHCP Service and NAT or not: default setting is start**

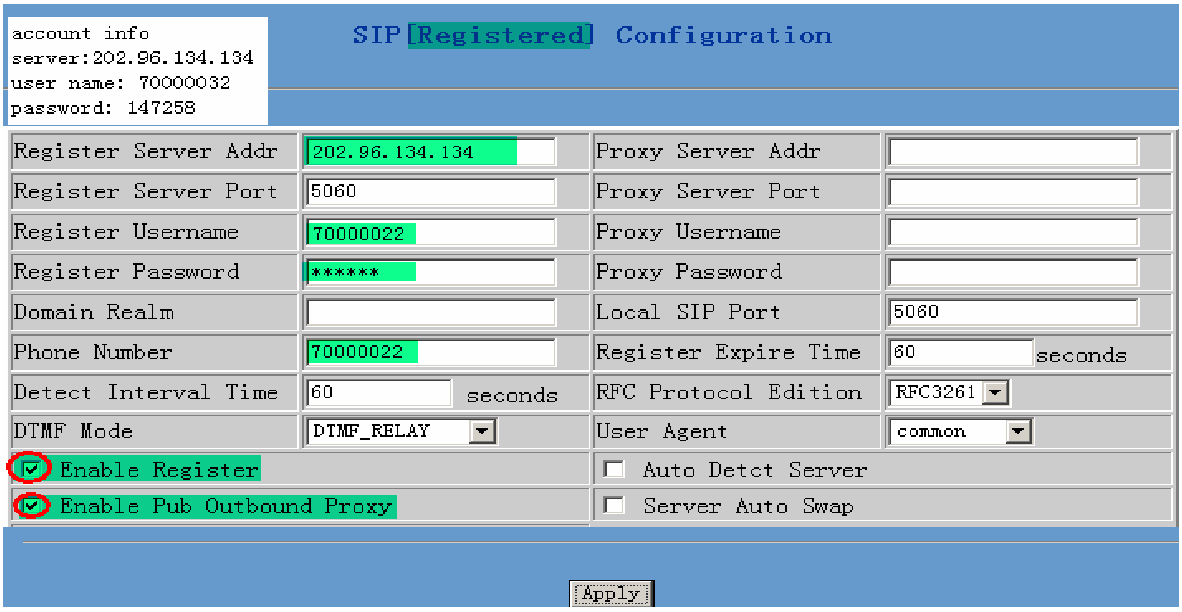
Start Bridge Mode or not（transparent mode）: Once start Bridge Mode, some parts of LAN config will be disabled, and the phone will no longer set IP address for LAN physical port， LAN and WAN will join in the same network;

4.6 VOIP Configuration

This section is to config signaling protocol for the SIP Server and Client.

4.6.1 SIP 1 configuration

User can configure specific parameter of SIP1 on this page;



Definition of each parameter described as below

SIP[Unregistered] Configuration	SIP register state; if register successfully, show "Registered" in the square bracket, otherwise show Unregistered
Register Server address	Set SIP register server IP address
Proxy Server addr	Set proxy server IP address (usually SIP will provide the same configuration of proxy server and register server, if different(such as different IP addresses), then each server's configuration should be modified separately)
Register Server Port	Set SIP register server signal port
Proxy Server Port	Set SIP proxy server signal port
Register Username	Set SIP register server account username (Usually it is the same with the config port number)
Proxy Username	Set the SIP proxy server account username
Register Password	Set password of SIP register server account
Proxy Password	Set password of SIP register account
Domain Realm	Enter the sip domain if any, otherwise FV8010 will use the proxy server address as sip domain. (Usually it is same with registered server and proxy server IP address).
Local SIP Port	Set local signal port, the default is 5060
Phone Number	Set assigned phone number
Register Expire Time	Set expire time of SIP server register, default is 120 seconds
Detect Interval Time	Set detection interval time of server, default is 120 seconds
RFC Protocol Edition	Enable the phone to use protocol edition. When the phone need to communicate with phones using SIP1.0 such as CISCO5300 and so on, need to modify into RFC2543. the default is to RFC3261;
DTMF Mode	Set DTMF sending mode, support RFC2833, DTMF_RELAY (inband audio) and SIP info
User Agent	Set the user agent if have, default is common

Enable Register	Configure enable/disable register
Auto Detct Server	Co-work with Server Auto Swap and Detect Interval Time. Enable this option, FV8010 will periodically detect whether the public SIP server is available, if the server is unavailable, the FV8010 will switch to the back-up SIP sever, and continue detecting the public sip server. FV8010 will switch back to the primary SIP server if the server is available again.
Enable Pub Outbound Proxy	Configure to enable to use public outbound proxy，if you have no stun server , advise to enable the option
Server Auto Swap	Configure main and backup auto-swap server； if the phone enables main and backup server function， the automatic detection and auto-swap functions should both be chosen

After finished the aforesaid network and VoIP configurations on the phone and network communication has been implemented，the user can make VoIP calls by the calling register and proxy server.

Note:

Some ISP internet may inhibit the phone to register and cancel the register in process, so user had better cancel apply or register soon and then submit registration repeatedly. Server may stop response of dialogue machine, then the phone receives no register/cancel login request and registration state will show incorrectness!

Configuration Example

Firstly users should get the account info from VOIP Service Provider (Including Server IP address, port, username, password etc.) and follow below procedure.

- **Config registered server and proxy server IP address and signaling port. (Support DNS for registered server and proxy server)**

Register Server Addr	10.1.1.139	Proxy Server Addr	192.1.1.139
Register Server Port	5060	Proxy Server Port	5060

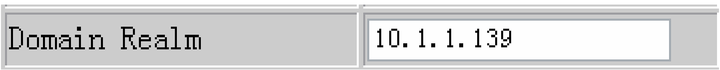
- **Config the username and password for registered server and proxy server.**

Register Username	client	Proxy Username	client
Register Password	••••	Proxy Password	••••

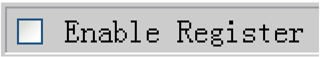
- **Config the phone number (Usually phone number is same with SIP account)**

Remark: due to the above register username is "client", so the phone number is different from SIP account)

- **Config the domain realm (Usually it is same with registered server and proxy server IP address, Let it be blank)**



- **Select below two option and registered in local outbound public proxy**



&

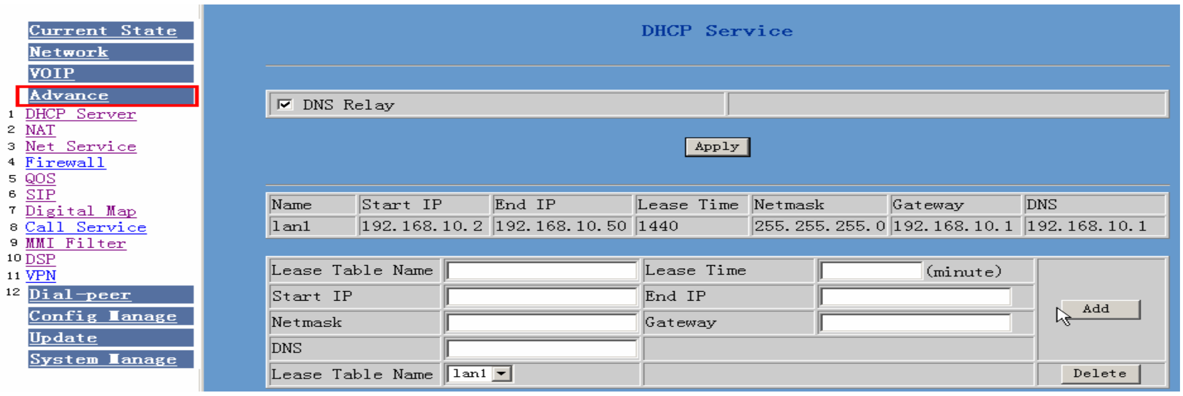

Usually these two option need to be selected, when you want to use SIP1.

4.7 Advance

4.7.1 DHCP server configuration

When FV8010 work as a router, This config is for network device which connect to FV8010 LAN port.

DNS Relay: DNS relay acts as a forwarder between the DNS Clients and the DNS Servers, DNS relay is designed for home/office networks where the users might want to dial into more than one Internet Service Provide (ISP)



DHCP server manage page.

User may trace and modify DHCP server information in this page.

DNS Relay: **enable DNS relay function.**

User may use below setting to add a new lease table.

Lease Table Name: **Lease table name.**

Lease Time: **DHCP server lease time.**

Start IP: **Start IP of lease table.**

End IP: **End IP of lease table. Network device connecting to the FV8010 LAN port can dynamic obtain the IP in the range between start IP and end IP.**

Netmask: **Netmask of lease table.**

Gateway: **Default gateway of lease table**

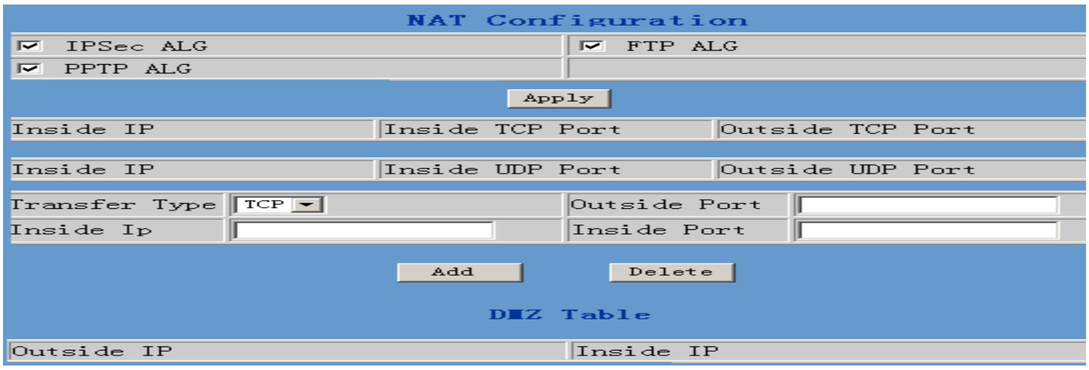
DNS: **Default DNS server of lease table.**

Notice: This setting won't take effect unless you save the config and reboot the device

4.7.2 NAT Configuration

This page is for NAT configuration, such port forward, DMZ.

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets. With NAT, the inside network continues to use its existing private or obsolete addresses. These addresses are converted into legal addresses before packets are forwarded onto the outside network.

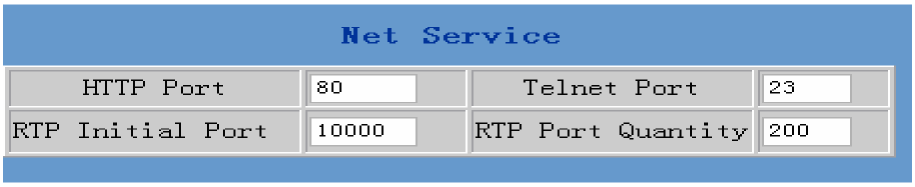


Advance NAT setting. Maximum 10 items for TCP and UDP port mapping.

IPSec ALG: **Enable/Disable IPSec ALG;**
FTP ALG: **Enable/Disable FTP ALG;**
PPTP ALG: **Enable/Disable PPTP ALG;**
Transfer Type: **Transfer type using port mapping.**
Inside IP: **LAN device IP for port mapping.**
Inside Port: **LAN device port for port mapping.**
Outside Port: **WAN port for port mapping.**

Click Add **to add new port mapping item and** Delete **to delete current port mapping item.**

4.7.3 NAT service configuration



4.7.3.1

Configure 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 . you change the port value to 8090, the accessing address is http://192.168.1.70:8090
But if the value is 0, that imply it can't be configured by web browser.

4.7.3.2

Configure telnet port，the default is 23 port. You can change the value to others .
Example: The ip address is 192.168.1.70 . you change the port value to 8023, the accessing address is telnet 192.168.1.70:8023

4.7.3.3

RTP Initial Port	10000

Enable RTP initial port configuration. It is dynamic allocation.

4.7.3.4

RTP Port Quantity	200

Configure the maximum quantity of RTP port. The default is 200；

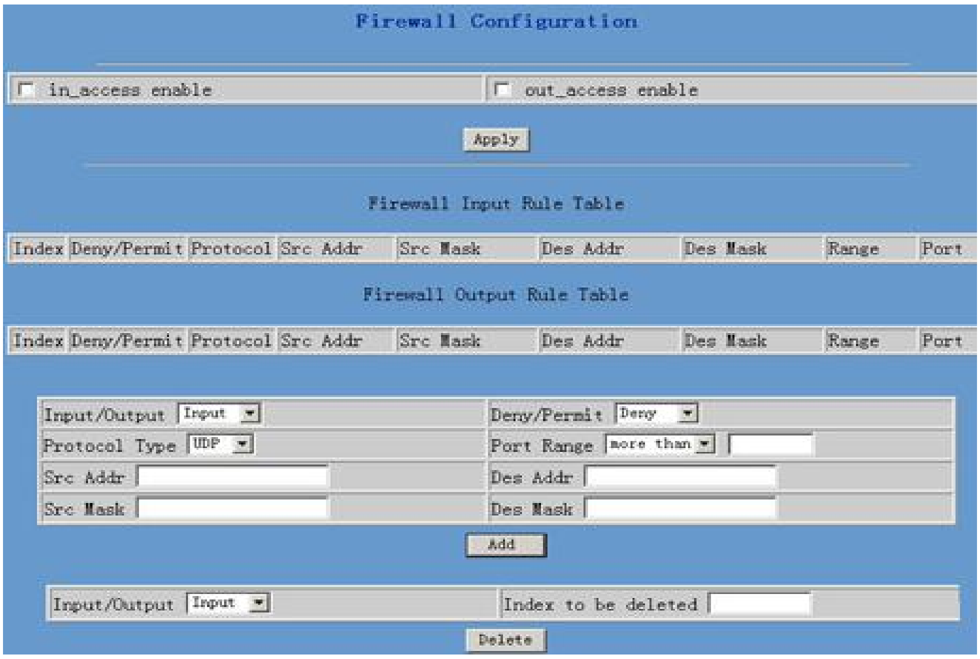
Leased IP Address	Client hardware Address

Leased IPMAC correspondence table of DHCP.The table will display all device getting ip address from FV8010 LAN port by DHCP .

Note ***The configuration on this page needs to be saved after modified and will go into effect after restarting.If the Telnet, HTTP port will be modified, the port is better to be set as greater than 1024,because the 1024 port system will save ports.***

※Set the HTTP port as 0， then the http service will be disabled.

4.7.4 Firewall



Firewall setting page. User may set up firewall to prevent unauthorized Internet users from accessing private networks connected to the Internet (input rule), or prevent unauthorized private network devices to access the internet.

Access list support two type limits: input access limit or output access limit. Each type supports 10 items maximum.

FV8010 firewall filter is base WAN port. So the source address or input destination address should be WAN port IP address.

Configuration:

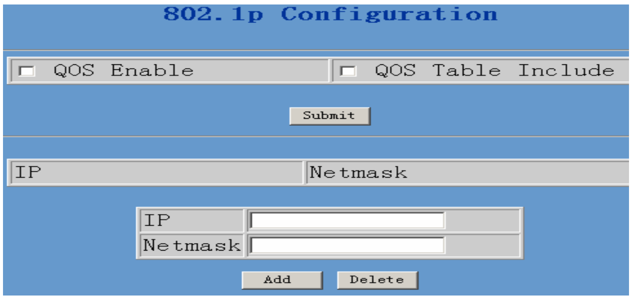
in access enable **Enable in access rule**
out access enable **Enable out access rule**
Input/Output: **Specify current adding rule is input rule or output rule.**
Deny/Permit: **Specify current adding rule is deny rule or permit rule.**
Protocol Type: **protocol using in this rule: TCP/IP/ICMP/UDP.**
Port Range: **port range if this rule**
Src Addr: **Source address. Can be single IP address or network address.**
Dest Addr: **Destination address. can be IP address or network address.**
Src Mask: **Source address mask. Indicate the source is dedicate IP if set to 255.255.255.255. Otherwise is network ID**
Des Mask: **Destination address mask. Indicate the source is dedicate IP if set to 255.255.255.255. Otherwise is network ID**

Example:
Intention: Computer A cannot ping computer B
Computer A connect with FV8010 LAN port
Computer A IP address is 192.168.10.2
FV8010 WAN port IP address is 192.168.0.187
FV8010 LAN port IP address is 192.168.10.1
Computer B IP address is 192.168.0.200
FV8010 firewall config

Index	Deny/Permit	Protocol	Src Addr	Src Mask	Des Addr	Des Mask	Ra
0	deny	ICMP	192.168.0.187	255.255.255.255	192.168.0.120	255.255.255.255	mo th

Input/Output	Output	Deny/Permit	Deny
Protocol Type	ICMP	Port Range	more than 0
Src Addr	192.168.0.187	Des Addr	192.168.0.120
Src Mask	255.255.255.255	Des Mask	255.255.255.255

4.7.5 QOS 802.1p Configuration



QoS Control based on 802.1p for different IP users. The QoS is used to mark the network communication priority in the data link/MAC sub-layer. FV8010 will sorted the packets using the QoS and sends it to the destination. QoS provides service classes for accessing traffics in Internet.

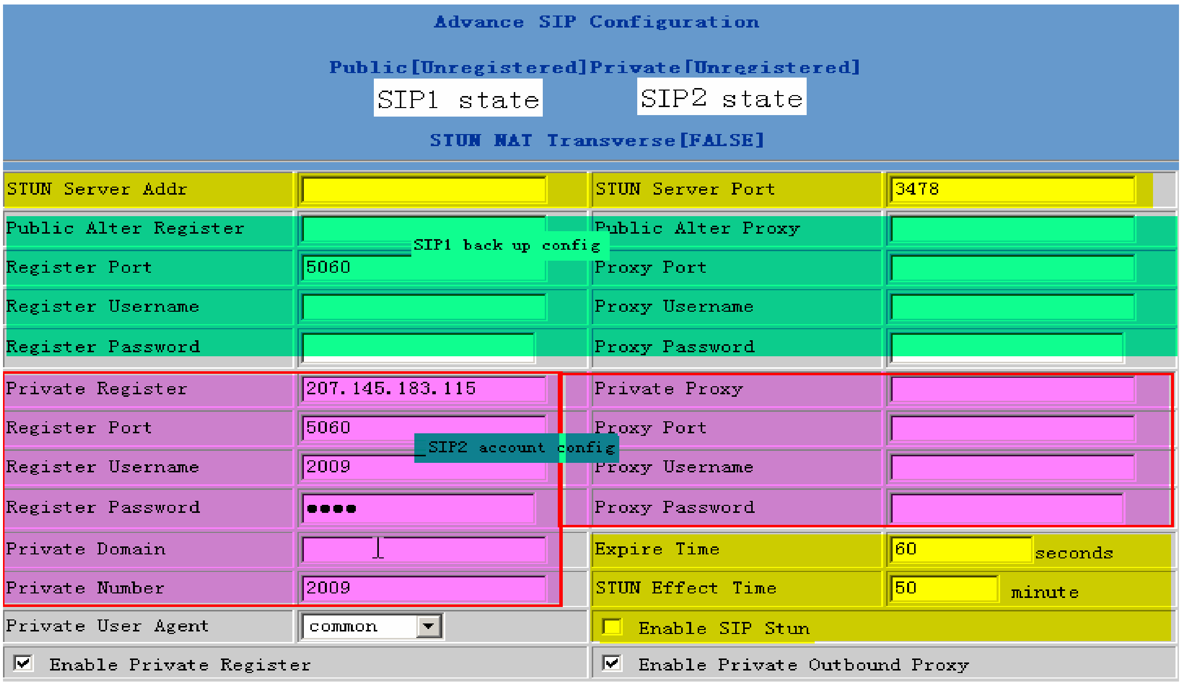
QoS Enable: **Enable QoS service.**

QoS Table: **Enable include QoS table, FV8010 will only provide QoS service to the network address included in the QoS table. Disable the option. FV8010 provides QoS service to the network address outside the QoS table.**

Delete **Enter the IP/MASK configure and select delete-to-delete corresponding item**

Add: **User can set the QoS Table using IP and Netmask. the IP can be network address (set netmask to 255.255.255.255)**

4.7.6 Advance



Public[Unregistered]Private[Unregistered]

To show the phone whether has been registered on public server or private server;

4.7.6.1 SIP STUN Configuration

STUN can support SIP terminal's penetration to NAT in the inner-net. In this way， as long as there is conventional SIP proxy and a STUN server placed in the public net, it will do; but STUN only supports three NAT modes： FULL CONE, restricted, port restricted.

STUN Server Addr	0.0.0.0

IF you have stun server .please input stun server address here.

STUN Server Port	3478

The STUN server default port is 3478

STUN Effect Time	minute

The unit is minute. if you have STUN server .please input interval time for STUN`S detection on NAT type.

☐ Enable SIP Stun

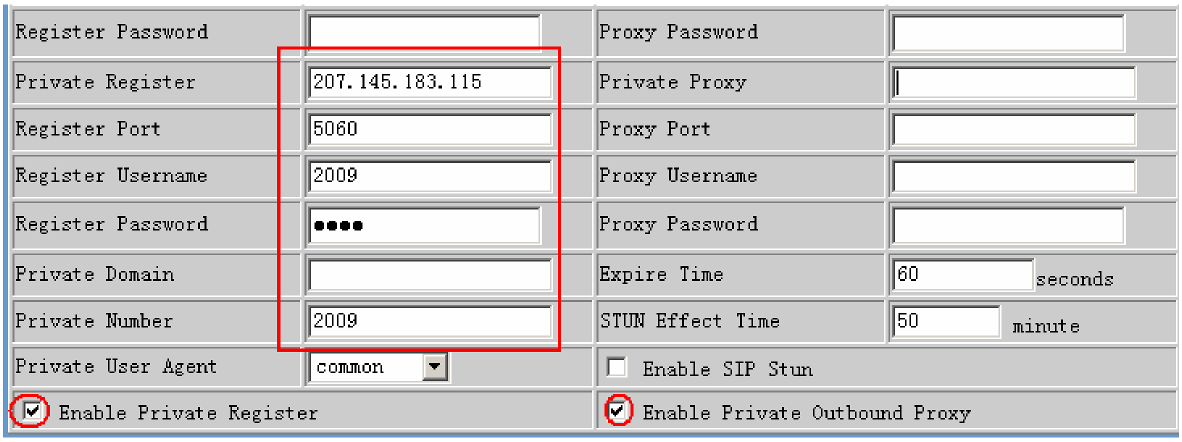
Configure enable/disable SIP STUN； if you have stun server .please enabe the option.

4.7.6.2 Public backup server configuration

Public Alter Register	10.1.1.11	Public Alter Proxy	0.0.0.0
Register Port	5060	Proxy Port	5060
Register Username	1234	Proxy Username	1234
Register Password	••••	Proxy Password	••••

the specific configuration parameter has the same meaning with public server. It should be noted that the username and password should be the same with the public main server.

4.7.6.3 Private server(SIP2) configuration.



Specific configuration parameter has the same meaning with public server.

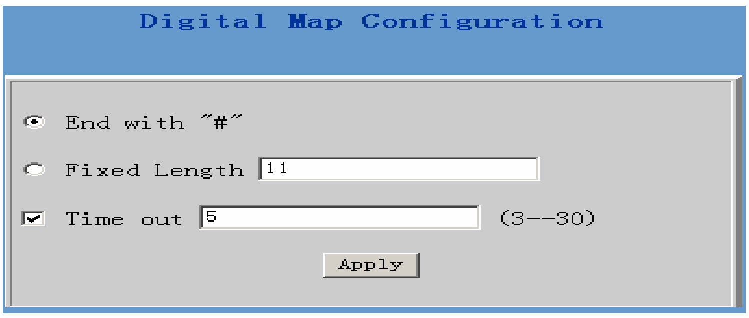
Configure permit/deny private server register；

Configure enable/disable private outbound proxy; if you have no stun server .advise to enable the option.

Note: about how to use SIP ,Please refer to the Dial peer chapter.

4.7.7 Digital map configuration

4.7.7.1 Fixed digital map



End With "#": **Use # as the end of dialing.**
Fixed Length: **When the length of the dialing match, the call will be sent.**
Timeout: **Specify the timeout of the last dial digit. The call will be sent after timeout**

4.7.7.2 User define flexible Digital map table

Digit map is a set of rules to determine when the user has finished dialing. Digital Map is based on some rules to judge when user end their dialing and send the number to the server. With digital map, users don't have to press '#' key or "call" key after dialing. If the number dialed matches some item in the digital map table, or it doesn't match with any item, this number will be sent out immediately. It is not like using dial peer . Using digital map won't change the number dialed, the number sent is the same as the number dialed.

X **Represents any one number between 0 and 9.**

Tn **Represents the last digit timeout. here [n] represents the time from 0~9 second, it is necessary. Tn must be the last two digits in the entry. If Tn is not included in the entry, we use T0 as default, it means system will sent the number immediately if the number matches the entry.**

. **(Dot) represents any number and no length limit.**

[ ] **Number location value range . It can be a number range(such as [1-4]), or number is separated by comma such as [1,3,5],, or use a list such as [234]**

Example:

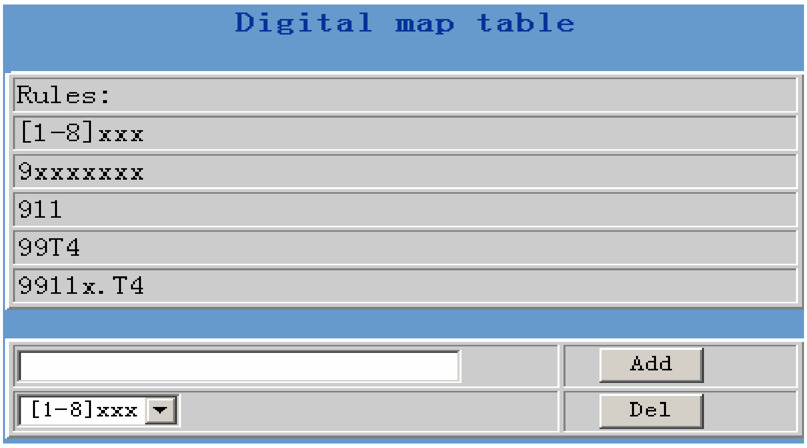
[1-8]xxx **Any 4 digits number between 1000 and 8999 sending out immediately**

9xxxxxxx **any 8 digits number starting with 9 sending out immediately**

911 **after finishing dialing 911 ,it will send out immediately**

99T4 **after finishing dial 911, it will send out in 4 second**

9911x.T4 **any more than 5 digits length starting with 9911, sending out in 4 second .**



Using digital map can be combined with dial peer . First digital map will determine when the user finished dialing, then convert this number to the number actually sent according to "dial peer table ".

Dial-Peer

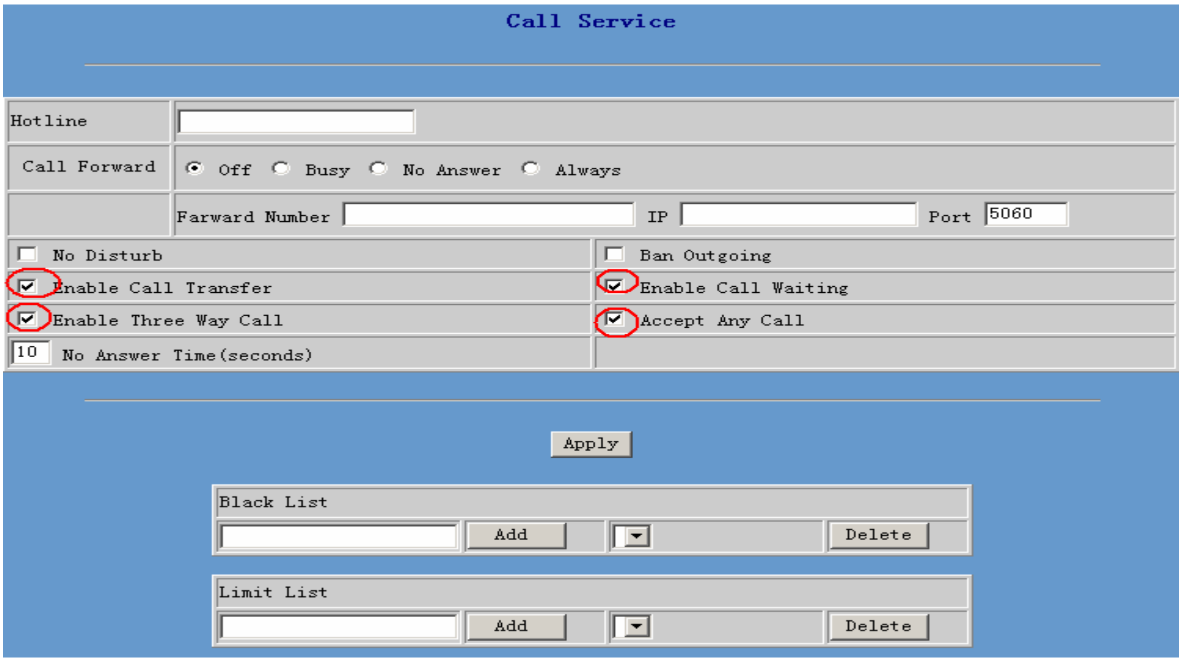
Number	Destination	Port	Alias	Suffix	Del length
2887	192.168.0.155	5060	no alias	no suffix	0
98765432	192.168.0.155	5060	no alias	no suffix	0
911	192.168.0.155	5060	no alias	no suffix	0
99	192.168.0.155	5060	no alias	no suffix	0
9911234	192.168.0.155	5060	no alias	no suffix	0

When user dial 2887 or 98765432、911 、99 、9911234, they will send out immediately. (digital map with dial peer)

4.7.8 Call Service Configuration

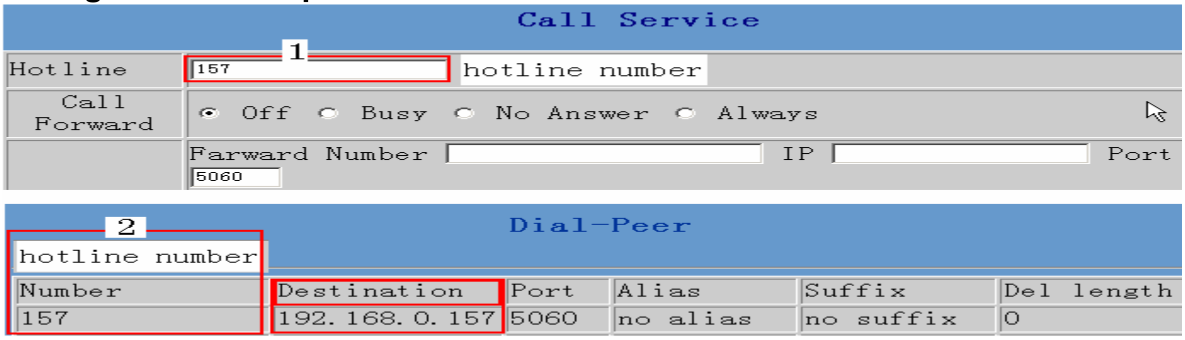
Value added service configuration

On this page, user can set value added services such as hot-line, call forwarding, call transfer (CT), call-waiting service, three way call, blacklist, out-limit list and so on.



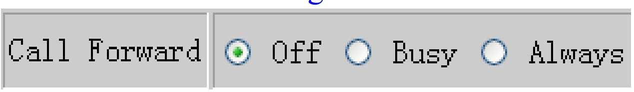
4.7.8.1 Hotline

Configure hot-line number of the port. With this number of the port，this hot-line number will be dialed automatically as soon as off-hook and user can's dial any other number. If you do not use hotline , please let it be blank. Configuration example:



4.7.8.2 Call feature

4.7.8.2.1 Call forwarding.



Call forward default is Disabling. when Off is selected，if the number dialed is engaged after the phone has received a call, then it will automatically transfer to the configured number according to the following picture (CF001) configuration. when No Answer is selected，if the phone do not receive the incoming call .it will automatically in 10 No Answer Time(seconds) forward to the configured number according to the following picture (CF001 forward) configuration. when Always is selected，then the phone will directly transfer all incoming call to the number that had configured in advance like the picture showing.

Picture:CF001

Note:

1 Number can be sip server extension number or DID number (any PSTN number)

2 the function has no relationship with the option Enable Call Transfer that enable or disable

If it is enabled . the phone will not ring when there is a incoming call . DND, do not disturb, enable this option to refuse any calls.

☐ Ban Outgoing

Enable this to forbid outgoing calls.

10 No Answer Time(seconds)

The unit is second. no answer call forward time setting.

4.7.8.2.2 Call Waiting configuration

☑ Enable Call Waiting

Configure enable/disable call waiting service; After it is enabled, user hold calls of the other party by <FLASH >button, by pressing <FLASH >button again, the call can go back to the previous call. If you want to use three way conference , this option must be enabled.

4.7.8.2.3 Call transfer configuration

☐ Enable Call Transfer

It is for enabling or disabling If it is enabled, when user A are talking with user B , A press <FLASH> button on the normal phone ,After dialing dial * then dial the third party number (C user) directly. the phone will transfer the calls to C. The result is C phone will ring (A will hang up) . User C pick up phone then user B will talk with C .
Operating process :

<FLASH> button +* + **third party number**

Example:
A are talking with B .

A click FLASH button (holding B line). then dial * **user C number** .

4.7.8.2.4 Three-way conference call

☐ Enable Three Way Call

Configure enable/disable three way call; When user A are talking with user B as the call origination, user A click <FLASH> button on the normal phone to hold user B line and then dial the third party user C. **after A talk with C** **, User A click<FLASH> button again to recover the talk with user B. At this**

time user A press * key to make C into the three way conference .

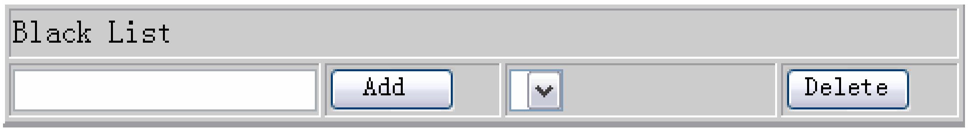
Operating process :

<FLASH> button + third party number + <FLASH> button + *

Example:
A are talking with B .
A click FLASH button (holding B line) .then dial C number .
A will talk with C .

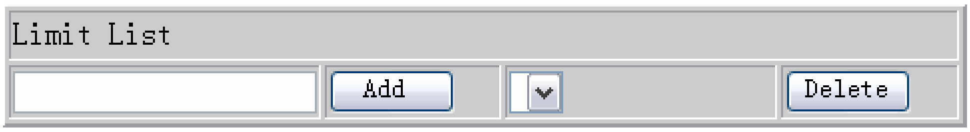
A click FLASH button again (holding C line), and A dial *
A 、B、 C make the three party conference sucessfully now

4.7.8.2.5 Black List



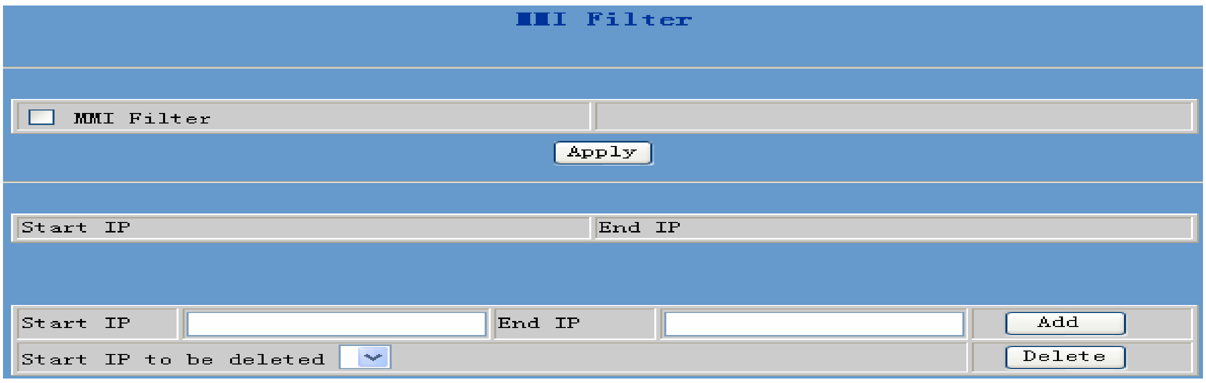
Incoming call in these phone numbers will be refused. It is for precluding incoming communication like Call ID. If user don't want to answer a certain phone number, please add this phone number to the list, and then this number will be unable to get through the phone.

4.7.8.2.6 Limit list



Outgoing calls with these phone numbers will be refused for example, if user don't want the phone to dial a certain number, please add the number to this table, and the user will be unable to get through this number.

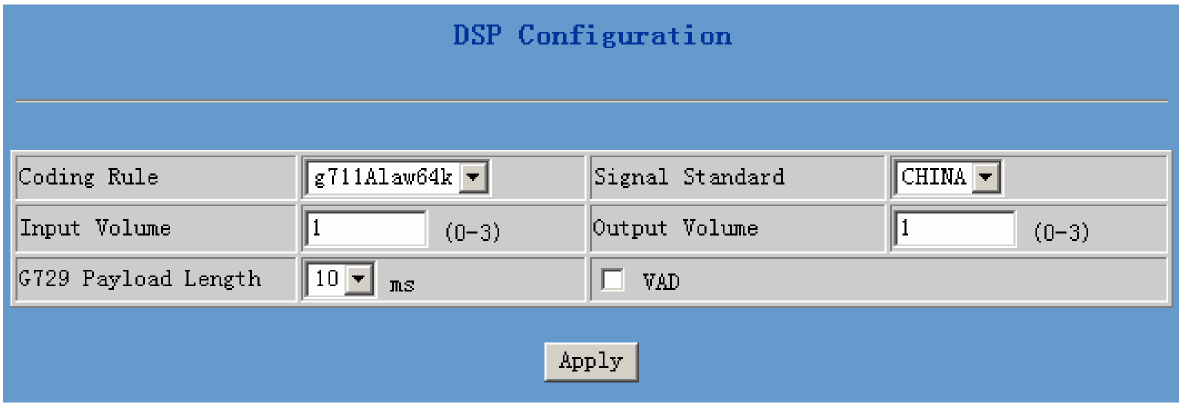
4.7.9 MMI Filter



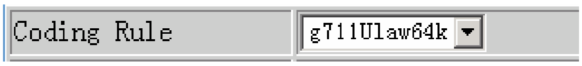
MMI filter is used to make access limit toFV8010.
When MMI filter is enable. Only IP address within the start IP and end IP can access FV8010.

4.7.10 DSP configuration

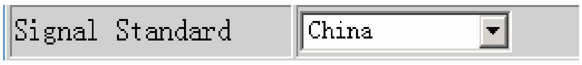
On this page, user can set speech coding，IO volume control, cue tone standard, caller ID standard and so on.



Configuration Explanation:



Configure Coding Rule according to network bandwidth; support G.711a/u G.729



Congfigure Signal Standard according to country's phone voice;

Normally, G729 Payload Length don't need be changed into 10 ms;

Handset out volume.

4.8 Dial peer

Number IP table configuration

Function of number IP table is one way to implement the phone's calling online, and the calling of the phone will be more flexible by configurating the number IP table. For example, user know the other party's number and IP and want to make direct call to the party by point-to-point mode: the other party's number is 1234, make a configuration of 1234 directly ,then the phone will send the called number1234 to the corresponding IP address; Or set numbers with prefix matching pattern, for example, user want to make a call to a number in a certain region (010), user can configure the corresponding number IP as 010T— protocol— IP, after that, whenever user dial numbers with 010 prefix(such as 010－62201234),the call will be made by this rule.

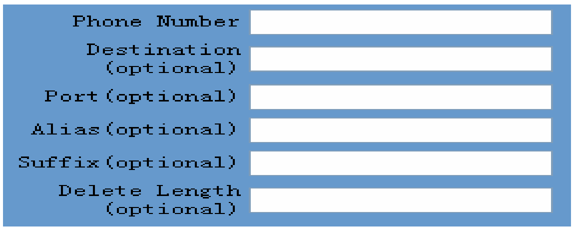
Bases on this configuration, we can also make the phone use different accounts and run speed calling without manual swap. When making deletion or modification, select the number first and click load, then click Modify and complete the operation.

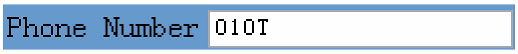
Display of calling number IP image list.

Dial-Peer

Number	Destination	Port	Alias	Suffix	Del length
157	192.168.0.157	5060	no alias	no suffix	0
187	192.168.0.187	5060	no alias	no suffix	0
9T	255.255.255.255	5060	del	no suffix	1
8T	0.0.0.0	5060	all:0755	no suffix	0
010T	0.0.0.0	5060	rep:8610	no suffix	3
6T	192.168.0.187	5060	no alias	12345	0
741	192.168.0.187	5060	no alias	999	0

Click Add, the following figure will be shown at the lower part of the page.





It is to add outgoing call number, there are two kinds of outgoing call number setup: One is exactitude matching, after this configuration has been done, when the number is totally the same with the user's calling

number, the phone will make the call with this number's IP address image or configuration; Another is prefix matching(be equivalent to PSTN's district number prefix function), if the previous N bits of this number are the same with that of the user's calling number(the prefix number length), then the phone will use this number's IP address image or configuration to make the call. When configurating the prefix matching, letter "T" should be added behind the prefix number to be distinguished from the exactitude matching.

Call Mode sip

Configure the calling line route: SIP and lifeline

Destination 192.168.10.11

Configure destination address, if it is point-to-point call, then input the opposite terminal's IP address, it can also be set as domain name and resolved the specific IP address by DNS server of the phone. If no configuration has been made, then the IP will be considered as 0.0.0.0. This is an optional configuration item.

Port(optional)

Configure the other party's protocol signal port, this is optional configuration item: when nothing is input, then the default of h323 protocol is 1720, the default of sip protocol is 5060; lifeline required no configuration of this item, shown as 0.

Alias(optional)

Configure alias, this is optional configuration item: it is the number to be used when the other party's number has prefix; when no configuration has been made, shown as no alias.

add:	xxx	add xxx before number. in this way it can help user save the dialing length;
all:	xxx	the number is all replaced by xxx; speed dialing can be implemented, for example, user configure the dialing number as 1, with the configuration "all" the actual calling number will be replaced;
del		delete n bit in the front part of the number, n can be decided by the replacing length this configuration can decide the protocol for appointed number
rep:	xxx	n bit in the front part of the number will be replaced. n is decided by the replacing length.

Suffix(optional)

Configure suffix, this is optional configuration item: it is the additive dial-out number behind the number; when no configuration has been made, shown as no suffix;

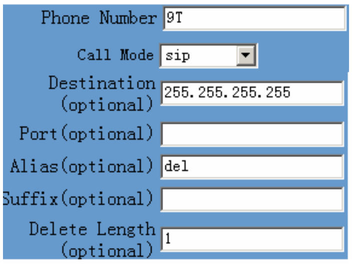
Example 1

T mean any length digit number.

Destination is 255.255.255.255 that mean calling out through SIP2 server.

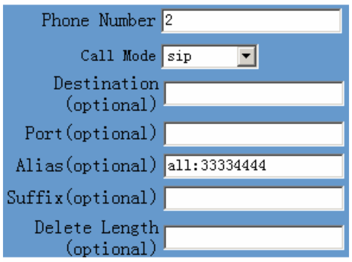
Destination is 0.0.0.0 that mean calling out through SIP1server

Config page | **Explaination** | **Example**



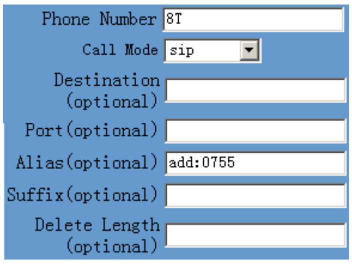
That means Any digits number starting with 9 pass throught SIP2 server.
Here alais is del
Delete Length is 1 that means the phone will delete the first number before send number to server

User dial 93333
SIP2 server receive 3333



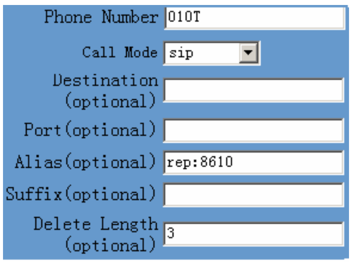
It can be used for speed calling
The number user dialed will be replaced fully by the number that is behind all:)
Here alias is all: (not all)

User dial 2
Sip1 server receive 33334444



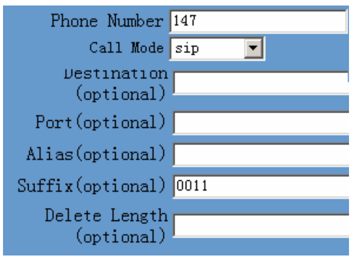
It can be used to add local area or prefix.before sending out.
It saves user dialing number .
Here alias is add: (not add)

User dial 8309
SIP1 server receive07558309



user want to dial PSTN（010 6228）by SIP1，while actually the called number should be 86106228，then we can configure called number as 010T, then rep：8610，and then set the replacing length as 3. So that when user make a call with 010 prefix, the number will be replaced as 8610 plus the number and then sent out.
Relace the number that user dialed before sending to SIP1 server.
Here alias is rep:(not rep)

User dial 010 6228
SIP1 server receive8610 6228



this is optional configuration item.it is to add number behind the number user had dialed. when no configuration has been made, shown as no suffix

User dial 147
Sip1 server receive 147 0011

Example 2

Dial-Peer

Number	Destination	Port	Alias	Suffix	Del length
20T	0.0.0.0	5060	no alias	no suffix	0
200T	255.255.255.255	5060	no alias	no suffix	0

When user dial 200 , It will pass through SIP2
When user dial 2009 , It will pass through SIP2
When user dial 20096, It will pass through SIP2
When user dial 201, It will pass through SIP1
When user dial 20, It will pass through SIP1

Example 3 (about lifeline)

Dial-Peer

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

Image of *T means when user connect PSTN line to the lifeline port, user could make PSTN call by add a "*" before the calling number.

Digital map table

Rule:
1
22
*

	Add
22	Delete

Dial-Peer

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

Add Delete Modify *T

Phone number = *T Call mode =lifeline When user dial * ,there is a second dial tone from the pstn line . then dial as directly using PSTN line.
Phone number = 1 Call mode =lifeline When user dial 1 ,there is a second dial tone from the pstn line . then dial as directly using PSTN line.
Phone number = 22 Call mode =lifeline When user dial 22,there is a second dial tone from the pstn line . then dial as directly using PSTN line.

Example 4

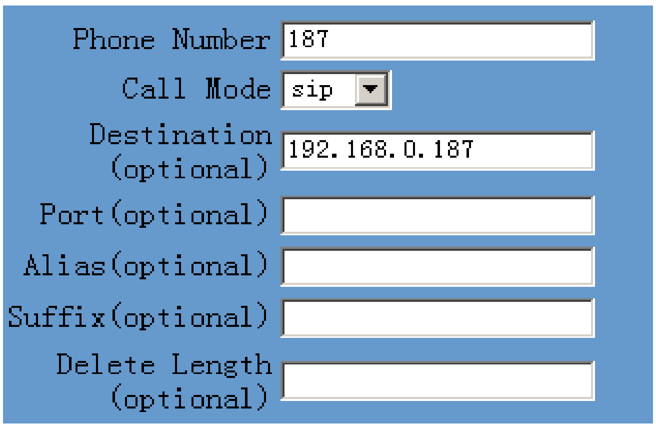
IP to IP calling

"Peer to Peer" calling mode: direct make calls and no need to set phone number thru proxy server (user could refer to Dial peer setting on web configuration charter).The phone should be operated under following condition (satisfy one option)

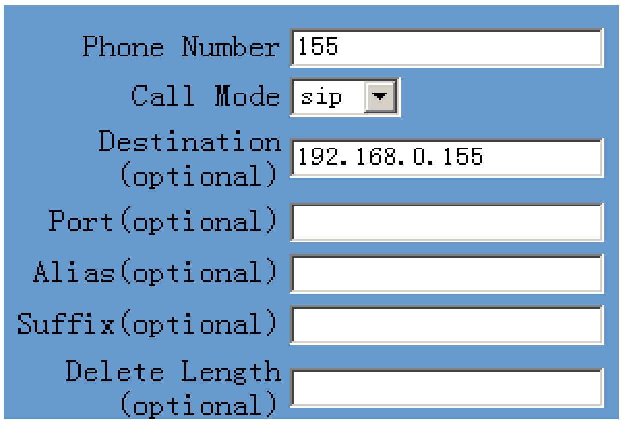
- **Requirement 1 both two FV8010 are assigned the public IP address individually**
- **Requirement 2 both two FV8010 using private IP address should be on the same LAN.**

If A dial number 187 , A can talk with B . If B dial number 155 , B can talk with A

A phone IP address 192.168.0.155
in dail peer config page



B phone IP address 192.168.0.187
in dail peer config page



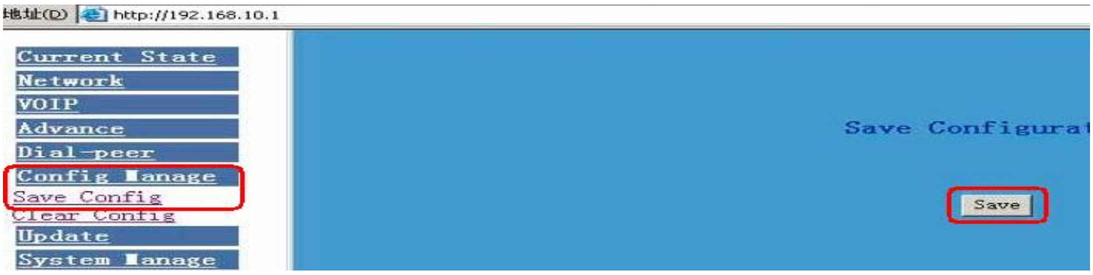
4.9 Config Manage (Save and Clear configuration)

Notice: clear config in admin mode, all settings restores to factory default; clear config in guest modem, all settings except sip, advance sip restore to factory default.

4.9.1 Save Config

Once change is made, Users should save the modified configuration to take effect, otherwise the IP Phone will go back to the last saved setting after phone reboot.

The interface of "Save Config" as below, please follow the four steps below to config.



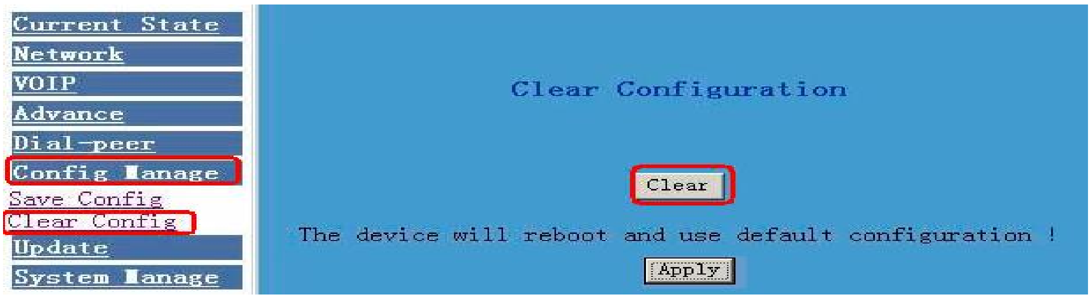
Enter "Config Manage" Menu →"Save Config" Submenu→ Click "Save" Button→ Return to "Current State" Web page

4.9.2 Clear Config

There are four method to clear config(set factory default), web 、telnet 、post mode、keypad.If the IP Phone doesn't work properly after modifying config, users can clear all modified config on "Clear Config" web page. The phone will clear all modified config and restore the default factory configuration. (Default network type for WAN is DHCP mode; default LAN IP address is 192.168.10.1)

Process Please follow the below steps to clear config:

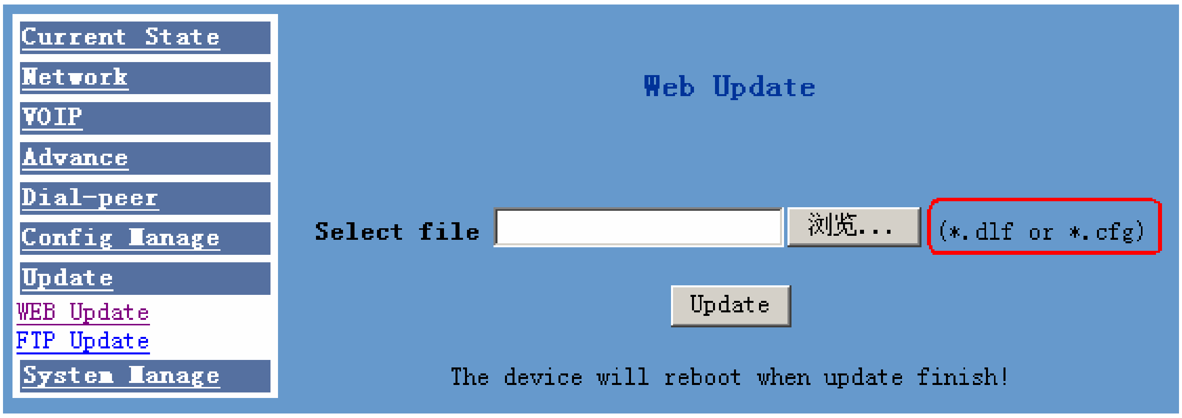
Enter "Config Manage" Menu →"Clear Config" →Click "Clear" Button →show "Submit Success" info on screen →Click "Return" button



4.10 Firmware Upgrade

4.10.1 Web Update

On this page, user can select the upgrade document (firmware or config file) from hard disk of the computer directly to run the system upgrade. After upgrade completed， reset the phone and it will be usable immediately. **Firmware format is *.dlf** as suffix



STEP:

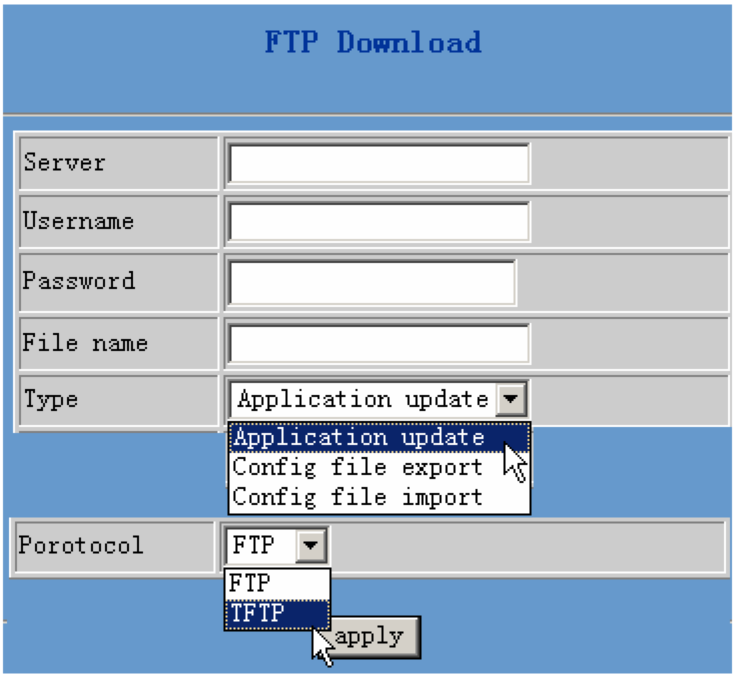
Enter Update menu →WEB Update submenu→ click “browse” button→ download upgrade document from hard disk (firmware or config file provided by manufacturer) → click “Update” button →reboot IP phone to go into effect

Note:

Under system upgrade progress, FV8010 may not be restarted normally due to some system reason (e.g. electricity shut off), users can re-download under post mode.

4.10.2 FTP and TFTP Update

Users can download upgrade documents or lead in configuration files thru FTP or TFTP mode. Please make sure export and import rights are authorized by FTP or TFTP server before using FTP update way.



Definition of each parameter described as below

Server	Set IP address for upload or download FTP/ TFTP server
Username	Set username of the upload or download FTP server. If user select TFTP mode, no need to input username and password
Password	Set upload or download of FTP server password
File name	Set file name for system upgrade documents or system configuration files. system file take .Z as suffix，configuration files take .cfg as suffix；
Type	Config export/import/upgrade file type [three options]: “Application update” is system documents upgrade “Config file export” is export configuration files to server “Config file import” is import configuration files to gateway
Protocol	Set transport protocol type [two options]:FTP and TFTP

STEP:

Enter Update menu →FTP Update submenu→ Config FTP/TFTP server → Config username and password of FTP server (if select TFTP mode, please skip this step) →key in file name → choosing file type from the dropdown menu→ choosing protocol type

Example: (export config file)

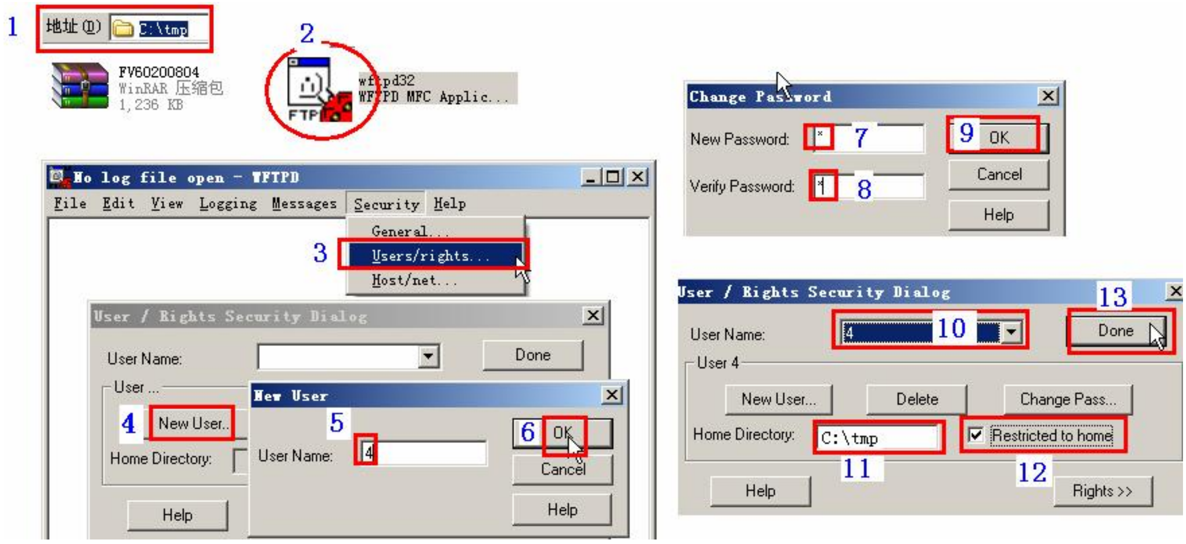
1 FTP

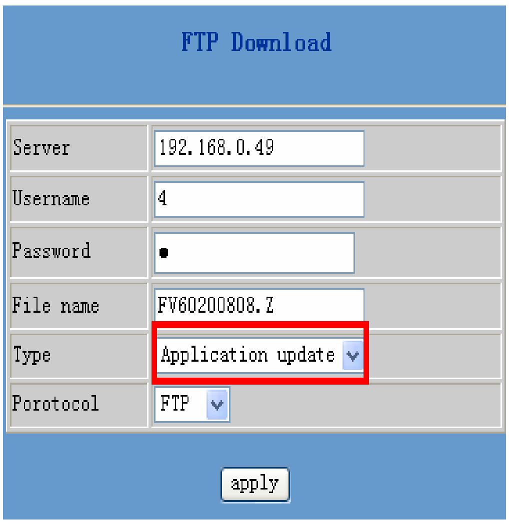
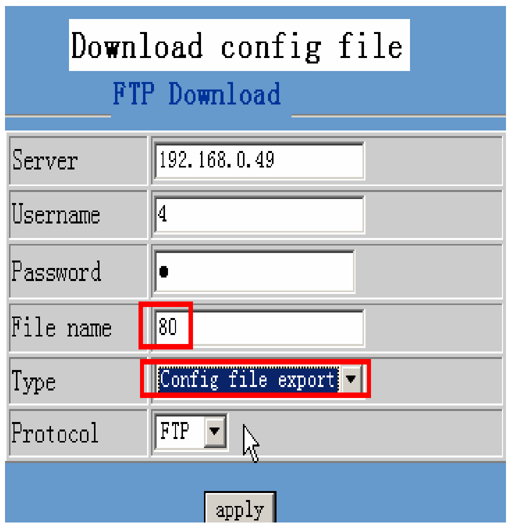
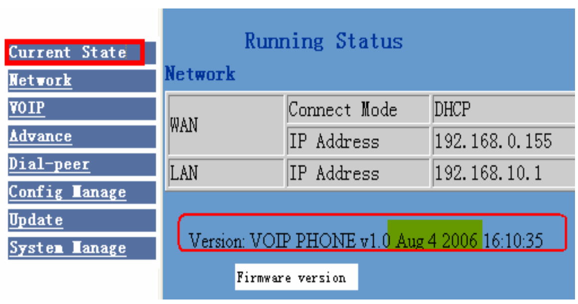
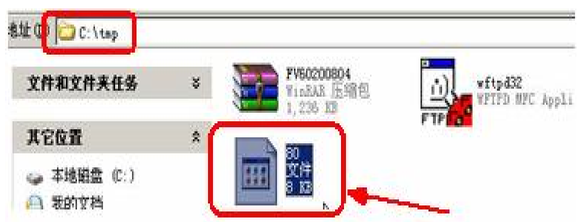
<1> Copy Wftpd32 software and FV8010 Firmware into a new Folder (example c:/tmp)

<2> Run wftd32.exe. Set a user name and password for FV8010 ftp

updating

The process is like the below picture showing from step 1 to step 13.

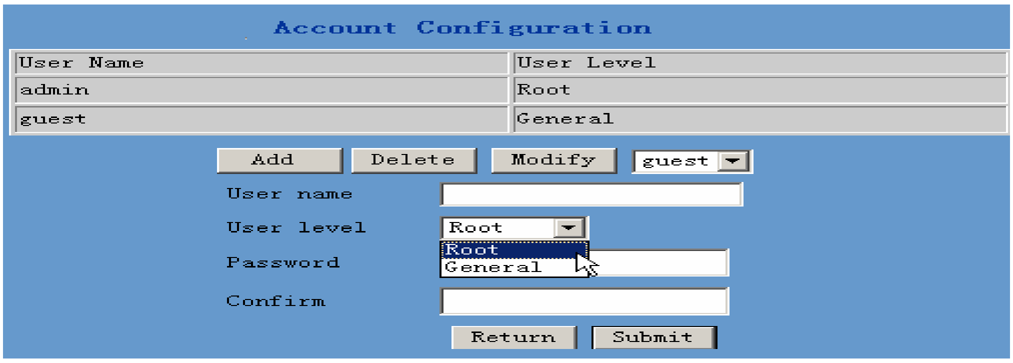


Update the firmware	Download config file to you PC
	
	
After it update successfully. You will find the new version in Current State	After you click apply , you can find the file that it had download to your pc <c:\temp>

4.11 System Manage

4.11.1 Account Manage (maximum 5 account)

Users can edit users (add or delete) account and modify existing users' authority on this web page.



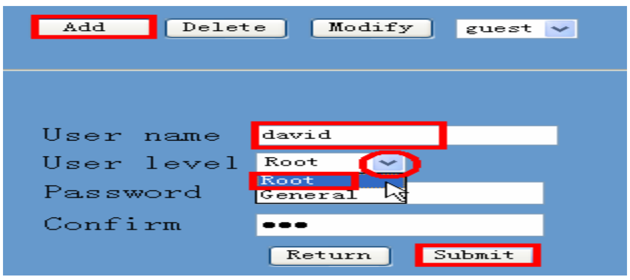
Definition of each parameter described as below

User Name	List existing phone user account name
User Level	Show existing user account level [two option]:Root and General: Root level users have the right to modify config; General level users have the right to read-only
Add	Add user account to IP phone
Delete	Delete increased user account
Modify	Modify increased user level and password

Operation Example

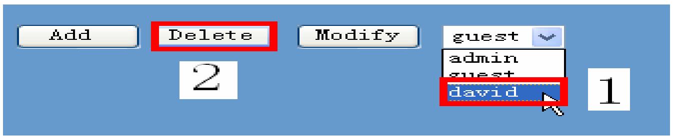
- **Add one new account**

Click "Add" button →input User name (No-Modify) →Choosing User level from dropdown menu →set new user password →confirm password →submit the new account info by clicking "submit" button →show "submit success" on screen →return to account configuration interface by clicking "Return" button



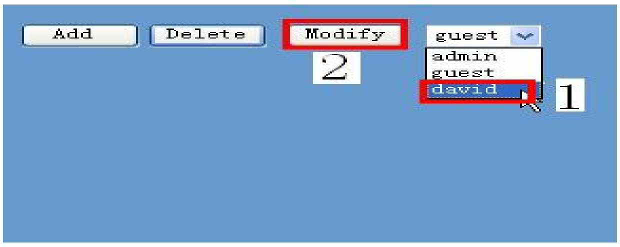
- **Delete increased account**

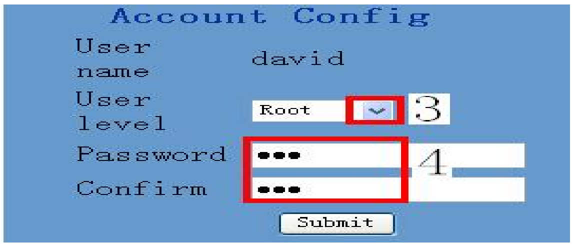
  Choosing the account need to del from dropdown menu→ Delete account by pressing "Delete button" →show "Submit Success" on screen



- **Modify increased account (For Root-level user account only)**

Choosing the modified account →enter below interface →modify user level or password →click "Submit" button to submit the modification



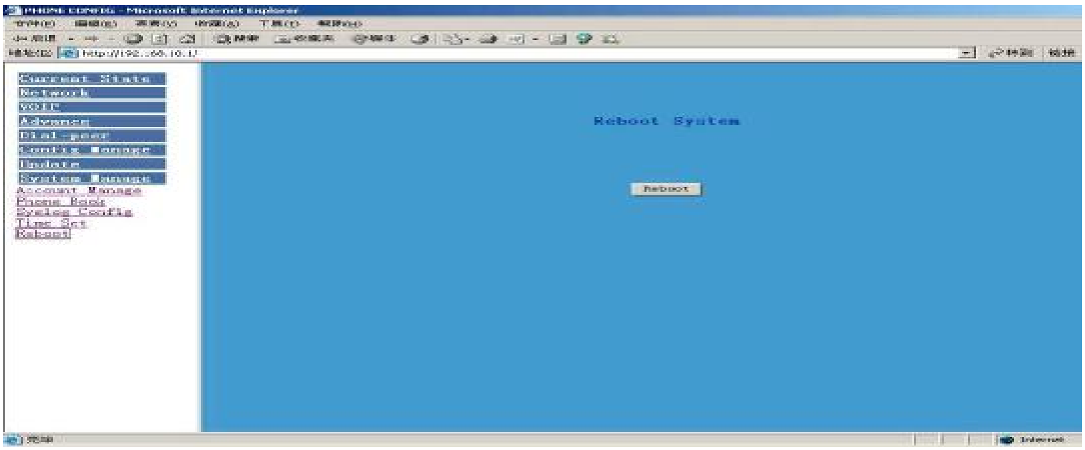


Owing to the phone's default account: accounts of the administrator level-admin account and the ordinary level－guest account are all weak account and weak password, the username and password will be easily to guess on public network, so the user had better modify the administrator and ordinary user.

Enter with manager level when making modification，create a administrator account and a browse account (you'd better not set the name as admin, administrator, guest, etc.)，set password and then save configuration，entering with new manager account, delete default manager and browse account and save configuration，security will be enhanced!

4.11.2.System Reboot

Once any change of phone configuration is made, users need to reset IP phone to go into effect. Users should save the modified configuration before system reboot, otherwise the phone system configuration will go back to last saved setting. The system reboot interface as below



5 Default Factory Setting

- **Gain IP address thru DHCP mode, WAN Port static IP is 192.168.1.179, LAN port IP is 192.168.10.1.Default is to start the DHCP service and NAT function.**
- **Default communication protocol is to use SIP, SIP port is 5060**
- **Default HTTP port is 80, Telnet port is 23**
- **Default number end is "#" button**
- **Default user account is admin and guest**

6 Configuration by phone

We have provided some command to config FV8010 by phone. We can connect one analog phone to "Phone" interface. We can input following command by Hand free or Handset.

Input #** Reboot Device;**
Input #*000 Clear configuration;
Input #*100 Gateway work at Static mode
Input #*101 Gateway work at DHCP mode
Input #*102 Gateway work at PPPoE mode
Input #*103 Gateway work at Bridge mode
Input #*104 Gateway work at Router mode
Input #*111 Get the IP address of Gateway by voice message
Input #*222 Get the Number of Gateway by voice message

7 Telnet configuration

7.1 Config Procedure

- Input command “cmd” on Run submenu under
  PC START menu, and then key in “telnet phone-IP-address
  enables users to config IP phone thru telnet.
- Input username and password, both default
  Username and password of Administrator account are “admin”
- Config IP Phone through command lines

Note:
1. *We suggest users to config IP Phone thru web browser instead of keypad or telnet.*
2. *After any change of configuration, please remember to make “write” command to save changes and then input “reload” command to reboot IP phone to take effect.*

7.2 Telnet basic Introduction

7.2.1 Basic structure

User may use telnet command to access and manage gateway.
FV8010 adopts tree structure for telnet. Every node contains its sub-nodes or local command. User can type “help” or “?” whenever to see sub-nodes and all local command under current node.
Besides local command, there are some global commands can be used in each node.

7.2.2 Basic command

Logout: exit telnet mode.
Write: save current settings.
Type sub-nodes name in current node to switch to sub-node.
Type “!” or “exit” in current node to return to parent-node.
Type “help” or “?” can see all sub-nodes and all local command under current node, every help item has comments such as <command> or <node> to distinguish sub-nodes and local command. Type “help” or “?” in command can see all parameters using in this command.
When typing node name or command, user no need to key the full name, use TAB button will make it more efficient.
There are two types in command parameters: optional and required. “required” parameter use “-” as prefix and “optional” use “_” as prefix. User may type “-” or “_” then press TAB button for complementarily.

7.3 Global Command

Global command is available under all nodes, FV8010 support following commands.

Command Name	Command function	Example
chinese	Set the language of help prompt info to Chinese	#chinese
clear	Clear screen	#clear
english	Set the language of help prompt info to English	#english
exit	Go back to upper level of node	#exit
help	1.Display help prompt info 2.Display all subnode under current node and local command	1． #help ping 2． #help
history	Display the history info for inputting command	#history
logout	Exit telnet config interface	#logout
ping	One test program using to check network or program availability	#ping www.google.com.
tree	Print out the tree structure of current node	#tree
who	Display current users login to PC	#who
Write	Save configuration to flash	#write
Reload	Reboot IP phone	#reload

Common Network command

Command Name	Command function	Example
ping	The same with above stated	#ping www.google.com
tracert	Print out the network path	#tracert www.google.com
show basic	Print current configuration status table	#show basic
show ip route	Print phone Router table	#show ip route
show ip arp	Print phone arp table	#show ip arp
show ip netstat	Run Netstat program	#show ip netstat
telnet	telnet another user host	#telnet 192.168.1.2
Set default	Clean phone configuration modification and restore default except network configuration	#setdefault
Set all default	Clean all configuration and restore default manufacturing setting	#setdefault all

7.4 Net configuration

7.4.1 LAN interface settings

Path: <config-interface-fastethernet-lan>#

Function	Command
[disable]enable bridge mode	[no]bridgemode
[disable]enable DHCP service	[no]dhcp-server
[disable]enable NAT	[no]nat
Show current DHCP rules	dhcpshow
Show LAN port IP address	ipshow
Show NAT info	natshow
Change LAN port IP address	ip –addr x.x.x.x –mask x.x.x.x

Example:

#config interfact fastethernet lan

<config-interface-fastethernet-lan>#ip –addr 192.168.1.10 –mask 255.255.255.0

7.4.2 WAN interface settings

path: <config-interface-fastethernet-wan>#

Function	Command
[disable]enable dhcp client	[no]dhcp
[disable]enable pppoe	[no]pppoe
[disable]enable QOS	[no]qos
Set default gateway IP	gateway x.x.x.x
Clear default gateway IP	no gateway
Set WAN port IP address	ip –addr x.x.x.x -mask x.x.x.x
Show WAN port settings	show

Example:

 # config interface fastethernet wan

<config-interface-fastethernet-wan>#ip –addr 202.112.241.100 –mask 255.255.255.0

You need to reconnect if the WAN port has been changed.

7.5 Netservice

path: <config-netservice>#

Function	Command
Set DNS address	dns -ip x.x.x.x _domain xxx
Set alternate DNS address	alterdns -ip x.x.x.x _domain xxx
Set hostname	hostname xxx
Set http access port	http-port xxx
Show http access setting	http-port
Set telnet access port	telnet-port xxx
Show telnet access port	telnet-port
Set RTP initial port and quantity	media-port –startport xxx –number xxxx

Add route rule	route –gateway x.x.x.x –addr x.x.x.x –mask x.x.x.x
Delete route rule	no route –gateway x.x.x.x –addr x.x.x.x –mask x.x.x.x
Show route info	Route
Show netservice info	show

Example:

#config netservice

<config-netservice>#dns –ip 202.112.10.36 _domain voip.com

<config-netservice>#media-port –startport 10000 –number 200

<config-netservice>#route –gateway 202.112.10.1 –addr 202.112.210.1 –mask 255.255.255.0

7.6 Port settings

path: <config-port>#

Function	Command
set callerid mode	callerid xxx
disable callerid	no callerid
Disable call forward	no callforward
[disable]enable call transfer	[no]calltransfer
[disable]enable call waiting	[no]callwaiting
Set DTMF gain	dtmfvolume xxx
[disable]enable3-way conference	[no]threetalk
Show port settings	show

7.7 SIP settings

path: <config-sip>#

Function	Command
[disable]enable registration	[no] register
[disable]enable auto detect server	[no] detect-server
Set sip domain	default-domain xxx
Set DTMF mode	dtmf-mode xxx
Set auto detect interval time	interval-time xxx
[disable]enable auto swap server	[no]swap-server
Set local SIP signal port	signalport xxx
Set proxy server	server proxy -ip x.x.x.x _port xxx _user xxx _password xxx
Set register server info	server register -ip x.x.x.x _port xxx –user xxx _password xxx
Set alter proxy info	alter-server proxy –ip x.x.x.x _port xxx _user xxx _password xxx
Set alter server info	alter-server register –ip x.x.x.x _port xxx _user xxx

	_password xxx
Show current sip info	show

Example:

#config sip server

<config-sip-server># server proxy ip 210.25.23.22 _port 5060 _user aaa _password 123456

7.8 User management

path: <config-user>#

Function	Command
Change user right.	access –user xxx –access xxx
Change user password	password –user xxx
Add new user	entry –user xxx –access 5 (or 12)
Delete user entry	no entry –user xxx
Show current sip info	show

Example:

#config user

<config-user>#entry –user abc –access 7

Example:<config-user>#access –user aaa –access 7

Note:

The command : **–user xxx –access digit**

Here if the digit is less 10 , then the user level is guest

If the digit is more that 10 ,then the user level is administrator

7.9 Debug (Level 0~7)

path: <debug>#

Function	Command
show debug setting	show
[disable]enable debug all modules	[no] all xxx
[disable]enable debug app module	[no] app xxx
[disable]enable debug cdr module	[no] cdr xxx
[disable]enable debug sip module	[no] sip xxx
[disable]enable debug h323 module	[no] h323 xxx
[disable]enable debug tel module	[no] tel xxx
[disable]enable debug dsp module	[no] dsp xxx

7.10 show system running info

path: <show>#

Function	Command
show: accesslist (firewall) settings	accesslist
show network status	basic
show current call info	call active

show CODEC capability	capability
show debug info	debugging
show LAN status and DHCP server info	dhcp-server
show digital-map info	dial-rule
show LAN info	interface fastethernet lan
show WAN info	interface fastethernet wan
show arp table info	ip arp
Show DNS gateway info	ip dns
Show netstate info	ip netstat
Show route info	ip route
Show icmp packets Stat.	ip icmp
Show igmp packets Stat.	ip igmp
Show ip packets Stat	ip ip
Show RTP packets Stat.	ip rtp
Show TCP packets Stat.	ip tcp
Show UDP packets Stat.	ip udp
show gateway memory	memory
show NAT information	nat
show caller-ID info	port callerID
show dsp info	port dsp
show hotline info	port hotline
show black list info	port in-limit
show outgoing limit info	port out-limit
show current phone number	port number
show current port status	port status
show PPPoE info	pppoe
show QoS table info	qos
show sip info	sip
show UDP tunnel info	udptunnel
show running time	uptime
show gateway version	version

7.11 Logout

Usage: #telnet –target -port

Login:xxx

Password:xxx #

#logout

7.12 tracert trace network path info

usage: #tracert –host

Example:#tracert www.google.com

7.13 update

usage:

 # update ftp –user xxx –password xxx –ip x.x.x.x –file xxx
 # update tftp –ip x.x.x.x –file xxx
Example:
 # update ftp –user abc –password 123 –ip 202.112.20.15 –file FV8010.z

7.14 upload configure file

usage:
 # upload ftp –user xxx –password xxx –ip x.x.x.x –file xxx
 # upload tftp –ip x.x.x.x –file xxx

7.15 download configure to flash

usage: #download tftp –ip x.x.x.x –file xxx
#download ftp –user xxx –password xxx –ip x.x.x.x –file xxx
Example:
#download ftp –user abc –password 123 –ip 202.112.20.15 –file FV8010.cfg

7.16 password

usage:
#password
Enter new password:xxx
Confirm new password:xxx

7.17 reload

usage: #reload
Reboot system

7.18 Network Diagnosis

There are some telnet commands for checking your network. Now Listing below for your information

Command	Function	Example
ping	Check if the destination is accessible	#ping www.google.com
tracert	Show network path info	#tracert www.google.com
show basic	Show network settings	#show basic
show ip route	Show route table	#show ip route
show ip arp	Show arp table	#show ip arp
show ip netstat	Netstat programe	#show ip netstat
telnet	Telnet to another device	#telnet 192.168.1.2

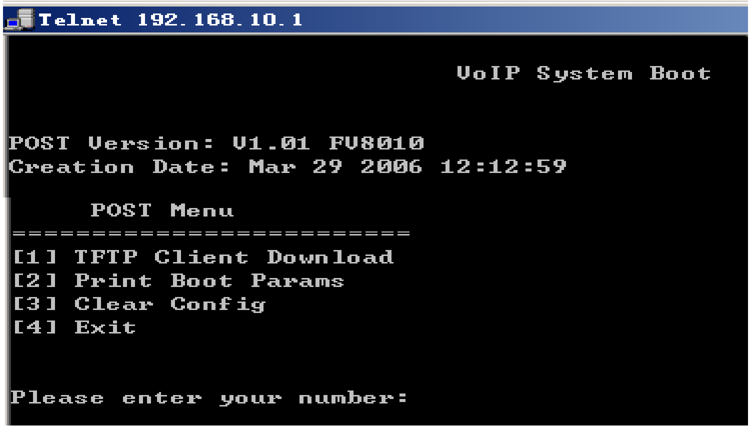
7.19 Restore to factory default

#setdefault (clear gateway settings expect network part)
#setdefault all (clear all settings.)

7.20 POST Mode(safe mode)

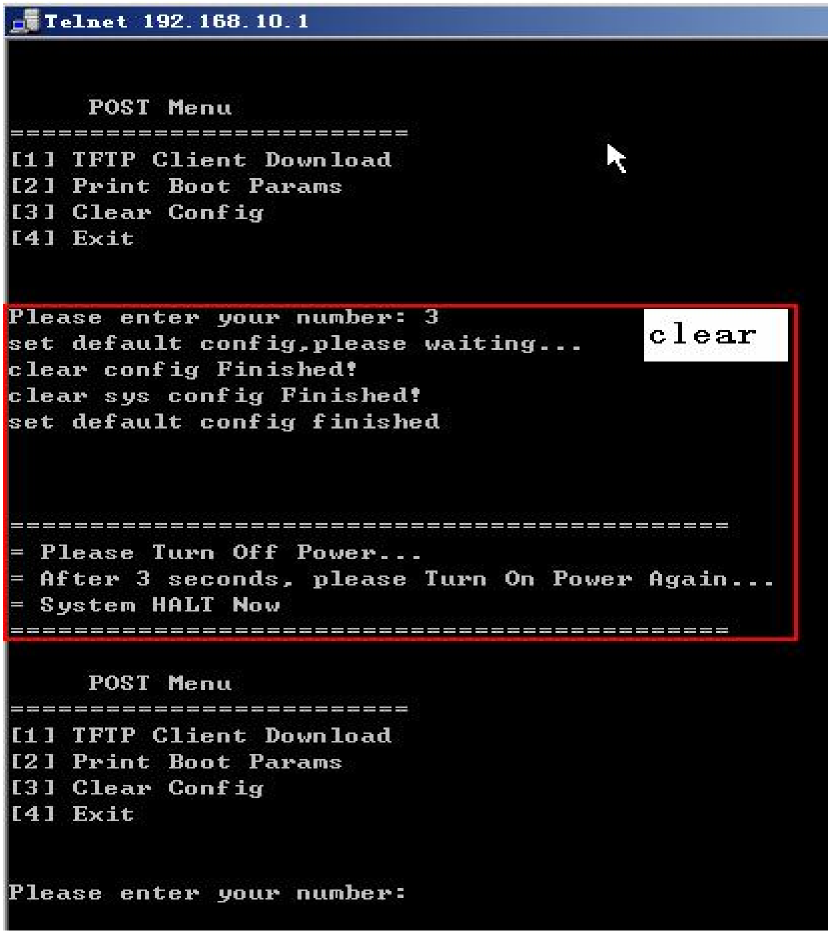
7.20.1 Access Post mode process

1 PC connect to FV8010 LAN port
2 Set your PC IP to be 192.168.10.205
3 Power off .
4 after power on ,within 4 seconds , telnet 192.168.10.1
5 config page is like below (if no page like the below .do step 4 again.)



7.20.2 Post mode clear

Input 3 and enter for clear configuration



7.20.3 post mode TFTP update firmware

Input 1 for TFTP update firmware

Process:

1 Run TFTP server

2 Copy firmware into your TFTP server

3 After access post mode , input 1 for selecting TFTP updating.

4 Input TFTP server address

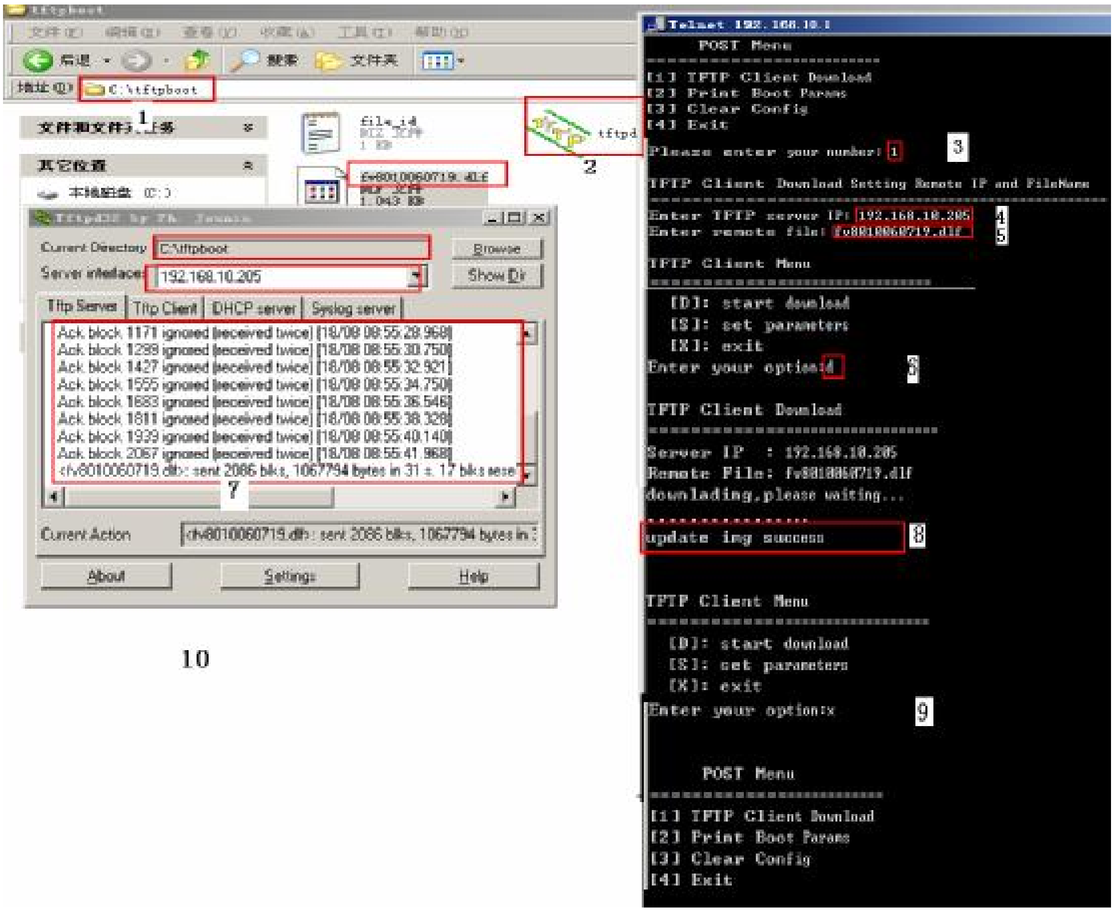
5 Input firmware name and then enter

6 Input d for starting download

7 If updating successfully ,It will display update img success

8 Input x for logout TFTP client

9 Input 4 for logout POST mode



FV8010 provide safe mode. When there is booting problem because of setting problem or firmware problem. User can restore the factory setting or upgrade to a new firmware to solve this problem.