i18

IP Video Intercom User Manual

Wall mounted **In-wall**

Safety Notices

1. Please use the specified power adapter. If you need to use the power adapter provided by other manufacturers under special circumstances, please make sure that the voltage and current provided is in accordance with the requirements of this product, meanwhile, please use the safety certificated products, otherwise may cause fire or get an electric shock.
2. Before using, please confirm that the temperature and environment is humidity suitable for the product to work. (Move the product from air conditioning room to natural temperature, which may cause this product surface or internal components produce condense water vapor, please open power use it after waiting for this product is natural drying).
3. Please do not let non-technical staff to remove or repair. Improper repair may cause electric shock, fire, malfunction, etc. It will lead to injury accident or cause damage to your product.
4. Do not use fingers, pins, wire, other metal objects or foreign body into the vents and gaps. It may cause current through the metal or foreign body, which may even cause electric shock or injury accident. If any foreign body or objection falls into the product please stop using。
5. Please do not discard the packing bags or store in places where children could reach, if children trap his head with it, may cause nose and mouth blocked, and even lead to suffocation。
6. Please use this product with normal usage and operating, in bad posture for a long time to use this product may affect your health.
7. Please read the above safety notices before installing or using this phone. They are crucial for the safe and reliable operation of the device.

Directory

A. Product introduction

i18 is a full digital natwork Video Intercom, with its core part adopts mature VoIP solution, stable and reliable performance, hands-free adopting digital full-duplex mode, voice loud, video clear, generous appearance, solid durable, easy for installation, comfortable keypad and low power consumption.

1. Appearance of the product

Single button

Dual button

2. Description

Picture	Description	Function
 	DSS Key LED	Network error: Blink with 2s Network running: Off Registration failed: Blink with 6s Registration succeeded: On

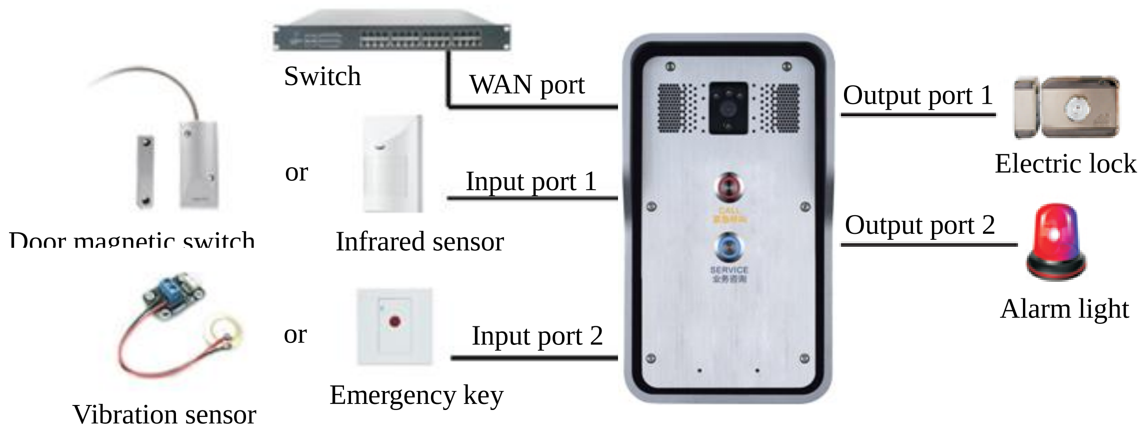
B. Start Using

Before you start to use the equipment, please make the following installation:

1. Confirm the connection

Confirm whether the equipment of the power cord, network cable connection and the boot-up is normal. (Check the state of indicator light)

1) Power port

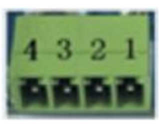


2) Power port

Power supply ways: 12v/DC or POE.

CN16		
1	2	
+12V	GND	
12V 1A/DC		

3) Security functions Input port

CN10				
4	3	2	1	
GND	IN2	GND	IN2	
Input port 2		**Input port 1**		

4) Security functions Output port

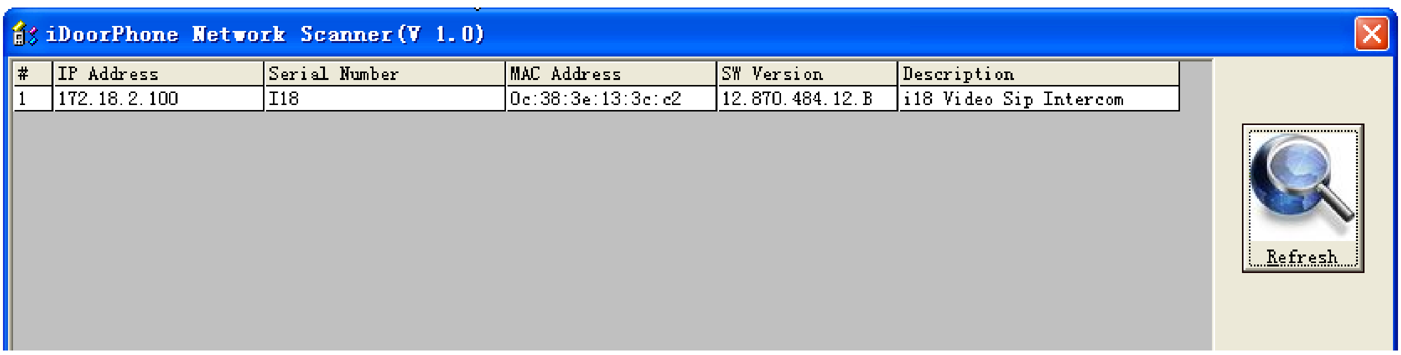
CN11					
6	5	4	3	2	1
NC2	COM	NO2	NC1	COM	NO1
Normally close	common port	Normally open	Normally close	common port	Normally open
Output port 2			Output port 1		

2. Quick Setting

The product provides a complete function and parameter setting. Users may need to have the network and SIP protocol knowledge to understand the meaning represented by all parameters. In order to let equipment users enjoy the high quality of voice service and low cost advantage brought by the device immediately, here we list some basic but compulsory setting options in this section to let users know how to operate without understanding such complex SIP protocols.

In prior to this step, please make sure your broadband Internet online can be normal operated, and complete the connection of the network hardware. The product factory default network mode is DHCP. Thus, only connect equipment with DHCP network environment that network can be automatically connected.

- Press and hold "#" key for 3 seconds and the door phone will report the IP address by voice, or use the "iDoorPhoneNetworkScanner.exe " software to find the IP address of the device.
  Note: when power on, 30s waiting is needed for device running.
- Log on to the WEB device configuration.
- In a SIP page configuration service account, user name, parameters that are required for server address register
- You can set DSS key in the Webpage (Intercom -> function key).
- You can set function parameters in the Webpage (Safeguarding).



C. Basic operation

1. Answer a call

When a call comes in, the device will answer automatically. If you cancel auto answer feature and set auto answer time, you will hear the bell ring at the set time and the device will auto answer after a timeout.

2. Call

Configure shortcut key as hot key and setup a number, then press shortcut key can call the configured number.

3. End Call

Enable DSS key hang up to end call.

4. Call record

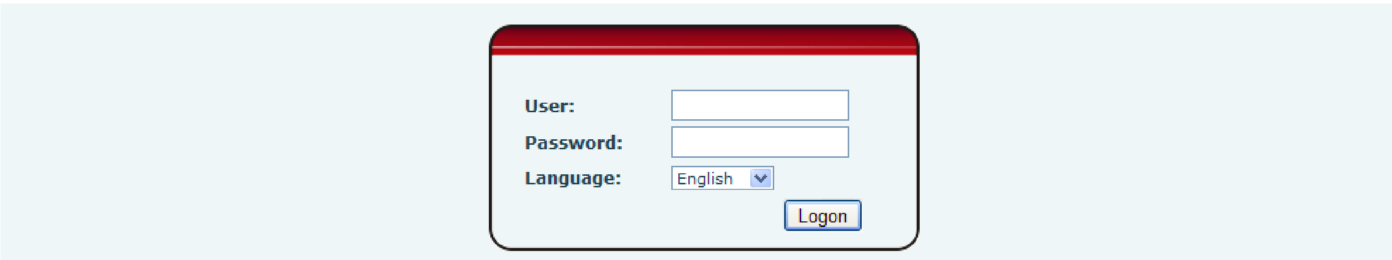
The device provides three call records, missed call, received call, dialed call. You can see call records of the webpage.

D. Page settings

1. Browser configuration

When the device and your computer are successfully connected to the network, enter the IP address of the device on the browser as http://xxx.xxx.xxx.xxx/ and you can see the login interface of the web page management.

Enter the user name and password and click the [logon] button to enter the settings screen.



After configuring the equipment, remember to click SAVE under the Maintenance tab. If this is not done, the equipment will lose the modifications when it has been rebooted.

2. Password Configuration

There are two levels of access: root level and general level. A user with root level access can browse and set all configuration parameters, while a user with general level can set all configuration parameters except server parameters for SIP

- Default user with general level:
  - Username: guest
  - Password: guest
- Default user with root level:
  - Username: admin
  - Password: admin

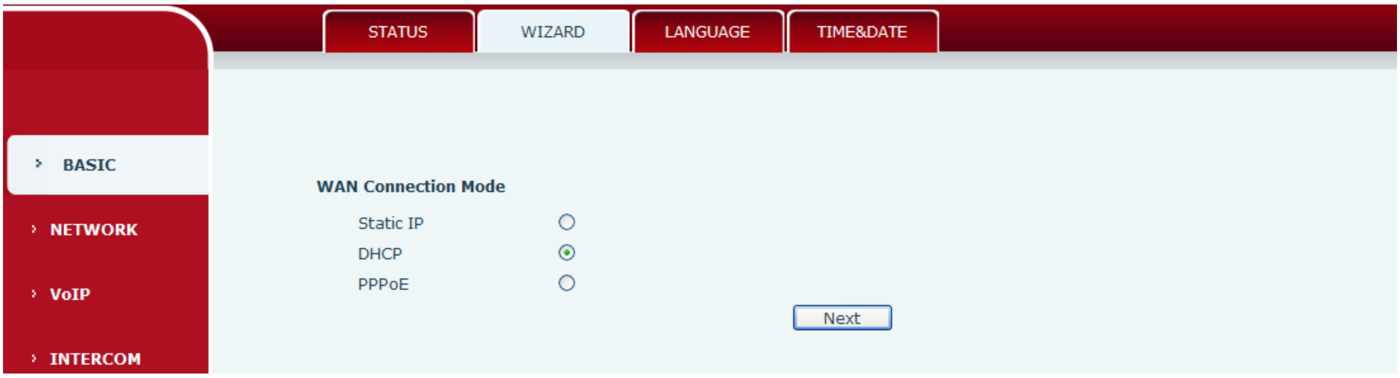
3. Configuration via WEB

(1) BASIC

a) STATUS

Status	
Field Name	**Explanation**
Network	Shows the configuration information for WAN and LAN port, including connection mode of WAN port (Static, DHCP, PPPoE),MAC address, IP address of WAN port.
Accounts	Shows the phone numbers and registration status for the 2 SIP LINES.

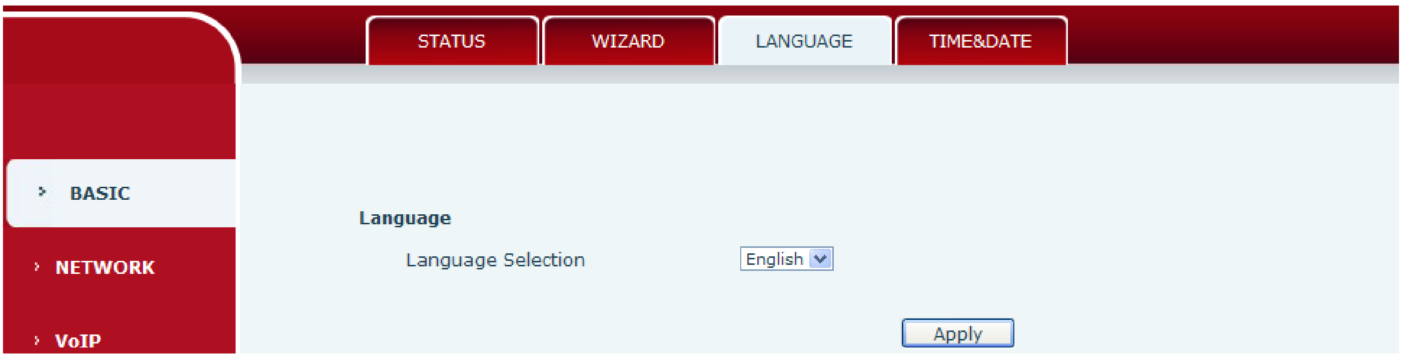
b) WIZARD



Wizard	
Field Name	**Explanation**
Select the appropriate network mode. The equipment supports three network modes:	
Static IP mode	The parameters of a Static IP connection must be provided by your ISP.
DHCP mode	In this mode, network parameter information will be obtained automatically from a DHCP server.
PPPoE mode	In this mode, you must enter your ADSL account and password.
Static IP mode is selected; Click <Next> to go to Quick SIP Settings, Click Back to return to the Wizard screen.	
After selecting DHCP and clicking NEXT, the Quick SIP Settings screen will appear. Click Back to return to the Wizard screen. Click <Next> to go to the Summary screen.	
If PPPoE is selected, this screen will appear. Enter the information provided by the ISP. Click <Next> to go to Quick SIP Setting. Click Back to return to the Wizard screen.	

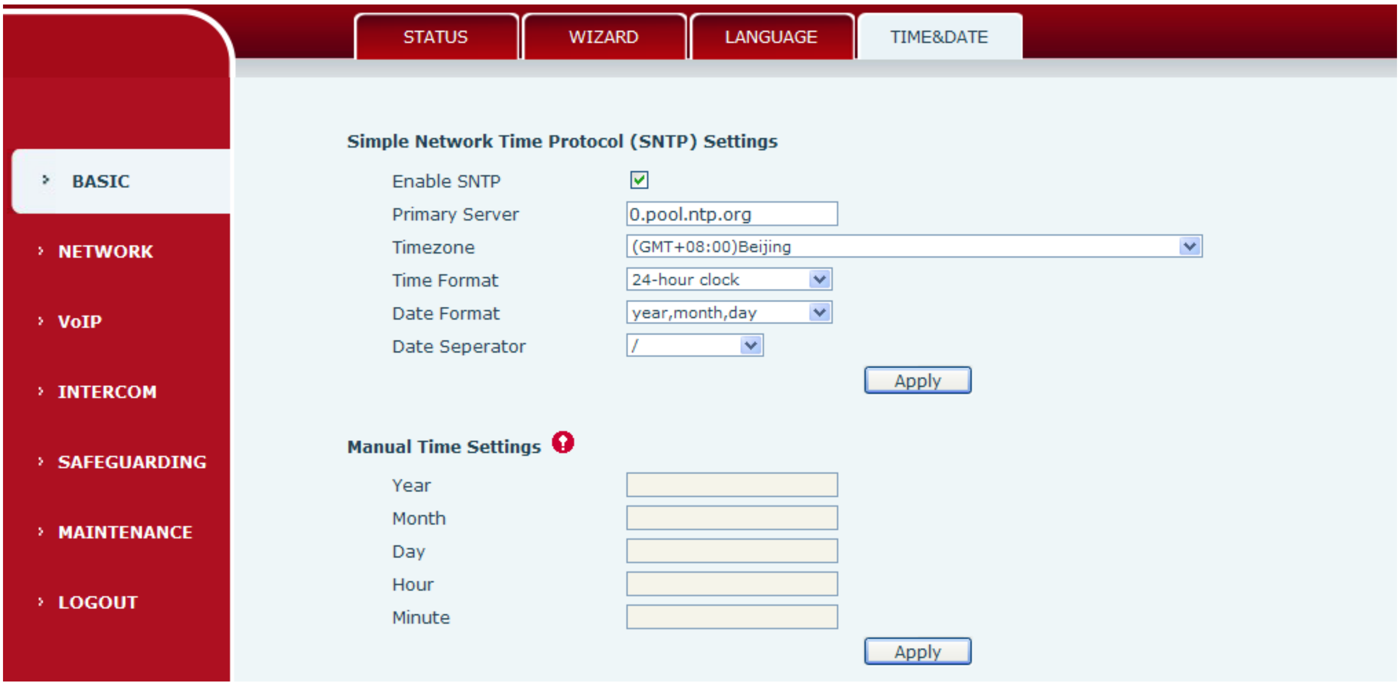
c) LANGUAGE

Set the current language.



d) TIME&DATE

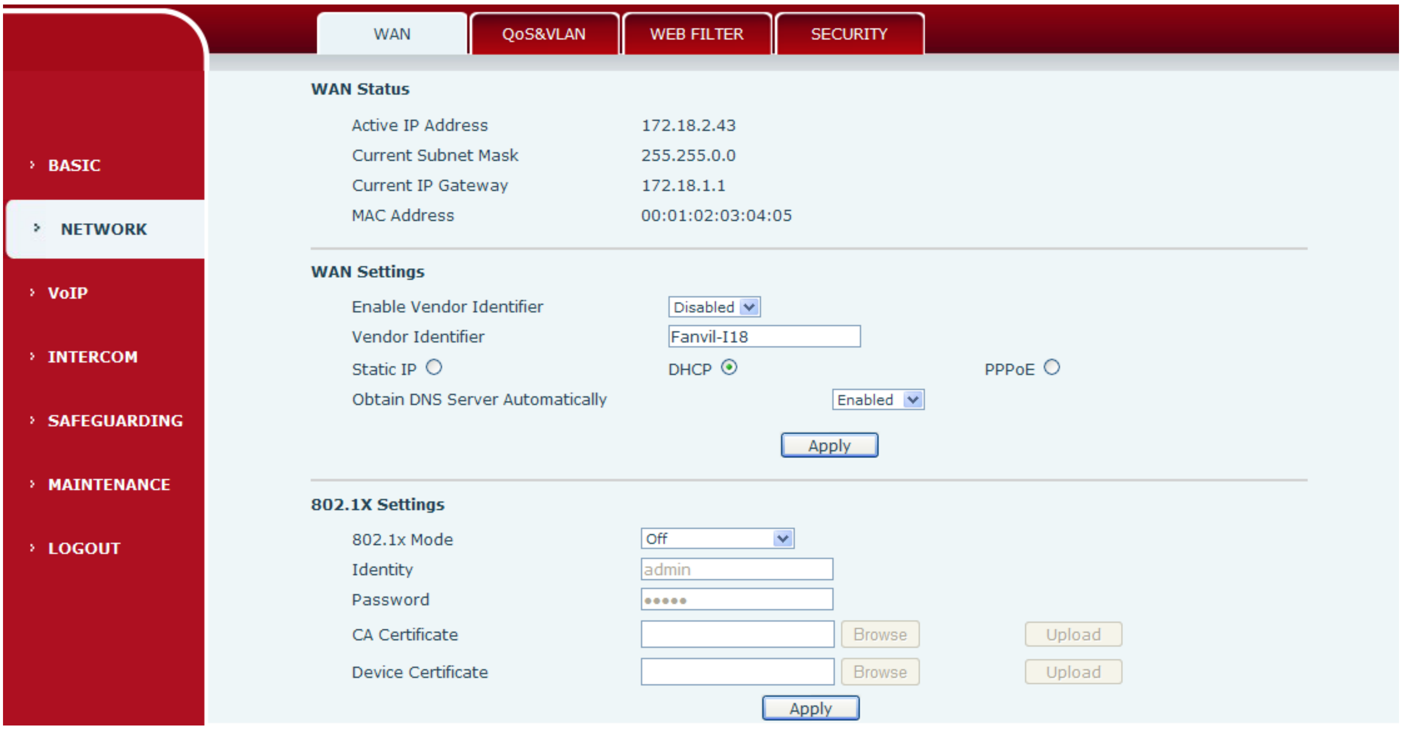
Set the time zone and SNTP (Simple Network Time Protocol) server on this page. Daylight Saving Time configuration and Manual Time and Date entry can also be done in this page.

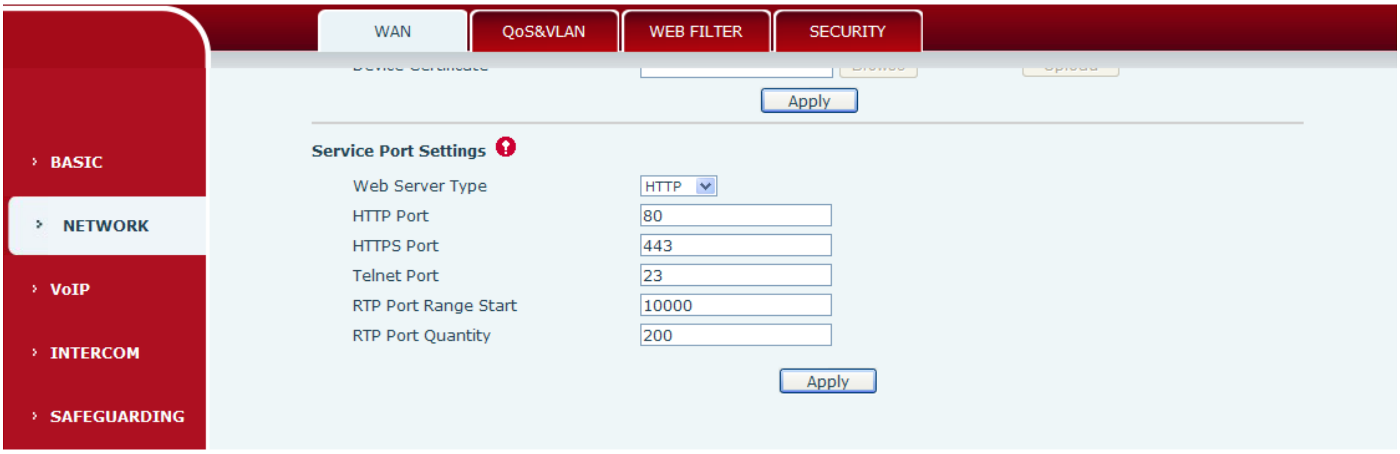


Time&Date	
Field Name	**Explanation**
System Current Time	
Display the current time	
Simple Network Time Protocol (SNTP) Settings	
Enable SNTP	Enable or Disable SNTP
Primary Server	IP address of Primary SNTP Server
Time zone	Local Time Zone
Time Format	Configuration time format, the default is 24 hours.
Date Format	Configure date display format, the default is (date) (month) (year)
Date Seperator	Configure the date seperator
Manual Time Settings	
Enter the values for the current year, month, day, hour and minute. All values are required. Be sure to disable SNTP service before entering manual time and date.	

(2) NETWORK

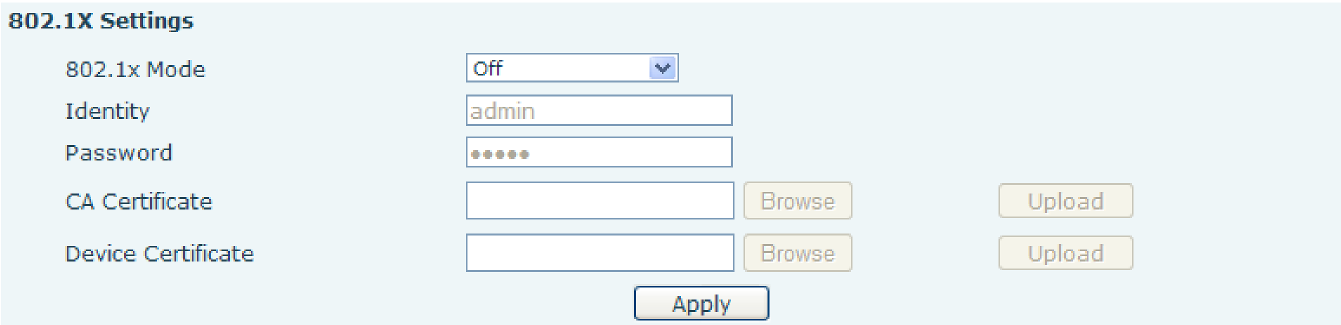
a) WAN



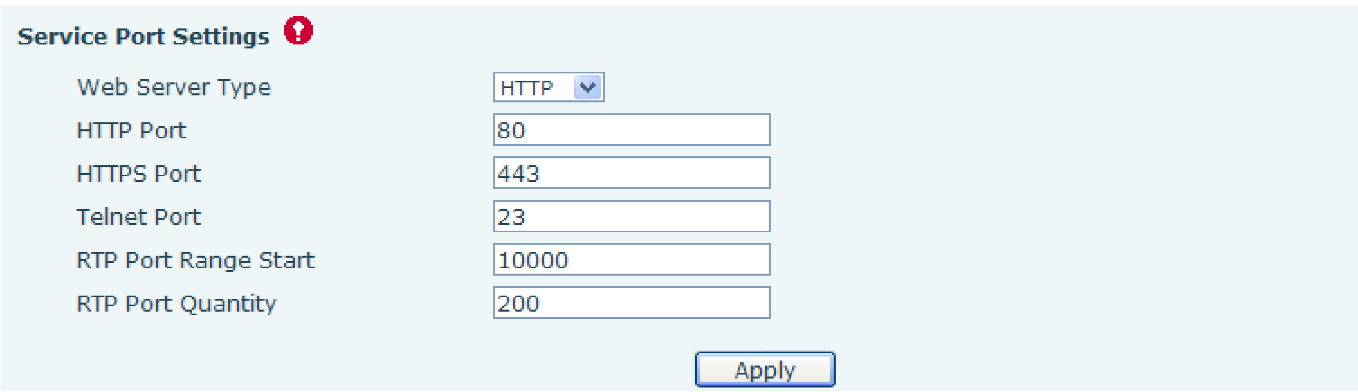


Field Name	Explanation
WAN Status	
Active IP address	The current IP address of the equipment
Current subnet mask	The current Subnet Mask
Current IP gateway	The current Gateway IP address
MAC address	The MAC address of the equipment

WAN Settings	
Enable Vendor Identifier	Enable or disable Vendor Identifier
Vendor Identifier	Configure display Vendor Identifier
Select the appropriate network mode. The equipment supports three network modes:	
Static	Network parameters must be entered manually and will not change. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
PPPoE	Account and Password must be input manually. These are provided by your ISP.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
After entering the new settings, click the APPLY button. The equipment will save the new settings and apply them. If a new IP address was entered for the equipment, it must be used to login to the phone after clicking the APPLY button.	
802.1X Settings	



User	802.1X user account
Password	802.1X password
Enable 812.1X	Enable or Disable 812.1X
CA Certificate	Choose the CA Certificate and then click upload to upgrade
Device Certificate	Choose the Device Certificate and then click upload to upgrade
Service port Settings	



Field Name	Explanation
Web Server Type	Specify Web Server Type – HTTP or HTTPS
HTTP Port	Port for web browser access. Default value is 80. To enhance security, change this from the default. Setting this port to 0 will disable HTTP access. 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.
HTTPS Port	Port for HTTPS access. Before using HTTPS, an HTTPS authentication certification must be downloaded into the equipment. Default value is 443. To enhance security, change this from the default.
Telnet Port	Port for Telnet access. The default is 23.
RTP Port Range Start	Set the beginning value for RTP Ports. Ports are dynamically allocated.
RTP Port Quantity	Set the maximum quantity of RTP Ports. The default is 200.
Note: 1) Any changes made on this page require a reboot to become active. 2) It is suggested that changes to HTTP Port and Telnet ports be values greater than 1024.Values less than 1024 are reserved. 3) If the HTTP port is set to 0, HTTP service will be disabled.	

b) QoS&VLAN

The equipment supports 802.1Q/P protocol and DiffServ configuration. Use of a Virtual LAN (VLAN) allows voice and data traffic to be separated.

- Chart 1 shows a network switch with no VLAN. Any broadcast frames will be transmitted to all other ports. For example, frames broadcast from Port 1 will be sent to Ports 2, 3, and 4.

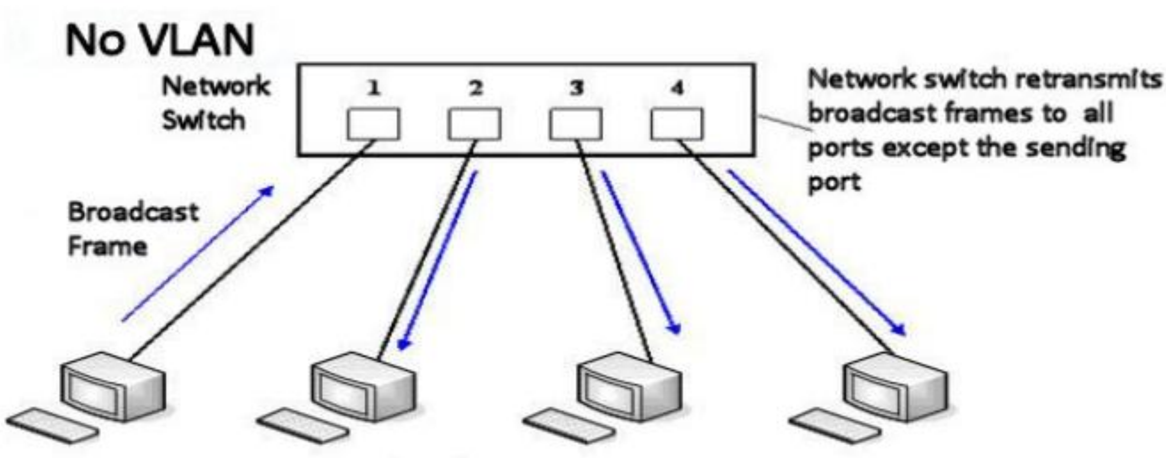


Chart 1

- Chart 2 shows an example with two VLANs indicated by red and blue. In this example, frames broadcast from Port 1 will only go to Port 2 since Ports 3 and 4 are in a different VLAN. VLANs can be used to divide a network by restricting the transmission of broadcast frames.

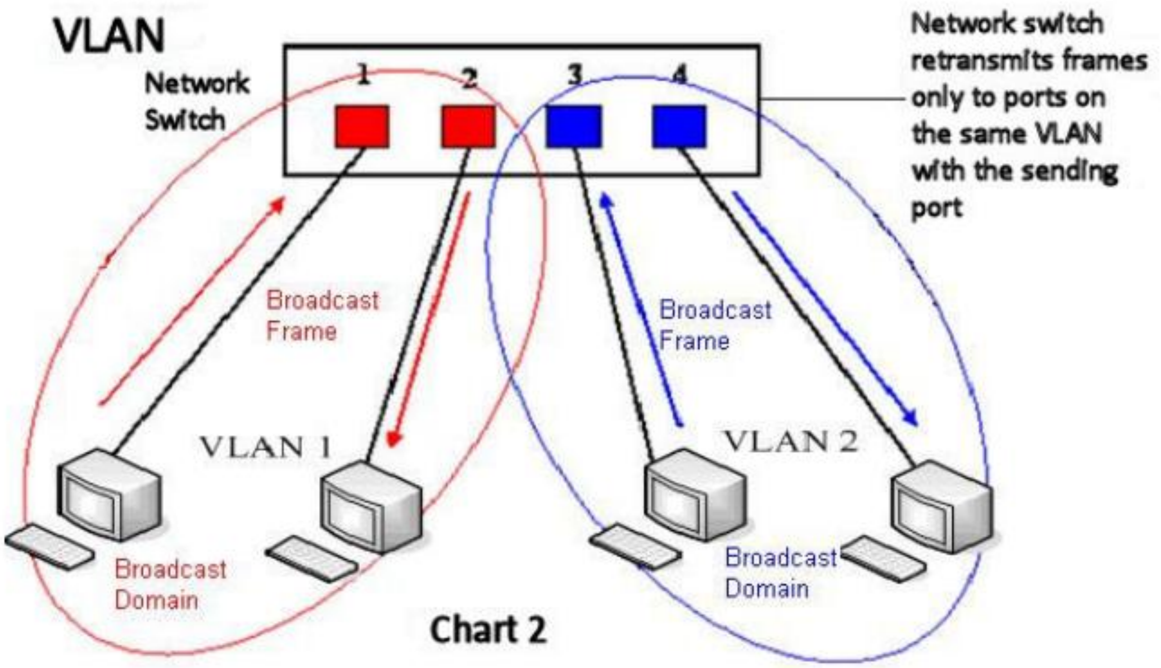
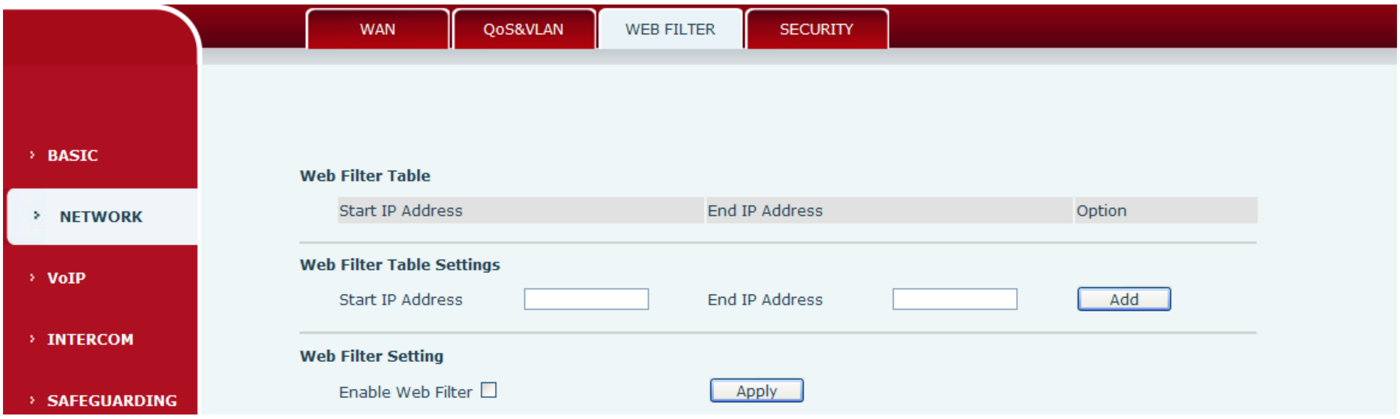


Chart 2

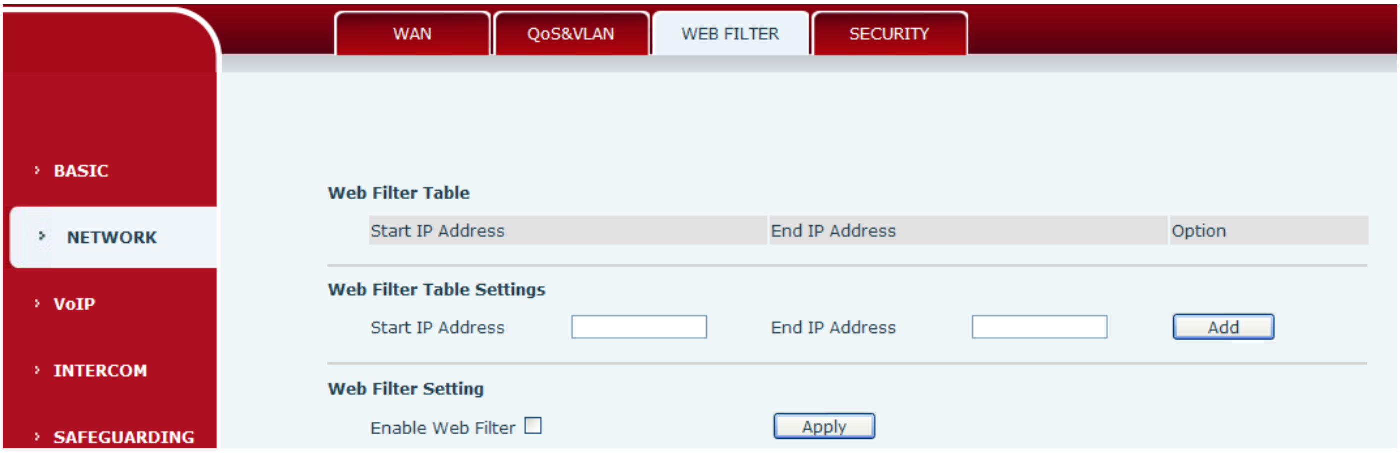
Note: In practice, VLANs are distinguished by the use of VLAN IDs.



QoS&VLAN	
Field Name	**Explanation**
Link Layer Discovery Protocol (LLDP) Settings	
Enable LLDP	Enable or Disable Link Layer Discovery Protocol (LLDP)
Packet Interval	The time interval for sending LLDP Packets
Enable Learning Function	Enables the telephone to synchronize its VLAN data with the Network Switch. The telephone will automatically synchronize DSCP, 802.1p, and VLAN ID values even if these values differ from those provided by the LLDP server.

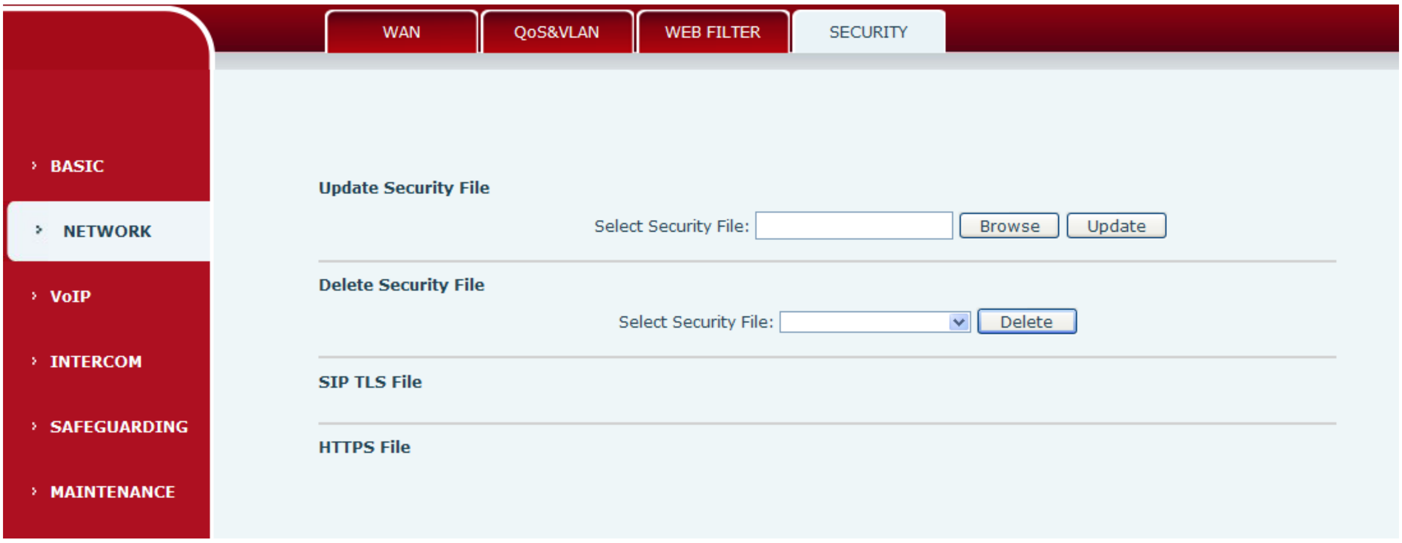
Field Name	Explanation
Quality of Service (QoS) Settings	
Enable DSCP	Enable or Disable Differentiated Services Code Point (DSCP)
SIP DSCP	Specify the value of the SIP DSCP in decimal
Audio RTP DSCP	Specify the value of the Audio DSCP in decimal
Video RTP DSCP	Specify the value of the Video DSCP in decimal
WAN Port VLAN Settings	
Enable WAN Port VLAN	Enable or Disable WAN Port VLAN
WAN Port VLAN ID	Specify the value of the WAN Port VLAN ID. Range is 0-4095
802.1P Priority	Specify the value of the 802.1p priority. Range is 0-7

c) WEB FILTER



Web filter
The Web filter is used to limit access to the equipment. When the web filter is enabled, only the IP addresses between the start IP and end IP can access the equipment.
Web Filter Table
Web page access allows display the IP network list.
Web Filter Table Settings
Beginning and Ending IP Address for MMI Filter, Click add this filter range to the Web Filter Table.
Web Filter Setting
Select to enable MMI Filter. Click <apply> Make filter settings effective.
Note: Be sure that the filter range includes the IP address of the configuration computer.

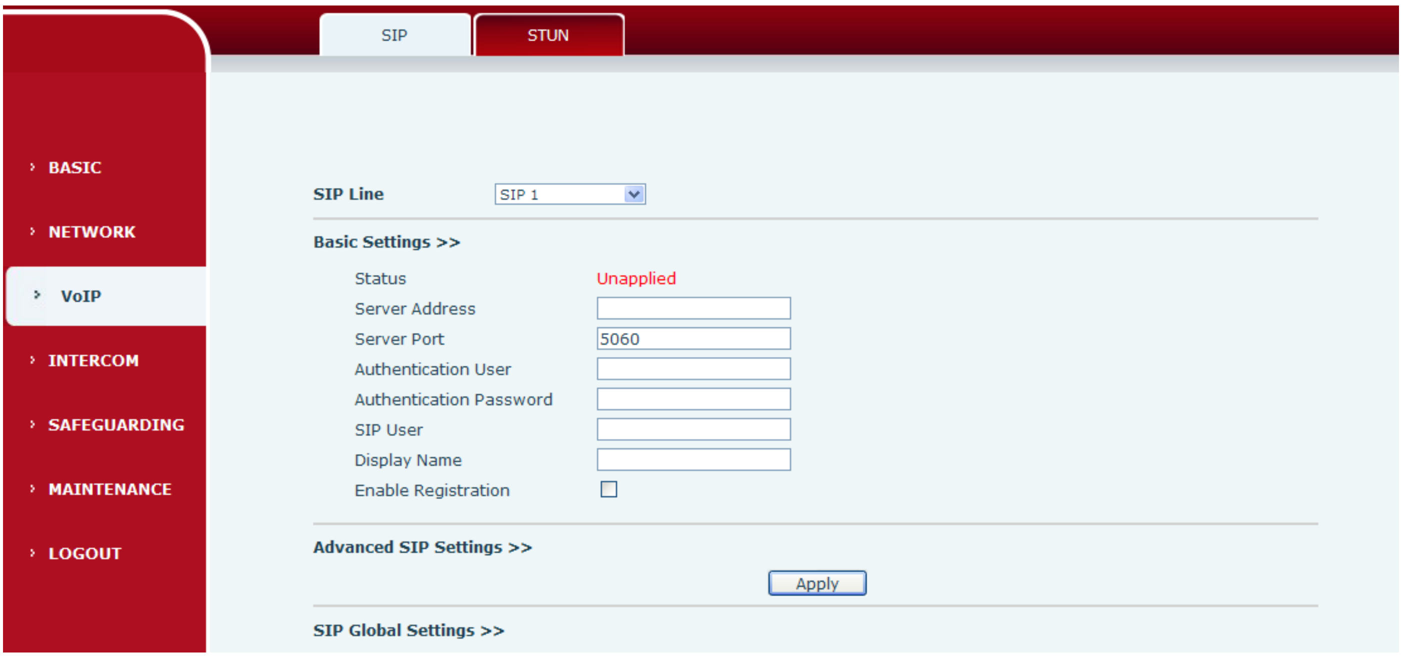
d) SECURITY

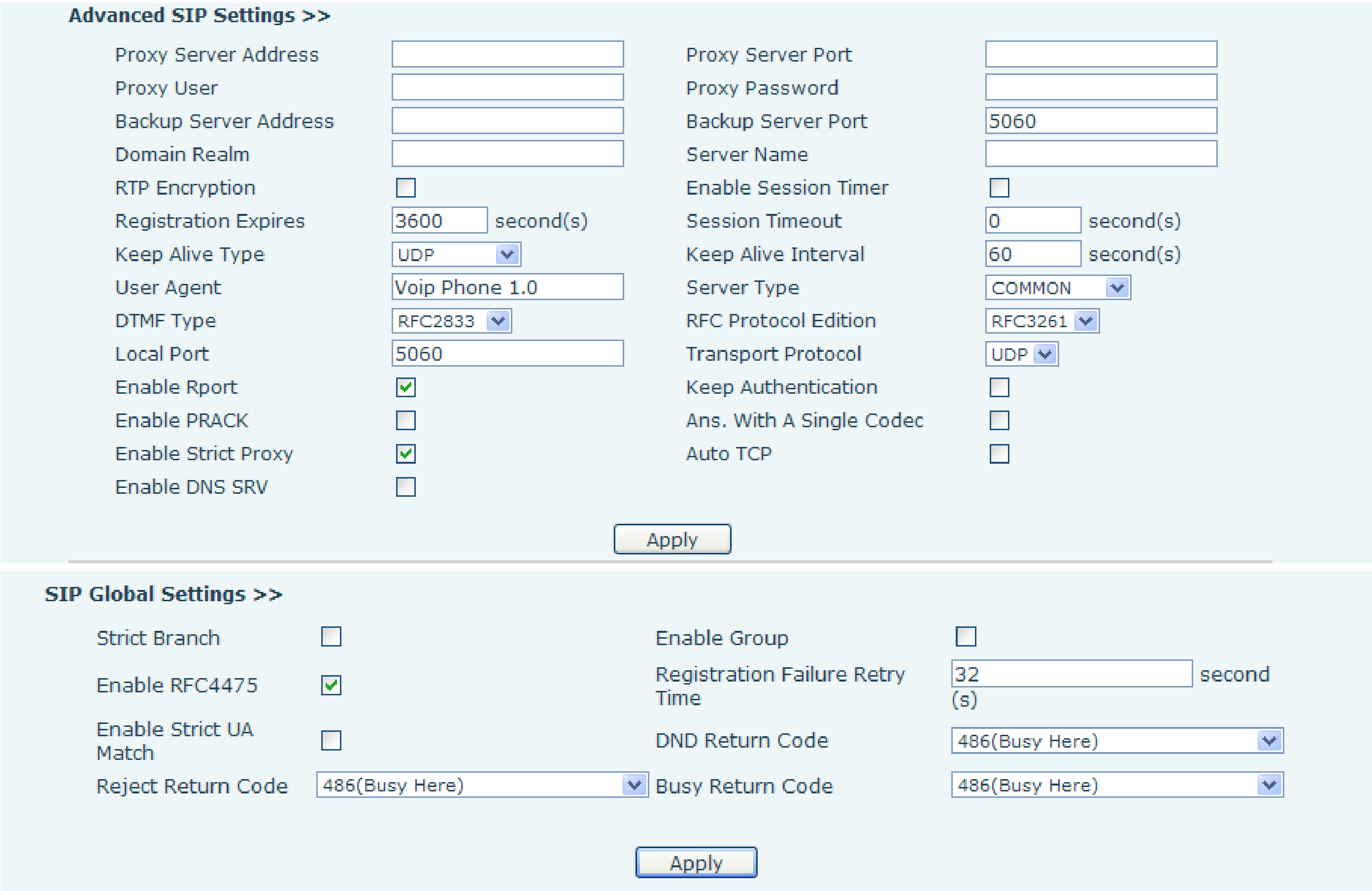


Field Name	Explanation
Update Security File	Select the security file to be updated. Click the Update button to update.
Delete Security File	Select the security file to be deleted. Click the Delete button to Delete.
SIP TLS Files	Show SIP TLS authentication certificate.
HTTPS Files	Show HTTPS authentication certificate.

(3) VOIP

a) SIP





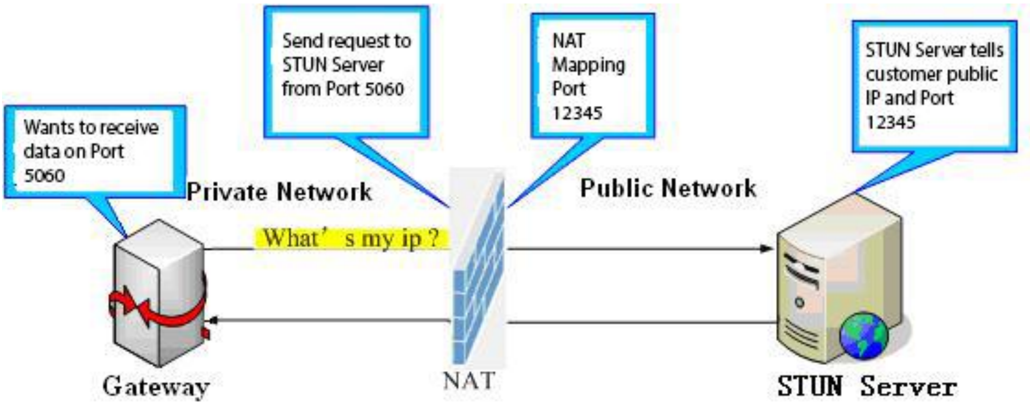
SIP	
Field Name	**Explanation**
Basic Settings (Choose the SIP line to configured)	
Status	Shows registration status. If the registration is successful done, it will display “has been registered”, otherwise will display “not registered”. The wrong password will display “403 errors” and account number failure will display “timeout”.
Server Address	SIP server IP address or URI.
Server Port	SIP server port. Default is 5060.
Authentication User	SIP account name (Login ID).
Authentication Password	SIP registration password.
SIP User	Phone number assigned by VoIP service provider. Equipment will not register if there is no phone number configured.
Display Name	Set the display name. This name is shown on Caller ID.
Enable Registration	Check to submit registration information.

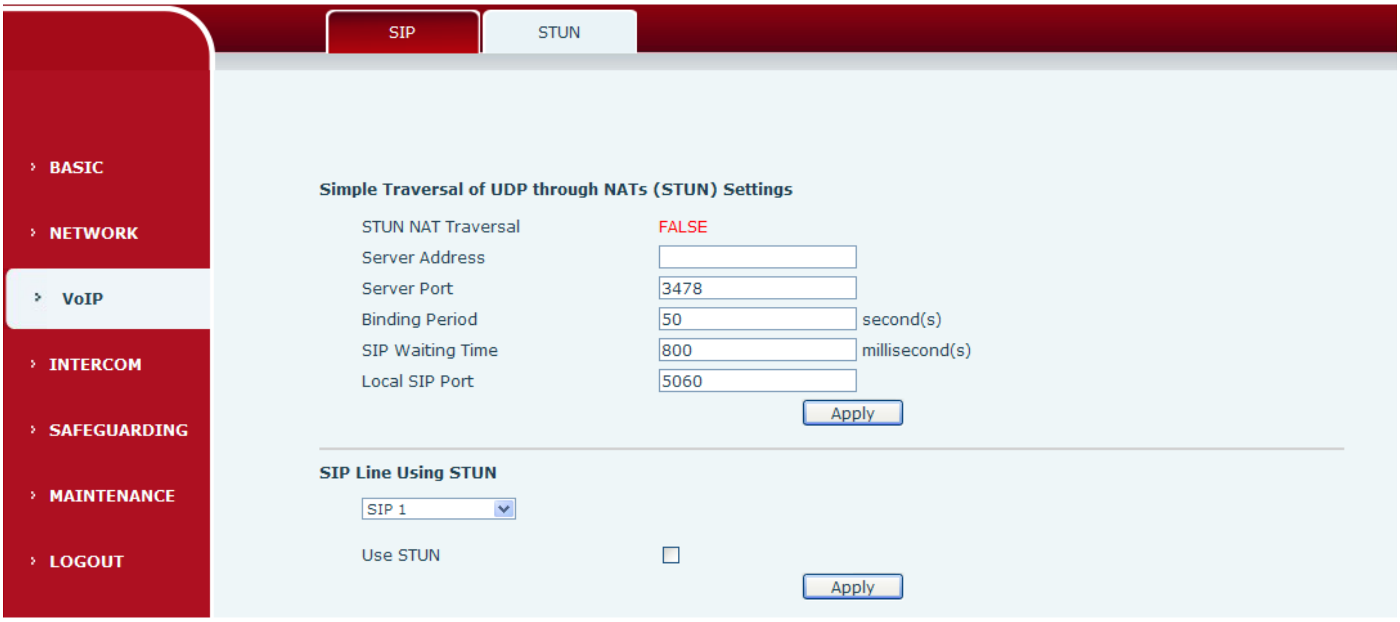
Field Name	Explanation
Advanced SIP Settings	
Proxy Server Address	SIP proxy server IP address or URI, (This is normally the same as the SIP Registrar Server)
Proxy Server Port	SIP Proxy server port. Normally 5060.
Proxy User	SIP Proxy server account.
Proxy Password	SIP Proxy server password.
Backup Server Address	Backup SIP Server Address or URI (This server will be used if the primary server is unavailable)
Backup Server Port	Backup SIP Server Port.
Domain Realm	SIP Domain if different than the SIP Register Server.
Server Name	Name of SIP Backup server
RTP Encryption	Enable/Disable RTP Encryption.
Enable Session Timer	If enabled, this will refresh the SIP session timer per RFC4028.
Registration Expires	SIP re-registration time. Default is 60 seconds. If the server requests a different time, the phone will change to that value.
Session Timeout	Refresh interval if Session Timer is enabled.
Keep Alive Type	Specifies the NAT keep alive type. If SIP Option is selected, the equipment will send SIP Option SIP messages to the server every NAT Keep Alive Period. The server will then respond with 200 OK. If UDP is selected, the equipment will send a UDP message to the server every NAT Keep Alive Period.
Keep Alive Interval	Set the NAT Keep Alive interval. Default is 60 seconds
User Agent	Set SIP User Agent value.
Server Type	Configures phone for unique requirements of selected server.
DTMF Type	DTMF sending mode. There are four modes: ● In-band ● RFC2833 ● SIP_INFO ● AUTO Different VoIP Service providers may require different modes.
RFC Protocol Edition	Select SIP protocol version RFC3261 or RFC2543. Default is RFC3261. Used for servers which only support RFC2543.
Local Port	SIP port. Default is 5060.

Field Name	Explanation
Transport Protocol	Configuration using the transport protocol, TCP, TLS or UDP, the default is UDP.
Enable Rport	Enable/Disable support for NAT traversal via RFC3581 (Rport).
Keep Authentication	Enable /disable registration with authentication. It will use the last authentication field which passed authentication by server. This will decrease the load on the server if enabled
Enable PRACK	Enable or disable SIP PRACK function. Default is OFF. It is suggested this be used.
Ans. With a Single Codec	If enabled phone will respond to incoming calls with only one codec.
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server it will use the source IP address, not the address in via field.
Auto TCP	Force the use of TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable DNS SRV	Enables use of DNS SRV records
SIP Global Settings	
Strict Branch	Enable Strict Branch - The value of the branch must be after"z9hG4bK" in the VIA field of the INVITE message received, or the phone will not respond to the INVITE. Note: This will affect all lines
Enable Group	Enable SIP Group Backup. This will affect all lines
Enable RFC4475	Enable or disable RFC4475,default is enable。
Registration Failure Retry Time	Registration failures retry time – If registrations fails, the phone will attempt to register again after registration failure retry time. This will affect all lines
Enable Strict UA Match	Enable or disable Strict UA Match
DND Return Code	Specify SIP Code returned for DND. Default is 480 - Temporarily Not Available.
Reject Return Code	Specify SIP Code returned for Rejected call. Default is 603 – Decline.
Busy Return Code	Specify SIP Code returned for Busy. Default is 486 – Busy Here.

b) STUN

STUN – Simple Traversal of UDP through NAT –A STUN server allows a phone in a private network to know its public IP and port as well as the type of NAT being used. The equipment can then use this information to register itself to a SIP server so that it can make and receive calls while in a private network.





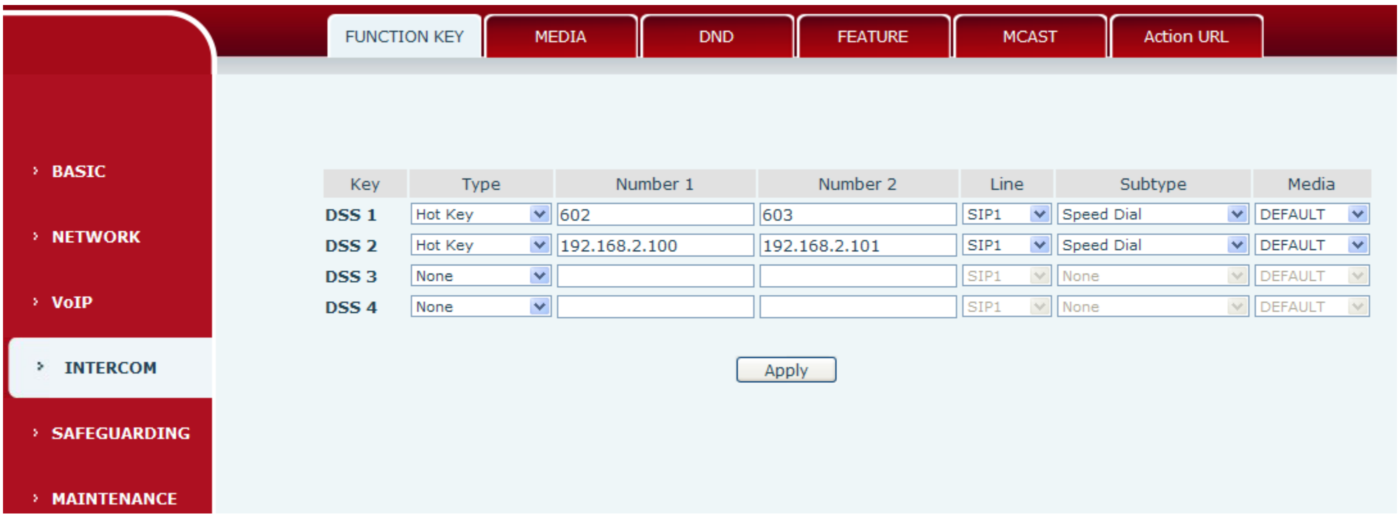
STUN	
Field Name	**Explanation**
STUN NAT Traversal	Shows whether or not STUN NAT Traversal was successful.
Server Address	STUN Server IP address
Server Port	STUN Server Port – Default is 3478.
Binding Period	STUN blinding period – STUN packets are sent at this interval to keep the NAT mapping active.
SIP Waiting Time	Waiting time for SIP. This will vary depending on the network.
Local SIP Port	Port configure the local SIP signaling

Field Name	Explanation
SIP Line Using STUN (SIP1 or SIP2)	
Use STUN	Use STUN
Note: the SIP STUN is used to achieve the SIP penetration of NAT, is the realization of a service, when the equipment configuration of the STUN server IP and port (usually the default is 3478), and select the Use Stun SIP server, the use of NAT equipment to achieve penetration.	

(4) INTERCOM

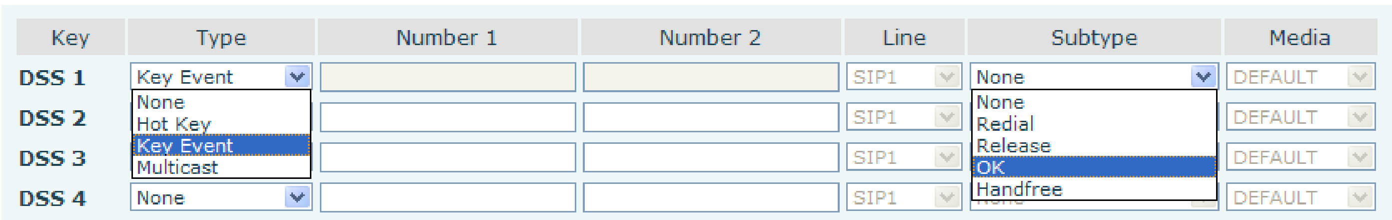
a) FUNCTICON KEY

This page configures audio parameters such as voice codec, speak volume, mic volume and ringer volume.



- **Key Event Settings**

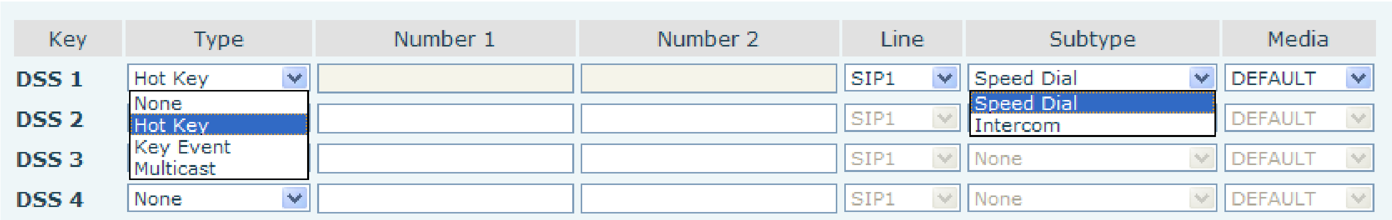
Set the key type to the Key Event.



DSS key type	Subtype	Usage
Key Event	None	Not responding
	Dial	Dial function
	Release	End calls
	OK	Identify key
	Handfree	The hand-free key(with hook dial, hang up)

➢ Hot key Settings

Enter the phone number in the input box, when you press the shortcut key, equipment will dial set telephone number. This button can also be used to set the IP address, press the shortcut key IP direct dial call.

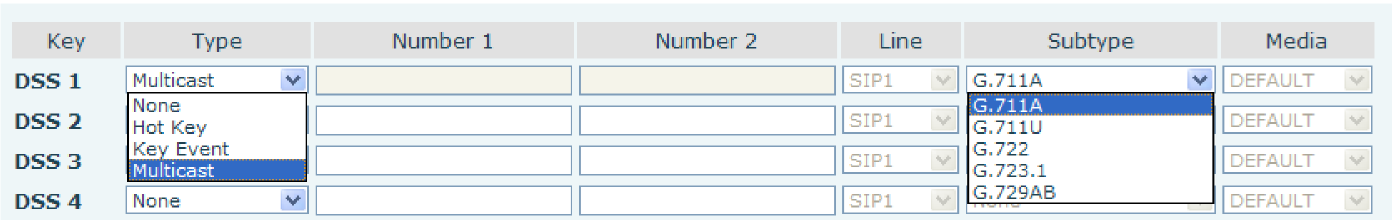


DSS key type	Number	Line	Subtype	Usage
Hot Key	Fill the called party's SIP account or address	The SIP account corresponding lines	Speed Dial	In Speed dial mode, with Enable Speed Dial Handdown Enable can define whether this call is allowed to be hang up by re-press the speed dial
			Intercom	In Intercom mode, if the caller's IP phone support intercom feature, can realize auto answer

➢ Multicast Settings

Multicast function is launched will voice messages sent to set the multicast address, all equipment to monitor the group multicast address can receive sponsors speech information, etc. Using multicast functionality can be simple and convenient to send notice to each member in the multicast.

Through the DSS Key configuration multicast calling WEB is as follows:



DSS key type	Number	Subtype	Usage
Multicast	Set the host IP address and port number, the middle separated by a colon	G.711A	Narrowband speech coding (4Khz)
		G.711U	
		G.722	Wideband speech coding (7Khz)
		G.723.1	Narrowband speech coding (4Khz)
		G.726-32	
		G.729AB	

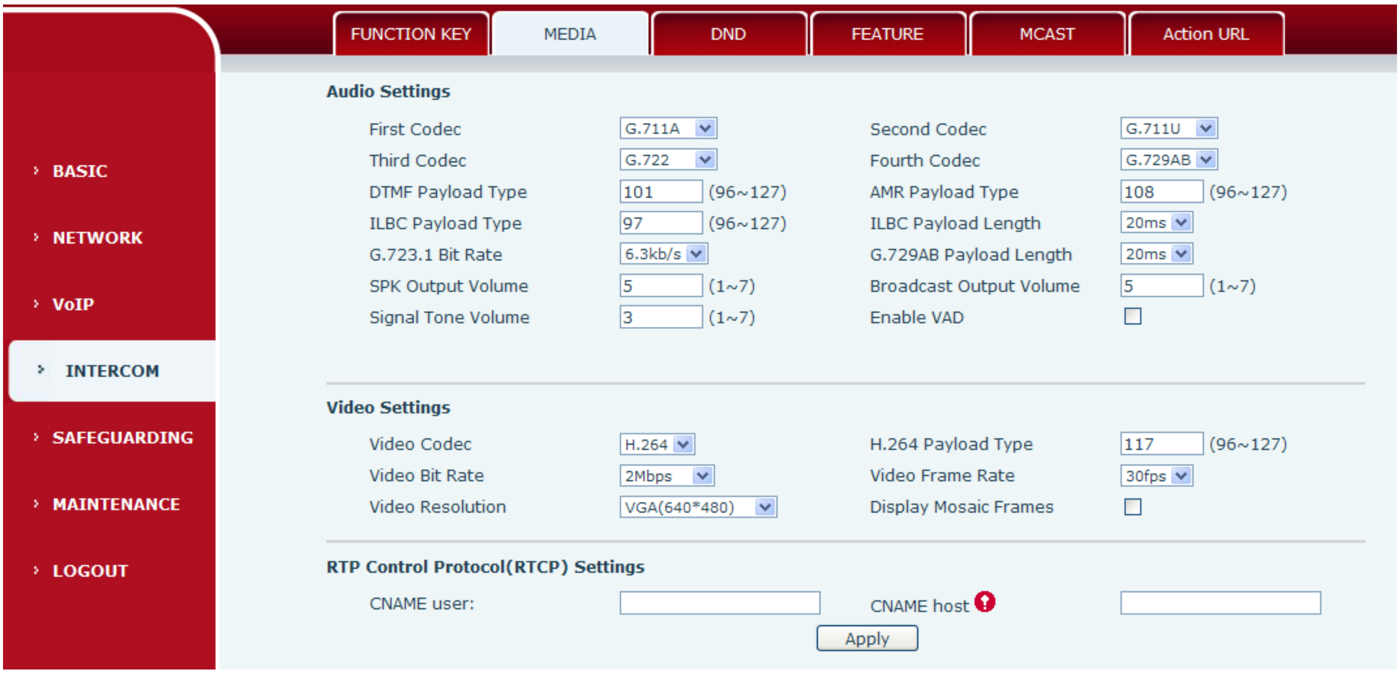
✧ operation mechanism

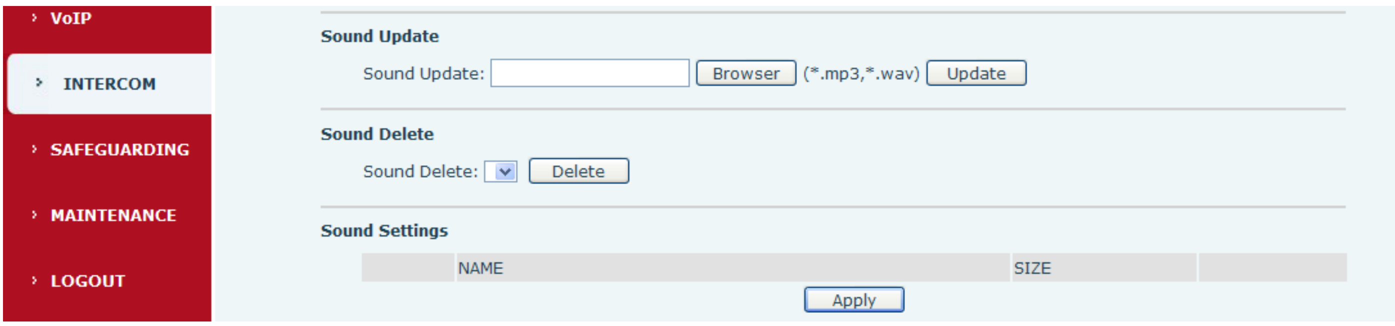
Device through the DSS Key configuration of multicast address and port and started coding; set by WEB to monitor the multicast address and port; device sends a multicast, listens to the address of the device can receive the multicast content.

✧ calling configuration

✧ The call is already exists, and three party or initiated multicast communication, so it will not be able to launch a new multicast call.

b) MEDIA



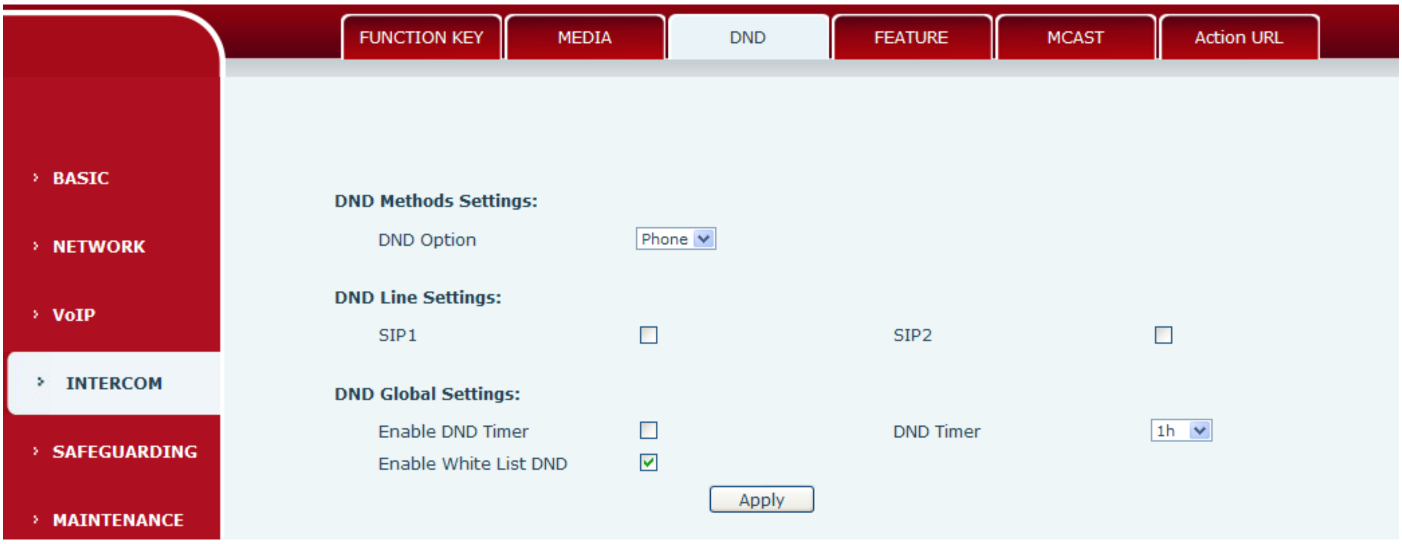


Media Settings	
Field Name	**Explanation**
First Codec	The first codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, ILBC, AMR.
Second Codec	The second codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, ILBC, AMR.
Third Codec	The third codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, ILBC and AMR.

Field Name	Explanation
Fourth Codec	The forth codec choice: G.711A/U, G.722, G.723.1, G.726-32, G.729AB, ILBC and AMR.
DTMF Payload Type	The RTP Payload type that indicates DTMF. Default is 101
AMR Payload Type	Set the AMR Payload type, Numerical based on between 96-127.
ILBC Payload Type	Set the ILBC Payload type, Numerical based on between 96-127.
ILBC Payload Length	Set the ILBC payload length.
G.723.1 Bit Rate	Choices are 5.3kb/s or 6.3kb/s.
G.729AB Payload Length	G.729AB Payload Length – Adjusts from 10 – 60 mSec.
SPK Output Volume	Set the speaker calls the volume level.
Broadcast Output Volume	Set the broadcast the output volume level.
Signal Tone Volume	Set the audio signal the output volume level.
Enable VAD	Enable or disable Voice Activity Detection (VAD). If VAD is enabled, G729 Payload length cannot be set greater than 20 mSec.
Video Settings	
Video Codec	Set the video codec used in video call (H.263, H.264)
H.264 Payload Type	Set the H.264 Payload type, Numerical based on between 96-127.
Video Bit Rate	Set the bandwidth of video call
Video Frame Rate	Set the video frame rate
Video Resolution	Set the video resolution; QCIF(176*144), CIF(352*288), VGA(640*480), 4CIF(704*576), 720P(1280x720). Note: 720P only on the four nuclear phone support, And need to choose above 2M of the bandwidth
Display Mosaic Frames	Enable or Disable display mosaic

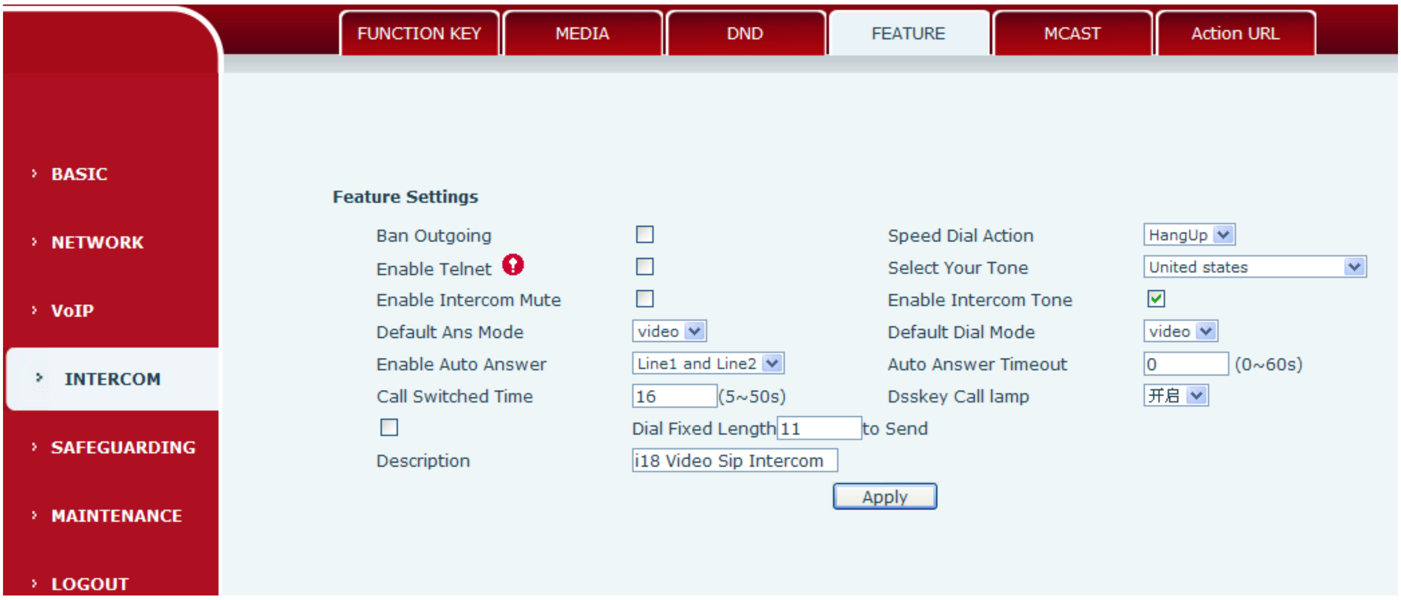
Field Name	Explanation
RTP Control Protocol(RTCP) Settings	
CNAME user	Set CNAME user
CNAME host	Set CNAME host
Sound Update	
Choose the ring tone files and then click update to apply	
Sound Delete	
Delete the ring tone file	
Sound Settings	
Set the ring tong files, format is .mp3 and .wav	

c) DND



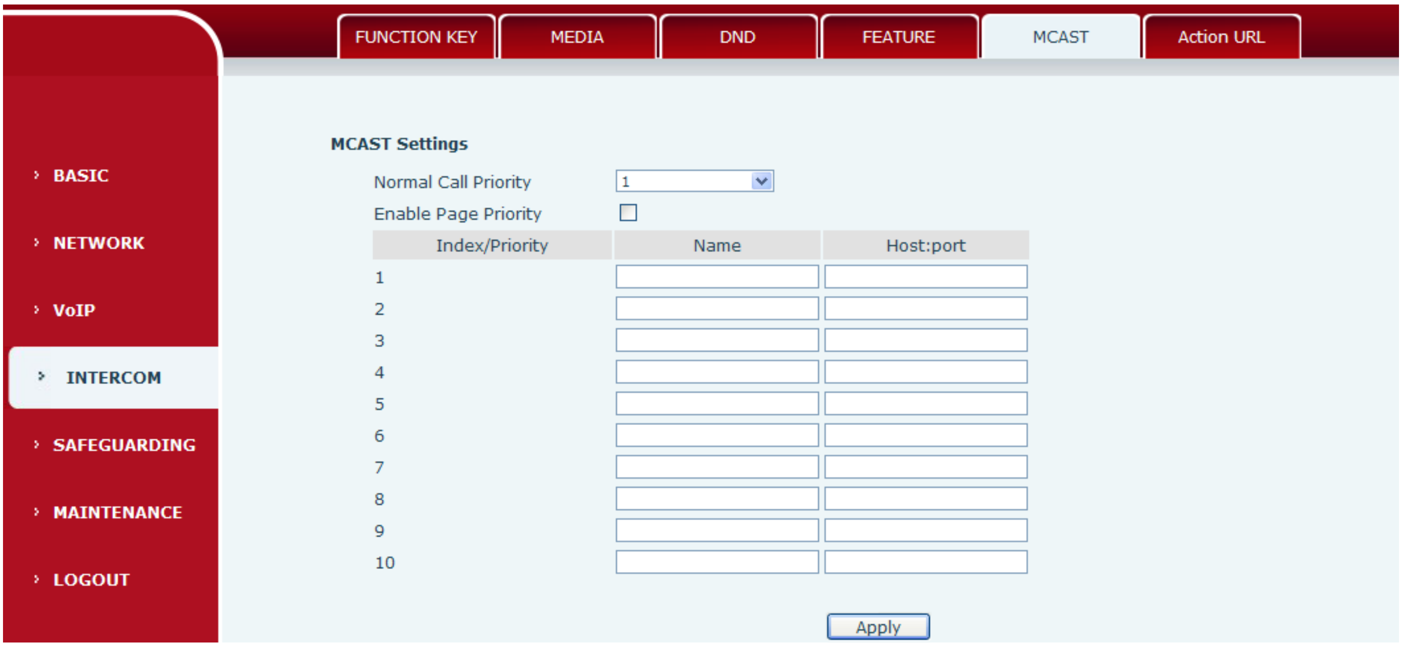
Field Name	Explanation
DND Methods Settings	
DND Option	Set the DND option, default is phone.
DND Line Settings	
SIP1	Enable or Disable sip1 DND
SIP2	Enable or Disable sip2 DND
DND Global Settings	
Enable DND Timer	Enable or disable DND timer
DND Timer	Set the DND time
Enable White List DND	Enable or disable white list DND

d) FEATURE



Feature	
Field Name	**Explanation**
Feature Settings	
Ban Outgoing	If enabled, no outgoing calls can be made.
Speed Dial Action	Default is Speed Dial Hand-down function
Enable Telnet	Enable or disable Telnet
Select Your Tone	Standard configuration signal sound.
Enable Intercom Mute	If enabled, mutes incoming calls during an intercom call.
Enable Intercom Tone	If enabled, plays intercom ring tone to alert to an intercom call.
Default Ans Mode	Set answer mode, default is video .
Default Dial Mode	Set dial mode, default is video.
Enable Auto Answer	Enable Auto Answer function
Auto Answer Timeout	Set Auto Answer Timeout
Call Switched Time	Set the call switched time.
Dsskey Call lamp	Configuration is enabled when the speed dial key to call light condition.
Dial Fixed Length to Send	The number will be sent to the server after the specified numbers of digits are dialed.
Description	device IP description

e) MCAST



It is easy and convenient to use multicast function to send notice to each member of the multicast via setting the multicast key on the device and sending multicast RTP stream to pre-configured multicast address. By configuring monitoring multicast address on the device, monitor and play the RTP stream which sent by the multicast address.

MCAST Settings

Equipment can be set up to monitor up to 10 different multicast address, used to receive the multicast RTP stream sent by the multicast address.

Here are the ways to change equipment receiving multicast RTP stream processing mode in the Web interface: set the ordinary priority and enable page priority.

- Priority:

In the drop-down box to choose priority of ordinary calls the priority, if the priority of the incoming flows of multicast RTP, lower precedence than the current common calls, device will automatically ignore the group RTP stream. If the priority of the incoming flow of multicast RTP is higher than the current common calls priority, device will automatically receive the group RTP stream, and keep the current common calls in state. You can also choose to disable in the receiving threshold drop-down box, the device will automatically ignore all local network multicast RTP stream.

- The options are as follows:
  - ✧ 1-10: To definite the priority of the common calls, 1 is the top level while 10 is the lowest
  - ✧ Disable: ignore all incoming multicast RTP stream
  - ✧ Enable the page priority:

Page priority determines the device how to deal with the new receiving multicast RTP stream when it is in multicast session currently. When Page priority switch is enabled, the device will automatically ignore the low priority multicast RTP stream but receive top-level priority multicast RTP stream, and keep the current multicast session in state; If it is not enabled, the device will automatically ignore all receiving multicast RTP stream.

- Web Settings:

MCAST Settings

Priority: 1

Enable Page Priority: ☑

Index/Priority	Name	Host:port
1	ss	239.1.1.1:1366
2	ee	239.1.1.1:1367

The multicast SS priority is higher than that of EE, which is the highest priority.

Note: when pressing the multicast key for multicast session, both multicast sender and receiver will beep.

Listener configuration

MCAST Settings

Priority: 3

Enable Page Priority: ☑

Index/Priority	Name	Host:port
1	group 1	224.0.0.2:2366
2	group 2	224.0.0.2:1366
3	group 3	224.0.0.6:3366
4		
5		
6		
7		
8		
9		
10		

- **Blue part (name)**

"Group 1","Group 2" and "Group 3" are your setting monitoring multicast name.The group name will be displayed on the screen when you answer the multicast. If you have not set, the screen will display the IP: port directly.

- **Purple part (host: port)**

It is a set of addresses and ports to listen, separated by a colon.

- **Pink part (index / priority)**

Multicast is a sign of listening, but also the monitoring multicast priority. The smaller number refers to higher priority.

- **Red part (priority)**

It is the general call, non multicast call priority. The smaller number refers to high priority. The followings will explain how to use this option:

- ✧ The purpose of setting monitoring multicast "Group 1" or "Group 2" or "Group 3" launched a multicast call.
- ✧ All equipment has one or more common non multicast communication.
- ✧ When you set the Priority for the disable, multicast any level will not answer, multicast call is rejected.
- ✧ when you set the Priority to a value, only higher than the priority of multicast can come in, if you set the Priority is 3, group 2 and group 3 for priority level equal to 3 and less than 3 were rejected, 1 priority is 2 higher than ordinary call priority device can answer the multicast message at the same time, keep the hold the other call.

- **Green part (Enable Page priority)**

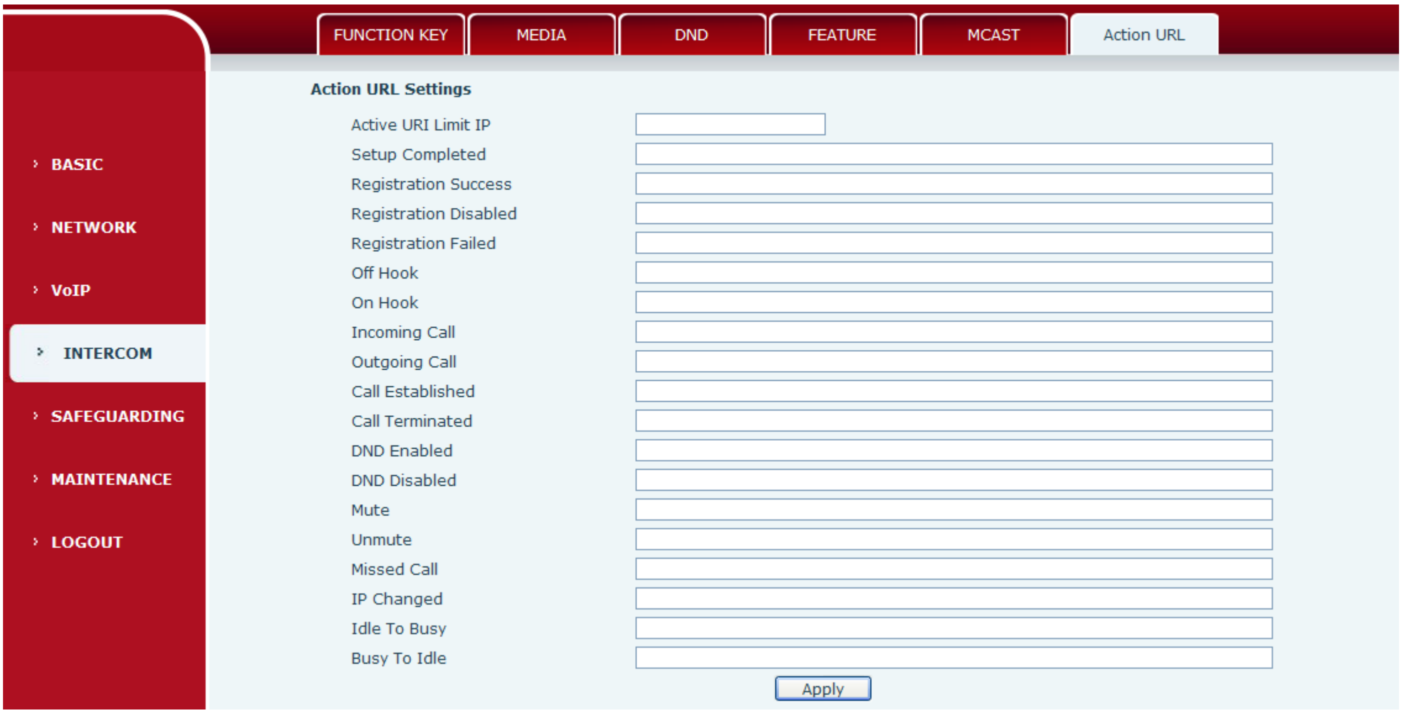
Set whether to open more priority is the priority of multicast, multicast is pink part number. Explain how to use:

- ✧ The purpose of setting monitoring multicast "group 1" or "3" set up listening "group of 1" or "3" multicast address multicast call.
- ✧ All equipment has been a path or multi-path multicast phone, such as listening to "multicast information group 2".
- ✧ If multicast is a new "group of 1", because "the priority group 1" is 2, higher than the current call "priority group 2" 3, so multicast call will can come in.
- ✧ If multicast is a new "group of 3", because "the priority group 3" is 4, lower than the current call "priority group 2" 3, "1" will listen to the equipment and maintain the "group of 2".

Multicast service

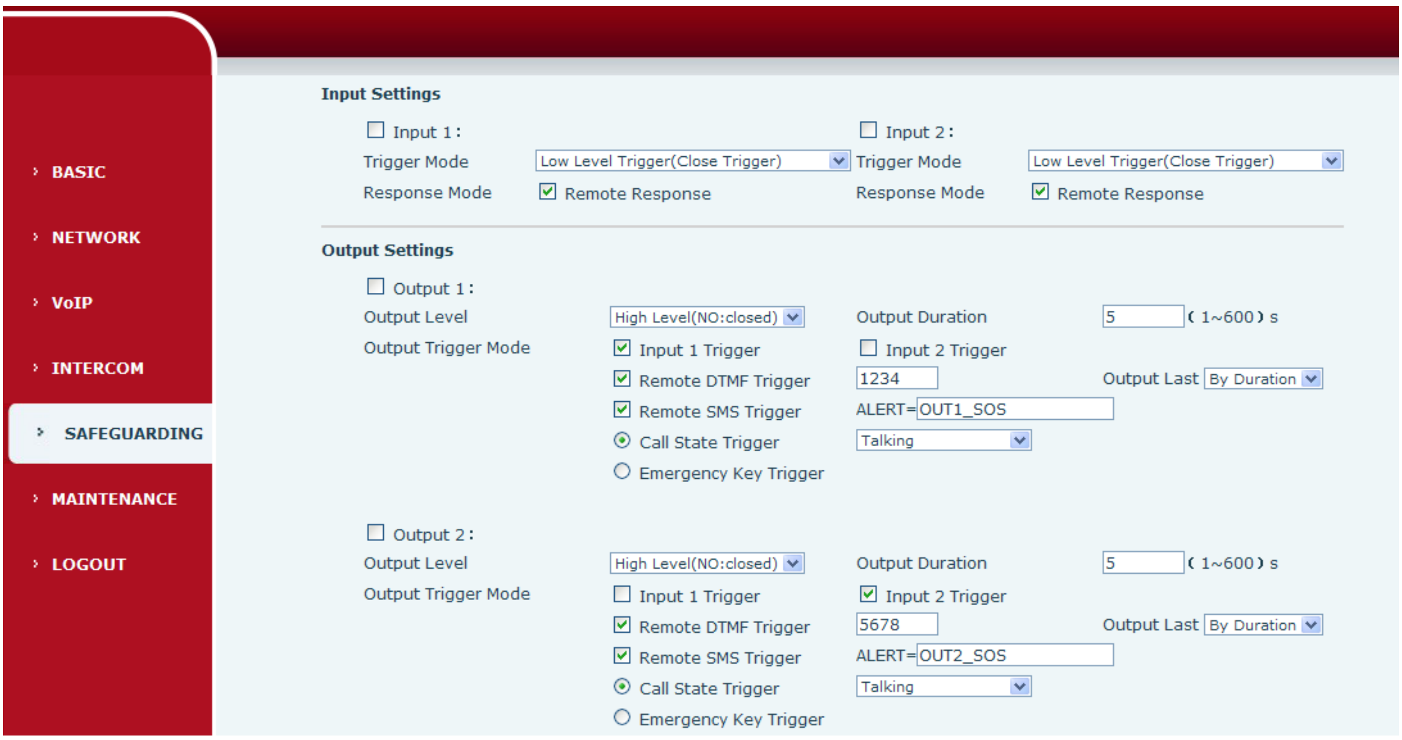
- **Send:** when configured ok, our key press shell on the corresponding equipment, equipment directly into the Talking interface, the premise is to ensure no current multicast call and 3-way of the case, the multicast can be established.
- **Lmonitor:** IP port and priority configuration monitoring device, when the call is initiated and incoming multicast, directly into the Talking interface equipment.

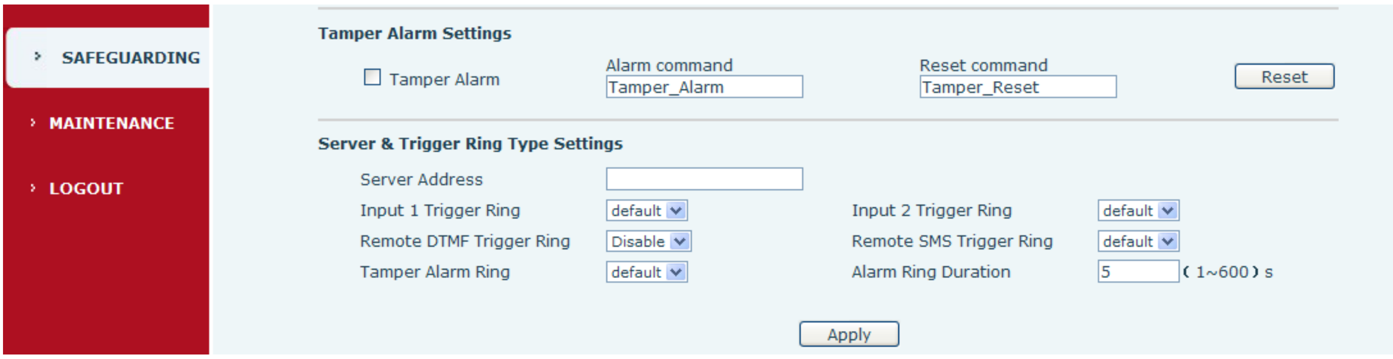
f) Action URL



Action URL Settings
URL for various actions performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is http://InternalServer /FileName.xml

(5) SAFEGUARDING



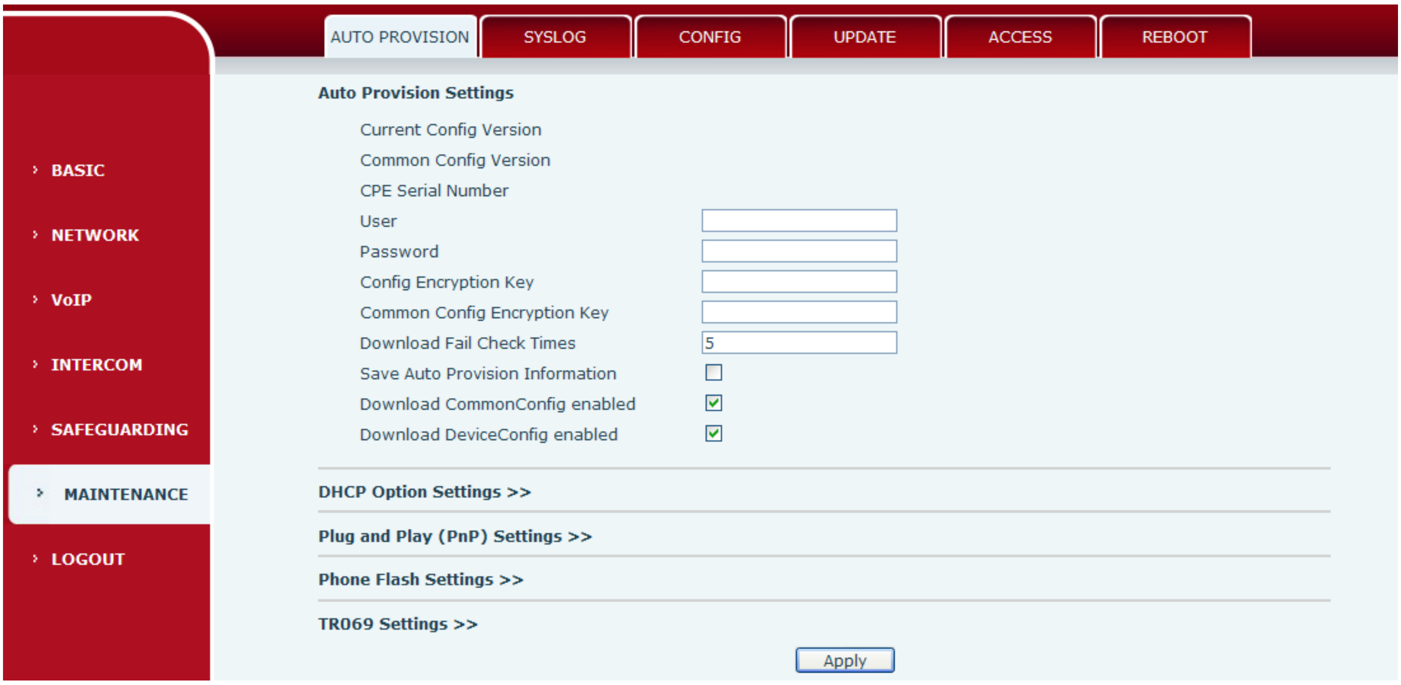


Safeguarding	
Field Name	**Explanation**
Input settings	
Input 1	Open /Close Input port1
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port 1 (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port 1 (high level) disconnected trigger.
Response Mode	Open /Close Input port1 the Remote Response
Input 2	Open /Close Input port2
Trigger Mode	When choosing the low level trigger (closed trigger), detect the input port 2 (low level) closed trigger.
	When choosing the high level trigger (disconnected trigger), detect the input port 2 (high level) disconnected trigger.
Response Mode	Open /Close Input port2 the Remote Response
Output Settings	
Output 1/2	Open/close, Output 1/Output 2
Output Level	When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.
	When choosing the high level trigger (NO: normally close), when meet the trigger condition, trigger the NO port close.
Output Duration	Changes in port, the duration of. The default is 5 seconds.
Output Trigger Mode: There are many kinds of trigger modes, multiple choices.	
Input port1 trigger	When the input port1 meet to trigger condition, the output port1 will trigger(The Port level time change, By < Output Duration > control)
Input port2 trigger	When the input port2 meet to trigger condition, the output port2 will trigger(The Port level time change, By < Output Duration > control)

Field Name	Explanation	
Remote DTMF trigger	By duration	Received the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, By < Output Duration > control)
	By Calling State	During the call, receive the terminal equipment to send the DTMF password, if correct, which triggers the corresponding output port (The Port level time change, (By call state control, after the end of the call, port to return the default state)
Remote SMS trigger	In the remote device or server to send instructions to ALERT=[instructions], if correct, which triggers the corresponding output port	
Call state trigger	The port output continuous time synchronization and trigger state changes, including the trigger conditions: 1, call; 2, call and singing; 3, singing; three models. (for example: the call trigger output port, will be in conversation state continued to output the corresponding level)	
Emergency key trigger	When the emergency call button to trigger the equipment shell, which triggers the corresponding output port(after the end of the call, port to return the default state)	
Tamper Alarm Settings		
Tamper Alarm	When the selection is enabled, the tamper detection enabled	
Alarm command	When detected someone tampering the equipment, will be sent alarm to the corresponding server	
Reset command	When the equipment receives the command of reset from server, the equipment will stop alarm	
Reset	Directly stop the alarm from equipment in the Webpage	
Server & Trigger Ring Type Settings		
Server Address	Configure remote response server address(including remote response server address and tamper alarm server address)	
Input 1 trigger ring	When the input port 1 triggering condition is satisfied, the corresponding ring tone or alarm	
Input 2 trigger ring	When the input port 2 triggering condition is satisfied, the corresponding ring tone or alarm	
Remote DTMF trigger ring	When received the remote DTMF command, whether to output the ringtone	
Remote SMS trigger ring	When receiving the remote SMS instructions, whether to output the ringtone	
Tamper alarm ring	When the detected someone tampering the equipment, plays the corresponding ringtone or alarm	
Alarm ring duration	duration of alarm ring(not including tamper alarm)	

(6) MAINTENANCE

a) AUTO PROVISION



The equipment supports PnP, DHCP, and Phone Flash to obtain configuration parameters. They will be queried in the following order when the equipment boots.

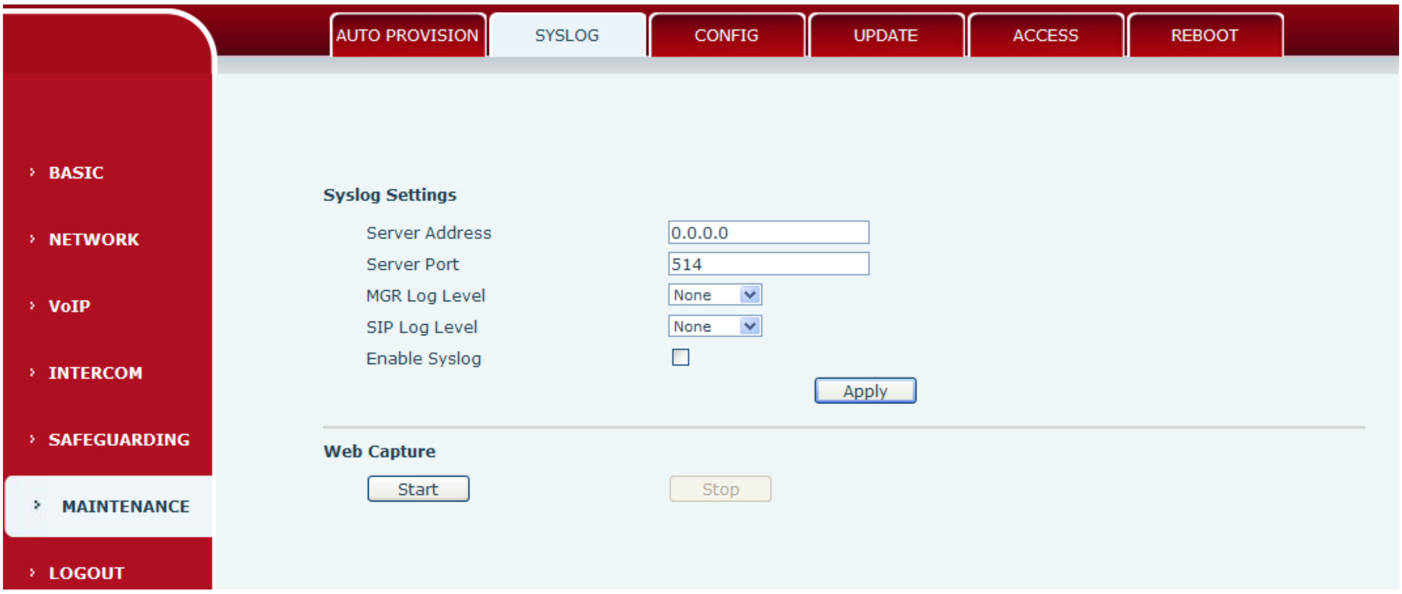
DHCP option → PnP server →Phone Flash

Field Name	**Explanation**
Auto Provision Settings	
Current Config Version	Show the current config file's version. If the version of configuration downloaded is higher than this, the configuration will be upgraded. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration
Common Config Version	Show the common config file's version. If the configuration downloaded and this configuration is the same, the auto provision will stop. If the endpoints confirm the configuration by the Digest method, the configuration will not be upgraded unless it differs from the current configuration.
CPE Serial Number	Serial number of the equipment
User	Username for configuration server. Used for FTP/HTTP/HTTPS. If this is blank the phone will use anonymous
Password	Password for configuration server. Used for FTP/HTTP/HTTPS.

Field Name	Explanation
Config Encryption Key	Encryption key for the configuration file
Common Config Encryption Key	Encryption key for common configuration file
Download Fail Check Times	Download failed and check times
Save Auto Provision Information	Save the auto provision username and password in the phone until the server url changes
Download CommonConfig enabled	Enable or disable download commonconfig
Download DeviceConfig enabled	Enable or disable download deviceconfig
DHCP Option Settings	
DHCP Option Setting	The equipment supports configuration from Option 43, Option 66, or a Custom DHCP option. It may also be disabled.
Custom DHCP Option	Custom option number. Must be from 128 to 254.
Plug and Play(PnP)Settings	
Enable PnP	If this is enabled, the equipment will send SIP SUBSCRIBE messages to a multicast address when it boots up. Any SIP server understanding that message will reply with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration.
PnP server	PnP Server Address
PnP port	PnP Server Port
PnP Transport	PnP Transfer protocol – UDP or TCP
PnP Interval	Interval time for querying PnP server. Default is 1 hour.
Phone Flash Settings	
Server Address	Set FTP/TFTP/HTTP server IP address for auto update. The address can be an IP address or Domain name with subdirectory.
Config File Name	Specify configuration file name. The equipment will use its MAC ID as the config file name if this is blank.
Protocol Type	Specify the Protocol type FTP, TFTP or HTTP.
Update Interval	Specify the update interval time. Default is 1 hour.

Field Name	Explanation
Update Mode	1. Disable – no update 2. Update after reboot – update only after reboot. 3. Update at time interval – update at periodic update interval
TR069 Settings	
Enable TR069	Enable/Disable TR069 configuration
Enable TR069 Warning Tone	Enable or disable TR069 Warning Tone
ACS Server Type	Select Common or CTC ACS Server Type.
ACS Server URL	ACS Server URL.
ACS User	User name for ACS.
ACS Password	ACS Password.
TR069 Auto Login	Enable/Disable TR069 Auto Login.

b) SYSLOG



Syslog is a protocol used to record log messages using a client/server mechanism. The Syslog server receives the messages from clients, and classifies them based on priority and type. Then these messages will be written into a log by rules which the administrator has configured.

There are 8 levels of debug information.

Level 0: emergency; System is unusable. This is the highest debug info level.

Level 1: alert; Action must be taken immediately.

Level 2: critical; System is probably working incorrectly.

Level 3: error; System may not work correctly.

Level 4: warning; System may work correctly but needs attention.

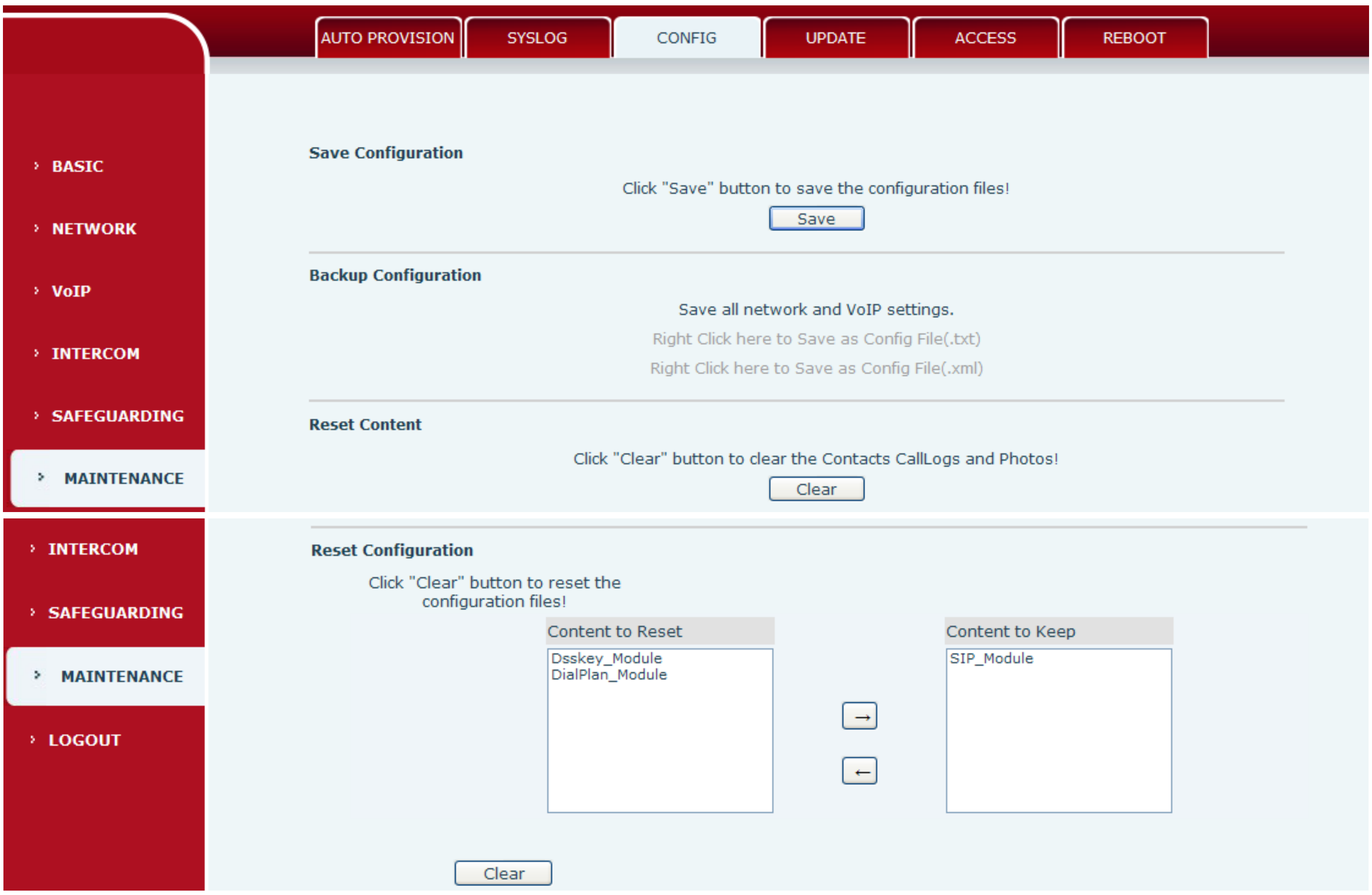
Level 5: notice; It is the normal but significant condition.

Level 6: Informational; It is the normal daily messages.

Level 7: debug; Debug messages normally used by system designer. This level can only be displayed via telnet.

Field Name	Explanation
Syslog settings	
Server Address	System log server IP address.
Server port	System log server port.
MGR log level	Set the level of MGR log.
SIP log level	Set the level of SIP log.
Enable syslog	Enable or disable system log.
Web Capture	
Start	Capture a packet stream from the equipment. This is normally used to troubleshoot problems.
Stop	Stop capturing the packet stream

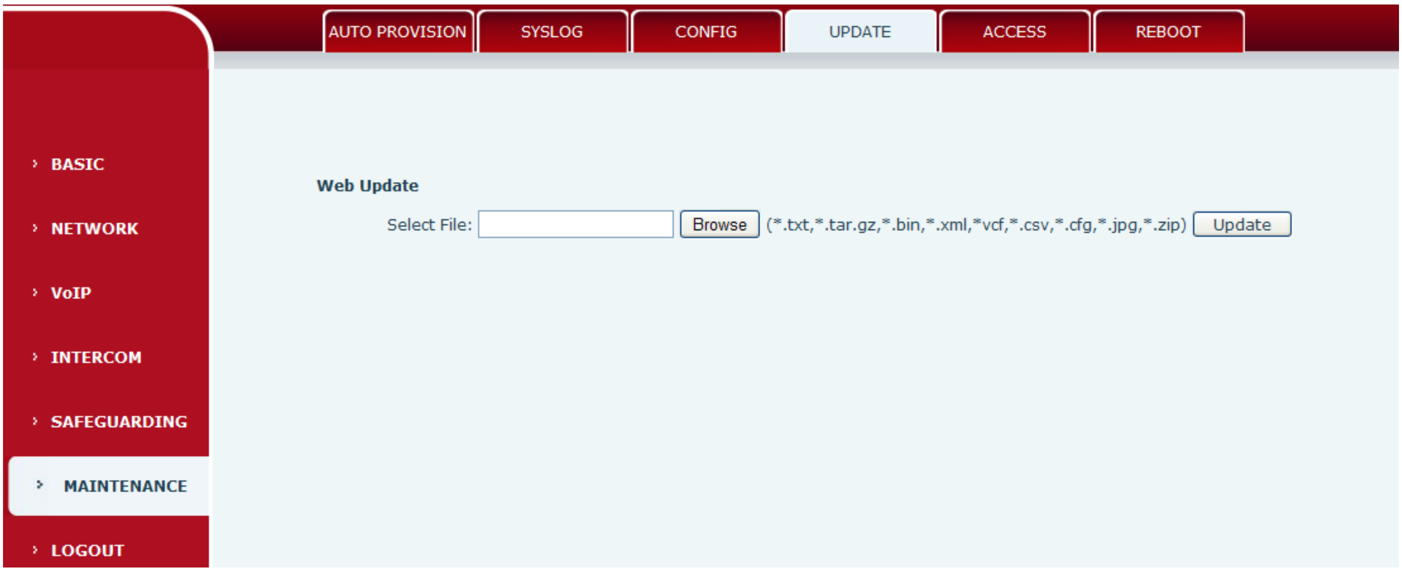
c) CONFIG



Field Name	Explanation
Save Configuration	Save the current equipment configuration. Clicking this saves all configuration changes and makes them effective immediately.
Backup Configuration	Save the equipment configuration to a txt or xml file. Please note to Right click on the choice and then choose “Save Link As.”
Reset Content	Click the "clear" button can reset phone records and photos.
Reset Configuration	To reset the system and Automatic restart the equipment.

d) UPDATE

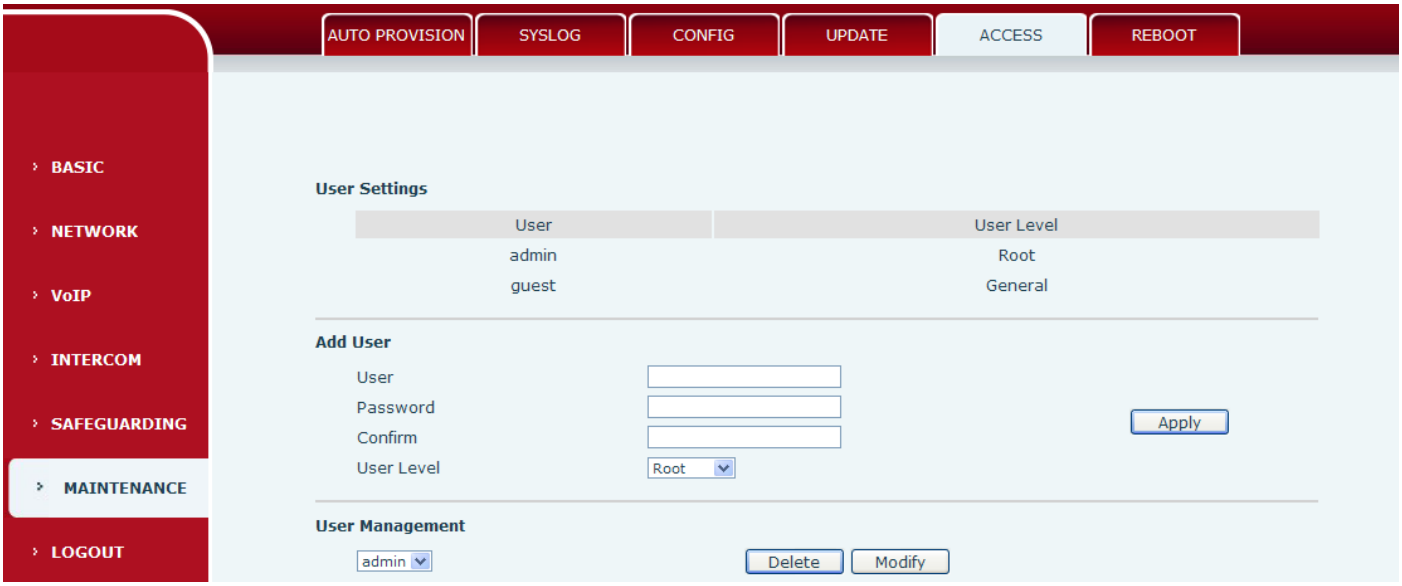
This page allows uploading configuration files to the equipment.



Field Name	Explanation
Web Update	Browse to the config file, and press Update to load it to the equipment. Various types of files can be loaded here including firmware, ring tones, local phonebook and config files in either text or xml format.

e) ACCESS

Through this page, user can add or remove users depends on their needs and can modify existing user permission.



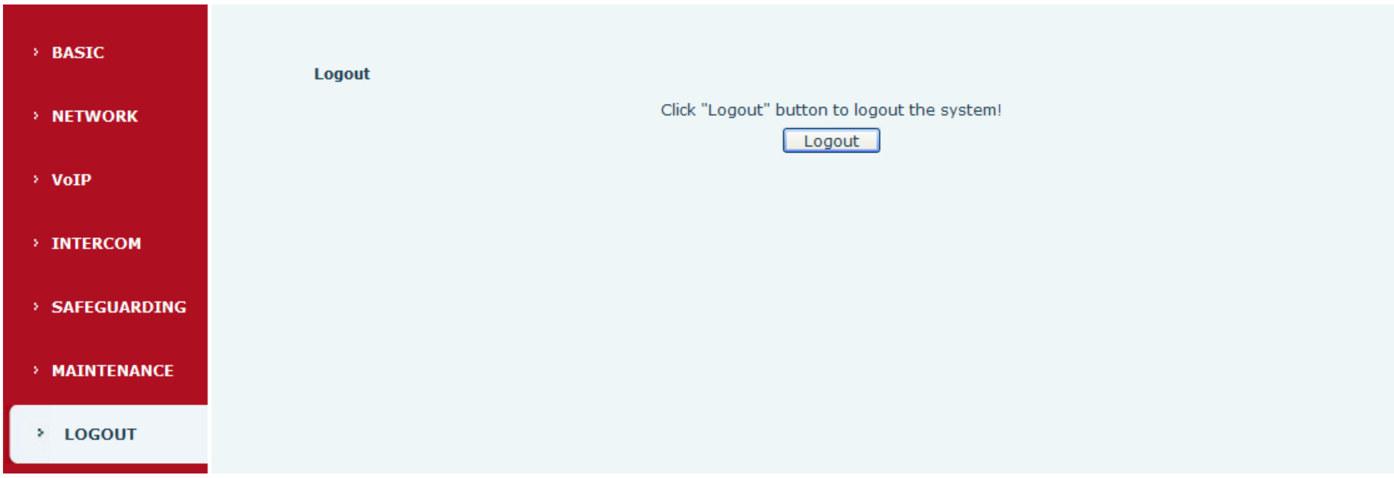
Field Name	Explanation
User Settings	
User	shows the current user name
User level	Show the user level; admin user can modify the configuration. General user can only read the configuration.
Add User	
User	Set User Account name
Password	Set the password
Confirm	Confirm the password
User level	There are two levels. Root user can modify the configuration. General user can only read the configuration.
User Management	
Select the account and click Modify to modify the selected account. Click Delete to delete the selected account. A General user can only add another General user.	

f) REBOOT

Some configuration modifications require a reboot to become effective. Clicking the Reboot button will lead to reboot immediately.

Note: Be sure to save the configuration before rebooting.

(7) LOGOUT



Click <Logout> from the web to exit. Users need to enter their user name and password again when visit next time.

E. Appendix

1. Technical parameters

Communication protocol		SIP 2.0(RFC-3261)
Main chipset		Freescale i.MX 6Quad
Key	**DSS key materials**	Stainless steel
	DSS Key	1 or 2
Speech flow	**Audio amplifier**	3W
	Volume control	Adjustable
	Full duplex speakerphone	Support (AEC)
	DTMF TYPE	In-band, Out-of-band(RFC 2833), SIP INFO
	wideband speech code	G.722
	Narrowband speech code	G711A/u, G.723.1, G.729AB, ILBC, AMR
Video	**Scope of broadband**	64kbps~4Mbps
	Video Framerate	10~30fps
	resolution	CIF, QCIF, VGA, 4CIF, 720P(HD)
	Video Codec	H.263, H.264
Port	**Security linkage**	2 embedded short circuit input interfaces
		2 embedded short circuit output interfaces
	External speakers	1 embedded audio output interfaces
	WAN	10/100BASE-TX s Auto-MDIX, RJ-45
Power supply mode		12V / 1A DC or PoE
Cables		CAT5 or better
Shell Material		Cast aluminium panel, Cast aluminium back shell
Working temperature		-40°C to 70°C
Working humidity		10% - 90%
Storage temperature		-40°C to 70°C
Installation way		Wall mounted or In-wall
Dimension		Wall mounted: 223*130*74mm In-wall: 270*150*61mm

2. Basic functions

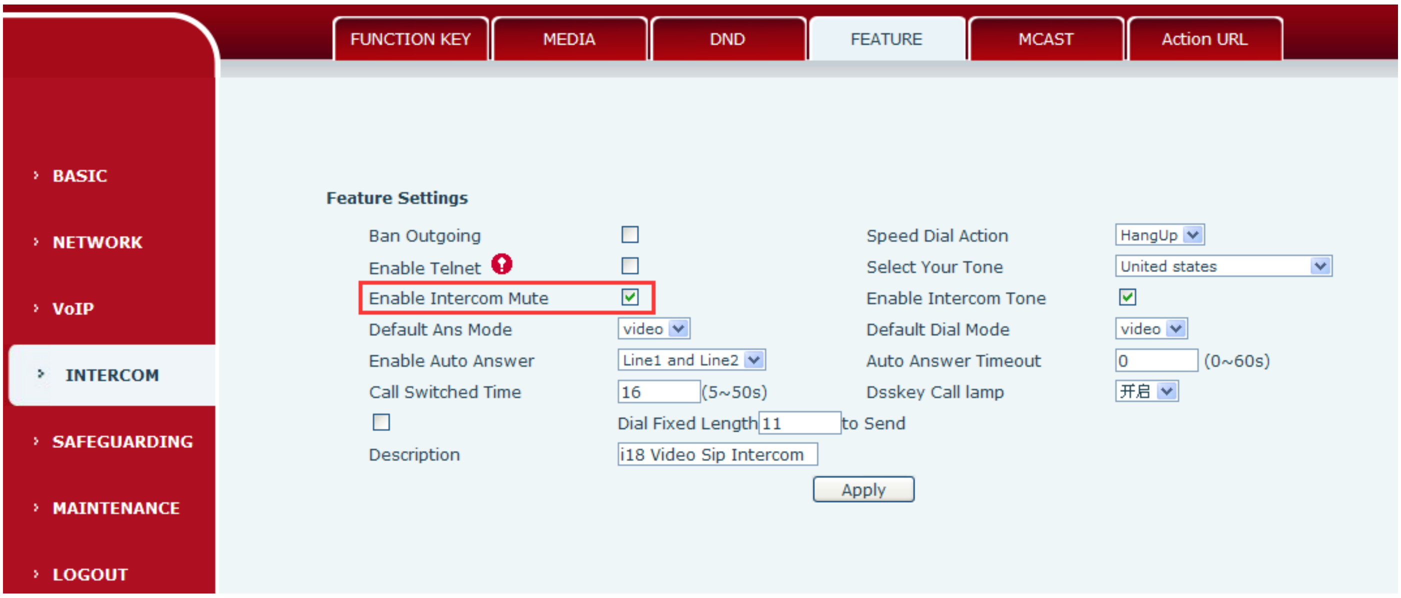
- 2 SIP Lines
- PoE Enabled
- Full-duplex speakerphone (HF)
- Intelligent DSS Keys (Speed Dial/intercom etc)
- Wall mounted / In-wall
- Special integrated noise reduction module
- Dual microphone Omnidirectional voice pickup
- 2 embedded short circuit input interfaces
- 2 embedded short circuit output interfaces. Support 4 controlled events: remote DTMF; remote server’s commands; interaction with short circuit input; talking status
- Output interface for active speaker
- Anti-tamper switch
- External power supply
- Record voice and video during calls (Optional)
- All in ONE: Radio and intercom, intelligent security function
- Industrial standard certifications: IP65， IK10， CE/FCC

3. Schematic diagram

4. The broadcast terminal configuration notice

✧ How to avoid an incoherency sound when the broadcast playing?

When the terminal use as broadcast, the speaker is loud, if not set mute for microphone, the AEC (echo cancellation) of equipment will be activated, which leads the sound incoherence. In order to avoid such circumstance, when the equipment turn to use as radio should be set as intercom mode, and activate the intercom mute, so as to ensure the broadcast quality.



✧ How to improve broadcasting tone quality?

In order to obtain better broadcast quality, recommend the use of the HD (G.722) mode for broadcast.

Voice bandwidth will be by the narrow width (G.722) of 4 KHz, is extended to broadband (G.722)7 KHz, when combined with the active speaker, the effect will be better.