



Yealink CP860 IP Phones Administrator Guide

Copyright

Copyright © 2014 YEALINK NETWORK TECHNOLOGY

Copyright © 2014 Yealink Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Yealink Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Yealink Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

Warranty

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS GUIDE ARE BELIEVED TO BE ACCURATE AND PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

YEALINK NETWORK TECHNOLOGY CO., LTD. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS GUIDE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Yealink Network Technology CO., LTD. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

Declaration of Conformity



Hereby, Yealink Network Technology CO., LTD. declares that this phone is in conformity with the essential requirements and other relevant provisions of the CE, FCC.

CE Mark Warning

This device is marked with the CE mark in compliance with EC Directives 2006/95/EC and 2004/108/EC.

Part 15 FCC Rules

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

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

Class B Digital Device or Peripheral

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

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

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.

GNU GPL INFORMATION

Yealink CP860 IP conference phone firmware contains third-party software under the GNU General Public License (GPL). Yealink uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license.

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded online:

<http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCatId=293&NewsCatId=293&CatId=293>.

About This Guide

The guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the IP phone system rather than the end-users. It provides details on the functionality and configuration of CP860 IP conference phones.

Many of the features described in this guide involve network settings, which could affect the IP phone's performance in the network. So an understanding of the IP networking and prior knowledge of IP telephony concepts are necessary.

Documentations

The following related documents for CP860 IP conference phones are available:

- Quick Start Guide, which describes how to assemble IP phones and configure the most basic features available on IP phones.
- User Guide, which describes basic and advanced features available on IP phones.
- Auto Provisioning Guide, which describes how to provision IP phones using the configuration files.
- y000000000037.cfg and <MAC>.cfg template configuration files.
- IP Phones Deployment Guide for BroadSoft UC-One Environments, which describes how to configure the BroadSoft features on the BroadWorks web portal and IP phones.

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online: <http://www.yealink.com/Support.aspx>.

In This Guide

The information detailed in this guide is applicable to the firmware version 72 or higher. The firmware format is like 37.x.0.x.rom. The second x from left should be greater than or equal to 72 (e.g., the firmware version of CP860 IP conference phone: 37.72.0.2.rom).

This administrator guide includes the following chapters:

- Chapter 1, "[Product Overview](#)" describes SIP components and SIP IP phones.
- Chapter 2, "[Getting Started](#)" describes how to install and connect IP phones and configuration methods.
- Chapter 3, "[Configuring Basic Features](#)" describes how to configure basic features on IP phones.
- Chapter 4, "[Configuring Advanced Features](#)" describes how to configure advanced features on IP phones.

- Chapter 5, "[Configuring Audio Features](#)" describes how to configure audio features on IP phones.
- Chapter 6, "[Configuring Security Features](#)" describes how to configure security features on IP phones.
- Chapter 7, "[Resource Files](#)" describes the resource files that can be downloaded by IP phones.
- Chapter 8, "[Troubleshooting](#)" describes how to troubleshoot IP phones and provides some common troubleshooting solutions.
- Chapter 9, "[Appendix](#)" provides the glossary, reference information about IP phones compliant with RFC 3261 and SIP call flows.

Table of Contents

About This Guide	v
Documentations	v
In This Guide	v
Table of Contents	vii
Product Overview	1
VoIP Principle	1
SIP Components	2
Introduction of CP860 IP Conference Phones	3
Physical Features of CP860 IP Conference Phones	4
Key Features of CP860 IP Conference Phones	4
Getting Started	7
Connecting the IP Phones	7
Connecting the Network and Power	7
Connecting the Optional Extension Microphones	9
Connecting the Optional USB Flash Drive	10
Connecting the Optional PC or Mobile Device	10
Initialization Process Overview	11
Verifying Startup	13
Reading Icons	13
Configuration Methods	14
Phone User Interface	15
Web User Interface	15
Configuration Files	15
Provisioning Server	16
Supported Provisioning Protocols	16
Setting up the Provisioning Server	17
Deploying Phones from the Provisioning Server	17
Configuring Basic Network Parameters	18
DHCP	18
Configuring Network Parameters Manually	24
Configuring Transmission Methods of the Internet Port	30
Upgrading Firmware	32

Configuring Basic Features 39

Contrast	40
Backlight	42
Web Server Type	43
User Password	46
Administrator Password	48
Phone Lock	50
Time and Date	54
Language	66
Loading Language Packs	66
Specifying the Language to Use	67
Logo Customization	70
Softkey Layout	72
Key as Send	77
Dial Plan	81
Replace Rule	82
Dial-now	84
Area Code	87
Block Out	89
Hotline	90
Directory	93
Search Source List in Dialing	94
Call Log	96
Missed Call Log	97
Local Directory	99
Live Dialpad	101
Call Waiting	103
Auto Redial	107
Auto Answer	109
Anonymous Call	112
Anonymous Call Rejection	116
Do Not Disturb	118
Busy Tone Delay	123
Return Code When Refuse	124
Early Media	126
180 Ring Workaround	126
Use Outbound Proxy in Dialog	128
SIP Session Timer	129
Call Hold	131
Session Timer	136
Call Forward	139
Call Transfer	147
Network Conference	150

Transfer on Conference Hang Up	152
Directed Call Pickup	153
Group Call Pickup.....	157
Call Return	160
Calling Line Identification Presentation	162
Connected Line Identification Presentation	164
DTMF	165
Suppress DTMF Display	169
Transfer via DTMF	172
Intercom.....	174
Outgoing Intercom Calls.....	174
Incoming Intercom Calls	175
Configuring Advanced Features.....	179
Distinctive Ring Tones	180
Tones	186
Remote Phone Book	192
LDAP.....	196
Message Waiting Indicator	204
Multicast Paging	208
Sending RTP Stream.....	208
Receiving RTP Stream	211
Action URL	215
Action URI.....	230
Server Redundancy.....	232
SIP Server Domain Name Resolution.....	239
Static DNS Cache	243
LLDP.....	251
VLAN	255
VPN.....	259
Quality of Service	262
Network Address Translation	266
SNMP	268
802.1X Authentication	272
TR-069 Device Management	278
IPv6 Support	283
Configuring Audio Features	291
Audio Codecs	291
Acoustic Clarity Technology.....	298
Acoustic Echo Cancellation	298
Background Noise Suppression.....	299
Automatic Gain Control	299

Voice Activity Detection	299
Comfort Noise Generation	301
Jitter Buffer	302
Configuring Security Features.....	305
Transport Layer Security.....	305
Secure Real-Time Transport Protocol.....	314
Encrypting Configuration Files	316
Resource Files	323
Replace Rule Template	324
Dial-now Template.....	325
Softkey Layout Template.....	326
Directory Template	327
Super Search Template.....	328
Local Contact File	330
Remote XML Phone Book.....	331
Troubleshooting.....	335
Troubleshooting Methods	335
Viewing Log Files.....	335
Capturing Packets	340
Enabling the Watch Dog Feature.....	341
Getting Information from Status Indicators.....	342
Analyzing Configuration Files	343
Troubleshooting Solutions	343
Why is the LCD screen blank?	343
Why doesn't the IP phone get an IP address?.....	344
How do I find the basic information of the IP phone?.....	344
Why doesn't the IP phone upgrade firmware successfully?.....	344
Why doesn't the IP phone display time and date correctly?	344
Why do I get poor sound quality during a call?	345
What is the difference between a remote phone book and a local phone book?	345
What is the difference between user name, register name and display name?	345
How to reboot the IP phone remotely?	345
Why does the IP phone use DOB format logo file instead of popular BMP, JPG and so on?	346
What will happen if I connect both PoE cable and power adapter? Which has the higher priority?.....	346
What is auto provisioning?	346
What is PnP?	346
Why doesn't the IP phone update the configuration?	347

What do “on code” and “off code” mean?	347
How to solve the IP conflict problem?	347
How to reset your phone to factory configurations?	347
How to restore the administrator password?	348
Appendix	349
Appendix A: Glossary	349
Appendix B: Time Zones	351
Appendix C: Configuring Programmable Key	353
Appendix D: SIP (Session Initiation Protocol)	356
RFC and Internet Draft Support	357
SIP Request	359
SIP Header	360
SIP Responses	361
SIP Session Description Protocol (SDP) Usage	364
Appendix E: SIP Call Flows	364
Successful Call Setup and Disconnect	365
Unsuccessful Call Setup—Called User is Busy	367
Unsuccessful Call Setup—Called User Does Not Answer	370
Successful Call Setup and Call Hold	372
Successful Call Setup and Call Waiting	374
Call Transfer without Consultation	379
Call Transfer with Consultation	383
Always Call Forward	388
Busy Call Forward	392
No Answer Call Forward	395
Call Conference	398
Index	403

Product Overview

This chapter contains the following information about CP860 IP conference phones:

- [VoIP Principle](#)
- [SIP Components](#)
- [Introduction of CP860 IP Conference Phones](#)

VoIP Principle

VoIP

VoIP (Voice over Internet Protocol) is a technology using the Internet Protocol instead of traditional Public Switch Telephone Network (PSTN) technology for voice communications.

It is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over IP networks. The H.323 and Session Initiation Protocol (SIP) are two popular VoIP protocols that are found in widespread implementation.

H.323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

It is widely implemented by voice and video conference equipment manufacturers, is used within various Internet real-time applications such as GnuGK and NetMeeting and is widely deployed by service providers and enterprises for both voice and video services over IP networks.

SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. It is an ASCII-based, application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides capabilities to:

- Determine the location of the target endpoint -- SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target endpoint -- Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint -- A call cannot be completed because the target endpoint is unavailable. SIP determines whether the called party is already on the IP phone or does not answer in the allotted number of rings. It then returns a message indicating why the target endpoint is unavailable.
- Establish a session between the origin and target endpoint -- The call can be completed, SIP establishes a session between endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the change of a media characteristic or codec.
- Handle the transfer and termination of calls -- SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

SIP Components

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function as one of the following roles:

- User Agent Client (UAC) -- A client application that initiates the SIP request.
- User Agent Server (UAS) -- A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and will make it challenging to put through a firewall. For this reason, it may be recommended to open the specific application type on the firewall. The UAC is also capable of using the information in the request URI to establish the course of the SIP request to its destination, as the request URI always specifies the host which is essential. The port and protocol are not always specified by the request URI. Thus if the request does not specify a port or protocol, a default port or protocol is contacted. It may be

preferential to use this method when not using an application layer firewall. Application layer firewalls like to know what applications are flowing through which ports and it is possible to use content types of other applications other than the one you are trying to let through what has been denied.

User agent server (UAS)

UAS is a server that hosts the application responsible for receiving the SIP requests from a UAC, and on reception it returns a response to the request back to the UAC. The UAS may issue multiple responses to the UAC, not necessarily a single response.

Communication between UAC and UAS is client/server and peer-to-peer.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but it functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the request.

Introduction of CP860 IP Conference Phones

This section introduces the CP860 IP conference phone. CP860 IP conference phones are endpoints in the overall network topology, which are designed to interoperate with other compatible equipments including application servers, media servers, internet-working gateways, voice bridges, and other endpoints. CP860 IP conference phones are characterized by a large number of functions, which simplify business communication with a high standard of security and can work seamlessly with a large number of SIP PBXs.

CP860 IP conference phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. The high-resolution graphic display provides content in multiple languages for system status, call log and directory access. CP860 IP conference phones also support advanced functionalities, including LDAP, Server Redundancy and Network Conference.

CP860 IP conference phones comply with the SIP standard (RFC 3261), and they can only be used within a network that supports this type of phone.

In order to operate as SIP endpoints in your network successfully, CP860 IP conference phones must meet the following requirements:

- A working IP network is established.
- Routers are configured for VoIP.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of CP860 IP conference phones is available.
- A call server is active and configured to receive and send SIP messages.

Physical Features of CP860 IP Conference Phones

This section lists the available physical features of CP860 IP conference phones.

CP860 IP conference phone



Physical Features:

- 192 x 64 graphic LCD
- One VoIP account
- HD Voice: HD Codec
- 1 mobile phone/PC port: 3.5mm
- 1xRJ45 10/100Mbps Ethernet port
- 2xEX mic ports
- 1xUSB2.0 port
- Security lock port
- 3 LED indicators
- Power adapter (optional): AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)

Key Features of CP860 IP Conference Phones

In addition to physical features introduced above, CP860 IP conference phones also support the following key features when running the latest firmware:

- **Phone Features**
 - **Call Options:** call waiting, call hold, call mute, call forward, call transfer, call pickup, conference.

- **Basic Features:** DND, auto redial, live dialpad, dial plan, hotline, caller identity, auto answer.
- **Advanced Features:** server redundancy, distinctive ring tones, remote phone book, LDAP, 802.1X authentication.
- **Codecs and Voice Features**
 - Codecs: G.722, PCMU, PCMA, G.729, G.723, G.726, iLBC
 - VAD, CNG, AEC, PLC, AJB, AGC
 - Full-duplex speakerphone with AEC
 - Built in microphone array, 360 degree voice pickup
- **Network Features**
 - SIP v1 (RFC2543), v2 (RFC3261)
 - IPv4/IPv6 support
 - NAT Traversal: STUN mode
 - DTMF: INBAND, RFC2833, SIP INFO
 - Proxy mode and peer-to-peer SIP link mode
 - IP assignment: Static/DHCP
 - TFTP/DHCP client
 - HTTP/HTTPS server
 - DNS client
 - NAT/DHCP server
- **Management**
 - FTP/TFTP/HTTP(S)/PnP auto-provision
 - Configuration: browser/phone/auto-provision
 - Direct IP call without SIP proxy
 - Dial number via SIP server
 - Dial URL via SIP server
- **Security**
 - HTTPS (server/client)
 - SRTP (RFC3711)
 - Transport Layer Security (TLS)
 - VLAN (802.1q), QoS
 - Digest authentication using MD5/MD5-sess
 - Secure configuration file via AES encryption
 - Phone lock for personal privacy protection
 - Admin/User configuration mode

Getting Started

This chapter provides basic information and installation instructions of CP860 IP conference phones.

This chapter provides the following sections:

- [Connecting the IP Phone](#)
- [Initialization Process Overview](#)
- [Verifying Startup](#)
- [Reading Icons](#)
- [Configuration Methods](#)
- [Provisioning Server](#)
- [Configuring Basic Network Parameters](#)
- [Upgrading Firmware](#)

Connecting the IP Phones

This section introduces how to install CP860 IP conference phones with the components in packaging contents.

1. Connecting the Network and Power
2. Connecting the Optional Extension Microphones Kit
3. Connecting the Optional USB Flash Drive
4. Connecting the Optional PC or Mobile Device

Note

A power adapter, PC or mobile device, extension microphone kit and USB flash drive are not included in packaging contents. You need to purchase them separately.

Connecting the Network and Power

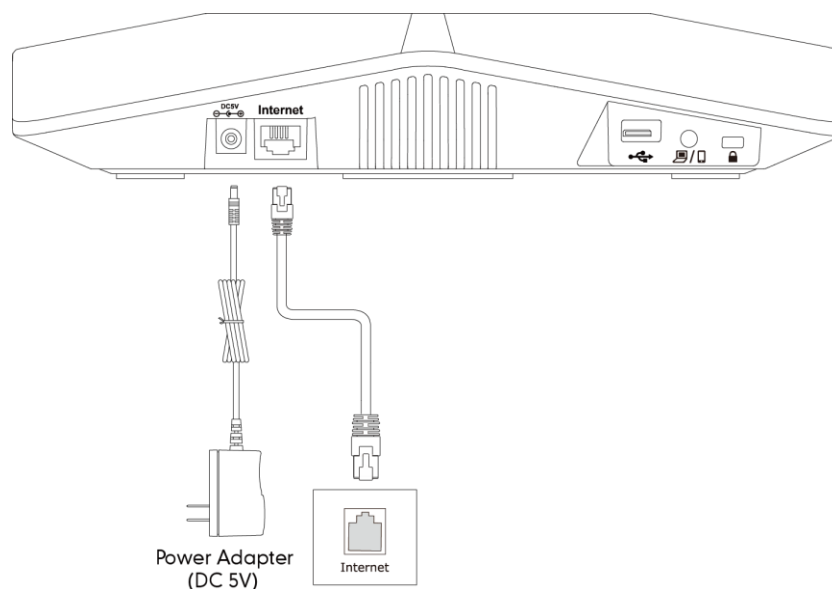
You have two options for power and network connections. Your system administrator will advise you which one to use.

- AC power
- Power over Ethernet (PoE)

AC Power (Optional)

To connect the AC power and network:

1. Connect the DC plug of the power adapter to the DC5V port on IP phones and connect the other end of the power adapter into an electrical power outlet.
2. Connect the included or a standard Ethernet cable between the Internet port on IP phones and the one on the wall or switch/hub device port.

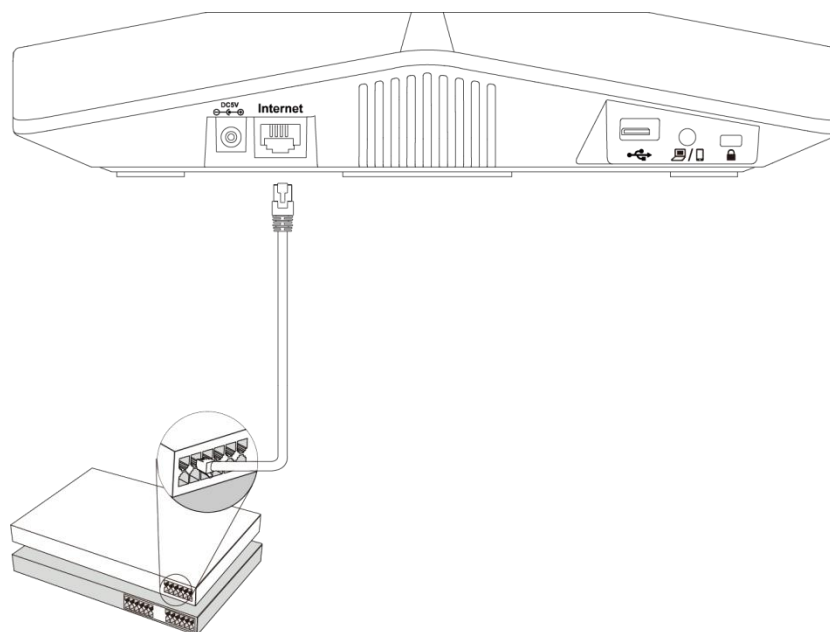


Power over Ethernet

With the included or a regular Ethernet cable, the CP860 IP conference phone can be powered from a PoE-compliant switch or hub.

To connect the PoE:

1. Connect the Ethernet cable between the Internet port on the IP phone and an available port on the in-line power switch/hub.

**Note**

If in-line power switch/hub is provided, you don't need to connect the phone to the power adapter. Make sure the switch/hub is PoE-compliant.

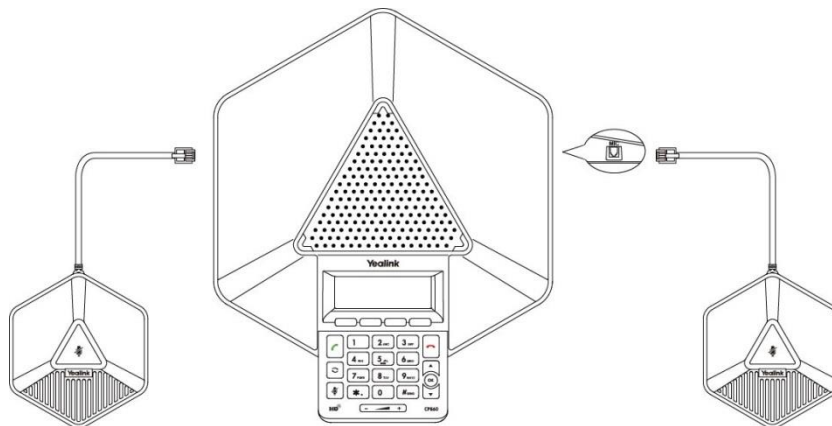
Important! Do not unplug or remove power to the phone while it is updating firmware and configurations.

Connecting the Optional Extension Microphones

You can connect optional extension microphones to enhance the room coverage of the conference phone. The Yealink-provided extension microphone kit contains two extension microphones.

To connect the extension microphones:

1. Connect the free end of the optional extension microphone cable to one of the MIC ports on the phone.

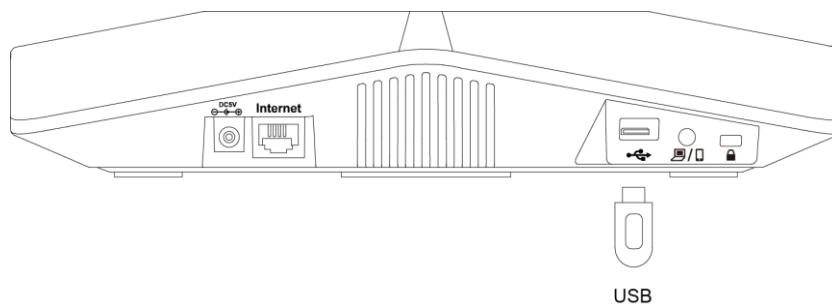


Connecting the Optional USB Flash Drive

You can connect a USB flash drive to record and play back calls.

To connect a USB flash drive:

1. Insert a USB flash drive into the USB port on the phone.

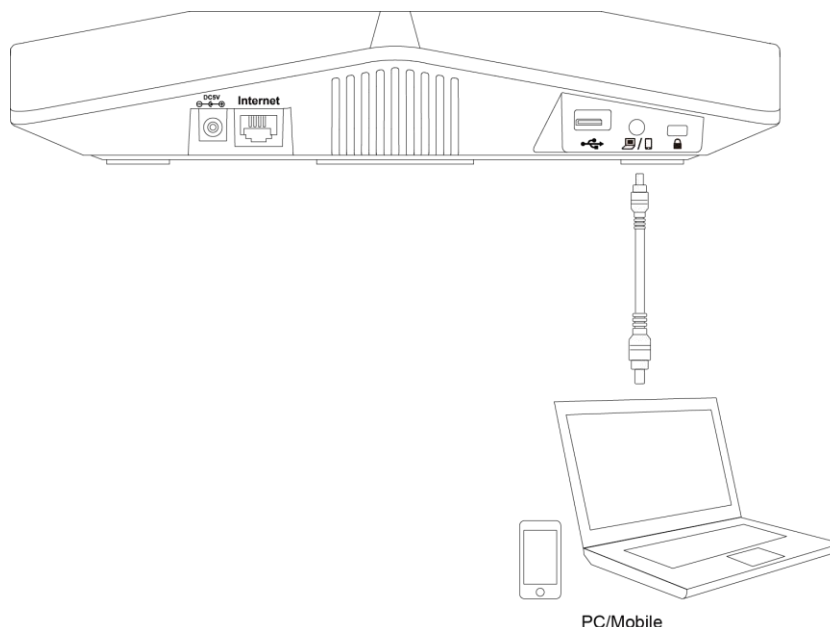


Connecting the Optional PC or Mobile Device

You can connect a PC or mobile device to listen to the PC or mobile audio using your conference phone.

To connect a PC or mobile device:

1. Connect one end of the 3.5mm jack cable to the PC/mobile port on the phone, and connect the other end to the headset jack on the mobile device or the AUX/MIC jack on the PC.



Initialization Process Overview

The initialization process of IP phones is responsible for network connectivity and operation of IP phones in your local network.

Once you connect your IP phone to the network and to an electrical supply, the IP phone begins its initialization process.

During the initialization process, the following events proceed:

Loading the ROM file

The ROM file resides in the flash memory of IP phones. IP phones come from the factory with a ROM file preloaded. During initialization, IP phones run a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If IP phones are connected to a switch, the switch notifies IP phones of the VLAN information defined on the switch (if using LLDP). IP phones can then proceed with the DHCP request for their network settings (if using DHCP).

Querying the DHCP (Dynamic Host Configuration Protocol) Server

IP phones are capable of querying a DHCP server. DHCP is enabled on IP phones by default. The following network parameters can be obtained from the DHCP server during initialization:

- IP Address
- Subnet Mask
- Gateway
- Primary DNS (Domain Name Server)
- Secondary DNS

You need to configure the network parameters of IP phones manually if any of them is not provided by the DHCP server. For more information on configuring network parameters manually, refer to [Configuring Network Parameters Manually](#) on page 24.

Contacting the auto provisioning server

CP860 IP conference phones support the FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured by default to use TFTP protocol. If IP phones are configured to obtain configurations from the TFTP server, they will connect to the TFTP server and download the configuration file(s) during startup. IP phones will be able to resolve and apply the configurations written in the configuration file(s). If IP phones do not obtain the configurations from the TFTP server, IP phones will use the configurations stored in the flash memory.

Updating firmware

If the access URL of the firmware is defined in the configuration file, the IP phone will download the firmware from the provisioning server. If the MD5 value of the downloaded firmware file differs from that of the image stored in the flash memory, the IP phone will perform a firmware update.

Downloading the resource files

In addition to configuration file(s), IP phones may require resource files before it can deliver service. These resource files are optional, but if some particular features are being deployed, these files are required.

The followings show examples of resource files:

- Language packs
- Ring tones
- Contact files

Verifying Startup

After connected to the power and network, the IP phone begins the initializing process by cycling through the following steps:

1. Three LED indicators on the phone illuminate solid red.
2. The message “Initializing...please wait” appears on the LCD screen when the IP phone starts up.
3. The main LCD screen displays the following:
 - Time and date
 - Soft key labels
4. Press the OK key to check the IP phone status, the LCD screen displays the valid IP address, MAC address, firmware version, etc.









If IP phones are first powered on or the phone settings are reset to factory defaults, the setup wizard will appear on the LCD screen after startup. For more information on the setup wizard, refer to *Yealink_CP860_User_Guide*, available online:

















<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

When the IP phone has successfully passed through these steps, it starts up properly and is ready for use.

Reading Icons

Icons associated with different features may appear on the LCD screen. The following table provides a description for each icon on CP860 IP conference phone models.

Icon	Description
	Network is unavailable
	Registered successfully
	Register failed
	Registering
	Hands-free speakerphone mode
	Voice Mail
	Auto Answer
	Do Not Disturb

Icon	Description
	Call Hold
	Call Mute
	Ringer volume is 0
	Keypad Lock
	Alphanumeric input mode
	Numeric input mode
	Multi-lingual lowercase letters input mode
	Multi-lingual uppercase letters input mode
	Multi-lingual uppercase and lowercase letters input mode
	Call Forward/Forwarded Calls
	Missed Calls
	Received Calls
	Placed Calls
	USB flash drive is inserted
	USB flash drive is detecting
	High Definition Voice

Configuration Methods

IP phones can be configured automatically through configuration files stored on a central provisioning server, manually via the phone user interface or web user interface, or by a combination of the automatic and manual methods.

The recommended method for configuring IP phones is automatically through a central provisioning server. If a central provisioning server is not available, the manual method will allow changes to most features.

The following sections describe how to configure IP phones using each method.

- [Phone User Interface](#)

- [Web User Interface](#)
- [Configuration Files](#)

Phone User Interface

An administrator or a user can configure and use IP phones via phone user interface. Specific features access is restricted to the administrator. These specific features are password protected by default. The default password is “admin”(case-sensitive). Not all features are available on phone user interface. For more information, refer to *Yealink_CP860_User_Guide*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Web User Interface

An administrator or a user can configure IP phones via web user interface. The default user name and password for the administrator to log into the web user interface are both “admin” (case-sensitive). Most features are available for configuring via web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to [Web Server Type](#) on page 43.

Configuration Files

An administrator can deploy and maintain a mass of IP phones using configuration files. The configuration files consist of:

- Common CFG file
- MAC-Oriented CFG file

Common CFG file

A common CFG file contains parameters that affect the basic operation of the IP phone, such as language and volume. It will be effectual for all IP phones of the same model. The common CFG file has a fixed name for each IP phone model. The name of the common CFG file for the CP860 IP conference phone model is y0000000000037.cfg.

MAC-Oriented CFG file

A MAC-Oriented CFG file contains parameters unique to a particular phone. It will only be effectual for a specific IP phone. The MAC-Oriented CFG file is named after the MAC address of the IP phone. For example, if the MAC address of a CP860 IP conference phone is 001565113af8, the name of the MAC-Oriented CFG file must be 001565113af8.cfg.

Central Provisioning

IP phones can be centrally provisioned from a provisioning server using the

configuration files (y000000000037.cfg and <MAC>.cfg). You can use a text-based editing application to edit configuration files, and then store configuration files to a provisioning server. For more information on the provisioning server, refer to [Provisioning Server](#) on page 16.

IP phones can obtain the provisioning server address during startup. Then IP phones download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

When modifying parameters, learn the following:

- Parameters in configuration files override those stored in IP phones' flash memory.
- The .cfg extension of the configuration files must be in lowercase.
- Each line in a configuration file must use the following format and adhere to the following rules:

```
variable-name = value
```

- Associate only one value with one variable.
- Separate variable name and value with equal sign.
- Set only one variable per line.
- Put the variable and value on the same line, and do not break the line.
- Comment the variable on a separated line. Use the pound (#) delimiter to distinguish the comments.

Provisioning Server

Supported Provisioning Protocols

IP phones perform the auto provisioning function of downloading configuration files, downloading resource files and upgrading firmware. The transfer protocol is used to download files from the provisioning server. IP phones support several transport protocols for provisioning, including FTP, TFTP, HTTP, and HTTPS protocols, and are configured to use the TFTP protocol by default. The provisioning server address can be IP address, domain name or URL. If a user name and password are specified as part of the provisioning server address, for example, <http://user:pwd@server/dir>, they will be used only if the server supports them.

Note

A URL should contain forward slashes instead of back slashes and should not contain spaces. Escape characters are not supported.

If a user name and password are not specified as part of the provisioning server address, the User Name and Password of the provisioning server configured on the IP phone will be used.

There are two types of FTP methods—active and passive. IP phones are not compatible with active FTP.

Setting up the Provisioning Server

The provisioning server can be on the local LAN or anywhere on the Internet. Use the following procedure as a recommendation if this is your first provisioning server setup. For more information on how to set up a provisioning server, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide*.

To set up the provisioning server:

1. Install a provisioning server application or locate a suitable existing server.
2. Create an account and home directory.
3. Set security permissions for the account.
4. Create configuration files and edit them as desired.
5. Copy the configuration files and resource files to the provisioning server.

For more information on how to deploy IP phones using configuration files, refer to [Deploying Phones from the Provisioning Server](#) on page 17.

Note

Typically all phones are configured with the same server account, but the server account provides a means of conveniently partitioning the configuration. Give each account a unique home directory on the server and change the configuration on a per-account basis.

Deploying Phones from the Provisioning Server

The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. During auto provisioning, IP phones download the common configuration file first, and then the MAC-oriented file. Therefore any parameter in the MAC-oriented configuration file will override the same one in the common configuration file.

Yealink supplies configuration files for each phone model, which is delivered with the IP phone firmware. The configuration files, supplied with each firmware release, must be used with that release. Otherwise, configurations may not take effect, and the IP phone will behave without exception. Before you configure parameters in the configuration files, Yealink recommends that you create new configuration files containing only those parameters that require changes.

To deploy IP phones from the provisioning server:

1. Create per-phone configuration files by performing the following steps:
 - a) Obtain a list of phone MAC addresses (the bar code label on the back of the IP phone or on the outside of the box).
 - b) Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
 - c) Edit the parameters in the file as desired.

2. Create new common configuration files by performing the following steps:
 - a) Create y000000000037.cfg files by using the Common CFG file from the distribution as templates.
 - b) Edit the parameters in the file as desired.
3. Copy configuration files to the home directory of the provisioning server.
4. Reboot IP phones to trigger the auto provisioning process.

IP phones discover the provisioning server address, and then download the configuration files from the provisioning server.

For more information on configuration files, refer to Configuration Files on page 15. For more information on encrypting configuration files, refer to [Encrypting Configuration Files](#) on page 316.

- **Zero Touch:** Zero Touch feature guides you to configure network settings and the provisioning server address via phone user interface after startup.
- **PnP:** PnP feature allows IP phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **DHCP:** DHCP option can be used to provide the address or URL of the provisioning server to IP phones. When the IP phone requests an IP address using DHCP, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static:** You can configure the static provisioning server address via phone user interface, via web user interface or using configuration files.

For more information on the above methods, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Configuring Basic Network Parameters

In order to get your IP phones running, you must perform basic network setup, such as IP address and subnet mask configuration. This section describes how to configure basic network parameters for IP phones.

Note

This section mainly introduces IPv4 network parameters. IP phones also support IPv6. For more information on IPv6, refer to [IPv6 Support](#) on page 283.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. IP

phones comply with the DHCP specifications documented in RFC 2131. If DHCP is used, IP phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters. Static DNS address(es) can be configured and used when DHCP is enabled.

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

DHCP can be initiated by simply connecting the IP phone with the network. IP phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with the specific values in the corresponding options.

The following table lists the common DHCP options supported by IP phones.

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client's subnet mask.
Time Offset	2	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client's subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.
Network Time Protocol Servers	42	Specify a list of the NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.

Parameter	DHCP Option	Description
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identify a bootfile when the 'file' field in the DHCP header has been used for DHCP options.

For more information on DHCP options, refer to
<http://www.ietf.org/rfc/rfc2131.txt?number=2131> or
<http://www.ietf.org/rfc/rfc2132.txt?number=2132>.

If you do not have the ability to configure the DHCP options for discovering the provisioning server on the DHCP server, an alternate method of automatically discovering the provisioning server address is required. Connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address is one possibility. For more information, refer to
<http://www.ietf.org/rfc/rfc3925.txt?number=3925>.

Procedure

DHCP can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure DHCP on the IP phone. Parameter: network.internet_port.type Configure static DNS address when DHCP is used. Parameter: network.static_dns_enable network.primary_dns network.secondary_dns
Local	Web User Interface	Configure DHCP on the IP phone. Configure static DNS address when DHCP is used. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network&q=load">http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure DHCP on the IP phone.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.type	0 or 2	0
<p>Description: Configures the Internet (WAN) port type for IPv4 when the IP address mode is configured as IPv4 or IPv4&IPv6.</p> <p>0-DHCP 2-Static IP Address</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->IPv4 Config</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv4</p>		
network.static_dns_enable	0 or 1	0
<p>Description: Enables or disables the IP phone to use manually configured static IPv4 DNS when the Internet (WAN) port type for IPv4 is configured as DHCP.</p> <p>0-Disabled 1-Enabled</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->IPv4 Config->Static DNS</p> <p>Phone User Interface: None</p>		
network.primary_dns	IPv4 Address	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the primary IPv4 DNS server when the static IPv4 DNS is enabled.</p> <p>Example: network.primary_dns = 202.101.103.55</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->IPv4 Config->Static IP Address->Primary DNS</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port->IPv4->Static IPv4 Client->Primary DNS</p>		
network.secondary_dns	IPv4 Address	Blank
<p>Description: Configures the secondary IPv4 DNS server when the static IPv4 DNS is enabled.</p> <p>Example: network.secondary_dns = 202.101.103.54</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->IPv4 Config->Static IP Address->Secondary DNS</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port->IPv4->Static IPv4 Client ->Secondary DNS</p>		

To configure DHCP via web user interface:

1. Click on **Network->Basic**.

2. In the **IPv4 Config** block, mark the **DHCP** radio box.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Network' tab is selected. On the left, there are 'Basic' and 'Advanced' sub-tabs. The main content area is titled 'Internet Port' and shows a dropdown menu for 'Mode(IPv4/IPv6)' set to 'IPv4'. Below this, the 'IPv4 Config' section is highlighted with a red box. It contains two radio buttons: 'DHCP' (selected) and 'Static IP Address'. Under 'Static IP Address', there are input fields for 'IP Address', 'Subnet Mask', and 'Gateway'. Below these are 'Static DNS' options with 'On' and 'Off' radio buttons, and input fields for 'Primary DNS' and 'Secondary DNS'. The 'IPv6 Config' section is also visible, with 'DHCP' selected and similar input fields for 'IP Address', 'IPv6 Prefix(0~128)', 'Gateway', and 'Static DNS'. At the bottom are 'Confirm' and 'Cancel' buttons. A 'NOTE' sidebar on the right contains information about DHCP, Static IP Address, and PPPoE.

3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
4. Click **OK** to reboot the phone.

To configure static DNS address when DHCP is used via web user interface:

1. Click on **Network->Basic**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. Mark the **On** radio box in the **Static DNS** field.

4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected. Under 'Internet Port', the 'Mode' is set to 'IPv4/IPv6'. In the 'IPv4 Config' section, the 'DHCP' radio button is selected. Below it, the 'Static DNS' section is expanded, showing 'Primary DNS' as 202.101.103.55 and 'Secondary DNS' as 202.101.103.54. The 'IPv6 Config' section is also visible, with 'DHCP' selected and 'IPv6 Static DNS' set to 'Off'.

5. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

To configure DHCP via phone user interface:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin)
->**Network->WAN Port->IPv4->DHCP IPv4 Client**.
2. Press the **Save** soft key to accept the change.
The IP phone reboots automatically to make settings effective after a period of time.

Configuring Network Parameters Manually

If DHCP is disabled or IP phones cannot obtain network parameters from the DHCP server, you need to configure them manually. The following parameters should be configured for IP phones to establish network connectivity:

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- Secondary DNS

Procedure

Network parameters can be configured manually using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure network parameters of the IP phone manually.</p> <p>Parameters:</p> <p>network.internet_port.type</p> <p>network.ip_address_mode</p> <p>network.internet_port.ip</p> <p>network.internet_port.mask</p> <p>network.internet_port.gateway</p> <p>network.primary_dns</p> <p>network.secondary_dns</p>
Local	Web User Interface	<p>Configure network parameters of the IP phone manually.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=network&q=load</p>
	Phone User Interface	<p>Configure network parameters of the IP phone manually.</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.type	0 or 2	0
<p>Description:</p> <p>Configures the Internet (WAN) port type for IPv4 when the IP address mode is configured as IPv4 or IPv4&IPv6.</p> <p>0-DHCP</p> <p>2-Static IP Address</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic-> IPv4 Config</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port->IPv4</p>		
network.ip_address_mode	0, 1 or 2	0

Parameters	Permitted Values	Default
<p>Description: Configures the IP address mode.</p> <p>0-IPv4 1-IPv6 2-IPv4&IPv6</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->Internet Port->Mode (IPv4/IPv6)</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port ->IP Mode</p>		
network.internet_port.ip	IPv4 Address	Blank
<p>Description: Configures the IPv4 address when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address.</p> <p>Example: network.internet_port.ip = 192.168.1.20</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Basic->IPv4 Config->Static IP Address->IP Address</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port ->IPv4->Static IPv4 Client->IPv4 Address</p>		
network.internet_port.mask	Subnet Mask	Blank
<p>Description: Configures the IPv4 subnet mask when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address.</p> <p>Example: network.internet_port.mask = 255.255.255.0</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take</p>		

Parameters	Permitted Values	Default
<p>effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv4 Config->Static IP Address->Subnet Mask</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port ->IPv4->Static IPv4 Client->Subnet Mask</p>		
network.internet_port.gateway	IPv4 Address	Blank
<p>Description:</p> <p>Configures the IPv4 default gateway when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address.</p> <p>Example:</p> <p>network.internet_port.gateway = 192.168.1.254</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv4 Config->Static IP Address->Gateway</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port->IPv4->Static IPv4 Client->Default Gateway</p>		
network.primary_dns	IPv4 Address	Blank
<p>Description:</p> <p>Configures the primary IPv4 DNS server when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address.</p> <p>Example:</p> <p>network.primary_dns = 202.101.103.55</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv4 Config->Static IP Address->Primary DNS</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv4->Static IPv4 Client->Primary DNS</p>		

Parameters	Permitted Values	Default
network.secondary_dns	IPv4 Address	Blank
<p>Description:</p> <p>Configures the secondary IPv4 DNS server when the IP address mode is configured as IPv4 or IPv4&IPv6, and the Internet (WAN) port type for IPv4 is configured as Static IP Address.</p> <p>Example:</p> <p>network.secondary_dns = 202.101.103.54</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic-> Pv4 Config->Static IP Address->Secondary DNS</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port ->IPv4->Static IPv4 Client->Secondary DNS</p>		

To configure the IP address mode via web user interface:

1. Click on **Network->Basic**.
2. Select the desired value from the pull-down list of **Mode (IPv4/IPv6)**.

The screenshot shows the Yealink CP860 web user interface. The 'Network' tab is selected, and the 'Basic' sub-tab is active. The 'Internet Port' section is highlighted with a red box, showing the 'Mode (IPv4/IPv6)' dropdown menu set to 'IPv4'. The 'IPv4 Config' section is also visible, showing options for DHCP and Static IP Address. The 'IPv6 Config' section is also visible, showing options for DHCP and Static IP Address. A 'NOTE' box on the right side of the page provides additional information about DHCP and Static IP Address configurations.

3. Click **Confirm** to accept the change.
- A dialog box pops up to prompt that settings will take effect after reboot.

- Click **OK** to reboot the phone.

To configure a static IPv4 address via web user interface:

- Click on **Network->Basic**.
- In the **IPv4 Config** block, mark the **Static IP Address** radio box.
- Enter the IP address, subnet mask, default gateway, primary DNS and secondary DNS in the corresponding fields.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is active, and the 'Basic' sub-tab is selected. The 'Internet Port' is set to 'IPv4'. In the 'IPv4 Config' section, the 'Static IP Address' radio button is selected. The IP Address field contains '192.168.1.10', the Subnet Mask field contains '255.255.255.0', and the Gateway field contains '198.168.1.254'. In the 'Static DNS' section, the 'On' radio button is selected. The Primary DNS field contains '202.101.103.55' and the Secondary DNS field contains '202.101.103.54'. The 'IPv6 Config' section shows the 'DHCP' radio button selected. A 'NOTE' box on the right explains DHCP and Static IP Address configurations. 'Confirm' and 'Cancel' buttons are at the bottom.

- Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after reboot.
- Click **OK** to reboot the phone.

To configure the IP address mode via phone user interface:

- Press **Menu->Settings->Advanced Settings** (Default password: admin)
->**Network->WAN Port**
- Press the ◀ or ▶ soft key to select **IPv4**, **IPv6** or **IPv4 & IPv6** from the **IP Mode** field.
- Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

To configure a static IPv4 address via phone user interface:

- Press **Menu->Settings->Advanced Settings** (Default password: admin)
->**Network->WAN Port**.
- Press ▼ to select **IPv4** and press the **Enter** soft key.
- Press ▼ to select **Static IPv4 Client** and press the **Enter** soft key.

4. Enter the desired values in the **IPv4 Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** fields respectively.
5. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Note

Wrong network settings may result in inaccessibility of your phone and may also have an impact on your network performance. For more information on these parameters, contact your network administrator.

Configuring Transmission Methods of the Internet Port

The CP860 IP conference phone has Internet port only. There are three optional methods of transmission configuration for Internet port:

- Auto-negotiation
- Half-duplex
- Full-duplex

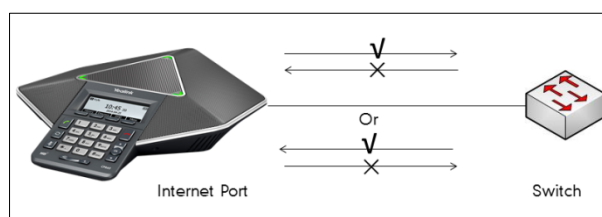
Auto-negotiation is configured for Internet port on the IP phone by default.

Auto-negotiation

Auto-negotiation means that all connected devices choose common transmission parameters (e.g., speed and duplex mode) to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both. You can configure the Internet port on IP phones to auto-negotiate during the transmission.

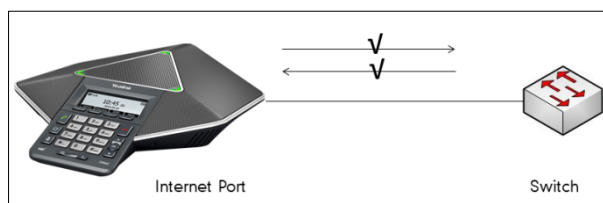
Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one device can send data on the line, but not receive data simultaneously. You can configure the half-duplex transmission on Internet port for IP phones to transmit in 10Mbps or 100Mbps.



Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. You can configure the full-duplex transmission on Internet port for IP phones to transmit in 10Mbps or 100Mbps.



Procedure

The transmission method of Internet port can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the transmission methods of Internet port. Parameters: network.internet_port.speed_duplex
Local	Web User Interface	Configure the transmission method of Internet port. Navigate to: <a href="http://<phoneIPAddress>/servlet?parameter=network-adv&q=load">http://<phoneIPAddress>/servlet?parameter=network-adv&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.speed_duplex	0, 1, 2, 3 or 4	0
Description: Configures the transmission method and speed of the Internet (WAN) port. 0 -Auto negotiate 1 -Full duplex, 10Mbps 2 -Full duplex, 100Mbps 3 -Half duplex, 10Mbps 4 -Half duplex, 100Mbps Note: If you change this parameter, the IP phone will reboot to make the change take effect. We recommend that you do not change this parameter. Web User Interface:		

Parameters	Permitted Values	Default
Network->Advanced->Port Link->WAN Port Link		
Phone User Interface:		
None		

To configure the transmission method of Ethernet port via web user interface:

1. Click on **Network->Advanced**.
2. Select the desired value from the pull-down list of **WAN Port Link**.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected, and the 'Advanced' sub-tab is active. The 'Port Link' section is highlighted with a red box, showing the 'WAN Port Link' dropdown menu set to 'Full Duplex 10Mbps'. Other configuration options include LLDP (Active, Enabled), VLAN (Active, Disabled), DHCP VLAN (Active, Enabled), Voice QoS (Voice QoS 0~63: 46, SIP QoS 0~63: 26), and Local RTP Port (Max RTP Port 1~65535: 11800, Min RTP Port 1~65535: 11780). A 'NOTE' sidebar on the right provides additional information about VLAN, QoS, and Local RTP Port.

3. Click **Confirm** to accept the change.

Upgrading Firmware

This section provides information on upgrading the IP phone firmware. Two methods of firmware upgrade:

- Manually, from the local system
- Automatically, from the provisioning server

The associated firmware name of the CP860 IP conference phone is 37.x.0.x.rom (x is replaced by the actual firmware version).

Note

You can download the latest firmware online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Do not unplug the network and power cables when the IP phone is upgrading firmware.

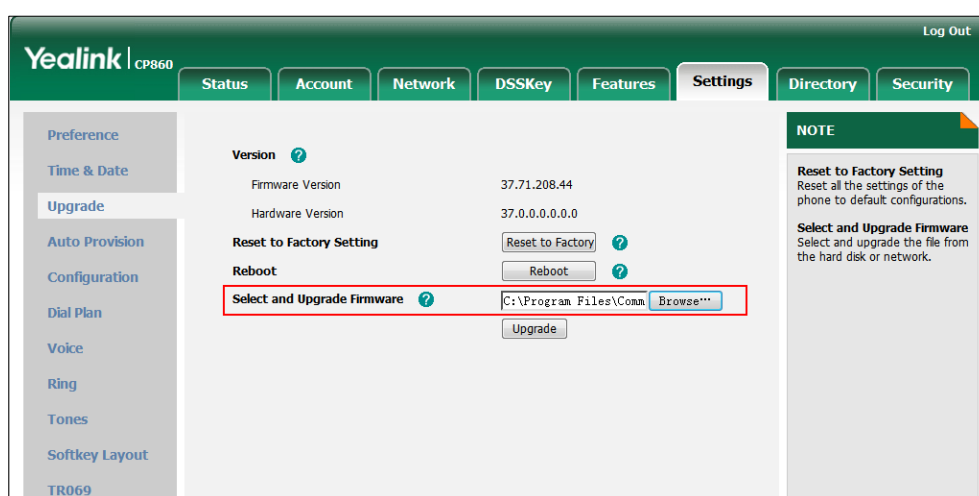
Upgrade via Web User Interface

To manually upgrade firmware via web user interface, you need to store the firmware to the local system in advance.

To upgrade firmware manually via web user interface:

1. Click on **Settings->Upgrade**.
2. Click **Browse**.
3. Locate the firmware from the local system.
4. Click **Upgrade**.

A dialog box pops up to prompt "Firmware of the SIP phone will be updated. It will take 5 minutes to complete. Please don't power off!".



5. Click **OK** to confirm the upgrade.

Note

Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.

Upgrade Firmware from the Provisioning Server

IP phones support using the FTP, TFTP, HTTP, and HTTPS protocols to download the configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

IP phones can download firmware stored on the provisioning server in one of two ways:

- Check for both configuration files and firmware stored on the provisioning server during booting up.
- Automatically check for configuration files and firmware at a fixed interval or specific time.

Method of checking for configuration files and firmware is configurable.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the way for the IP phone to check for configuration files.</p> <p>Parameters:</p> <p>auto_provision.power_on</p> <p>auto_provision.repeat.enable</p> <p>auto_provision.repeat.minutes</p> <p>auto_provision.weekly.enable</p> <p>auto_provision.weekly.begin_time</p> <p>auto_provision.weekly.end_time</p> <p>auto_provision.weekly.dayofweek</p> <p>Specify the access URL of firmware.</p> <p>Parameter:</p> <p>firmware.url</p>
Local	Web User Interface	<p>Configure the way for the IP phone to check for configuration files.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?parameter=settings-autop&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_provision.power_on	0 or 1	1
<p>Description:</p> <p>Enables or disables the IP phone to perform an auto provisioning process when powered on.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>Web User Interface:</p> <p>Settings->Auto Provision->Power On</p> <p>Phone User Interface:</p> <p>None</p>		
auto_provision.repeat.enable	0 or 1	0

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to perform an auto provisioning process repeatedly. 0-Disabled 1-Enabled Web User Interface: Settings->Auto provision->Repeatedly Phone User Interface: None		
auto_provision.repeat.minutes	Integer from 1 to 43200	1440
Description: Configures the interval (in minutes) for the IP phone to perform an auto provisioning process repeatedly. Note: It works only if the parameter "auto_provision.repeat.enable" is set to 1(Enabled). Web User Interface: Settings->Auto provision->Interval (minutes) Phone User Interface: None		
auto_provision.weekly.enable	0 or 1	0
Description: Enables or disables the IP phone to perform an auto provisioning process weekly. 0-Disabled 1-Enabled Web User Interface: Settings->Auto provision->Weekly Phone User Interface: None		
auto_provision.weekly.begin_time	Time from 00:00 to 23:59	00:00

Parameters	Permitted Values	Default
Description: Configures the begin time of the day for the IP phone to perform an auto provisioning process weekly. Note: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled). Web User Interface: Settings->Auto provision->Time Phone User Interface: None		
auto_provision.weekly.end_time	Time from 00:00 to 23:59	00:00
Description: Configures the end time of the day for the IP phone to perform an auto provisioning process weekly. Note: It works only if the parameter "auto_provision.weekly.enable" is set to 1(Enabled). Web User Interface: Settings->Auto provision->Time Phone User Interface: None		
auto_provision.weekly.dayofweek	0,1,2,3,4,5,6 or a combination of these digits	0123456
Description: Configures the days of the week for the IP phone to perform an auto provisioning process weekly. 0-Sunday 1-Monday 2-Tuesday 3-Wednesday 4-Thursday 5-Friday 6-Saturday Example: auto_provision.weekly.dayofweek = 01 means the IP phone will perform an auto		

Parameters	Permitted Values	Default
provisioning process every Sunday and Monday. Note: It works only if the parameter “auto_provision.weekly.enable” is set to 1(Enabled). Web User Interface: Settings->Auto provision->Day of week Phone User Interface: None		
firmware.url	URL within 511 characters	Blank
Description: Configures the access URL of the firmware file. Example: firmware.url = http://192.168.1.20/2.71.0.140.rom Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Settings->Upgrade->Select and Upgrade Firmware Phone User Interface: None		

To configure the way for the IP phone to check for new configuration files via web user interface:

1. Click on **Settings->Auto Provision**.

2. Make the desired change.

Yealink CP860 Log Out

Settings

Auto Provision

PNP Active ☒ On ☐ Off ?

DHCP Active ☒ On ☐ Off ?

Custom Option(128~254) ?

DHCP Option Value ?

Server URL ?

User Name ?

Password ?

Common AES Key ?

MAC-Oriented AES Key ?

Zero Active ?

Wait Time(0~100s) ?

Power On ☒ On ☐ Off ?

Repeatedly ☐ On ☒ Off ?

Interval(Minutes) ?

Weekly ☐ On ☒ Off ?

Time ? : ~ :

Day of Week ? ☒ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

?

NOTE

Auto Provision
The auto provision parameters for administrator.

3. Click **Confirm** to accept the change.

When the “Power On” is set to **On**, the IP phone will check configuration files stored on the provisioning server during startup and then will download firmware from the server.

Configuring Basic Features

This chapter provides information for making configuration changes for the following basic features:

- [Contrast](#)
- [Backlight](#)
- [Web Server Type](#)
- [User Password](#)
- [Administrator Password](#)
- [Phone Lock](#)
- [Time and Date](#)
- [Language](#)
- [Logo Customization](#)
- [Softkey Layout](#)
- [Key as Send](#)
- [Dial Plan](#)
- [Hotline](#)
- [Directory](#)
- [Search Source List in Dialing](#)
- [Call Log](#)
- [Missed Call Log](#)
- [Local Directory](#)
- [Live Dialpad](#)
- [Call Waiting](#)
- [Auto Redial](#)
- [Auto Answer](#)
- [Anonymous Call](#)
- [Anonymous Call Rejection](#)
- [Do Not Disturb](#)
- [Busy Tone Delay](#)
- [Return Code When Refuse](#)
- [Early Media](#)
- [180 Ring Workaround](#)

- [Use Outbound Proxy in Dialog](#)
- [SIP Session Timer](#)
- [Session Timer](#)
- [Call Hold](#)
- [Call Forward](#)
- [Call Transfer](#)
- [Network Conference](#)
- [Transfer on Conference Hang Up](#)
- [Directed Call Pickup](#)
- [Group Call Pickup](#)
- [Call Return](#)
- [Calling Line Identification Presentation](#)
- [Connected Line Identification Presentation](#)
- [DTMF](#)
- [Suppress DTMF Display](#)
- [Transfer via DTMF](#)
- [Intercom](#)

Contrast

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience. When configured properly, contrast allows users to read the LCD's display with minimal eyestrain.

Procedure

Contrast can be configured using the configuration files or locally.

Local	y000000000037.cfg	Configure the contrast of the LCD screen. Parameters: phone_setting.contrast
	Web User Interface	Configure the contrast of the LCD screen. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-preference&q=load">http://<phoneIPAddress>/servlet?p=settings-preference&q=load

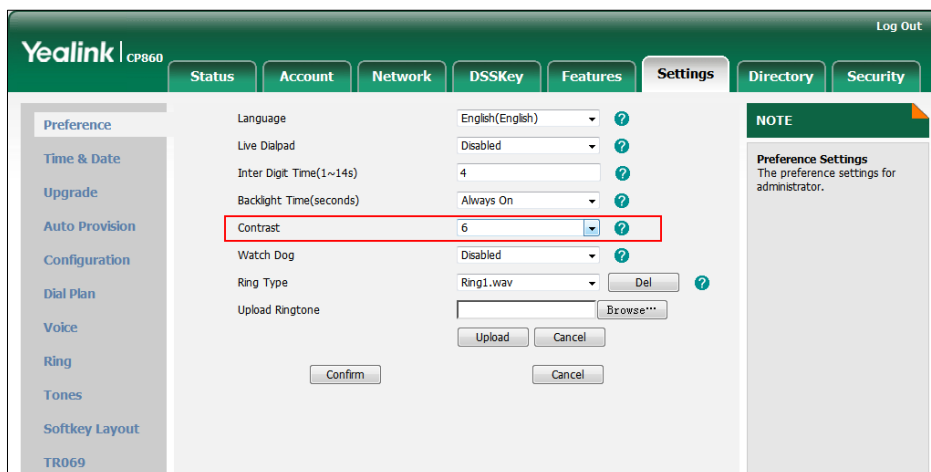
	Phone User Interface	Configure the contrast of the LCD screen.
--	----------------------	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.contrast	Integer from 1 to 10	6
<p>Description: Configures the contrast of the LCD screen.</p> <p>Note: We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level.</p> <p>Web User Interface: Settings->Preference->Contrast</p> <p>Phone User Interface: Menu->Settings->Basic Settings->Display->Contrast</p>		

To configure contrast via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Contrast**.



3. Click **Confirm** to accept the change.

To configure contrast via phone user interface:

1. Press **Menu->Settings-> Basic Settings ->Display->Contrast**.
2. Press the ◀ or ▶ soft key to increase or decrease the intensity of contrast.
The default contrast level is 6.
3. Press the **Save** soft key to accept the change.

Backlight

Backlight determines the brightness of the LCD screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off the backlight when the IP phone is inactive.

You can configure the backlight time as one of the following types:

- **Always On:** Backlight is turned on permanently.
- **15s, 30s, 60s, 120s, 300s, 600s or 1800s:** Backlight is turned off when the IP phone is inactive after a preset period of time. It is automatically turned on if the status of the IP phone changes or any key is pressed.

Procedure

Backlight can be configured using the configuration files or locally.

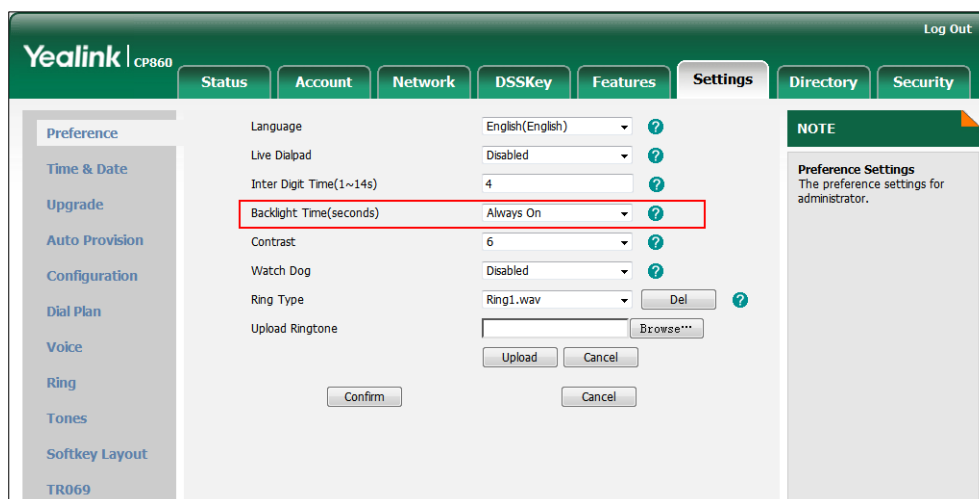
Configuration File	y000000000037.cfg	Configure the backlight of the LCD screen. Parameters: phone_setting.backlight_time
Local	Web User Interface	Configure the backlight of the LCD screen. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-preference&q=load">http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.backlight_time	0, 15, 30, 60, 120, 300, 600 or 1800	0
Description: Configures the delay time (in seconds) to turn off the backlight when the IP phone is inactive. 0-Always on, 15-15s, 30-30s, 60-60s, 120-120s, 300-300s, 600-600s, 1800-1800s If it is set to 60, the LCD backlight will be turned off when the IP phone is inactive for 60 seconds. Web User Interface: Settings->Preference->Backlight Time (seconds) Phone User Interface: Menu->Settings->Basic Settings->Display->Backlight Settings		

To configure the backlight via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Backlight Time (seconds)**.



3. Click **Confirm** to accept the change.

To configure the backlight via phone user interface:

1. Press **Menu->Settings->Basic Settings->Display->Backlight Settings**.
2. Press the ◀ or ▶ soft key to select the desired value from the **Backlight Time** field.
3. Press the **Save** soft key to accept the change.

Web Server Type

Web server type determines access protocol of the IP phone's web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages returned by the web server. Both the HTTP and HTTPS port numbers are configurable.

Procedure

Web server type can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify the web access type, HTTP port and HTTPS port. Parameters: wui.http_enable network.port.http wui.https_enable network.port.https
---------------------------	-------------------	--

Local	Web User Interface	Specify the web access type, HTTP port and HTTPS port. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Specify the web access type.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
wui.http_enable	0 or 1	1
<p>Description: Enables or disables the IP phone to access its web user interface using HTTP protocol.</p> <p>0-Disabled 1-Enabled</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->Web Server->HTTP</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Network->Webserver Type->HTTP Status</p>		
network.port.http	Integer from 1 to 65535	80
<p>Description: Configures the HTTP port for the IP phone to access its web user interface using the HTTP protocol.</p> <p>The default HTTP port is 80.</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->Web Server->HTTP Port (1~65535)</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Network->Webserver Type->HTTP Port</p>		
wui.https_enable	0 or 1	1

Parameters	Permitted Values	Default
<p>Description: Enables or disables the IP phone to access its web user interface using HTTPS protocol.</p> <p>0-Disabled 1-Enabled</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network-> Advanced-> Web Server->HTTPS</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network-> Webserver Type-> HTTPS Status</p>		
network.port.https	Integer from 1 to 65535	443
<p>Description: Configures the HTTPS port for the IP phone to access its web user interface using the HTTPS protocol.</p> <p>The default HTTPS port is 443.</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->Web Server->HTTPS Port (1~65535)</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Network->Webserver Type->HTTPS Port</p>		

To configure the web server type via web user interface:

1. Click on **Network->Advanced**.
2. In the **Web Server** block, select the desired value from the pull-down list of **HTTP**.
3. Enter the HTTP port in the **HTTP Port (1~65535)** field.
The default HTTP port is 80.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the HTTPS port in the **HTTPS Port (1~65535)** field.

The default HTTPS port is 443.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected. Under the 'Web Server' section, the 'HTTP' status is 'Enabled' and the 'HTTP Port' is '80'. The 'HTTPS' status is 'Enabled' and the 'HTTPS Port' is '443'. A red box highlights these settings. On the right, a 'NOTE' section provides information about VLAN, QoS, and Local RTP Port.

6. Click **Confirm** to accept the change.

A dialog box pops up to prompt that the settings will take effect after reboot.

7. Click **OK** to reboot the phone.

To configure the web server type via phone user interface:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin) **->Network->Webserver Type**.
2. Press the ◀ or ▶ soft key to select the desired value in the **HTTP Status** field.
3. Enter the HTTP port in the **HTTP Port** field.
4. Press the ◀ or ▶ soft key to select the desired value in the **HTTPS Status** field.
5. Enter the HTTPS port in the **HTTPS Port** field.
6. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make the settings effective after a period of time.

User Password

Some menu options are protected by two privilege levels, user and administrator, each with its own password. When logging into the web user interface, you need to enter the user name and password to access various menu options.

A user or an administrator can change the user password. The default user password is "user". For security reasons, the user or the administrator should change the default user password as soon as possible.

Procedure

User password can be changed using the configuration files or locally.

Configuration File	y000000000037.cfg	Change the user password of the IP phone. Parameter: security.user_password
Local	Web User Interface	Change the user password of the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=security&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	String within 32 characters	user
<p>Description:</p> <p>Configures the password of the user for web server access.</p> <p>The IP phone uses “user” as the default user password.</p> <p>The valid value format is username:new password.</p> <p>Example:</p> <p>security.user_password = user:password123 means setting the password of user (current user name is “user”) to password123.</p> <p>Note: IP phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.</p> <p>Web User Interface:</p> <p>Security->Password</p> <p>Phone User Interface:</p> <p>None</p>		

To change the user password via web user interface:

1. Click on **Security->Password**.
2. Select **user** from the pull-down list of **User Type**.
3. Enter a new password in the **New Password** and **Confirm Password** fields.

Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).

- Click **Confirm** to accept the change.

Note

If logging into the web user interface of the IP phone with the user credential, the user needs to enter the current user password in the **Old Password** field.

Administrator Password

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges. The administrator password can only be changed by an administrator. The default administrator password is "admin". For security reasons, the administrator should change the default administrator password as soon as possible.

Procedure

Administrator password can be changed using the configuration files or locally.

Configuration File	y000000000037.cfg	Change the administrator password. Parameter: security.user_password
Local	Web User Interface	Change the administrator password. Navigate to: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	String within 32 characters	admin
<p>Description: Configures the password of the administrator for web server access. The IP phone uses “admin” as the default administrator password.</p> <p>Example: security.user_password = admin:password123 means setting the password of administrator (current user name is “admin”) to password123.</p> <p>Note: IP phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.</p> <p>Web User Interface: Security->Password</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Set Password</p>		

To change the administrator password via web user interface:

1. Click on **Security->Password**.
2. Select **admin** from the pull-down list of **User Type**.
3. Enter the current administrator password in the **Old Password** field.
4. Enter a new administrator password in the **New Password** and **Confirm Password** fields.

Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).

5. Click **Confirm** to accept the change.

To change the administrator password via phone user interface:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin) ->**Set Password**.
2. Enter the current administrator password in the **Current PWD** field.

3. Enter a new administrator password in the **New PWD** field and **Confirm PWD** field.
Valid characters are ASCII characters 32-126(0x20-0x7E).
4. Press the **Save** soft key to accept the change.

Phone Lock

Phone lock is used to lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, a user must enter the password to unlock it. IP phones offer three types of phone lock: Menu Key, Function Keys and All Keys. The IP phone will not be locked immediately after the IP phone lock type is configured. One of the following steps is also needed:

- Long press the pound key when the IP phone is idle.
- Press the keypad lock key (if configured) when the IP phone is idle.

In addition to the above steps, you can configure IP phones to automatically lock the keypad after a period of time.

Procedure

Phone lock can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the IP phone lock type.</p> <p>Parameters:</p> <p>phone_setting.phone_lock.enable</p> <p>phone_setting.phone_lock.lock_key_type</p> <p>Change the unlock PIN.</p> <p>Parameter:</p> <p>phone_setting.phone_lock.unlock_pin</p> <p>Configure the IP phone to automatically lock the keypad after a time interval.</p> <p>Parameter:</p> <p>phone_setting.phone_lock.lock_time_out</p> <p>Assign a keypad lock key.</p> <p>Parameter:</p> <p>programablekey.X.type</p>
Local	Web User Interface	<p>Configure the phone lock type.</p> <p>Configure the unlock PIN.</p> <p>Configure the IP phone to automatically lock the keypad after a time interval.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=feat</p>

		<p>ures-phonelock&q=load</p> <p>Assign a keypad lock key.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=dsskey&model=2&q=load</p>
	Phone User Interface	<p>Configure the phone lock type.</p> <p>Configure the unlock PIN.</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.phone_lock.enable	0 or 1	0
<p>Description:</p> <p>Enables or disables phone lock feature.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>Web User Interface:</p> <p>Features->Phone Lock->Keypad Lock Enable</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Keypad Lock->Keypad Lock Enable</p>		
phone_setting.phone_lock.lock_key_type	0, 1 or 2	0
<p>Description:</p> <p>Configures the type of phone lock.</p> <p>Menu Key: The Menu soft key is locked.</p> <p>Function Keys: the mute key, redial key, OK, up and down navigation keys and soft keys are locked.</p> <p>All Keys: All keys are locked, except the volume key, on-hook key, off-hook key and keypad keys.</p> <p>0-All Keys</p> <p>1-Function Keys</p> <p>2-Menu Key</p> <p>Web User Interface:</p> <p>Features->Phone Lock->Keypad Lock Type</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Keypad</p>		

Parameters	Permitted Values	Default
Lock->Keypad Lock Type		
phone_setting.phone_lock.unlock_pin	characters within 15 digits	123
<p>Description: Configures the password for unlocking the keypad.</p> <p>Web User Interface: Features->Phone Lock->Phone Unlock PIN (0~15 Digit)</p> <p>Phone User Interface: Menu->Settings->Basic Settings->Phone Unlock PIN</p>		
phone_setting.phone_lock.lock_time_out	Integer from 0 to 3600	0
<p>Description: Configures the interval (in seconds) to automatically lock the keypad. The default value is 0 (the keypad is locked only by long pressing the pound key or pressing the keypad lock key).</p> <p>Note: It works only if the type of phone lock is preset.</p> <p>Web User Interface: Features->Phone Lock->Phone Lock Time Out (0~3600s)</p> <p>Phone User Interface: None</p>		
programmablekey.X.type (X=1-6, 9, 13)	50	0
<p>Description: Configures a programmable key as a keypad lock key on the IP phone. The digit 50 stands for the key type Keypad Lock. For more information on how to configure the programmable key, refer to Appendix C: Configuring Programmable Key on page 353.</p> <p>Example: programmablekey.1.type = 50</p> <p>Web User Interface: DSSKey->Programmable Key->Type</p> <p>Phone User Interface: None</p>		

To configure phone lock via web user interface:

1. Click on **Features->Phone Lock**.
2. Select the desired type from the pull-down list of **Keypad Lock Enable**.
3. Select the desired type from the pull-down list of **Keypad Lock Type**.
4. Enter unlock PIN (numeric characters) in the **phone Unlock PIN (0~15 Digit)** field.
5. Enter the desired time in the **phone Lock Time Out (0~3600s)** field.

6. Click **Confirm** to accept the change.

To configure a keypad lock key via web user interface:

1. Click on **DSSKey->Programmable Key**.
2. In the desired programmable key field, select **Keypad Lock** from the pull-down list of **Type**.

3. Click **Confirm** to accept the change.

To configure phone lock type via phone user interface:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin) -> **Keypad Lock**.
2. Press the ◀ or ▶ soft key to select the desired value from the **Keypad Lock Enable** field.

3. Press the ◀ or ▶ soft key to select the desired type from the **Lock type** field.
4. Press the **Save** soft key to accept the change.

To configure the unlock PIN via phone user interface:

1. Press **Menu->Settings->Basic Settings->Phone Unlock PIN**.
2. Enter the current unlock PIN in the **Current PIN** field.
3. Enter the new unlock PIN in the **New PIN** field.
4. Enter the new unlock PIN again in the **Confirm PIN** field.
5. Press the **Save** soft key to accept the change.

Time and Date

IP phones maintain a local clock and calendar. Time and date are displayed on the idle screen of the IP phone. Time and date are synced automatically from the NTP server by default. The NTP server can be obtained by DHCP or configured manually. If IP phones cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date display can use one of several different formats.

Time Zone

A time zone is a region on Earth that has a uniform standard time. It is convenient for areas in close commercial or other communication to keep the same time. When configuring IP phones to obtain the time and date from the NTP server, you must set the time zone.

Daylight Saving Time

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summertime so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn. Many countries have used the DST at various times, details vary by location. The DST can be adjusted automatically from the time zone configuration. Typically, there is no need to change this setting.

The following table lists available methods for configuring time and date:

Option	Methods of Configuration
Time Zone	Configuration Files Web User Interface Phone User Interface
Time	Web User Interface Phone User Interface

Option	Methods of Configuration
Time Format	Configuration Files Web User Interface Phone User Interface
Date	Web User Interface Phone User Interface
Date Format	Configuration Files Web User Interface Phone User Interface
Daylight Saving Time	Configuration Files Web User Interface

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure NTP by DHCP priority feature and DHCP time features.</p> <p>Parameters:</p> <p>local_time.manual_ntp_srv_prior</p> <p>local_time.dhcp_time</p> <p>Configure the NTP server, time zone and DST.</p> <p>Parameters:</p> <p>local_time.ntp_server1</p> <p>local_time.ntp_server2</p> <p>local_time.interval</p> <p>local_time.time_zone</p> <p>local_time.time_zone_name</p> <p>local_time.summer_time</p> <p>local_time.dst_time_type</p> <p>local_time.start_time</p> <p>local_time.end_time</p> <p>local_time.offset_time</p> <p>Configure the time and date manually.</p> <p>Parameter:</p> <p>local_time.manual_time_enable</p> <p>Configure the time and date</p>
--------------------	-----------	--

		<p>formats.</p> <p>Parameters:</p> <p>local_time.time_format</p> <p>local_time.date_format</p>
Local	Web User Interface	<p>Configure NTP by DHCP priority feature.</p> <p>Configure the NTP server, time zone and DST.</p> <p>Configure the time and date manually.</p> <p>Configure the time and date formats.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-datetime&q=load</p>
	Phone User Interface	<p>Configure the NTP server and time zone.</p> <p>Configure the time and date manually.</p> <p>Configure the time and date formats.</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
local_time.manual_ntp_srv_prior	0 or 1	0
<p>Description:</p> <p>Enables or disables the IP phone to use manually configured NTP server preferentially.</p> <p>0-Disabled (use the NTP server obtained by DHCP preferentially)</p> <p>1-Enabled (use the NTP server configured manually preferentially)</p> <p>Web User Interface:</p> <p>Settings->Time & Date->NTP By DHCP Priority</p> <p>Phone User Interface:</p> <p>None</p>		
local_time.dhcp_time	0 or 1	0

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to update time with the offset time obtained from the DHCP server. 0 -Disabled 1 -Enabled Note: It is only available to offset from GMT 0. Web User Interface: Settings->Time & Date->DHCP Time Phone User Interface: Menu->Settings->Basic Settings->Time & Date->DHCP Time		
local_time.ntp_server1	IP Address or Domain Name	cn.pool.ntp.org
Description: Configures the IP address or the domain name of the NTP server 1. Example: local_time.ntp_server1 = 192.168.0.5 Web User Interface: Settings-> Time & Date->Primary Server Phone User Interface: Menu->Settings->Basic Settings->Time & Date->SNTP Settings->NTP Server1		
local_time.ntp_server2	IP Address or Domain Name	cn.pool.ntp.org
Description: Configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured or cannot be accessed, the IP phone will request the time and date from the NTP server 2. Example: local_time.ntp_server2 = 192.168.0.6 Web User Interface: Settings->Time & Date->Secondary Server Phone User Interface: Menu->Settings->Basic Settings->Time & Date->SNTP Settings->NTP Server2		
local_time.interval	Integer from 15 to 86400	1000

Parameters	Permitted Values	Default
Description: Configures the interval (in seconds) to update time and date from the NTP server. Example: local_time.interval = 1000 Web User Interface: Settings->Time & Date->Synchronism (15~86400s) Phone User Interface: None		
local_time.time_zone	-11 to +13	+8
Description: Configures the time zone. For more available time zones, refer to Appendix B: Time Zones on page 351. Example: local_time.time_zone = +8 Web User Interface: Settings->Time & Date->Time Zone Phone User Interface: Menu->Settings->Basic Settings->Time & Date->SNTP Settings->Time Zone		
local_time.time_zone_name	String within 32 characters	China(Beijing)
Description: Configures the time zone name. For more available time zone names, refer to Appendix B: Time Zones on page 351. Example: local_time.time_zone_name = China(Beijing) Web User Interface: Settings->Time & Date->Time Zone Phone User Interface: Menu->Settings->Basic Settings->Time & Date->SNTP Settings->Time Zone		
local_time.summer_time	0, 1 or 2	2

Parameters	Permitted Values	Default
Description: Configures Daylight Saving Time (DST) feature. 0 -Disabled 1 -Enabled 2 -Automatic Web User Interface: Settings->Time & Date->Daylight Saving Time Phone User Interface: Menu->Settings->Basic Settings->Time & Date->SNTP Settings->Daylight Saving		
local_time.dst_time_type	0 or 1	0
Description: Configures the DST time type. 0 -By Date 1 -By Week Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). Web User Interface: Settings-> Time & Date->Fixed Type Phone User Interface: None		
local_time.start_time	Time	1/1/0
Description: Configures the start time of the DST. Value formats are: <ul style="list-style-type: none"> Month/Day/Hour (for By Date) Month/Day of Week Last in Month/Day of Week/Hour of Day (for By Week) If "local_time.dst_time_type" is set to 0 (By Date), use the mapping: MM: 1=Jan, 2=Feb,..., 12=Dec DD:1=the first day in a month,..., 31= the last day in a month HH:0=1am, 1=2am,..., 23=12pm If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=Jan, 2=Feb,..., 12=Dec Day of Week Last in Month: 1=the first week in a month,..., 5=the last week in a month Day of Week: 1=Mon, 2=Tues,..., 7=Sun		

Parameters	Permitted Values	Default
<p>Hour of Day: 0=1am, 1=2am,..., 23=12pm</p> <p>Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>For DST By Date:</p> <p>Settings-> Time & Date->Start Date</p> <p>For DST By Week:</p> <p>Settings-> Time & Date->DST Start Month/DST Start Day of Week/DST Start Day of Week Last in Month/ Start Hour of Day</p> <p>Phone User Interface:</p> <p>None</p>		
local_time.end_time	Time	12/31/23
<p>Description:</p> <p>Configures the end time of the DST.</p> <p>Value formats are:</p> <ul style="list-style-type: none"> Month/Day/Hour (for By Date) Month/Day of Week Last in Month/Day of Week/Hour of Day (for By Week) <p>If "local_time.dst_time_type" is set to 0 (By Date), use the mapping:</p> <p>MM: 1=Jan, 2=Feb,..., 12=Dec</p> <p>DD:1=the first day in a month,..., 31= the last day in a month</p> <p>HH: 0=1am, 1=2am,..., 23=12pm</p> <p>If "local_time.dst_time_type" is set to 1 (By Week), use the mapping:</p> <p>Month: 1=Jan, 2=Feb,..., 12=Dec</p> <p>Day of Week Last in Month: 1=the first week in a month,..., 5=the last week in a month</p> <p>Day of Week: 1=Mon, 2=Tues,..., 7=Sun</p> <p>Hour of Day: 0=1am, 1=2am,..., 23=12pm</p> <p>Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>For DST By Date:</p> <p>Settings->Time & Date->End Date</p> <p>For DST By Week:</p> <p>Settings->Time & Date->DST Stop Month/DST Stop Day of Week/DST Stop Day of Week Last in Month/End Hour of Day</p>		

Parameters	Permitted Values	Default
local_time.offset_time	Integer from -300 to 300	Blank
Description: Configures the offset time (in minutes) of DST. Note: It works only if the parameter "local_time.summer_time" is set to 1 (Enabled). Web User Interface: Settings->Time & Date->Offset (minutes) Phone User Interface: None		
local_time.manual_time_enable	0 or 1	0
Description: Configures the IP phone to obtain time from the NTP server or manual settings. 0-NTP 1-Manual Web User Interface: Settings->Time & Date->Manual Time Phone User Interface: None		
local_time.time_format	0 or 1	1
Description: Configures the time format. 0-12 Hour 1-24 Hour If it is set to 0 (12 Hour), the time will be displayed in 12-hour format with AM or PM specified. If it is set to 1 (24 Hour), the time will be displayed in 24-hour format (e.g., 2:00 PM displays as 14:00). Web User Interface: Settings-> Time & Date->Time Format Phone User Interface: Menu->Settings->Basic Settings->Time & Date ->Time & Date Format->Time Format		
local_time.date_format	0, 1, 2, 3, 4, 5 or 6	0

Parameters	Permitted Values	Default
<p>Description:</p> <p>Configures the date format.</p> <p>0-WWW MMM DD</p> <p>1-DD-MMM-YY</p> <p>2-YYYY-MM-DD</p> <p>3-DD/MM/YYYY</p> <p>4-MM/DD/YY</p> <p>5-DD MMM YYYY</p> <p>6-WWW DD MMM</p> <p>Web User Interface:</p> <p>Settings->Time & Date->Date Format</p> <p>Phone User Interface:</p> <p>Menu->Settings->Basic Settings->Time & Date->Time & Date Format->Date Format</p>		

To configure NTP by DHCP priority feature via web user interface:

1. Click on **Settings->Time & Date**.
2. Select the desired value from the pull-down list of **NTP By DHCP Priority**.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is active, and the 'Time & Date' sub-tab is selected. The 'NTP By DHCP Priority' dropdown menu is highlighted with a red rectangle and is currently set to 'High'. Other visible settings include 'DHCP Time' set to 'Disabled', 'Time Zone' set to '+8 China(Beijing)', 'Primary Server' and 'Secondary Server' both set to 'cn.pool.ntp.org', 'Synchronism' set to '1000', 'Daylight Saving Time' set to 'Enabled', 'Fixed Type' set to 'DST By Date', 'Start Date' and 'End Date' fields, 'Offset(minutes)' field, 'Manual Time' set to 'Disabled', 'Time Format' set to 'Hour 24', and 'Date Format' set to 'WWW MMM DD'. A 'NOTE' section on the right provides additional information about the 'Time Zone' and 'NTP Server' settings.

3. Click **Confirm** to accept the change.

To configure the NTP server, time zone and DST via web user interface:

1. Click on **Settings->Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.

4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Select the desired value from the pull-down list of **Daylight Saving Time**.

If you select **Enabled**, do one of the following:

- Mark the **DST By Date** radio box in the **Fixed Type** field.

Enter the start time in the **Start Date** field.

Enter the end time in the **End Date** field.

- Mark the **DST By Week** radio box in the **Fixed Type** field.

Select the desired values from the pull-down lists of **DST Start Month**, **DST Start Day of Week**, **DST Start Day of Week Last in Month**, **DST Stop Month**, **DST Stop Day of Week** and **DST Stop Day of Week Last in Month**.

Enter the desired time in the **Start Hour of Day** field.

Enter the desired time in the **End Hour of Day** field.

The screenshot shows the 'Time & Date' configuration page in the Yealink CP860 web interface. The 'Fixed Type' section is highlighted with a red box, indicating the DST settings. The 'End Hour of Day' field is set to 12. Other settings include DHCP Time (Disabled), Time Zone (+8 China(Beijing)), NTP By DHCP Priority (High), Primary Server (cn.pool.ntp.org), Secondary Server (cn.pool.ntp.org), Synchronism (15~86400s), Daylight Saving Time (Enabled), Offset (minutes), Manual Time (Disabled), Time Format (Hour 24), and Date Format (WWW MMM DD).

7. Enter the desired offset time in the **Offset (minutes)** field.
8. Click **Confirm** to accept the change.

To configure the time and date manually via web user interface:

1. Click on **Settings->Time & Date**.
2. Select **Enabled** from the pull-down list of **Manual Time**.
3. Enter the time and date in the corresponding fields.

The screenshot shows the 'Time & Date' configuration page in the Yealink CP860 web interface. The 'Manual Time' section is highlighted with a red box, indicating the manual time settings. The 'Manual Time' field is set to Enabled. Other settings include DHCP Time (Disabled), Time Zone (+8 China(Beijing)), NTP By DHCP Priority (High), Primary Server (cn.pool.ntp.org), Secondary Server (cn.pool.ntp.org), Synchronism (15~86400s), Daylight Saving Time (Enabled), Offset (minutes), Manual Time (Enabled), Time Format (Hour 24), and Date Format (WWW MMM DD).

4. Click **Confirm** to accept the change.

To configure the time and date format via web user interface:

1. Click on **Settings->Time & Date**.

2. Select the desired value from the pull-down list of **Time Format**.
3. Select the desired value from the pull-down list of **Date Format**.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is selected, and the 'Time & Date' section is active. The 'Time Format' and 'Date Format' fields are highlighted with a red box. The 'Time Format' is set to 'Hour 24' and the 'Date Format' is set to 'WWW MMM DD'. Other settings include DHCP Time (Disabled), Time Zone (+8 China(Beijing)), NTP By DHCP Priority (High), Primary and Secondary NTP Servers (cn.pool.ntp.org), Synchronism (15~86400s), Daylight Saving Time (Enabled), Fixed Type (DST By Date), Start and End Dates, Offset (minutes), and Manual Time (Disabled). A 'NOTE' section on the right explains the Time Zone and NTP Server settings.

4. Click **Confirm** to accept the change.

To configure the NTP server and time zone via phone user interface:

1. Press **Menu->Settings->Basic Settings->Time & Date->SNTP Settings**.
2. Press the ◀ or ▶ soft key to select the time zone that applies to your area from the **Time Zone** field.
The default time zone is "+8 China(Beijing)".
3. Enter the domain names or IP addresses in the **NTP Server1** and **NTP Server2** fields respectively.
4. Press the ◀ or ▶ soft key to select **Automatic** from the **Daylight Saving** field.
5. Press the **Save** soft key to accept the change.

To configure the time and date manually via phone user interface:

1. Press **Menu->Settings->Basic Settings->Time & Date->Manual Settings**.
2. Enter the specific time and date.
3. Press the **Save** soft key to accept the change.

To configure the time and date formats via phone user interface:

1. Press **Menu Settings->Basic Settings->Time & Date->Time & Date Format**.
2. Press the ◀ or ▶ soft key to select the desired time format (12 Hour or 24 Hour) from the **Time Format** field.
3. Press the ◀ or ▶ soft key to select the desired date format from the **Date Format** field.
4. Press the **Save** soft key to accept the change.

Language

IP phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.

The following table lists the languages supported by the phone user interface and the web user interface respectively.

Phone User Interface	Web User Interface
English	English
Chinese_S	Chinese_S
Chinese_T	Chinese_T
French	French
German	German
Italian	Italian
Polish	Portuguese
Portuguese	Spanish
Russian	Turkish
Spanish	Polish
Turkish	Russian

Loading Language Packs

Not all of the supported languages are available for selection. Languages available for selection depend on language packs currently loaded to IP phones. You can make languages available for use on the phone user interface by loading language packs to the IP phone. Language packs can only be loaded using the configuration files.

The following table lists available languages and the associated language packs:

Available Language	Associated Language Pack
English	lang+English.txt
Simplified Chinese	lang-Chinese_S.txt
Traditional Chinese	lang-Chinese_T.txt
German	lang-German.txt
French	lang-French.txt
Italian	lang-Italian.txt
Polish	lang-Polish.txt
Portuguese	lang-Portuguese.txt

Available Language	Associated Language Pack
Spanish	lang-Spanish.txt
Turkish	lang-Turkish.txt
Russian	lang-Russian.txt

To update translation of a built-in language, the file name of the language file cannot be changed. For more information, refer to

Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide.

Procedure

Loading language pack can only be performed using the configuration files.

Configuration File	y000000000037.cfg	Specify the access URL of the language pack. Parameter: gui_lang.url
--------------------	-------------------	---

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
gui_lang.url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the language pack.</p> <p>Example: The following example uses HTTP to download a new Russian language pack "lang-Russian.txt" from the provisioning server 192.168.10.25. gui_lang.url = http://192.168.10.25/lang-Russian.txt</p> <p>Note: The language packs you load are dependent on available language packs from the provisioning server. You can download the language pack to the phone user interface only.</p> <p>Web User Interface: None</p> <p>Phone User Interface: None</p>		

Specifying the Language to Use

The default language used on the phone user interface is English. The default language used on the web user interface depends on the language preferences in the browser (if

the language is not supported by the IP phone, the web user interface uses English). You can specify the languages for the phone user interface and web user interface respectively.

Procedure

Specify the language for the web user interface or the phone user interface using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify the languages for the phone user interface and the web user interface. Parameters: lang.gui lang.wui
Local	Web User Interface	Specify the language for the web user interface. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Specify the language for the phone user interface.

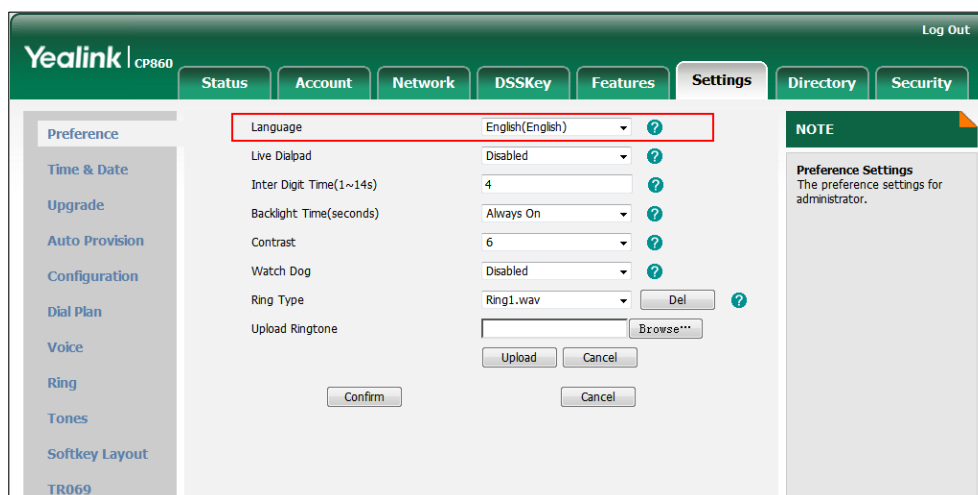
Details of Configuration Parameters:

Parameters	Permitted Values	Default
lang.gui	Refer to the following content	English
Description: Configures the language used on the phone user interface. Permitted Values: English, Chinese_S, Chinese_T, German, French, Turkish, Italian, Polish, Spanish, Russian or Portuguese Example: lang.gui = English Web User Interface: None Phone User Interface: Menu->Settings->Basic Settings->Language		
lang.wui	Refer to the following content	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the language used on the web user interface.</p> <p>Example: lang.wui = English</p> <p>Permitted Values: English, Chinese_S, Chinese_T, German, French, Turkish, Italian, Polish, Spanish, Russian or Portuguese</p> <p>Note: If the language of your browser is not supported by the IP phone, the web user interface will use English by default.</p> <p>Web User Interface: Settings->Preference->Language</p> <p>Phone User Interface: None</p>		



To specify the language for the web user interface via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired language from the pull-down list of **Language**.



3. Click **Confirm** to accept the change.

To specify the language for the phone user interface via phone user interface:

1. Press **Menu->Settings->Basic Settings->Language**.
2. Press  or  to select the desired language.
3. Press the **Save** soft key to accept the change.

Logo Customization

Logo customization allows unifying the IP phone appearance or displaying a custom image on the idle screen such as a company logo, instead of the default system logo. The logo file format must be *.dob, and the resolution of the LCD screen is 192*64 graphic.

Note

Before uploading your custom logo to IP phones, ensure the logo file is in the correct format. For more information on customizing a logo file, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide*.

Procedure

The logo shown on the idle screen can be configured using the configuration files or locally.

Configuration File	y0000000000037.cfg	Configure the logo shown on the idle screen and specify the access URL of the custom logo file. Parameters: phone_setting.lcd_logo.mode lcd_logo.url
Local	Web User Interface	Configure the logo shown on the idle screen. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.lcd_logo.mode	0, 1 or 2	0
Description: Configures the logo mode of the LCD screen. 0 -Disabled 1 -System logo 2 -Custom logo If it is set to 0 (Disabled), the IP phone is not allowed to display a logo. If it is set to 1 (System logo), the LCD screen will display the system logo. If it is set to 2 (Custom logo), the LCD screen will display the custom logo (you need		

Parameters	Permitted Values	Default
<p>to upload a custom logo file to the IP phone).</p> <p>Web User Interface: Features->General Information->Use Logo</p> <p>Phone User Interface: None</p>		
lcd_logo.url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the custom logo file.</p> <p>Example: The following example uses HTTP to download the custom logo file (logo.dob) from the provisioning server 192.168.10.25. lcd_logo.url = http://192.168.10.25/logo.dob</p> <p>Web User Interface: Features->General Information->Upload Logo(192*64)</p> <p>Phone User Interface: None</p>		

To configure a custom logo via web user interface:

1. Click on **Features->General Information**.
2. Select **Custom logo** from the pull-down list of **Use Logo**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' section is expanded. In the 'General Information' section, the 'Use Logo' dropdown is set to 'Custom logo'. Below it, the 'Upload Logo(192*64)' field contains the text 'F:\custom_log.dob' and a 'Browse...' button. The 'Upload' and 'Cancel' buttons are located below the field. A red box highlights the 'Use Logo' dropdown and the 'Upload Logo' field. On the right side, there is a 'NOTE' box with the following text:

NOTE

Call Waiting
This call feature allows your phone to accept other incoming calls during the conversation.

Key As Send
Select * or # as the send key.

Hotline Number
When you pick up the phone, it will dial out the hotline number automatically.

3. Click **Browse** to select the logo file from your local system.
4. Click **Upload** to upload the file.
5. Click **Confirm** to accept the change.

The custom logo screen and the idle screen are displayed alternately.

Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the LCD screen to best meet users' requirements. In addition to specifying which soft keys to display, you can determine their display order. It can be configured based on call states.

You can configure the softkey layout using the softkey layout templates for different call states. For more information on how to configure a softkey layout template, refer to [Softkey Layout Template](#) on page 326.

The following table lists the soft keys available for IP phones in different states:

Call State		Default Soft Key	Optional Soft Key
CallFailed		NewCall Empty Empty Empty	Empty Switch Cancel
CallIn		Answer Forward Silence Reject	Empty Switch
Connecting	Connecting	Empty Empty Empty Cancel	Empty Switch
	SemiAttendTrans	Transfer Empty Empty Cancel	Empty Switch
Dialing		Send IME Delete Cancel	Empty History Directory Switch GPickup

Call State		Default Soft Key	Optional Soft Key
			DPickup
RingBack	RingBack	Empty Empty Empty Cancel	Empty Switch
	SemiAttendTransBack	Transfer Empty Empty Cancel	Empty Switch
Talking	Talk	Transfer Hold Conference Cancel	Empty Mute SWAP NewCall Switch Answer Reject Start Record Pause Record Resume Record Stop Record
	Hold	Transfer Resume NewCall Cancel	Empty Switch Answer Reject Start Record Pause Record Resume Record Stop Record
	Held	Empty Empty Empty Cancel	Empty Switch Answer Reject NewCall Start Record Pause Record

Call State		Default Soft Key	Optional Soft Key
			Resume Record Stop Record
	PreTrans	Transfer IME Delete Cancel	Empty Directory Switch Send
	Conferenced	Empty Hold Split Cancel	Empty Switch Answer Reject Mute Manager Start Record Pause Record Resume Record Stop Record

Procedure

Softkey layout can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify the access URL of the softkey layout template. Parameters: custom_softkey_call_failed.url custom_softkey_call_in.url custom_softkey_connecting.url custom_softkey_dialing.url custom_softkey_ring_back.url custom_softkey_talking.url
Local	Web User Interface	Configure the softkey layout. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-softkey&q=load">http://<phoneIPAddress>/servlet?p=settings-softkey&q=load





Details of Configuration Parameters:

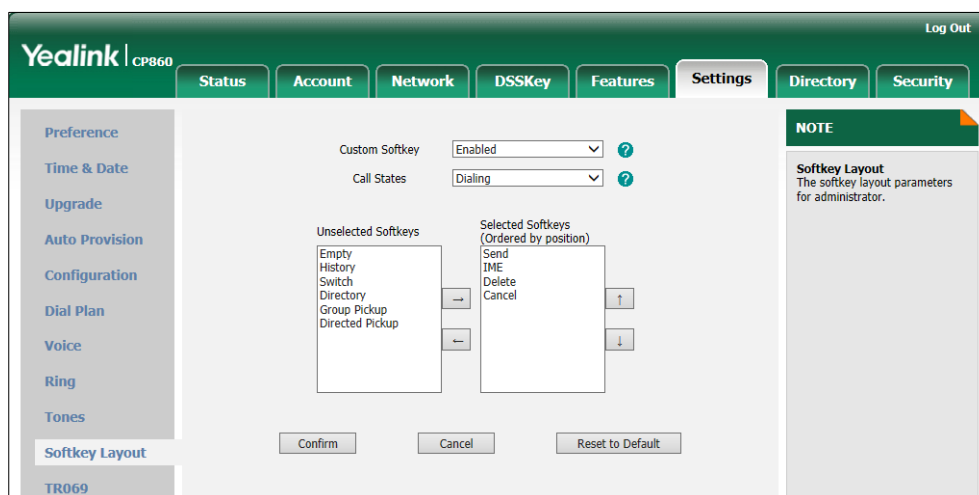
Parameters	Permitted Values	Default
custom_softkey_call_failed.url	URL within 511 characters	Blank
<p>Description:</p> <p>Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Call Failed state.</p> <p>Example:</p> <p>The following example uses HTTP to download the CallFailed state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port.</p> <p>custom_softkey_call_failed.url = http://10.2.8.16:8080/XMLfiles/CallFailed.xml</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
custom_softkey_call_in.url	URL within 511 characters	Blank
<p>Description:</p> <p>Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Call In state.</p> <p>Example:</p> <p>The following example uses HTTP to download the CallIn state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port.</p> <p>custom_softkey_call_in.url = http://10.2.8.16:8080/XMLfiles/CallIn.xml</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
custom_softkey_connecting.url	URL within 511 characters	Blank
<p>Description:</p> <p>Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Connecting state.</p> <p>Example:</p> <p>The following example uses HTTP to download the Connecting state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port.</p> <p>custom_softkey_connecting.url = http://10.2.8.16:8080/XMLfiles/Connecting.xml</p>		

Parameters	Permitted Values	Default
Web User Interface: None Phone User Interface: None		
custom_softkey_dialing.url	URL within 511 characters	Blank
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Dialing state. Example: The following example uses HTTP to download the Dialing state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_dialing.url = http://10.2.8.16:8080/XMLfiles/Dialing.xml Web User Interface: None Phone User Interface: None		
custom_softkey_ring_back.url	URL within 511 characters	Blank
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the RingBack state. Example: The following example uses HTTP to download the RingBack state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port. custom_softkey_ring_back.url = http://10.2.8.16:8080/XMLfiles/RingBack.xml Web User Interface: None Phone User Interface: None		
custom_softkey_talking.url	URL within 511 characters	Blank
Description: Configures the access URL of the custom file for the soft key presented on the LCD screen when in the Talking state.		

Parameters	Permitted Values	Default
<p>Example:</p> <p>The following example uses HTTP to download the Talking state file from the "XMLfiles" directory on provisioning server 10.2.8.16 using 8080 port.</p> <p>custom_softkey_talking.url = http://10.2.8.16:8080/XMLfiles/Talking.xml</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		

To configure softkey layout via web user interface:

1. Click on **Settings->Softkey Layout**.
2. Select the desired value from the pull-down list of **Custom Softkey**.
3. Select the desired state from the pull-down list of **Call States**.
4. Select the desired soft key from the **Unselected Softkeys** column and click  .
The selected soft key appears in the **Selected Softkeys** column. If more than four soft keys are selected, a **More** soft key will appear on the LCD screen.
5. Repeat the step 4 to add more soft keys to the **Selected Softkeys** column.
6. Click  to remove the soft key from the **Selected Softkeys** column.
7. Click  or  to adjust the display order of the soft key.



8. Click **Confirm** to accept the change.

Key as Send

Key as send allows assigning the pound key or asterisk key as a send key. Send sound allows the IP phone to play a key tone when a user presses the send key. Key tone allows the IP phone to play a key tone when a user presses any key. Send sound works

only if Key tone is enabled.

Procedure

Key as send can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure a send key.</p> <p>Parameter:</p> <p>features.key_as_send</p> <p>Configure a key tone and send tone.</p> <p>Parameters:</p> <p>features.key_tone</p> <p>eatures.send_key_tone</p>
Local	Web User Interface	<p>Configure a send key.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet ?p=features-general&q=load</p> <p>Configure a key tone and send tone.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet ?p=features-audio&q=load</p>
	Phone User Interface	Configure the send key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.key_as_send	0, 1 or 2	1
<p>Description:</p> <p>Configures the "#" or "*" key as the send key.</p> <p>0-Disabled</p> <p>1-# key</p> <p>2-* key</p> <p>If it is set to 0 (Disabled), neither "#" nor "*" can be used as a send key.</p> <p>If it is set to 1 (# key), the pound key is used as the send key.</p> <p>If it is set to 2 (* key), the asterisk key is used as the send key.</p> <p>Web User Interface:</p> <p>Features-> General Information->Key As Send</p>		

Parameters	Permitted Values	Default
Phone User Interface: Menu->Features->Key as Send		
features.key_tone	0 or 1	1
Description: Enables or disables the IP phone to play a tone when a user presses a key on your phone keypad. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a key on your phone keypad. Web User Interface: Features->Audio->Key Tone Phone User Interface: None		
features.send_key_tone	0 or 1	1
Description: Enables or disables the IP phone to play a tone when a user presses a send key. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the IP phone will play a tone when a user presses a send key. Note: It works only if the parameter “features.key_tone” is set to 1 (Enabled). Web User Interface: Features->Audio->Send Sound Phone User Interface: None		

To configure a send key via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Key As Send**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. In the 'General Information' section, the 'Key As Send' dropdown menu is highlighted with a red rectangle, and the '#' option is selected. Other settings like 'Call Waiting', 'Auto Redial', and 'Play Hold Tone' are also visible. A 'NOTE' section on the right provides additional information about the 'Key As Send' feature.

3. Click **Confirm** to accept the change.

To configure a key tone and send tone via web user interface:

1. Click on **Features->Audio**.
2. Select the desired value from the pull-down list of **Key Tone**.
3. Select the desired value from the pull-down list of **Send Sound**.

The screenshot shows the Yealink CP860 web interface. The 'Audio Settings' tab is selected. In the 'Audio Settings' section, the 'Key Tone' and 'Send Sound' dropdown menus are highlighted with a red rectangle, and the 'Enabled' option is selected for both. Other settings like 'Call Waiting Tone' and 'Redial Tone' are also visible. A 'NOTE' section on the right provides additional information about the audio parameters.

4. Click **Confirm** to accept the change.

To configure key as send via phone user interface:

1. Press **Menu->Features->Key as Send**.
2. Press the ◀ or ▶ soft key to select # or * from the **Key as Send** field, or select **Disable** to disable this feature.

3. Press the **Save** soft key to accept the change.

Note

Send tone works only if key tone is enabled.
Key tone is enabled by default.

Dial Plan

Regular expression, often called a pattern, is an expression that specifies a set of strings. A regular expression provides a concise and flexible means to “match” (specify and recognize) strings of text, such as particular characters, words, or patterns of characters. Regular expression is used by many text editors, utilities, and programming languages to search and manipulate text based on patterns.

Regular expression can be used to define IP phone dial plan. Dial plan is a string of characters that governs the way for IP phones to process the inputs received from the IP phone’s keypads. IP phones support the following dial plan features:

- [Replace Rule](#)
- [Dial-now](#)
- [Area Code](#)
- [Block Out](#)

You need to know the following basic regular expression syntax when creating dial plan:

.	The dot “.” can be used as a placeholder or multiple placeholders for any string. Example: “12.” would match “123”, “1234”, “12345”, “12abc”, etc.
x	The “x” can be used as a placeholder for any character. Example: “12x” would match “121”, “122”, “123”, “12a”, etc.
-	The dash “-” can be used to match a range of characters within the brackets. Example: “[5-7]” would match the number “5”, “6” or “7”.
,	The comma “,” can be used as a separator within the bracket. Example: “[2,5,8]” would match the number “2”, “5” or “8”.
[]	The square bracket “[]” can be used as a placeholder for a single character which matches any of a set of characters. Example: “91[5-7]1234” would match “9151234”, “9161234”, “9171234”.
()	The parenthesis “()” can be used to group together patterns, for instance, to logically combine two or more patterns. Example:

	"([1-9])([2-7])3" would match "923", "153", "673", etc.
\$	<p>The "\$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example:</p> <p>A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001\$145\$2". When you dial out "0012354599" on your phone, the IP phone will replace the number with "90012354599". "\$1" means three digits in the first parenthesis, that is, "235". "\$2" means two digits in the second parenthesis, that is, "99".</p>

Replace Rule

Replace rule is an alternative string that replaces the numbers entered by the user. IP phones support up to 100 replace rules, which can be created either one by one or in batch using a replace rule template. For more information on the replace rule template, refer to [Replace Rule Template](#) on page 324.

Procedure

Replace rule can be created using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Create the replace rule for the IP phone.</p> <p>Parameters:</p> <p>dialplan.replace.prefix.X</p> <p>dialplan.replace.replace.X</p> <p>Configure the access URL of the replace rule template.</p> <p>Parameter:</p> <p>dialplan_replace_rule.url</p>
Local	Web User Interface	<p>Create the replace rule for the IP phone.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.replace.prefix.X (X ranges from 1 to 100)	String within 32 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the entered number to be replaced. Example: dialplan.replace.prefix.1 = 00 Web User Interface: Settings->Dial Plan->Replace Rule->Prefix Phone User Interface: None		
dialplan.replace.replace.X (X ranges from 1 to 100)	String within 32 characters	Blank
Description: Configures the alternate number to replace the entered number. Example: dialplan.replace.replace.1 = 123456 Web User Interface: Settings->Dial Plan->Replace Rule->Replace Phone User Interface: None		
dialplan_replace_rule.url	URL within 511 characters	Blank
Description: Configures the access URL of the replace rule template file. Example: dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml Web User Interface: None Phone User Interface: None		

To create a replace rule via web user interface:

1. Click on **Settings->Dial Plan->Replace Rule**.
2. Enter the string in the **Prefix** field.

3. Enter the string in the **Replace** field.

4. Click **Add** to add the replace rule.

Dial-now

Dial-now is a string used to match the numbers entered by the user. When entered numbers match the predefined dial-now rule, IP phones will automatically dial out the numbers without pressing the send key. IP phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on the dial-now template, refer to [Dial-now Template](#) on page 325.

Delay Time for Dial-now Rule

IP phones will automatically dial out the entered number, which matches the dial-now rule, after a specified period of time.

Procedure

Dial-now rule can be created using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Create the dial-now rule for the IP phone.</p> <p>Parameters:</p> <p>dialplan.dialnow.rule.X</p> <p>Configure the delay time for the dial-now rule and the access URL of the dial-now template.</p> <p>Parameters:</p> <p>phone_setting.dialnow_delay</p>
---------------------------	-------------------	--

		Configure the access URL of the dial-now template. Parameters: dialplan_dialnow.url
Local	Web User Interface	Create the dial-now rule for the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=settings-dialnow&q=load Configure the delay time for the dial-now rule. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.dialnow.rule.X (X ranges from 1 to 100)	String within 511 characters	Blank
Description: Configures the dial-now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the numbers without pressing the send key. Example: dialplan.dialnow.rule.1 = 123 Web User Interface: Settings->Dial Plan->Dial-now-> Rule Phone User Interface: None		
phone_setting.dialnow_delay	Integer from 1 to 14	1
Description: Configures the delay time (in seconds) for the dial-now rule. When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the entered number after the specified delay time. Web User Interface:		

Parameters	Permitted Values	Default
Features->General Information->Time-Out for Dial-Now Rule		
Phone User Interface:		
None		
dialplan_dialnow.url	URL within 511 characters	Blank
Description:		
Configures the access URL of the dial-now rule template file.		
Example:		
dialplan_dialnow.url = http://192.168.10.25/dialnow.xml		
Web User Interface:		
None		
Phone User Interface:		
None		

To create a dial-now rule via web user interface:

1. Click on **Settings->Dial Plan->Dial-now**.
2. Enter the desired value in the **Rule** field.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Settings' tab is active, and the 'Dial Plan' sub-tab is selected. A table titled 'Dial-now Rule' has columns for 'Index' and 'Dial-now Rule'. Below the table, a text input field contains 'Rule 1001', with 'Add', 'Edit', and 'Del' buttons underneath. A 'NOTE' section on the right explains digit matching syntax: 'Digit 0-9 *' for specific digits, '[digit-digit]' for ranges, '[digit-digit,digit]' for comma-separated lists, 'x' for single characters, and '.' for arbitrary numbers of digits.

3. Click **Add** to add the dial-now rule.

To configure the delay time for the dial-now rule via web user interface:

1. Click on **Features->General Information**.

- Enter the desired time within 1-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. Under the 'General Information' section, the 'Time-Out for Dial-Now Rule' field is highlighted with a red box and contains the value '1'. Other visible fields include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Hotline Number', 'Hotline Delay(0~10s)' (4), 'Busy Tone Delay (Seconds)' (0), 'Return Code When Refuse' (486 (Busy Here)), 'Return Code When DND' (480 (Temporarily Not A)), 'RFC 2543 Hold' (Disabled), and 'Use Outbound Proxy In Dialog' (Enabled). A 'NOTE' section on the right provides details for 'Call Waiting', 'Key As Send', and 'Hotline Number'.

- Click **Confirm** to accept the change.

Area Code

Area codes are also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When the entered numbers match the predefined area code rule, the IP phone will automatically add the area code before the numbers when dialing out them. IP phones only support one area code rule.

Procedure

Area code rule can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Create the area code rule and specify the maximum and minimum lengths of the entered numbers. Parameters: dialplan.area_code.code dialplan.area_code.min_len dialplan.area_code.max_len
Local	Web User Interface	Create the area code rule and specify the maximum and minimum lengths of entered numbers.

		Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-areacode&q=load">http://<phoneIPAddress>/servlet?p=settings-areacode&q=load
--	--	--

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.area_code.code	String within 16 characters	Blank
Description: Configures the area code to be added before the entered numbers when dialing out. Example: dialplan.area_code.code = 010 Web User Interface: Settings->Dial Plan->Area Code->Code Phone User Interface: None		
dialplan.area_code.min_len	Integer from 1 to 15	1
Description: Configures the minimum length of the entered numbers. Web User Interface: Settings->Dial Plan->Area Code->Min Length (1-15) Phone User Interface: None		
dialplan.area_code.max_len	Integer from 1 to 15	15
Description: Configures the maximum length of the entered numbers. Note: The value must be larger than the minimum length. Web User Interface: Settings->Dial Plan->Area Code->Max Length (1-15) Phone User Interface: None		

To configure an area code rule via web user interface:

1. Click on **Settings->Dial Plan->Area Code**.

2. Enter desired values in the **Code**, **Min Length (1-15)** and **Max Length (1-15)** fields.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is active, and the 'Block Out' sub-tab is selected. The 'Code' field is set to '0592', 'Min Length (1-15)' is set to '1', and 'Max Length (1-15)' is set to '15'. A red rectangle highlights these three input fields. Below the fields are 'Confirm' and 'Cancel' buttons. On the right side, a 'NOTE' section explains the digit matching syntax: 'Digit 0-9 *' identifies a specific digit, '[digit-digit]' identifies any digit in a range, '[digit-digit,digit]' identifies a range with a comma-separated list, 'x' matches any single digit/character, and '.' matches an arbitrary number of digits.

3. Click **Confirm** to accept the change.

Block Out

Block out rule prevents users from dialing out specific numbers. When the entered numbers match the predefined block out rule, the LCD screen prompts "Forbidden Number". IP phones support up to 10 block out rules.

Procedure

Block out rule can be created using the configuration files or locally.

Configuration File	y000000000037.cfg	Create the block out rule for the IP phone. Parameters: dialplan.block_out.number.X
Local	Web User Interface	Create the block out rule for the IP phone. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-blackout&q=load">http://<phoneIPAddress>/servlet?p=settings-blackout&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.block_out.number.X (X ranges from 1 to 10)	String within 32 characters	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the block out numbers.</p> <p>Example: dialplan.block_out.number.1 = 1234</p> <p>Web User Interface: Settings->Dial Plan->Block Out->BlockOut NumberX</p> <p>Phone User Interface: None</p>		

To create a block out rule via web user interface:

1. Click on **Settings->Dial Plan->Block Out**.
2. Enter the desired value in the **BlockOut Number** field.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is active, and the 'Block Out' sub-tab is selected. The 'BlockOut Number1' field is highlighted with a red box and contains the value '1002'. Below it are fields for BlockOut Number2 through BlockOut Number10. At the bottom are 'Confirm' and 'Cancel' buttons. A 'NOTE' section on the right explains the syntax for digit ranges and characters.

3. Click **Confirm** to add the block out rule.

Hotline

Hotline is a point-to-point communication link in which a call is automatically directed to the preset hotline number. The IP phone automatically dials out the hotline number after the designated period of time when pressing the off-hook key. IP phones only support one hotline number.

Procedure

Hotline can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the hotline number.</p> <p>Parameter:</p> <p>features.hotline_number</p> <p>Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number.</p> <p>Parameter:</p> <p>features.hotline_delay</p>
Local	Web User Interface	<p>Configure the hotline number.</p> <p>Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-general&q=load</p>
	Phone User Interface	<p>Configure the hotline number.</p> <p>Specify the time (in seconds) the IP phone waits to automatically dial out the hotline number.</p>

Details of Configuration Parameters:

Parameter	Permitted Values	Default
features.hotline_number	String within 32 characters	Blank
<p>Description:</p> <p>Configures the hotline number that the IP phone automatically dials out when pressing the off-hook key. Leaving it blank disables hotline feature.</p> <p>Example:</p> <p>features.hotline_number = 3601</p> <p>Web User Interface:</p> <p>Features->General Information->Hotline Number</p> <p>Phone User Interface:</p> <p>Menu->Features->Hot Line->Number</p>		
features.hotline_delay	Integer from 0 to 10	4

Parameter	Permitted Values	Default
<p>Description:</p> <p>Configures the waiting time (in seconds) for the IP phone to automatically dial out the hotline number.</p> <p>If it is set to 0 (0s), the IP phone will immediately dial out the preconfigured hotline number when you press the off-hook key.</p> <p>If it is set to a value greater than 0, the IP phone will wait the designated seconds before dialing out the predefined hotline number when you press the off-hook key.</p> <p>Web User Interface:</p> <p>Features->General Information->Hotline Delay (0~10s)</p> <p>Phone User Interface:</p> <p>Menu->Features->Hot Line->Hotline Delay</p>		

To configure hotline via web user interface:

1. Click on **Features->General Information**.
2. Enter the hotline number in the **Hotline Number** field.
3. Enter the delay time in the **Hotline Delay (0~10s)** field.

The screenshot shows the Yealink CP860 web user interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. In the 'General Information' section, the 'Hotline Number' field is set to '1009' and the 'Hotline Delay(0~10s)' field is set to '4'. These two fields are highlighted with a red rectangular box. Other settings visible include 'Call Waiting' (Enabled), 'Auto Redial' (Enabled), 'Auto Redial Interval' (10), 'Auto Redial Times' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Busy Tone Delay' (0), 'Return Code When Refuse' (486), 'Return Code When DND' (480), and 'Time-Out for Dial-Now Rule' (1). A 'NOTE' section on the right provides additional information about the 'Call Waiting', 'Key As Send', and 'Hotline Number' features.

4. Click **Confirm** to accept the change.

To configure hotline via phone user interface:

1. Press **Menu->Features->Hot Line**.
2. Enter the hotline number in the **Number** field.
3. Enter the delay time in the **Hotline Delay** field.
4. Press the **Save** soft key to accept the change.

Directory

Directory provides easy access to frequently used lists. The lists can be Local Directory, History, Remote Phone Book and LDAP. The desired list(s) can be added to Directory using a directory file. For more information on the directory file, refer to [Directory Template](#) on page 327.

Procedure


Directory can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify the access URL of the Directory file. Parameter: directory_setting.url
Local	Web User Interface	Configure the Directory. Navigate to: http://<phoneIPAddress>/servlet ?p=contacts-favorite&q=load



Details of the Configuration Parameter:

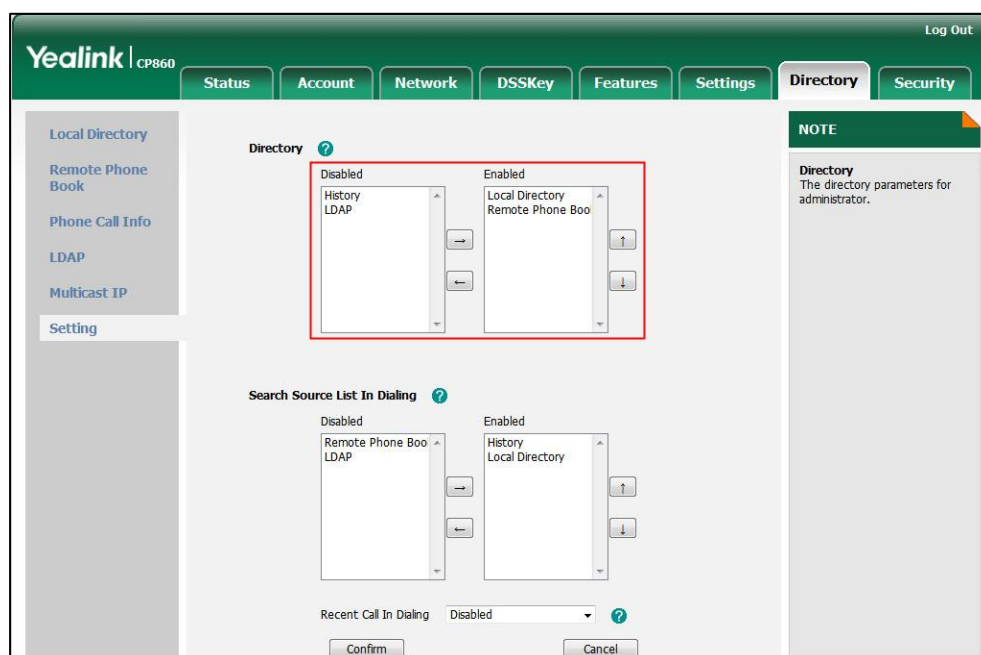
Parameter	Permitted Values	Default
directory_setting.url	URL within 511 characters	Blank
Description: Configures the access URL of the directory template. Example: directory_setting.url = http://192.168.1.20/favorite_setting.xml Web User Interface: Directory->Setting->Directory Phone User Interface: None		

To configure the directory via web user interface:

1. Click on **Directory->Setting**.
2. In the **Directory** block, select the desired list from the **Disabled** column and then click  .
The selected list appears in the **Enabled** column.
3. Repeat the step 2 to add more lists to the **Enabled** column.
4. To remove a list from the **Enabled** column, select the desired list and then

click  .

5. To adjust the display order of enabled lists, select the desired list and then click  or  .



6. Click **Confirm** to accept the change.

The IP phone LCD screen will display the enabled list(s) in the adjusted order.

Search Source List in Dialing

Search source list in dialing allows the IP phone to automatically search entries from the search source list based on the entered string, and display results on the dialing screen. The search source list can be Local Directory, History, Remote Phone Book and LDAP. You can configure the search source list in dialing using a super search file. For more information on the super search template, refer to [Super Search Template](#) on page 328.

Procedure

Search source list can be configured using the configuration files or locally.





Configuration File	y000000000037.cfg	Specify the access URL of the super search file. Parameter: super_search.url
Local	Web User Interface	Configure the search source list in dialing. Navigate to: http://<phoneIPAddress>/servlet

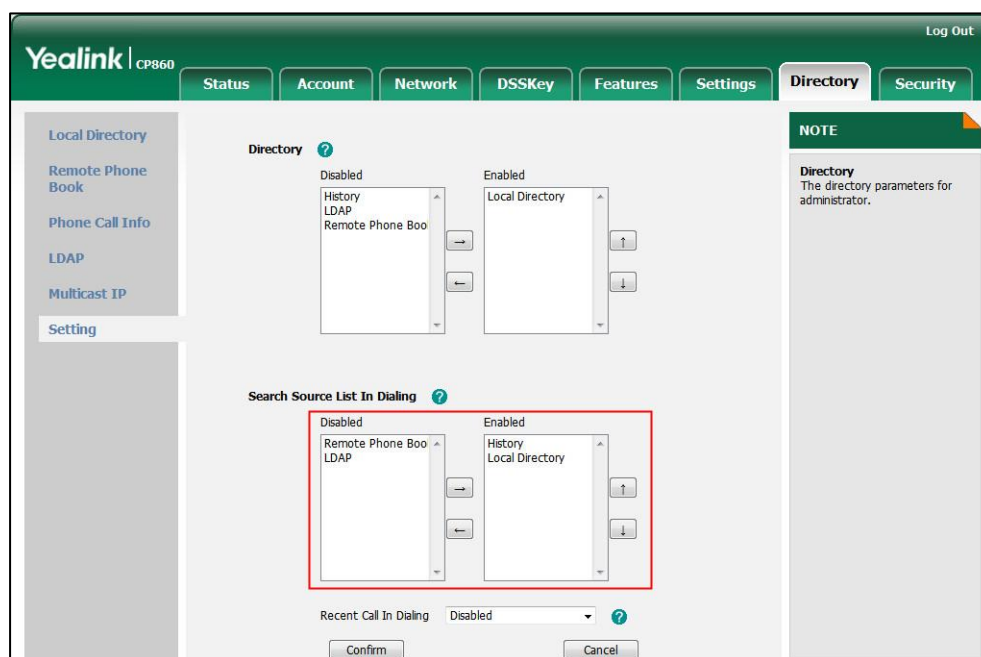
		?p=contacts-favorite&q=load
--	--	-----------------------------

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
super_search.url	URL within 511 characters	Blank
Description: Configures the access URL of the super search template.		
Web User Interface: Directory->Setting->Search Source List In Dialing		
Phone User Interface: None		

To configure search source list in dialing via web user interface:

1. Click on **Directory->Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and click  .
The selected list appears in the **Enabled** column.
3. Repeat step 2 to add more lists to the **Enabled** column.
4. To remove a list from the **Enabled** column, select the desired list and then click  .
5. To adjust the display order of the enabled list, select the desired list, and click  or  .



6. Click **Confirm** to accept the change.

The dialing screen displays the search results in the adjusted order.

Call Log

Call log contains call information such as remote party identification, time and date, and call duration. IP phones maintain a local call log. Call log consists of four lists: Missed calls, Placed calls, Received calls and Forwarded calls. Each call log list supports up to 100 entries. To store call information, you must enable the save call log feature in advance.

Procedure

Call log can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the call log. Parameter: features.save_call_history
Local	Web User Interface	Configure the call log. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the call log.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.save_call_history	0 or 1	1
Description: Enables or disables the IP phone to save call log. 0-Disabled 1-Enabled If it is set to 0 (Disabled), the IP phone cannot log the placed calls, received calls, missed calls and the forwarded calls in the call log lists. Web User Interface: Features->General Information->Save Call Log Phone User Interface: Menu->Features->History Setting->History Record		

To configure the call log via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Save Call Log**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. Under 'General Information', the 'Save Call Log' option is highlighted with a red box, and its dropdown menu is set to 'Enabled'. Other options include Call Waiting (Enabled), Call Waiting On Code, Call Waiting Off Code, Auto Redial (Disabled), Auto Redial Interval (10), Auto Redial Times (10), Key As Send (#), and Reserve # in User Name (Enabled). A 'NOTE' section on the right provides information about Call Waiting, Key As Send, and Hotline Number.

3. Click **Confirm** to accept the change.

To configure the call log via phone user interface:

1. Press **Menu-> Features-> History Setting**.
2. Press the ◀ or ▶ soft key to select the desired value from the **History Record** field.
3. Press the **Save** soft key to accept the change.

Missed Call Log

Missed call log allows IP phones to display the number of the missed calls with an indicator icon on the idle screen, and to log the missed calls in the Missed Calls list when the IP phone misses calls. Once the user accesses the Missed calls list, the prompt message and indicator icon on the idle screen disappear.

Procedure

Missed call log can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the missed call log feature. Parameter: account.X.missed_calllog
Local	Web User Interface	Configure the missed call log feature. Navigate to:

		http://<phoneIPAddress>/servlet ?p=account-basic&q=load&acc =0
--	--	--

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.missed_callog (X = 1)	0 or 1	1
<p>Description:</p> <p>Enables or disables the IP phone to record missed calls for account X.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>If it is set to 0 (Disabled), there is no indicator displaying on the LCD screen, the IP phone does not log the missed call in the Missed Calls list.</p> <p>If it is set to 1 (Enabled), a prompt message "<number> New Missed Call(s)" along with an indicator icon is displayed on the IP phone idle screen when the IP phone misses calls.</p> <p>Web User Interface:</p> <p>Account->Basic->Missed Call Log</p> <p>Phone User Interface:</p> <p>None</p>		

To configure missed call log via web user interface:

1. Click on **Account-> Basic**.
2. Select the desired value from the pull-down list of **Missed Call Log**.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Account' tab is selected, and the 'Basic' sub-tab is active. On the left sidebar, 'Register' is selected, and 'Basic' is highlighted. The main configuration area lists several parameters: Proxy Require, Local Anonymous, Send Anonymous Code, On Code, Off Code, Anonymous Call Rejection, Auto Answer, Auto Answer Mute, and Ring Type. The 'Missed Call Log' parameter is highlighted with a red box and is set to 'Enabled'. A 'NOTE' box on the right states: 'Basic: The basic parameters for administrator. Proxy Require: A special parameter just for Nortel server. If you login to Nortel server, the value should be, com.nortelnetworks.firewall'. At the bottom, there are 'Confirm' and 'Cancel' buttons.

3. Click **Confirm** to accept the change.

Local Directory

The IP phone maintains a local directory. The local directory can store up to 1000 contacts and 48 groups (including the default groups: Company, Family and Friend). When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the ring tone and group for the contact. Contacts and groups can be added either one by one or in batch using a local contact file. For more information on how to customize a contact file, refer to [Directory Template](#) on page 327.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y0000000000037.cfg	Specify the access URL of the local contact file. Parameter: local_contact.data.url
Local	Web User Interface	Add a new group and a contact to the local directory. Navigate to: http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&group=
	Phone User Interface	Add a new group and a contact to the local directory.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
local_contact.data.url	URL within 511 characters	Blank
Description: Configures the access URL of the local contact file. Example: local_contact.data.url = http://192.168.10.25/contact.xml Web User Interface: Directory->Local Directory->Import Local Directory File Phone User Interface: None		

To add a new group to the local directory via web user interface:

1. Click on **Directory->Local Directory**.

2. In the **Group Setting** block, enter the new group name in the **Group** field.
3. Select the desired group ring tone from the pull-down list of **Ring**.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Directory' tab is active. On the left, a sidebar lists 'Local Directory', 'Remote Phone Book', 'Phone Call Info', 'LDAP', 'Multicast IP', and 'Setting'. The main content area is divided into two sections: 'Local Directory' and 'Group Setting'. The 'Local Directory' section contains a table with columns: Index, Name, Office Number, Mobile Number, Other Number, and All Contacts. The table has 10 rows, with the first two rows populated: Index 1 with Name 'Gj' and Office Number '5002', and Index 2 with Name 'Gjg' and Office Number '5002'. Below the table are pagination controls (Page 1, Prev, Next, Hang Up, Delete All, Delete, Move To, All Contacts) and a 'Directory' form with fields for Name, Office Number, Mobile Number, Other Number, Ring Tone (set to Auto), and Group (set to All Contacts). The 'Group Setting' section is highlighted with a red box and contains a 'Group' field with the value 'group1', a 'Ring' dropdown set to 'Auto', and buttons for 'Add', 'Edit', 'Delete', and 'Delete All'. Below this is an 'Import Local Directory File' section with 'Import XML', 'Export XML', 'Import CSV', and 'Export CSV' buttons, each with a 'Browse...' button. On the right, a 'NOTE' section provides instructions for adding, deleting, and moving contacts, and an 'Export' section with an 'Export' button.

4. Click **Add** to add the group.

To add a contact to the local directory via web user interface:

1. Click on **Directory->Local Directory**.
2. Enter the name and the office, mobile or other numbers in the corresponding fields.
3. Select the desired ring tone from the pull-down list of **Ring Tone**.
4. Select the desired group from the pull-down list of **Group**.

The screenshot shows the Yealink CP860 web interface with the 'Directory' tab active. The 'Local Directory' section is highlighted with a red box and contains a form with fields for Name (Joy), Office Number (1008), Mobile Number (123456), Other Number (123564), Ring Tone (Auto), and Group (All Contacts). The 'Group Setting' section is also visible, showing a 'Group' field with the value 'group1', a 'Ring' dropdown set to 'Auto', and buttons for 'Add', 'Edit', 'Delete', and 'Delete All'. The 'Import Local Directory File' section is also visible, showing 'Import XML', 'Export XML', 'Import CSV', and 'Export CSV' buttons, each with a 'Browse...' button. On the right, a 'NOTE' section provides instructions for adding, deleting, and moving contacts, and an 'Export' section with an 'Export' button.

- Click **Add** to add the contact.

To add a group to the local directory via phone user interface:

- Press **Menu->Directory->Local Directory**.
- Press the **AddGrp** soft key.
- Enter the desired group name in the **Name** field.
- Press the ◀ or ▶ soft key to select the desired ring tone from the **Ring Tones** field.
- Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

To add a contact to the local directory via phone user interface:

- Press **Menu->Directory->Local Directory**.
- Select the desired contact group and press the **Enter** soft key.
- Press the **Add** soft key.
- Enter the name and the office, mobile or other numbers in the corresponding fields.
- Press the ◀ or ▶ soft key to select the desired ring tone from the **Ring Tones** field.
- Press the **Save** soft key to accept the change.

Live Dialpad

Live dialpad allows IP phones to automatically dial out the entered phone number after a specified period of time.

Procedure

Live dialpad can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure live dialpad. Parameters: phone_setting.predial_autodial phone_setting.inter_digit_time
Local	Web User Interface	Configure live dialpad. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-preference&q=load">http://<phoneIPAddress>/servlet?p=settings-preference&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.predial_autodial	0 or 1	0

Parameters	Permitted Values	Default
<p>Description: Enables or disables live dialpad feature.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), the IP phone will automatically dial out the entered phone number in the pre-dialing screen without pressing a send key.</p> <p>Web User Interface: Settings->Preference->Live Dialpad</p> <p>Phone User Interface: None</p>		
phone_setting.inter_digit_time	Integer from 1 to 14	4
<p>Description: Configures the time (in seconds) for the IP phone to automatically dial out the entered digits without pressing a send key.</p> <p>Note: It works only if the parameter "phone_setting.predial_autodial" is set to 1 (Enabled).</p> <p>Web User Interface: Settings->Preference->Inter Digit Time (1~14s)</p> <p>Phone User Interface: None</p>		

To configure live dialpad via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Live Dialpad**.

- Enter the desired delay time in the **Inter Digit Time (1~14s)** field.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is selected. In the 'Preference' section, the 'Inter Digit Time(1~14s)' field is highlighted with a red box and contains the value '4'. Other settings include Language (English(English)), Live Dialpad (Enabled), Backlight Time(seconds) (Always On), Contrast (6), Watch Dog (Disabled), Ring Type (Ring1.wav), and Upload Ringtone. There are 'Confirm' and 'Cancel' buttons at the bottom.

- Click **Confirm** to accept the change.

Call Waiting

Call waiting allows IP phones to receive a new incoming call when there is already an active call. The new incoming call is presented to the user visually on the LCD screen. Call waiting tone allows the IP phone to play a short tone, to remind the user audibly of a new incoming call during conversation. Call waiting tone works only if call waiting is enabled.

The call waiting on code and call waiting off code configured on IP phones are used to activate/deactivate the server-side call waiting feature. They may vary on different servers.

Procedure

Call waiting and call waiting tone can be configured using the configuration files or locally.

Configuration File	y0000000000037.cfg	Configure call waiting. Parameters: call_waiting.enable call_waiting.tone call_waiting.on_code call_waiting.off_code
Local	Web User Interface	Configure call waiting. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure call waiting.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
call_waiting.enable	0 or 1	1
<p>Description: Enables or disables call waiting feature.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 0 (Disabled), a new incoming call is automatically rejected by the IP phone with a busy message while during a call.</p> <p>If it is set to 1 (Enabled), the LCD screen will present a new incoming call while during a call.</p> <p>Web User Interface: Features->General Information->Call Waiting</p> <p>Phone User Interface: Menu->Features->Call Waiting->Call Waiting</p>		
call_waiting.tone	0 or 1	1
<p>Description: Enables or disables the IP phone to play the call waiting tone when the IP phone receives an incoming call during a call.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), the IP phone will perform an audible indicator when receiving a new incoming call during a call.</p> <p>Note: It works only if the parameter "call_waiting.enable" is set to 1 (Enabled).</p> <p>Web User Interface: Features->Audio->Call Waiting Tone</p> <p>Phone User Interface: Menu->Features->Call Waiting->Play Tone</p>		
call_waiting.on_code	String within 32 characters	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the call waiting on code to activate the server-side call waiting feature. The IP phone will send the call waiting on code to the server when you activate call waiting feature on the IP phone.</p> <p>Example: call_waiting.on_code = *71</p> <p>Web User Interface: Features->General Information->Call Waiting On Code</p> <p>Phone User Interface: Menu->Features->Call Waiting->On Code</p>		
call_waiting.off_code	String within 32 characters	Blank
<p>Description: Configures the call waiting off code to deactivate the server-side call waiting feature. The IP phone will send the call waiting off code to the server when you deactivate call waiting feature on the IP phone.</p> <p>Example: call_waiting.off_code = *72</p> <p>Web User Interface: Features->General Information->Call Waiting Off Code</p> <p>Phone User Interface: Menu->Features->Call Waiting->Off Code</p>		

To configure call waiting via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Call Waiting**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.

- (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.

Yealink CP860 Log Out

Status Account Network DSSKey **Features** Settings Directory Security

Forward&DND

General Information

Call Waiting	Enabled	?
Call Waiting On Code	*71	?
Call Waiting Off Code	*72	?
Auto Redial	Enabled	?
Auto Redial Interval (1~300s)	10	?
Auto Redial Times (1~300)	10	?
Key As Send	#	?
Reserve # in User Name	Enabled	?
Hotline Number		?
Hotline Delay(0~10s)	4	?
Busy Tone Delay (Seconds)	0	?
Return Code When Refuse	486 (Busy Here)	?
Return Code When DND	480 (Temporarily Not Av.)	?
Time-Out for Dial-Now Rule	1	?

NOTE

Call Waiting
This call feature allows your phone to accept other incoming calls during the conversation.

Key As Send
Select * or # as the send key.

Hotline Number
When you pick up the phone, it will dial out the hotline number automatically.

- Click **Confirm** to accept the change.

To configure the call waiting tone via web user interface:

- Click on **Features->Audio**.
- Select the desired value from the pull-down list of **Call Waiting Tone**.

Yealink CP860 Log Out

Status Account Network DSSKey **Features** Settings Directory Security

Forward&DND

General Information

Audio

Intercom

Transfer

Call Pickup

Remote Control

Phone Lock

Action URL

Power LED

Audio Settings

Call Waiting Tone	Enabled	?
Key Tone	Enabled	?
Send Sound	Enabled	?
Redial Tone		?

Confirm Cancel

NOTE

Audio
The audio parameters for administrator.

- Click **Confirm** to accept the change.

To configure call waiting and call waiting tone via phone user interface:

- Press **Menu->Features->Call Waiting**.
- Press the ◀ or ▶ soft key to select **Enable** from the **Call Waiting** field.
- Press the ◀ or ▶ soft key to select **Enable** from the **Play Tone** field.
- (Optional.) Enter the call waiting on code or off code respectively in the **On Code** or **Off Code** field.
- Press the **Save** soft key to accept the change.

Auto Redial

Auto redial allows IP phones to redial a busy number after the first attempt. Both the number of attempts and waiting time between redials are configurable.

Procedure

Auto redial can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure auto redial feature. Parameters: auto_redial.enable auto_redial.interval auto_redial.times
Local	Web User Interface	Configure auto redial feature. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load
	Phone User Interface	Configure auto redial.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_redial.enable	0 or 1	0
Description: Enables or disables the IP phone to automatically redial the dialed number when the callee is temporarily unavailable. 0-Disabled 1-Enabled If it is set to 1 (Enabled), the IP phone will dial the previous dialed out number automatically when the dialed number is temporarily unavailable. Web User Interface: Features->General Information->Auto Redial Phone User Interface: Menu->Features->Auto Redial->Auto Redial		
auto_redial.interval	Integer from 1 to 300	10

Parameters	Permitted Values	Default
Description: Configures the interval (in seconds) for the IP phone to wait between redials. The IP phone redials the dialed number at regular intervals till the callee answers the call. Web User Interface: Features->General Information->Auto Redial Interval (1~300s) Phone User Interface: Menu->Features->Auto Redial->Redial Interval		
auto_redial.times	Integer from 1 to 300	10
Description: Configures the auto redial times when the callee is temporarily unavailable. The IP phone tries to redial the dialed number as many times as configured till the callee answers the call. Web User Interface: Features->General Information->Auto Redial Times (1~300) Phone User Interface: Menu->Features->Auto Redial->Redial Times		

To configure auto redial via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Auto Redial**.
3. Enter the desired time interval (in seconds) in the **Auto Redial Interval (1~300s)** field.

The default waiting time is 10s.

- Enter the desired times in the **Auto Redial Times (1~300)** field.

The default value is 10.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. Under 'General Information', the 'Auto Redial' section is highlighted with a red box. The 'Auto Redial' dropdown is set to 'Enabled', 'Auto Redial Interval (1~300s)' is set to '10', and 'Auto Redial Times (1~300)' is set to '10'. Other settings visible include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Key As Send' (Set to '#'), 'Reserve # in User Name' (Enabled), 'Hotline Number', 'Hotline Delay(0~10s)' (Set to 4), 'Busy Tone Delay (Seconds)' (Set to 0), 'Return Code When Refuse' (Set to 486 (Busy Here)), 'Return Code When DND' (Set to 480 (Temporarily Not Av.)), and 'Time-Out for Dial-Now Rule' (Set to 1).

- Click **Confirm** to accept the change.

To configure auto redial via phone user interface:

- Press **Menu->Features->Auto Redial**.
- Press the ◀ or ▶ soft key to select **Enable** from the **Auto Redial** field.
- Enter the desired time in the **Redial Interval** field.
The default time interval is 10 seconds.
- Enter the desired times in the **Redial Times** field.
The default value is 10.
- Press the **Save** soft key to accept the change.

Auto Answer

Auto answer allows IP phones to automatically answer an incoming call. Auto answer mute allows IP phones to mute the local microphone when an incoming call is answered automatically. Auto-Answer delay defines a period of delay time before the IP phone automatically answers incoming calls.

Procedure

Auto answer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure auto answer. Parameter: account.X.auto_answer Configure auto answer mute. Parameter:
--------------------	-----------	--

		account.X.auto_answer_mute_enable
	y000000000037.cfg	Specify a period of delay time for auto answer. Parameter: features.auto_answer_delay
Local	Web User Interface	Configure auto answer. Navigate to: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0 Specify a period of delay time for auto answer. http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure auto answer.

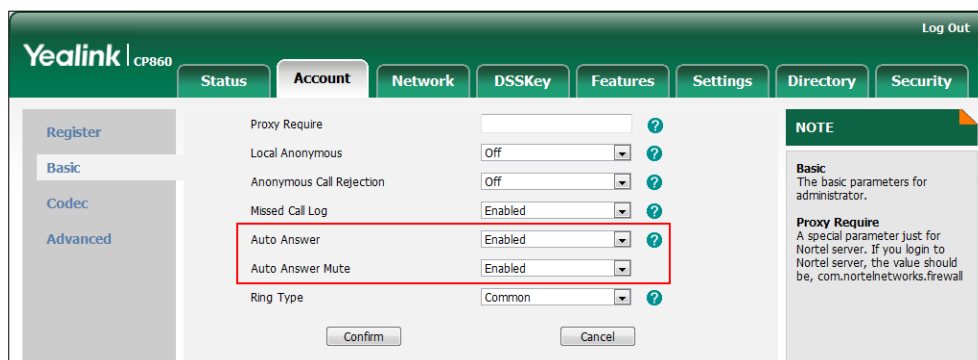
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.auto_answer (X = 1)	0 or 1	0
Description: Enables or disables auto answer feature for account X. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the IP phone can automatically answer an incoming call. Note: The IP phone can automatically answer multiple incoming calls when auto answer is enabled. Web User Interface: Account->Basic->Auto Answer Phone User Interface: Menu->Features->Auto Answer->Auto Answer		
account.X.auto_answer_mute_enable (X = 1)	0 or 1	1
Description: Enables or disables auto answer mute feature for account X. 0 -Disabled 1 -Enabled		

Parameters	Permitted Values	Default
<p>If it is set to 1 (Enabled), the IP phone can mute the local microphone when an incoming call is answered automatically.</p> <p>Web User Interface: Account->Basic->Auto Answer Mute</p> <p>Phone User Interface: Menu->Features->Auto Answer->Auto Answer Mute</p>		
features.auto_answer_delay (X = 1)	Integer from 1 to 4	1
<p>Description: Configures the delay time (in seconds) before the IP phone automatically answers an incoming call.</p> <p>Web User Interface: Features-> General Information->Auto-Answer Delay (1~4s)</p> <p>Phone User Interface: None</p>		

To configure auto answer and auto answer mute via web user interface:

1. Click on **Account-> Basic**.
2. Select the desired value from the pull-down list of **Auto Answer**.
3. Select the desired value from the pull-down list of **Auto Answer Mute**.



4. Click **Confirm** to accept the change.

To configure a period of delay time for auto answer via web user interface:

1. Click on **Features->General Information**.

2. Enter the desired time (in seconds) in the **Auto-Answer Delay (1~4s)** field.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. In the 'General Information' section, the 'Auto-Answer Delay (1~4s)' field is highlighted with a red box and contains the value '3'. Other settings include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'DTMF Replace Tran' (Disabled), 'Allow IP Call' (Enable), 'IP Direct Auto Answer' (Disabled), 'Call List Show Number' (Disabled), 'Voice Mail Tone' (Enable), and 'DHCP Hostname' (CP860). A 'NOTE' section on the right provides information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

3. Click **Confirm** to accept the change.

To configure auto answer and auto answer mute via phone user interface:

1. Press **Menu->Features->Auto Answer**.
2. Press the ◀ or ▶ soft key to select **Enable** from the **Auto Answer** field.
3. Press the ◀ or ▶ soft key to select **Enable** from the **Auto Answer Mute** field.
4. Press the **Save** soft key to accept the change.

Anonymous Call

Anonymous call allows the caller to conceal the identity information displayed on the callee's screen. The callee's phone LCD screen prompts an incoming call from anonymity.

Example of anonymous SIP header:

```
Via: SIP/2.0/UDP 10.2.8.183:5063;branch=z9hG4bK1535948896
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=128043702
To: <sip:1011@10.2.1.199>
Call-ID: 1773251036@10.2.8.183
CSeq: 1 INVITE
Contact: <sip:1012@10.2.8.183:5063>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE
```



```

Max-Forwards: 70
User-Agent: Yealink CP860 37.72.0.2
Privacy: id
Supported: replaces
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1012@10.2.1.199>
Content-Length: 302

```

The anonymous call on code and anonymous call off code configured on IP phones are used to activate/deactivate the server-side anonymous call feature. They may vary on different servers. Send Anonymous Code feature allows IP phones to select anonymous call on or anonymous call off code to the server.

Procedure

Anonymous call can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure anonymous call. Parameters: account.X.anonymous_call account.X.send_anonymous_code account.X.anonymous_call_oncode account.X.anonymous_call_offcode
Local	Web User Interface	Configure anonymous call. Navigate to: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.anonymous_call (X = 1)	0 or 1	0
Description: Enables or disables anonymous call feature. 0-Disabled 1-Enabled If it is set to 1 (Enabled), the IP phone will block its identity from showing up to the callee when placing a call. The callee's phone LCD screen presents anonymous		

Parameters	Permitted Values	Default
<p>instead of the caller's identity.</p> <p>Web User Interface: Account->Basic->Local Anonymous</p> <p>Phone User Interface: Menu->Features->Anonymous Call->Local Anonymous</p>		
account.X.send_anonymous_code (X = 1)	0 or 1	0
<p>Description: Configures the IP phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature.</p> <p>0-Off Code 1-On Code</p> <p>If it is set to 0 (Off Code), the IP phone will send anonymous off code to deactivate the server-side anonymous call feature.</p> <p>If it is set to 1 (On Code), the IP phone will send anonymous on code to activate the server-side anonymous call feature.</p> <p>Web User Interface: Account->Basic->Send Anonymous Code</p> <p>Phone User Interface: Menu->Features->Anonymous Call->Anonymous Code</p>		
account.X.anonymous_call_oncode (X = 1)	String within 32 characters	Blank
<p>Description: Configures the anonymous call on code to activate the server-side anonymous call feature.</p> <p>Example: account.1.anonymous_call_oncode = *86</p> <p>Note: It works only if the parameter "account.X.send_anonymous_code" is set to 1 (On Code).</p> <p>Web User Interface: Account->Basic->Anonymous Call->On Code</p> <p>Phone User Interface:</p>		

Parameters	Permitted Values	Default
Menu->Features->Anonymous Call->On Code		
account.X.anonymous_call_offcode (X = 1)	String within 32 characters	Blank
<p>Description: Configures the anonymous call off code to deactivate the server-side anonymous call feature.</p> <p>Example: account.1.anonymous_call_offcode = *87</p> <p>Note: It works only if the parameter "account.X.send_anonymous_code" is set to 0 (Off Code).</p> <p>Web User Interface: Account->Basic->Anonymous Call->Off Code</p> <p>Phone User Interface: Menu->Features->Anonymous Call->Off Code</p>		

To configure the anonymous call via web user interface:

1. Click on **Account-> Basic**.
2. Select the desired value from the pull-down list of **Local Anonymous**.
3. (Optional.) Select the desired value from the pull-down list of **Send Anonymous Code**.
4. (Optional.) Enter the anonymous call on code in the **On Code** field.
5. (Optional.) Enter the anonymous call off code in the **Off Code** field.

The screenshot shows the Yealink CP860 web interface. The 'Account' tab is selected, and the 'Basic' sub-tab is active. The configuration page for 'Basic' is displayed. A red box highlights the following settings:

- Proxy Require: [Empty field]
- Local Anonymous: On
- Send Anonymous Code: On Code
- On Code: *86
- Off Code: *87

Other visible settings include:

- Anonymous Call Rejection: Off
- On Code: [Empty field]
- Off Code: [Empty field]
- Missed Call Log: Enabled
- Auto Answer: Disabled
- Auto Answer Mute: Enabled
- Ring Type: Common

Buttons at the bottom are 'Confirm' and 'Cancel'. A 'NOTE' section on the right states: 'Basic: The basic parameters for administrator. Proxy Require: A special parameter just for Nortel server. If you login to Nortel server, the value should be, com.nortelnetworks.firewall'.

6. Click **Confirm** to accept the change.

To configure the anonymous call via phone user interface:

1. Press **Menu->Features->Anonymous Call**.
2. Press the ◀ or ▶ soft key to select **Enable** from the **Local Anonymous** field.
3. (Optional.) Press the ◀ or ▶ soft key to select the desired value from the **Anonymous Code** field.
4. (Optional.) Enter the anonymous call on code in the **On Code** field.
5. (Optional.) Enter the anonymous call off code in the **Off Code** field.
6. Press the **Save** soft key to accept the change.

Anonymous Call Rejection

Anonymous call rejection allows IP phones to automatically reject incoming calls from callers whose identity has been deliberately concealed. The anonymous caller's LCD screen presents "Anonymity Disallowed".

The anonymous call rejection on code and anonymous call rejection off code configured on IP phones are used to activate/deactivate the server-side anonymous call rejection feature. They may vary on different servers.

Procedure

Anonymous call rejection can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure anonymous call rejection. Parameters: account.X.reject_anonymous_call account.X.anonymous_reject_oncode account.X.anonymous_reject_offcode
Local	Web User Interface	Configure anonymous call rejection. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure anonymous call rejection.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.reject_anonymous_call (X = 1)	0 or 1	0

Parameters	Permitted Values	Default
Description: Enables or disables anonymous call rejection feature. 0-Disabled 1-Enabled If it is set to 1 (Enabled), the IP phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone LCD screen presents "Anonymity Disallowed". Web User Interface: Account->Basic->Anonymous Call Rejection Phone User Interface: Menu->Features->Anonymous Call->Anonymous Rejection		
account.X.anonymous_reject_oncode (X = 1)	String within 32 characters	Blank
Description: Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature. The IP phone will send the anonymous call rejection on code to the server when you activate anonymous call rejection feature on the IP phone. Example: account.1.anonymous_reject_oncode = *88 Web User Interface: Account->Basic->Anonymous Call Rejection->On Code Phone User Interface: Menu->Features->Anonymous Call->Reject On Code		
account.X.anonymous_reject_offcode (X = 1)	String within 32 characters	Blank
Description: Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature. The IP phone will send the anonymous call rejection off code to the server when you deactivate anonymous call rejection feature on the IP phone. Example: account.1.anonymous_reject_offcode = *89		

Parameters	Permitted Values	Default
Web User Interface: Account->Basic->Anonymous Call Rejection->Off Code Phone User Interface: Menu->Features->Anonymous Call->Reject Off Code		

To configure anonymous call rejection via web user interface:

1. Click on **Account->Basic**.
2. Select the desired value from the pull-down list of **Anonymous Call Rejection**.
3. (Optional.) Enter the anonymous call rejection on code in the **On Code** field.
4. (Optional.) Enter the anonymous call rejection off code in the **Off Code** field.

5. Click **Confirm** to accept the change.

To configure anonymous call rejection via phone user interface:

1. Press **Menu->Features->Anonymous Call**.
2. Press or to scroll to the **Anonymous Rejection** field.
3. Press the or soft key to select **Enable** from the **Anonymous Rejection** field.
4. (Optional.) Enter the anonymous call rejection on code in the **Reject On Code** field.
5. (Optional.) Enter the anonymous call rejection off code in the **Reject Off Code** field.
6. Press the **Save** soft key to accept the change.

Do Not Disturb

Do Not Disturb (DND) allows IP phones to ignore incoming calls. A user can activate or deactivate DND using the DND soft key or DND key. The DND configurations on IP phones may be overridden by the server settings. The server-side DND feature disables the local DND and call forward settings. If the server-side DND feature is enabled on

any of the IP phone's registrations, the other registrations are not affected. For more information on call forward, refer to [Call Forward](#) on page 139.

The DND on code and DND off code configured on IP phones are used to activate/deactivate the server-side DND feature. They may vary on different servers.

Return Message When DND

This feature defines the return code and the reason of the SIP response message for the rejected incoming call when DND is enabled on IP phones. The caller's LCD screen displays the received return code.

Procedure

DND can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Assign a DND key. Parameters: programablekey.X.type Configure DND. Parameters: features.dnd.enable features.dnd.on_code features.dnd.off_code Specify return code and reason of the SIP response message. Parameter: features.dnd_refuse_code
Local	Web User Interface	Assign a DND key. Navigate to: http://<phoneIPAddress>/servlet?p=dsskey&model=2&q=load Configure DND. Navigate to: http://<phoneIPAddress>/servlet?p=features-forward&q=load Specify return code and reason of the SIP response message. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Assign a DND key.

		Configure DND.
--	--	----------------

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dnd.enable	0 or 1	0
Description: Enables or disables DND feature. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the IP phone will reject incoming calls on all accounts. Web User Interface: Features->Forward& DND->DND->DND Status Phone User Interface: Menu->Features->DND->DND Enable		
features.dnd.on_code	String within 32 characters	Blank
Description: Configures the DND on code to activate the server-side DND feature. The IP phone will send the DND on code to the server when you activate DND feature on the IP phone. Example: features.dnd.on_code = *88 Web User Interface: Features->Forward& DND->DND->DND On Code Phone User Interface: Menu->Features->DND-> On Code		
features.dnd.off_code	String within 32 characters	Blank
Description: Configures the DND off code to deactivate the server-side DND feature. The IP phone will send the DND off code to the server when you deactivate DND feature on the IP phone. Example: features.dnd.off_code = *86 Web User Interface:		

Parameters	Permitted Values	Default
Features->Forward& DND->DND->DND Off Code Phone User Interface: Menu->Features->DND->Off Code		
features.dnd_refuse_code	404, 480 or 486	480
Description: Configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone LCD screen. 404 -No Found 480 -Temporarily not available 486 -Busy here If it is set to 486 (Busy here), the caller's LCD screen will display the reason "Busy here" when the callee enables DND. Web User Interface: Features->General Information->Return Code When DND Phone User Interface: None		
programmablekey.X.type (X=1-6, 9, 13)	5	0
Description: Configures a programmable key as a DND key on the IP phone. The digit 5 stands for the key type DND . For more information on how to configure the programmable key, refer to Appendix C: Configuring Programmable Key on page 353. Web User Interface: DSSKey->Programmable Key->Type Phone User Interface: None		

To configure a DND key via web user interface:

1. Click on **DSSKey->Programmable Key**.

- In the desired programmable key field, select **DND** from the pull-down list of **Type**.

The screenshot shows the 'DSSKey' configuration page in the Yealink CP860 web interface. The 'MUTE' key is highlighted with a red box. The 'Type' dropdown for the MUTE key is set to 'DND', and the 'Line' dropdown is set to 'N/A'. The interface includes tabs for Status, Account, Network, DSSKey, Features, Settings, Directory, and Security. A 'Programable Key' table lists various keys like SoftKey 1-4, Up, Down, OK, and MUTE. A 'NOTE' section on the right provides information about Key Type, Key Event, and Intercom.

- Click **Confirm** to accept the change.

To configure the DND feature via web user interface:

- Click on **Features->Forward & DND**.
- In the **DND** block, mark the desired radio box in the **DND Status** field.
- (Optional.) Enter the DND on code in the **DND On Code** field.
- (Optional.) Enter the DND off code in the **DND Off Code** field.

The screenshot shows the 'Forward & DND' configuration page in the Yealink CP860 web interface. The 'DND Status' field is highlighted with a red box, showing the 'On' radio button selected. The 'DND On Code' field is set to '*88' and the 'DND Off Code' field is set to '*86'. The interface includes tabs for Status, Account, Network, DSSKey, Features, Settings, Directory, and Security. A 'Forward&DND' section on the left lists various features like General Information, Audio, Intercom, Transfer, Call Pickup, Remote Control, Phone Lock, Action URL, and Power LED. A 'NOTE' section on the right provides information about Forward, Target, On Code, and Off Code.

- Click **Confirm** to accept the change.

To specify the return code via web user interface:

- Click on **Features->General Information**.

- Select the desired type from the pull-down list of **Return Code When DND**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. Under the 'General Information' section, the 'Return Code When DND' is set to '480 (Temporarily Not Av.)'. A red box highlights this setting. To the right, a 'NOTE' section contains the following information:

- Call Waiting**: This call feature allows your phone to accept other incoming calls during the conversation.
- Key As Send**: Select * or # as the send key.
- Hotline Number**: When you pick up the phone, it will dial out the hotline number automatically.

- Click **Confirm** to accept the change.

Busy Tone Delay

Busy tone is audible to the other party, indicating that the call connection has been broken when one party releases a call. Busy tone delay can define a period of time during which the busy tone is audible.

Procedure

Busy tone delay can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the busy tone delay feature. Parameter: features.busy_tone_delay
Local	Web User Interface	Configure the busy tone delay feature. Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.busy_tone_delay	0, 3 or 5	0
<p>Description:</p> <p>Configures the duration time (in seconds) for the busy tone.</p> <p>When one party releases the call, a busy tone is audible to the other party indicating that the call connection breaks.</p> <p>0-without a busy tone</p> <p>3-3s</p> <p>5-5s</p> <p>If it is set to 3 (3s), a busy tone is audible for 3 seconds on the IP phone.</p> <p>Web User Interface:</p> <p>Features->General Information->Busy Tone Delay (Seconds)</p> <p>Phone User Interface:</p> <p>None</p>		

To configure busy tone delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Busy Tone Delay (Seconds)**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' section is expanded. The 'Busy Tone Delay (Seconds)' dropdown menu is highlighted with a red box, showing the value '0' selected. Other settings visible include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Auto Redial' (Enabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Hotline Number', 'Hotline Delay(0~10s)' (4), 'Return Code When Refuse' (486 (Busy Here)), 'Return Code When DND' (480 (Temporarily Not Av.)), and 'Time-Out for Dial-Now Rule' (1). A 'NOTE' section on the right provides additional information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

3. Click **Confirm** to accept the change.

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for call rejection. The caller's LCD screen displays the reason according to the

return code received. Available return codes and reasons are:

- 404 (Not found)
- 480 (Temporarily not available)
- 486 (Busy here)

Procedure

Return code for call rejection can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the return code when refusing a call. Parameter: features.normal_refuse_code
Local	Web User Interface	Configure the return code when refusing a call. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	404, 480 or 486	486
<p>Description:</p> <p>Configures a return code and reason of SIP response messages when the IP phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen.</p> <p>404-No Found</p> <p>480-Temporarily not available</p> <p>486-Busy here</p> <p>If it is set to 486 (Busy here), the caller's phone LCD screen will display the message "Busy here" when the callee rejects the incoming call.</p> <p>Web User Interface:</p> <p>Features->General Information->Return Code When Refuse</p> <p>Phone User Interface:</p> <p>None</p>		

To specify the return code when refusing a call via web user interface:

1. Click on **Features->General Information**.

2. Select the desired value from the pull-down list of **Return Code When Refuse**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected. Under the 'General Information' section, the 'Return Code When Refuse' dropdown menu is highlighted with a red box, showing '486 (Busy Here)' selected. Other settings visible include 'Call Waiting' (Enabled), 'Auto Redial' (Enabled), 'Hotline Number' (empty), and 'Return Code When DND' (480 (Temporarily Not Av.)).

3. Click **Confirm** to accept the change.

Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established. Current implementation supports early media through the 183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

Procedure

180 ring workaround can be configured using the configuration files or locally.

Configuration File	y0000000000037.cfg	Configure 180 ring workaround. Parameter: phone_setting.is_deal180
Local	Web User Interface	Configure 180 ring workaround. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	0 or 1	1
<p>Description:</p> <p>Enables or disables the IP phone to deal with the 180 SIP message received after the 183 SIP message.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>If it is set to 1 (Enabled), the IP phone will resume and play the local ringback tone upon a subsequent 180 message received.</p> <p>Web User Interface:</p> <p>Features->General Information->180 Ring Workaround</p> <p>Phone User Interface:</p> <p>None</p>		

To configure 180 ring workaround via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **180 Ring Workaround**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' section is active. A list of configuration parameters is displayed, including 'Call Waiting', 'Auto Redial', 'Key As Send', and '180 Ring Workaround'. The '180 Ring Workaround' parameter is highlighted with a red box and is currently set to 'Enabled'. A 'NOTE' section on the right provides additional information about the 'Call Waiting' and 'Hotline Number' features.

3. Click **Confirm** to accept the change.

Use Outbound Proxy in Dialog

An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the IP phone is configured to use an outbound proxy server within a dialog, all SIP request messages from the IP phone will be sent to the outbound proxy server forcefully.

Note

To use this feature, make sure the outbound server has been correctly configured on the IP phone.

Procedure

Use outbound proxy in dialog can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify whether to use outbound proxy in a dialog. Parameter: sip.use_out_bound_in_dialog
Local	Web User Interface	Specify whether to use outbound proxy in a dialog. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_out_bound_in_dialog	0 or 1	1
Description: Enables or disables the IP phone to keep sending SIP requests to the outbound proxy server in a dialog. 0-Disabled 1-Enabled If it is set to 1 (Enabled), all the SIP request messages from the IP phone will be forced to send to the outbound proxy server in a dialog. Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Features->General Information->Use Outbound Proxy In Dialog Phone User Interface:		

Parameter	Permitted Values	Default
None		

To specify whether to use outbound proxy server in a dialog via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Use Outbound Proxy in Dialog**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. A list of configuration parameters is displayed, including 'Call Waiting', 'Auto Redial', 'Key As Send', and 'Use Outbound Proxy in Dialog'. The 'Use Outbound Proxy in Dialog' parameter is highlighted with a red rectangular box, and its value is set to 'Enabled'. To the right of the configuration list, there is a 'NOTE' section with information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

3. Click **Confirm** to accept the change.

SIP Session Timer

SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 will continue until the retransmitting time reaches the T2 value. Timer T4 represents the time the network will take to clear messages between the SIP client and server. These session timers are configurable on IP phones.

Procedure

SIP session timer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure SIP session timer. Parameters: account.X.advanced.timer_t1 account.X.advanced.timer_t2
---------------------------	-----------	--

		account.X.advanced.timer_t4
Local	Web User Interface	Configure SIP session timer. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.advanced.timer_t1 (X = 1)	Float from 0.5 to 10	0.5
Description: Configures the SIP session timer T1 (in seconds). T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. Web User Interface: Account->Advanced->SIP Session Timer T1 (0.5~10s) Phone User Interface: None		
account.X.advanced.timer_t2 (X = 1)	Float from 2 to 40	4
Description: Configures the session timer T2 (in seconds). T2 represents the maximum retransmit interval for non-INVITE requests and INVITE responses. Web User Interface: Account->Advanced->SIP Session Timer T2 (2~40s) Phone User Interface: None		
account.X.advanced.timer_t4 (X = 1)	Float from 2.5 to 60	5

Parameters	Permitted Values	Default
Description: Configures the session timer of T4 (in seconds). T4 represents the maximum duration a message will remain in the network.		
Web User Interface: Account->Advanced->SIP Session Timer T4 (2.5~60s)		
Phone User Interface: None		

To configure session timer via web user interface:

1. Click on **Account->Advanced**.
2. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.
The default value is 0.5s.
3. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.
The default value is 4s.
4. Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.
The default value is 5s.

The screenshot shows the Yealink CP860 web interface. The 'Account' tab is selected, and the 'Advanced' sub-tab is active. A red box highlights the 'SIP Session Timer' configuration area, which includes three input fields: 'SIP Session Timer T1 (0.5~10s)' with a value of 0.5, 'SIP Session Timer T2 (2~40s)' with a value of 4, and 'SIP Session Timer T4 (2.5~60s)' with a value of 5. Other settings visible include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'DTMF Type' (RFC2833), 'DTMF Info Type' (DTMF-Relay), 'DTMF Payload Type(96~127)' (101), 'Retransmission' (Disabled), 'Subscribe for MWI' (Disabled), 'MWI Subscription Period(Seconds)' (3600), 'Subscribe MWI To Voice Mail' (Disabled), and 'Voice Mail'.

5. Click **Confirm** to accept the change.

Call Hold

Call hold provides a service of placing an active call on hold. When a call is placed on hold, the IP phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. IP phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the

"c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0). Call hold tone allows IP phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

IP phones also support Music on Hold (MoH) feature. MoH is the business practice of playing recorded music to fill the silence that would be heard by the party who has been placed on hold. To use this feature, specify a SIP URI pointing to a MoH server account. When a call is placed on hold, the IP phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party.

Procedure

Call hold can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the call hold tone and call hold tone delay.</p> <p>Parameters:</p> <p>features.play_hold_tone.enable</p> <p>features.play_hold_tone.delay</p> <p>Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used.</p> <p>Parameters:</p> <p>sip.rfc2543_hold</p>
	<MAC>.cfg	<p>Configure MoH on a per-line basis.</p> <p>Parameter:</p> <p>account.X.music_server_uri</p>
Local	Web User Interface	<p>Configure the call hold tone and call hold tone delay.</p> <p>Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used.</p> <p>Navigate to:</p> <p><a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load</p> <p>Configure MoH on a per-line basis.</p> <p>Navigate to:</p> <p><a href="http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=">http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=</p>

		0
--	--	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.play_hold_tone.enable	0 or 1	1
Description: Enables or disables the IP phone to play a tone when there is a call on hold. 0 -Disabled 1 -Enabled Web User Interface: Features->General Information->Play Hold Tone Phone User Interface: None		
features.play_hold_tone.delay	Integer from 3 to 3600	30
Description: Configures the interval (in seconds) at which the IP phone plays a hold tone. If it is set to 30 (30s), the IP phone will play a hold tone every 30 seconds when you have held a call on the IP phone. Note: It works only if the parameter "features.play_hold_tone.enable" is set to 1 (Enabled). Web User Interface: Features->General Information->Play Hold Tone Delay Phone User Interface: None		
sip.rfc2543_hold	0 or 1	0
Description: Enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. 0 -Disabled 1 -Enabled If it is set to 0 (Disabled), SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. If it is set to 1 (Enabled), SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold. Web User Interface:		

Parameters	Permitted Values	Default
Features->General Information->RFC 2543 Hold		
Phone User Interface: None		
account.X.music_server_uri (X = 1)	SIP URI within 256 characters	Blank
Description: Configures the address of the Music On Hold server. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@sip.com, <sip:moh@sip.com>, <yealink.com> or yealink.com. Example: account.1.music_server_uri = <10.1.3.165> Note: The DNS query in this parameter only supports A query. Web User Interface: Account->Advanced->Music Server URI Phone User Interface: None		

To configure call hold method via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **RFC 2543 Hold**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' section is expanded. The 'RFC 2543 Hold' option is highlighted with a red box. The interface includes a sidebar with navigation links like 'Forward&DND', 'General Information', 'Audio', 'Intercom', 'Transfer', 'Call Pickup', 'Remote Control', 'Phone Lock', 'Action URL', and 'Power LED'. The main content area lists various settings with dropdown menus and checkboxes. A 'NOTE' box on the right provides additional information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

3. Click **Confirm** to accept the change.

To configure call hold tone and call hold tone delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Play Hold Tone**.
3. Enter the desired time in the **Play Hold Tone Delay** field.

The screenshot displays the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. In the 'General Information' section, the 'Play Hold Tone' dropdown menu is set to 'Enabled', and the 'Play Hold Tone Delay' text field contains the value '30'. These two fields are highlighted with a red rectangular box. Other visible fields include 'Call Waiting' (Enabled), 'Call Waiting On Code', 'Call Waiting Off Code', 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Auto-Answer Delay(1~4s)' (3), 'IP Direct Auto Answer' (Disabled), 'Call List Show Number' (Disabled), 'Voice Mail Tone' (Enable), and 'DHCP Hostname' (CP860). A sidebar on the left lists various configuration categories, and a 'NOTE' section on the right provides additional context for several features.

4. Click **Confirm** to accept the change.

To configure MoH via web user interface:

1. Click on **Account->Advanced**.

2. Enter the SIP URI (e.g., sip:moh@sip.com) in the **Music Server URI** field.

The screenshot shows the Yealink CP860 web interface with the 'Account' tab selected. The 'Advanced' section is expanded, showing various SIP settings. The 'Music Server URI' field is highlighted with a red box and contains the value 'sip:moh@sip.com'. Other visible settings include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1' (0.5), 'SIP Session Timer T2' (4), 'SIP Session Timer T4' (5), 'DTMF Type' (RFC2833), 'Conference URI' (empty), 'Early Media' (Disabled), 'SIP Server Type' (Default), 'Directed Call Pickup Code' (empty), 'Group Call Pickup Code' (empty), 'Distinctive Ring Tones' (Disabled), and 'Unregister When Reboot' (Disabled). A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.'

3. Click **Confirm** to accept the change.

Session Timer

Session timer allows a periodic refresh of SIP sessions through a re-INVITE request, to determine whether a SIP session is still active. Session timer is specified in RFC 4028. IP phones support two refresher modes: UAC and UAS. The UAC mode means refreshing the session from the client, while the UAS mode means refreshing the session from the server. The session expiration and session refresher are negotiated via the Session-Expires header in the INVITE message. The negotiated refresher will send a re-INVITE request at or before the negotiated session expiration.

Procedure

Session timer can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure session timer. Parameters: account.X.session_timer.enable account.X.session_timer.expires account.X.session_timer.refresher
Local	Web User Interface	Configure session timer. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc=

		0
--	--	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.session_timer.enable (X = 1)	0 or 1	0
Description: Enables or disables the session timer. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), IP phone will send periodic re-INVITE requests to refresh the session during a call. Web User Interface: Account->Advanced->Session Timer Phone User Interface: None		
account.X.session_timer.expires (X = 1)	Integer from 30 to 7200	1800
Description: Configures the IP phone to refresh the session during a call at regular intervals (in seconds). If it is set to 1800 (1800s), the IP phone will refresh the session during a call before 1800 seconds. Example: account.1.session_timer.expires = 1800 Web User Interface: Account->Advanced->Session Expires (30~7200s) Phone User Interface: None		
account.X.session_timer.refresher (X = 1)	0 or 1	0

Parameters	Permitted Values	Default
<p>Description:</p> <p>Configures the session timer refresher.</p> <p>0-UAC</p> <p>1-UAS</p> <p>If it is set to 0 (UAC), refreshing the session is performed by the IP phone.</p> <p>If it is set to 1 (UAS), refreshing the session is performed by a SIP server.</p> <p>Web User Interface:</p> <p>Account-> Advanced-> Session Refresher</p> <p>Phone User Interface:</p> <p>None</p>		

To configure session timer via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired value from the pull-down list of **Session Timer**.
3. Enter the desired time interval in the **Session Expires (30~7200s)** field.
4. Select the desired refresher from the pull-down list of **Session Refresher**.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Account' tab is selected, and the 'Advanced' sub-tab is active. On the left sidebar, 'Register', 'Basic', 'Codec', and 'Advanced' are listed. The main content area displays various configuration parameters. A red box highlights the following fields:

- Session Timer:** A dropdown menu currently set to 'Enabled'.
- Session Expires(30~7200s):** A text input field containing the value '1800'.
- Session Refresher:** A dropdown menu currently set to 'UAC'.

Other visible parameters include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (0.5), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'DTMF Type' (RFC2833), 'Music Server URI' (sip:moh@sp.com), 'Directed Call Pickup Code', 'Group Call Pickup Code', 'Distinctive Ring Tones' (Disabled), and 'Unregister When Reboot' (Disabled). A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.' At the bottom, there are 'Confirm' and 'Cancel' buttons.

5. Click **Confirm** to accept the change.

Call Forward

Call forward allows users to redirect an incoming call to a third party. IP phones redirect an incoming INVITE message by responding with a 302 Moved Temporarily message, which contains a Contact header with a new URI that should be tried. Three types of call forward:

- **Always Forward** -- Forward the incoming calls immediately.
- **Busy Forward** -- Forward the incoming call when the IP phone or the specified account is busy.
- **No Answer Forward** -- Forward the incoming call after a period of ring time.

The server-side call forward settings disable the local call forward settings. If the server-side call forward feature is enabled on any of the IP phone's registrations, the other registrations are not affected. DND activated on the IP phone disables the local no answer forward settings.

The call forward on code and call forward off code configured on IP phones are used to activate/deactivate the server-side call forward feature. They may vary on different servers.

IP phones support the redirected call information sent by the SIP server with Diversion header, per draft-levy-sip-diversion-08, or History-info header, per RFC 4244. The Diversion/History-info header is used to inform the IP phone of a call's history. For example, when a phone has been set to enable call forward, the Diversion/History-info header allows the receiving phone to indicate who the call was from, and from which phone number it was forwarded.

Forward International

Forward international allows users to forward an incoming call to an international telephone number. This feature is enabled by default.

Procedure

Call forward can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure call forward. Parameters: forward.always.enable forward.always.target forward.always.on_code forward.always.off_code forward.busy.enable forward.busy.target forward.busy.on_code
---------------------------	-------------------	--

		forward.busy.off_code forward.no_answer.enable forward.no_answer.target forward.no_answer.timeout forward.no_answer.on_code forward.no_answer.off_code features.fwd_diversion_enable Configure forward international. Parameter: forward.international.enable
Local	Web User Interface	Configure call forward. Navigate to: http://<phoneIPAddress>/servlet ?p=features-forward&q=load Configure forward international. Navigate to: http://<phoneIPAddress>/ servlet?p=features-general&q=load
	Phone User Interface	Configure call forward.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
forward.always.enable	0 or 1	0
Description: Enables or disables always forward feature. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), incoming calls are forwarded to the destination number immediately. Web User Interface: Features->Forward &DND->Always Forward->On/Off Phone User Interface: Menu->Features->Call Forward->Always Forward->Always Forward		
forward.always.target	String within 32 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the destination number the IP phone forwards all incoming calls to. Web User Interface: Features->Forward &DND->Always Forward->Target Phone User Interface: Menu->Features->Call Forward->Always Forward->Forward To		
forward.always.on_code	String within 32 characters	Blank
Description: Configures the always forward on code to activate the server-side always forward feature. The IP phone will send the always forward on code and the pre-configured destination number to the server when you activate always forward feature on the IP phone. Example: forward.always.on_code = *73 Web User Interface: Features->Forward &DND->Always Forward->On Code Phone User Interface: Menu->Features->Call Forward->Always Forward->On Code		
forward.always.off_code	String within 32 characters	Blank
Description: Configures the always forward off code to deactivate the server-side always forward feature. The IP phone will send the always forward off code to the server when you deactivate always forward feature on the IP phone. Example: forward.always.off_code = *74 Web User Interface: Features->Forward &DND->Always Forward->Off Code Phone User Interface: Menu->Features->Call Forward->Always Forward->Off Code		
forward.busy.enable	0 or 1	0
Description: Enables or disables busy forward feature.		

Parameters	Permitted Values	Default
0-Disabled 1-Enabled If it is set to 1 (Enabled), incoming calls are forwarded to the destination number when the callee is busy. Web User Interface: Features->Forward &DND->Busy Forward->On/Off Phone User Interface: Menu->Features->Call Forward->Busy Forward->Busy Forward		
forward.busy.target	String within 32 characters	Blank
Description: Configures the destination number the IP phone forwards incoming calls to when busy. Example: forward.busy.target = 3602 Web User Interface: Features->Forward &DND->Busy Forward->Target Phone User Interface: Menu->Features->Call Forward->Busy Forward->Forward To		
forward.busy.on_code	String within 32 characters	Blank
Description: Configures the busy forward on code to activate the server-side busy forward feature. The IP phone will send the busy forward on code and the pre-configured destination number to the server when you activate busy forward feature on the IP phone. Example: forward.busy.on_code = *75 Web User Interface: Features->Forward &DND->Busy Forward->On Code Phone User Interface: Menu->Features->Call Forward->Busy Forward->On Code		
forward.busy.off_code	String within 32 characters	Blank
Description:		

Parameters	Permitted Values	Default
<p>Configures the busy forward off code to deactivate the server-side busy forward feature. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature on the IP phone.</p> <p>Example:</p> <p>forward.busy.off_code = *76</p> <p>Web User Interface:</p> <p>Features->Forward &DND->Busy Forward->Off Code</p> <p>Phone User Interface:</p> <p>Menu->Features->Call Forward->Busy Forward->Off Code</p>		
forward.no_answer.enable	0 or 1	0
<p>Description:</p> <p>Enables or disables no answer forward feature.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>If it is set to 1 (Enabled), incoming calls are forwarded to the destination number after a period of ring time.</p> <p>Web User Interface:</p> <p>Features->Forward &DND->No Answer Forward->On/Off</p> <p>Phone User Interface:</p> <p>Menu->Features->Call Forward->No Answer Forward->No Answer Forward</p>		
forward.no_answer.target	String within 32 characters	Blank
<p>Description:</p> <p>Configures the destination number the IP phone forwards incoming calls to after a period of ring time.</p> <p>Example:</p> <p>forward.no_answer.target = 3603</p> <p>Web User Interface:</p> <p>Features->Forward &DND->No Answer Forward->Target</p> <p>Phone User Interface:</p> <p>Menu->Features->Call Forward->No Answer Forward->Forward To</p>		
forward.no_answer.timeout	Integer from 0 to 20	2

Parameters	Permitted Values	Default
Description: Configures ring times (N) to wait before forwarding incoming calls. Incoming calls will be forwarded when not answered after N*6 seconds. Web User Interface: Features->Forward &DND->No Answer Forward->After Ring Time (0~120s) Phone User Interface: Menu->Features->Call Forward->No Answer Forward->After Ring Time		
forward.no_answer.on_code	String within 32 characters	Blank
Description: Configures the no answer forward on code to activate the server-side no answer forward feature. The IP phone will send the no answer forward on code and the pre-configured destination number to the server when you activate no answer forward feature on the IP phone. Example: forward.no_answer.on_code = *77 Web User Interface: Features->Forward &DND->No Answer Forward->On Code Phone User Interface: Menu->Features->Call Forward->No Answer Forward->On Code		
forward.no_answer.off_code	String within 32 characters	Blank
Description: Configures the no answer forward off code to deactivate the server-side no answer forward feature. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the IP phone. Example: forward.no_answer.off_code = *78 Web User Interface: Features->Forward &DND->No Answer Forward->Off Code Phone User Interface: Menu->Features->Call Forward->No Answer Forward->Off Code		
features.fwd_diversion_enable	0 or 1	1

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to present the diversion information when an incoming call is forwarded to your IP phone. 0-Disabled 1-Enabled Web User Interface: Features->General Information->Diversion/History-Info Phone User Interface: None		
forward.international.enable	0 or 1	1
Description: Enables or disables the IP phone to forward incoming calls to international numbers (the prefix is 00). 0-Disabled 1-Enabled Web User Interface: Features->General Information->Fwd International Phone User Interface: Menu->Settings->Advanced Settings->FWD International->FWD International		

To configure call forward via web user interface:

1. Click on **Features->Forward & DND**.
2. In the **Forward** block, mark the desired radio box in the **Mode** field.
 - 1) Mark the desired radio box in the **Always Forward/Busy Forward/No Answer Forward** field.
 - 2) Enter the destination number you want to forward in the **Target** field.
 - 3) (Optional.) Enter the on code and off code in the **On Code** and **Off Code** fields.

- 4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time (0~120s)** (only for the no answer forward).

The screenshot shows the Yealink CP860 web interface. The 'Forward' tab is selected. The 'Forward' section is highlighted with a red box. It contains three sub-sections: 'Always Forward', 'Busy Forward', and 'No Answer Forward'. The 'No Answer Forward' section is currently selected, showing 'After Ring Time(0~120s)' set to 12. Below this, there are fields for 'Target', 'On Code', and 'Off Code'. The 'DND' section is also visible below the 'Forward' section, with 'DND Emergency' set to 'Disabled' and 'DND Status' set to 'Off'.

3. Click **Confirm** to accept the change.



To configure the forward international feature via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Fwd International**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. The 'Fwd International' option is highlighted with a red box, and it is currently set to 'Enabled'. Other settings visible include 'Call Waiting' (Enabled), 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'Reserve # in User Name' (Enabled), 'Send Pound Key' (Disabled), 'Diversion/History-Info' (Enabled), 'IP Direct Auto Answer' (Disabled), 'Call List Show Number' (Disabled), 'Voice Mail Tone' (Enable), and 'DHCP Hostname' (CP860). The 'Confirm' and 'Cancel' buttons are at the bottom.

3. Click **Confirm** to accept the change.

To enable call forward via phone user interface:

1. Press **Menu->Features->Call Forward**.
2. Press  or  to select the desired forwarding type, and then press the **Enter** soft key.
3. Depending on your selection:
 - a.) If you select **Always Forward**:
 - 1) Press the ◀ or ▶ soft key to select **Enable** from the **Always Forward** field.
 - 2) Enter the destination number you want to forward all incoming calls to in the **Forward to** field.
 - 3) (Optional.) Enter the always forward on code or off code respectively in the **On Code** or **Off Code** field.
 - b.) If you select **Busy Forward**:
 - 1) Press the ◀ or ▶ soft key to select **Enable** from the **Busy Forward** field.
 - 2) Enter the destination number you want to forward all incoming calls to when the phone is busy in the **Forward to** field.
 - 3) (Optional.) Enter the busy forward on code or off code respectively in the **On Code** or **Off Code** field.
 - c.) If you select **No Answer Forward**:
 - 1) Press the ◀ or ▶ soft key to select **Enable** from the **No Answer Forward** field.
 - 2) Enter the destination number you want to forward all unanswered incoming calls to in the **Forward to** field.
 - 3) Press the ◀ or ▶ soft key to select the ring time to wait before forwarding from the **After Ring Time** field.
The default ring time is 12 seconds.
 - 4) (Optional.) Enter the no answer forward on code or off code respectively in the **On Code** or **Off Code** field.
4. Press the **Save** soft key to accept the change.

Call Transfer

Call transfer enables IP phones to transfer an existing call to another party. IP phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

- **Blind Transfer** -- Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in the Refer-To header.
- **Semi-attended Transfer** -- Transfer a call after hearing the ringback tone.

Semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

- **Attended Transfer** -- Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Normally, call transfer is completed by pressing the transfer key. Blind transfer on hook and attended transfer on hook features allow the IP phone to complete the transfer through pressing the on-hook key.

When a user performs a semi-attended transfer, semi-attended transfer determines whether to display the prompt "1 New Missed Call(s)" ("n" indicates the number of the missed calls) on the destination party's LCD screen.

Procedure

Call transfer can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Specify whether to complete the transfer through pressing the on-hook key.</p> <p>Parameters:</p> <p>transfer.blind_tran_on_hook_enable</p> <p>transfer.on_hook_trans_enable</p> <p>Configure the semi-attended transfer feature.</p> <p>Parameter:</p> <p>transfer.semi_attend_tran_enable</p>
Local	Web User Interface	<p>Specify whether to complete the transfer through pressing the on-hook key.</p> <p>Configure the semi-attended transfer feature.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-transfer&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
transfer.blind_tran_on_hook_enable	0 or 1	1

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to complete the blind transfer through pressing the on-hook key instead of pressing the Tran soft key. 0 -Disabled 1 -Enabled Web User Interface: Features->Transfer->Blind Transfer On Hook Phone User Interface: None		
transfer.on_hook_trans_enable	0 or 1	1
Description: Enables or disables the IP phone to complete the semi-attended/attended transfer through pressing the on-hook key instead of pressing the Tran soft key. 0 -Disabled 1 -Enabled Web User Interface: Features->Transfer->Semi-Attend Transfer On Hook Phone User Interface: None		
transfer.semi_attend_tran_enable	0 or 1	1
Description: Enables or disables the transferee party's phone to prompt a missed call on the LCD screen before displaying the caller ID when performing a semi-attended transfer. 0 -Enabled 1 -Disabled Web User Interface: Features->Transfer->Semi-Attended Transfer Phone User Interface: None		

To configure call transfer via web user interface:

1. Click on **Features->Transfer**.

2. Select the desired values from the pull-down lists of **Semi-Attended Transfer**, **Blind Transfer On Hook** and **Semi-Attend Transfer On Hook**.

3. Click **Confirm** to accept the change.

Network Conference

Network conference, also known as centralized conference, provides users with flexibility of call with multiple participants (more than three). IP phones implement network conference using the REFER method specified in RFC 4579. This feature depends on support from a SIP server.

Procedure

Network conference can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure network conference. Parameters: account.X.conf_type account.X.conf_uri
Local	Web User Interface	Configure network conference. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc= 0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.conf_type (X = 1)	0 or 2	0

Parameters	Permitted Values	Default
Description: Configures the network conference type. 0 -Local Conference 2 -Network Conference If it is set to 0 (Local Conference), conferences are set up on the IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. Web User Interface: Account->Advanced->Conference Type Phone User Interface: None		
account.X.conf_uri (X = 1)	SIP URI within 511 characters	Blank
Description: Configures the network conference URI. Example: account.1.conf_uri = conference@example.com Note: It works only if the parameter "account.X.conf_type" is set to 2 (Network Conference). Web User Interface: Account->Advanced->Conference URI Phone User Interface: None		

To configure the network conference via web user interface:

1. Click on **Account->Advanced**.
2. Select **Network Conference** from the pull-down list of **Conference Type**.

3. Enter the conference URI in the **Conference URI** field.

4. Click **Confirm** to accept the change.

Transfer on Conference Hang Up

For local conference, all parties drop the call when the conference initiator drops the conference call. For local conference, transfer on conference hang up allows the other two parties to remain connected when the conference initiator drops the conference call.

Procedure

Transfer on conference hang up feature can be configured using the configuration files or locally.

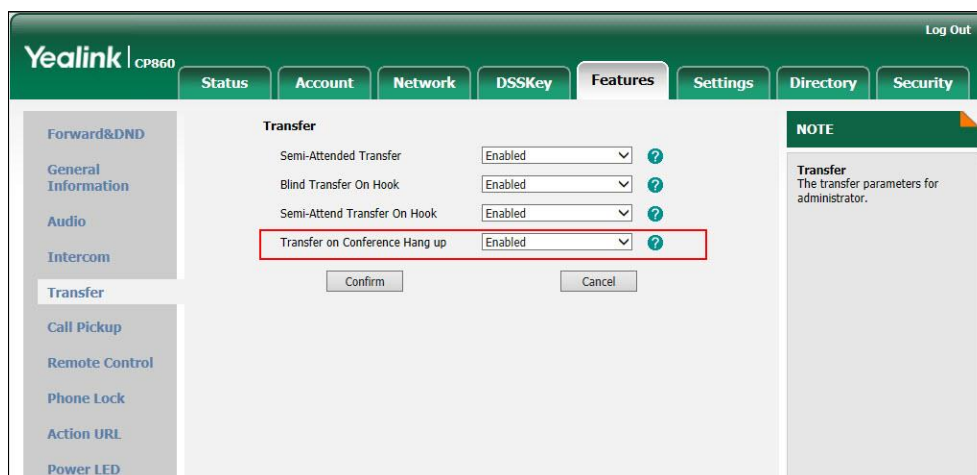
Configuration File	y000000000037.cfg	Configure transfer on conference hang up. Parameter: transfer.tran_others_after_conf_enable
Local	Web User Interface	Configure transfer on conference hang up. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-transfer&q=load">http://<phoneIPAddress>/servlet?p=features-transfer&q=load

Details of the Configuration Parameter:

Parameter & Description	Permitted Values	Default
transfer.tran_others_after_conf_enable	0 or 1	0
<p>Description:</p> <p>Enables or disables the IP phone to transfer the local conference call to the two parties after the conference initiator drops the local conference call.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>If it is set to 1 (Enabled), the other two parties remain connected when the conference initiator drops the conference call.</p> <p>Note: It is only applicable to the local conference.</p> <p>Web User Interface:</p> <p>Features->Transfer->Transfer on Conference Hang up</p> <p>Phone User Interface:</p> <p>None</p>		

To configure Transfer on Conference Hang up via web user interface:

1. Click on **Features->Transfer**.
2. Select the desired value from the pull-down list of **Transfer on Conference Hang up**.



3. Click **Confirm** to accept the change.

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. A user can pick up the incoming call by pressing the DPickup soft key. This feature

depends on support from a SIP server. For many SIP servers, directed call pickup requires a directed pickup code, which can be configured on a phone or per-line basis.

Procedure

Directed call pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the directed call pickup code on a per-line basis. Parameter: account.X.direct_pickup_code
	y000000000037.cfg	Configure directed call pickup features on a phone basis. Parameters: features.pickup.direct_pickup_enable features.pickup.direct_pickup_code
Local	Web User Interface	Configure the directed call pickup feature on a phone. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-callpickup&q=load">http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the directed call pickup code on a phone basis. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-callpickup&q=load">http://<phoneIPAddress>/servlet?p=features-callpickup&q=load Configure the directed call pickup code on a per-line basis. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.direct_pickup_enable	0 or 1	0
Description: Enables or disables the IP phone to display the DPickup soft key when the IP phone is in the pre-dialing screen. 0-Disabled 1-Enabled Web User Interface: Features->Call Pickup->Directed Call Pickup Phone User Interface: None		
features.pickup.direct_pickup_code	String within 32 characters	Blank
Description: Configures the directed call pickup code on a phone basis. Example: features.pickup.direct_pickup_code = *97 Note: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. Web User Interface: Features->Call Pickup->Directed Call Pickup Code Phone User Interface: None		
account.X.direct_pickup_code (X = 1)	String within 32 characters	Blank
Description : Configures the directed call pickup code on a per-line basis. Example: account.1.direct_pickup_code = *68 Note: The directed call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. Web User Interface:		

Parameters	Permitted Values	Default
Account->Advanced->Directed Call Pickup Code		
Phone User Interface:		
None		

To configure the directed call pickup feature on a phone basis via web user interface:

1. Click on **Features->Call Pickup**.
2. Select the desired value from the pull-down list of **Directed Call Pickup**.
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Features' tab is selected. On the left sidebar, 'Call Pickup' is highlighted under the 'Forward&DND' section. The main content area is titled 'Call Pickup' and contains the following fields:

- Directed Call Pickup:** A dropdown menu set to 'Enabled'.
- Directed Call Pickup Code:** A text input field containing '*97'.
- Group Call Pickup:** A dropdown menu set to 'Disabled'.
- Group Call Pickup Code:** An empty text input field.

At the bottom of the form are 'Confirm' and 'Cancel' buttons. A red box highlights the 'Directed Call Pickup' dropdown and the 'Directed Call Pickup Code' field. On the right side, there is a 'NOTE' section with the text: 'Call Pickup: The call pickup parameters for administrator.'

4. Click **Confirm** to accept the change.

To configure the directed call pickup code on a per-line basis via web user interface:

1. Click on **Account->Advanced**.

- Enter the directed call pickup code in the **Directed Call Pickup Code** field.

- Click **Confirm** to accept the change.

Group Call Pickup

Group call pickup is used for picking up incoming calls within a pre-defined group. If the group receives many incoming calls at once, the user will pick up the first incoming call by pressing the GPickup soft key. This feature depends on support from a SIP server. For many SIP servers, group call pickup requires a group pickup code, which can be configured on a phone or per-line basis.

Procedure

Group call pickup can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configures the group call pickup code on a per-line basis. Parameter: account.X.group_pickup_code
	y000000000037.cfg	Configures the group call pickup features on a phone basis. Parameters: features.pickup.group_pickup_enable features.pickup.group_pickup_

		code
Local	Web User Interface	<p>Configure the group call pickup feature on a phone basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-callpickup&q=load</p> <p>Configure the group call pickup code on a phone basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=features-callpickup&q=load</p> <p>Configure the group call pickup code on a per-line basis.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.group_pickup_enable	0 or 1	0
<p>Description:</p> <p>Enables or disables the IP phone to display the GPickup soft key when the IP phone is in the pre-dialing screen.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>Web User Interface:</p> <p>Features->Call Pickup->Group Call Pickup</p> <p>Phone User Interface:</p> <p>None</p>		
features.pickup.group_pickup_code	String within 32 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the group call pickup code on a phone basis. Example: features.pickup.group_pickup_code = *98 Note: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. Web User Interface: Features->Call Pickup->Group Call Pickup Code Phone User Interface: None		
account.X.group_pickup_code (X = 1)	String within 32 characters	Blank
Description: Configures the group pickup code on a per-line basis. Example: account.1.group_pickup_code = *69 Note: The group call pickup code configured on a per-line basis takes precedence over that configured on a phone basis. Web User Interface: Account->Advanced->Group Call Pickup Code Phone User Interface: None		

To configure the group call pickup feature on a phone basis via web user interface:

1. Click on **Features->Call Pickup**.
2. Select the desired value from the pull-down list of **Group Call Pickup**.

- Enter the group call pickup code in the **Group Call Pickup Code** field.

- Click **Confirm** to accept the change.

To configure the group call pickup code on a per-line basis via web user interface:

- Click on **Account->Advanced**.
- Enter the group call pickup code in the **Group Call Pickup Code** field.

- Click **Confirm** to accept the change.

Call Return

Call return, also known as last call return, allows users to place a call back to the last caller. Call return is implemented on IP phones using a call return key.

Procedure

Call return key can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Assign a call return key. Parameter: programablekey.X.type
Local	Web User Interface	Assign a call return key. Navigate to: http://<phoneIPAddress>/servlet ?p=dsskey&model=2&q=load

Details of Configuration Parameters:

Parameter	Permitted Values	Default
programablekey.X.type (X=1-6, 9, 13)	7	0
<p>Description: Configures a programable key as a call return key on the IP phone. The digit 7 stands for the key type Call Return. For more information on how to configure the programable key, refer to Appendix C: Configuring Programmable Key on page 353.</p> <p>Example: programablekey.2.type = 7</p> <p>Web User Interface: DSSKey->Programable Key->Type</p> <p>Phone User Interface: None</p>		

To configure a call return key via web user interface:

1. Click on **DSSKey->Programmable Key**.

- In the desired programmable key field, select **Call Return** from the pull-down list of **Type**.

The screenshot shows the Yealink CP860 web interface. The 'DSSKey' tab is selected. The 'Programable Key' sidebar on the left lists keys 1 through 4, Up, Down, OK, and MUTE. The 'MUTE' key is highlighted with a red box. In the 'MUTE' row, the 'Type' dropdown is set to 'Call Return'. The 'Line' dropdown is set to 'N/A'. The 'Value' field is empty. The 'Label' field is empty. The 'Extension' field is empty. The 'NOTE' section on the right contains information about Key Type, Key Event, and Intercom.

- Click **Confirm** to accept the change.

Calling Line Identification Presentation

Calling line identification presentation (CLIP) allows IP phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. IP phones support deriving caller identity from three types of SIP header: From, P-Asserted-Identity and Remote-Party-ID. Identity presentation is based on the identity in the relevant SIP header.

If the caller has existed in the local directory, the local name assigned to the caller should be preferentially displayed and stored in the call log.

For more information on calling line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

CLIP can be configured using the configuration files or locally.

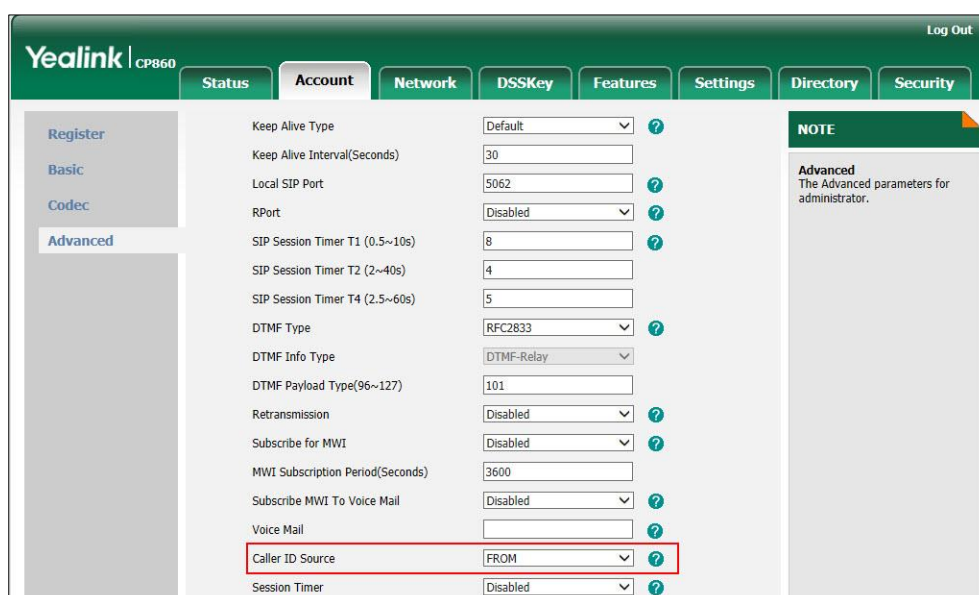
Configuration File	<MAC>.cfg	Configure the presentation of the caller identity. Parameter: account.X.cid_source
Local	Web User Interface	Configure the presentation of the caller identity. Navigate to: <code>http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</code>

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cid_source (X = 1)	0, 1, 2, 3, 4 or 5	0
<p>Description:</p> <p>Configures the presentation of the caller identity when receiving an incoming call.</p> <p>0-FROM (Derives the name and number of the caller from the "From" header).</p> <p>1-PAI (Derives the name and number of the caller from the "PAI" header. If the server does not send the "PAI" header, displays "anonymity" on the callee's phone).</p> <p>2-PAI-FROM (Derives the name and number of the caller from the "PAI" header preferentially. If the server does not send the "PAI" header, derives from the "From" header).</p> <p>3-RPID-PAI-FROM</p> <p>4-PAI-RPID-FROM</p> <p>5-RPID-FROM</p> <p>Web User Interface:</p> <p>Account->Advanced->Caller ID Source</p> <p>Phone User Interface:</p> <p>None</p>		

To configure the presentation of the caller identity via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired value from the pull-down list of the **Caller ID Source**.



- Click **Confirm** to accept the change.

Connected Line Identification Presentation

Connected line identification presentation (COLP) allows IP phones to display the identity of the connected party specified for outgoing calls. IP phones can display the Dialed Digits, or the identity in a SIP header (Remote-Party-ID or P-Asserted-Identity) received, or the identity in the From header carried in the UPDATE message sent by the callee as described in RFC 4916. Connected line identification presentation is also known as Called line identification presentation. In some cases, the remote party will be different from the called line identification presentation due to call diversion.

If the callee has existed in the local directory, the local contact name assigned to the callee should be preferentially displayed.

For more information on connected line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

COLP can be configured only using the configuration files.

Configuration File	<MAC>.cfg	Configure the presentation of the callee identity. Parameter: account.X.cp_source
---------------------------	-----------	--

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.cp_source (X = 1)	0, 1 or 2	0
Description: Configures the presentation of the callee's identity. 0 -PAI-RPID (Derives the name and number of the callee from the "PAI" header preferentially. If the server does not send the "PAI" header, derives from the "RPID" header). 1 -Dialed Digits (Preferentially displays the dialed digits on the caller's phone). 2 -RFC 4916 (Derives the name and number of the callee from "From" header in the Update message). When the RFC 4916 is enabled on the IP phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the callee, and displays the identity in the		

Parameter	Permitted Values	Default
From header.		
Web User Interface:		
None		
Phone User Interface:		
None		

DTMF

DTMF (Dual Tone Multi-frequency), better known as touch-tone, is used for telecommunication signaling over analog telephone lines in the voice-frequency band. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's keypad during a call. Each key pressed on the IP phone generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

The DTMF keypad is laid out in a 4×4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a sinusoidal tone for each of two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1447 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** --DTMF digits are transmitted by RTP Events compliant to RFC 2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by the SIP INFO messages.

The method of transmitting DTMF digits is configurable on a per-line basis.

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening to. The payload type for the RTP Event packets is

configurable. IP phones default to 101 for the payload type, which use the definition to negotiate with the other end during call establishment.

The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.

INBAND

DTMF digits are transmitted within the audio of the IP phone conversation. It uses the same codec as your voice and is audible to the conversation partners.

SIP INFO

DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message is sent along the signaling path of the call. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the method of transmitting DTMF digit and the payload type. Parameters: account.X.dtmf.type account.X.dtmf.dtmf_payload account.X.dtmf.info_type
	y00000000037.cfg	Configure the number of times for the IP phone to send the end RTP Event packet. Parameter: features.dtmf.repetition
Local	Web User Interface	Configure the method of transmitting DTMF digits and the payload type. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0 Configure the number of times for the IP phone to send the end

		RTP Event packet. Navigate to: <a href="http://<phoneIPAddress>/servlet?<p=features-general&q=load>">http://<phoneIPAddress>/servlet?<p=features-general&q=load>
--	--	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.dtmf.type (X = 1)	0, 1, 2 or 3	1
Description: Configures the DTMF type. 0-INBAND 1-RFC 2833 2-SIP INFO 3-AUTO or SIP INFO If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band. If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If it is set to 3 (AUTO or SIP INFO), the IP phone negotiates with the other end to use INBAND or RFC 2833, if there is no negotiation, using SIP INFO by default. Web User Interface: Account-> Advanced->DTMF Type Phone User Interface: None		
account.X.dtmf.dtmf_payload (X = 1)	Integer from 96 to 127	101
Description: Configures the RFC 2833 payload type. Web User Interface: Account-> Advanced->DTMF Payload Type (96~127) Phone User Interface: None		
account.X.dtmf.info_type	1, 2 or 3	0

Parameters	Permitted Values	Default
(X = 1)		
<p>Description: Configures the DTMF info type when the DTMF type is configured as "SIP INFO", "AUTO or SIP INFO".</p> <p>0-Disabled 1-DTMF-Relay 2-DTMF 3-Telephone-Event</p> <p>Web User Interface: Account->Advanced->DTMF Info Type</p> <p>Phone User Interface: None</p>		
features.dtmf.repetition	1, 2 or 3	3
<p>Description: Configures the repetition times for the IP phone to send the end RTP EVENT packet during an active call.</p> <p>Web User Interface: Features->General Information->DTMF Repetition</p> <p>Phone User Interface: None</p>		

To configure the method of transmitting DTMF digits via web user interface:

1. Click on **Account-> Advanced**.
2. Select the desired value from the pull-down list of **DTMF Type**.
If **SIP INFO** or **AUTO or SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

- Enter the desired value in the **DTMF Payload Type (96~127)** field.

The screenshot shows the Yealink CP860 web interface. The 'Account' tab is active, and the 'Advanced' sub-tab is selected. The 'DTMF Type' dropdown is set to 'RFC2833'. The 'DTMF Payload Type(96~127)' field is highlighted with a red box and contains the value '101'. Other fields include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1 (0.5~10s)' (8), 'SIP Session Timer T2 (2~40s)' (4), 'SIP Session Timer T4 (2.5~60s)' (5), 'Retransmission' (Disabled), 'Subscribe for MWI' (Disabled), and 'MWI Subscription Period(Seconds)' (3600). A 'NOTE' section on the right states: 'Advanced: The Advanced parameters for administrator.'

- Click **Confirm** to accept the change.

To configure the number of times to send the end RTP Event packet via web user interface:

- Click on **Features->General Information**.
- Select the desired value (1-3) from the pull-down list of **DTMF Repetition**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is active, and the 'General Information' sub-tab is selected. The 'DTMF Repetition' dropdown is highlighted with a red box and contains the value '3'. Other fields include 'Call Waiting' (Enabled), 'Call Waiting On Code' (empty), 'Call Waiting Off Code' (empty), 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (set to '#'), 'Reserve # in User Name' (Enabled), 'Play Local DTMF Tone' (Enabled), 'Multicast Codec' (G722), 'Play Hold Tone' (Enabled), 'Call List Show Number' (Disabled), 'Voice Mail Tone' (Enable), and 'DHCP Hostname' (CP860). A 'NOTE' section on the right contains information about 'Call Waiting', 'Key As Send', and 'Hotline Number'. At the bottom, there are 'Confirm' and 'Cancel' buttons.

- Click **Confirm** to accept the change.

Suppress DTMF Display

Suppress DTMF display allows IP phones to suppress the display of DTMF digits. The digits are displayed as “*” on the LCD screen. Suppress DTMF display delay defines

whether to display the DTMF digits for a short period of time before displaying as "***".

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure suppress DTMF display and suppress DTMF display delay. Parameters: features.dtmf.hide features.dtmf.hide_delay
Local	Web User Interface	Configure suppress DTMF display and suppress DTMF display delay. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-general&q=load">http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.hide	0 or 1	0
Description: Enables or disables the IP phone to suppress the display of DTMF digits during an active call. 0-Disabled 1-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks. Web User Interface: Features->General Information->Suppress DTMF Display Phone User Interface: None		
features.dtmf.hide_delay	0 or 1	0

Parameters	Permitted Values	Default
<p>Description:</p> <p>Enables or disables the IP phone to display the DTMF digits for a short period before displaying asterisks during an active call.</p> <p>0-Disabled 1-Enabled</p> <p>Note: It works only if the parameter “features.dtmf.hide” is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>Features->General Information->Suppress DTMF Display Delay</p> <p>Phone User Interface:</p> <p>None</p>		

To configure suppress DTMF display and suppress DTMF display delay via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **Suppress DTMF Display**.
3. Select the desired value from the pull-down list of **Suppress DTMF Display Delay**.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' section is active. A list of settings is displayed, including 'Call Waiting', 'Auto Redial', 'Auto Redial Interval', 'Auto Redial Times', 'Key As Send', 'Reserve # in User Name', 'Time-Out for Dial-Now Rule', 'RFC 2543 Hold', 'Use Outbound Proxy In Dialog', '180 Ring Workaround', 'PswPrefix', 'PswLength', 'PswDial', 'Save Call Log', 'Suppress DTMF Display', 'Suppress DTMF Display Delay', and 'Play Local DTMF Tone'. The 'Suppress DTMF Display' and 'Suppress DTMF Display Delay' settings are highlighted with a red box, both set to 'Enabled'. A 'NOTE' section on the right provides additional information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

4. Click **Confirm** to accept the change.

Transfer via DTMF

Call transfer is implemented via DTMF on some traditional servers. The IP phone sends specified DTMF digits to the server for transferring calls to third parties.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure transfer via DTMF. Parameters: features.dtmf.replace_tran features.dtmf.transfer
Local	Web User Interface	Configure transfer via DTMF. Navigate to: http://<phoneIPAddress>/servl et?p=features-general&q=loa d

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.replace_tran	0 or 1	0
Description: Enables or disables the IP phone to send DTMF sequences for transfer function when pressing the transfer soft key or the TRAN key. 0-Disabled 1-Enabled If it is set to 0 (Disabled), the IP phone will perform the transfer as normal when pressing the transfer key during a call. If it is set to 1 (Enabled), the IP phone will transmit the designated DTMF digits to the server for completing call transfer when pressing the transfer key during a call. Web User Interface: Features->General Information->DTMF Replace Tran Phone User Interface: None		
features.dtmf.transfer	String within 32 characters	Blank

Parameters	Permitted Values	Default
<p>Description:</p> <p>Configures the DTMF digits to be transmitted to perform call transfer. Valid values are: 0-9, *, # and A-D.</p> <p>Example:</p> <p>features.dtmf.transfer = 123</p> <p>Note: It works only if the parameter “features.dtmf.replace_tran” is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>Features->General Information->Tran Send DTMF</p> <p>Phone User Interface:</p> <p>None</p>		

To configure transfer via DTMF feature via web user interface:

1. Click on **Features->General Information**.
2. Select the desired value from the pull-down list of **DTMF Replace Tran**.
3. Enter the specified DTMF digits in the **Tran Send DTMF** field.

The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'General Information' sub-tab is active. In the 'General Information' section, the 'DTMF Replace Tran' dropdown menu is set to 'Enabled', and the 'Tran Send DTMF' text input field contains the value '123'. These two fields are highlighted with a red rectangular box. Below these fields are other configuration options like 'Play Local DTMF Tone', 'Call List Show Number', 'Voice Mail Tone', and 'DHCP Hostname'. The interface also includes a sidebar on the left with various navigation links and a 'NOTE' section on the right with additional information.

4. Click **Confirm** to accept the change.

Intercom

Intercom allows establishing an audio conversation directly. The IP phone can answer intercom calls automatically. This feature depends on support from a SIP server.

Outgoing Intercom Calls

Intercom is a useful feature in office environments to quickly connect with an operator or secretary. Users can press an intercom key to automatically initiate an outgoing intercom call with a remote extension.

Procedure

Intercom key can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Assign an intercom key. Parameters: programablekey.X.type programablekey.X.value
Local	Web User Interface	Assign an intercom key. Navigate to: http://<phoneIPAddress>/servlet ?p=dsskey&model=2&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
programablekey.X.type (X=1-6, 9, 13)	14	0
Description: Configures a programmable key to be an intercom key. The digit 14 stands for the key type Intercom . For more information on how to configure the programmable key, refer to Appendix C: Configuring Programmable Key on page 353. Example: programablekey.2.type = 14 Web User Interface: DSSKey->Programmable Key->Type Phone User Interface: None		

Parameters	Permitted Values	Default
programmablekey.X.value (X=1-6, 9, 13)	String within 99 characters	blank
Description: Configures the intercom number.		
Example: programmablekey.2.value = 1008		
Web User Interface: DSSKey->Programmable Key->Value		
Phone User Interface: None		

To configure an intercom key via web user interface:

1. Click on **DSSKey->Programmable Key**.
2. In the desired programmable key field, select **Intercom** from the pull-down list of **Type**.
3. Enter the remote extension number in the **Value** field.

The screenshot shows the Yealink CP860 web interface. The 'DSSKey' tab is selected. Under 'Programmable Key', there is a table with columns: Key, Type, Line, Value, Label, and Extension. The 'MUTE' key is highlighted with a red box. Its configuration is: Type: Intercom, Line: Line 1, Value: 6008. Below the table are buttons for 'Confirm', 'Cancel', and 'Reset to default'. On the right, there is a 'NOTE' section with information about Key Type, Key Event, and Intercom.

4. Click **Confirm** to accept the change.

Incoming Intercom Calls

The IP phone can process incoming calls differently depending on settings. Four options are configurable for incoming intercom calls.

Accept Intercom

Accept Intercom allows the IP phone to automatically answer an incoming intercom call.

Intercom Mute

Intercom Mute allows the IP phone to mute the microphone for incoming intercom calls.

Intercom Tone

Intercom Tone allows the IP phone to play a warning tone before answering an intercom call.

Intercom Barge

Intercom Barge allows the IP phone to automatically answer an incoming intercom call while an active call is in progress. The active call will be placed on hold.

Procedure

Incoming intercom calls can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the incoming intercom call feature. Parameters: features.intercom.allow features.intercom.mute features.intercom.tone features.intercom.barge
Local	Web User Interface	Configure the incoming intercom call feature. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-intercom&q=load">http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure the incoming intercom call feature.

Details of Configuration Parameters:

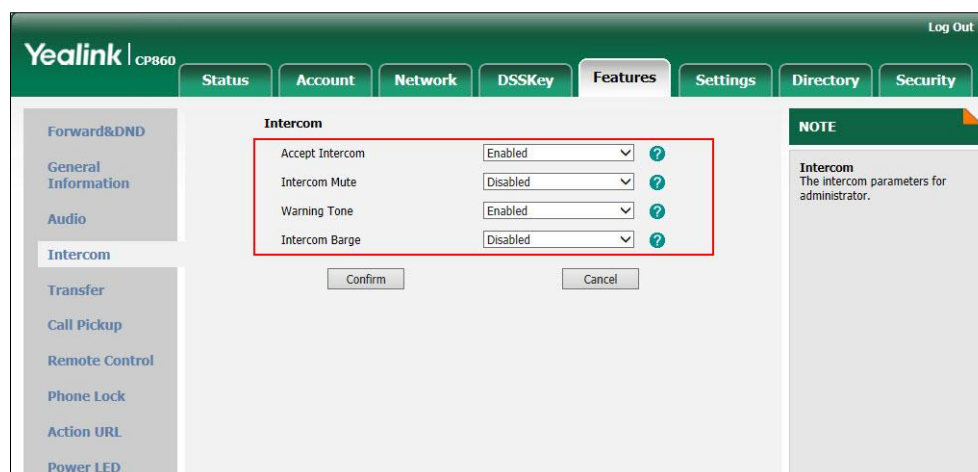
Parameters	Permitted Values	Default
features.intercom.allow	0 or 1	1
Description: Enables or disables the IP phone to automatically answer an incoming intercom call. 0-Disabled 1-Enabled If it is set to 0 (Disabled), the IP phone will reject incoming intercom calls and sends a busy signal to the caller. If it is set to 1 (Enabled), the IP phone will automatically answer an incoming intercom call.		

Parameters	Permitted Values	Default
Web User Interface: Features->Intercom->Accept Intercom Phone User Interface: Menu->Features->Intercom->Accept Intercom		
features.intercom.mute	0 or 1	0
Description: Enables or disables the IP phone to mute the microphone when answering an intercom call. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the microphone is muted for intercom calls, and then the other party cannot hear you. Note: It works only if the parameter "features.intercom.allow" is set to 1 (Enabled). Web User Interface: Features->Intercom ->Intercom Mute Phone User Interface: Menu->Features->Intercom->Intercom Mute		
features.intercom.tone	0 or 1	1
Description: Enables or disables the IP phone to play a warning tone when receiving an intercom call. 0 -Disabled 1 -Enabled Note: It works only if the parameter "features.intercom.allow" is set to 1 (Enabled). Web User Interface: Features->Intercom->Warning Tone Phone User Interface: Menu->Features->Intercom->Warning Tone		
features.intercom.barge	0 or 1	0

Parameters	Permitted Values	Default
<p>Description:</p> <p>Enables or disables the IP phone to automatically answer an incoming intercom call while there is already an active call on the IP phone.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 0 (Disabled), the IP phone will handle an incoming intercom call like a waiting call while there is already an active call on the IP phone.</p> <p>If it is set to 1 (Enabled), the IP phone will automatically answer the intercom call while there is already an active call on the IP phone and place the active call on hold.</p> <p>Note: It works only if the parameter "features.intercom.allow" is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>Features->Intercom->Intercom Barge</p> <p>Phone User Interface:</p> <p>Menu->Features->Intercom->Intercom Barge</p>		

To configure intercom via web user interface:

1. Click on **Features->Intercom**.
2. Select the desired values from the pull-down lists of **Accept Intercom**, **Intercom Mute**, **Warning Tone** and **Intercom Barge**.



3. Click **Confirm** to accept the change.

Configuring Advanced Features

This chapter provides information for making configuration changes for the following advanced features:

- [Distinctive Ring Tones](#)
- [Tones](#)
- [Remote Phone Book](#)
- [LDAP](#)
- [Message Waiting Indicator](#)
- [Multicast Paging](#)
- [Action URL](#)
- [Action URI](#)
- [Server Redundancy](#)
- [Static DNS Cache](#)
- [LLDP](#)
- [VLAN](#)
- [VPN](#)
- [Quality of Service](#)
- [Network Address Translation](#)
- [SNMP](#)
- [802.1X Authentication](#)
- [TR-069 Device Management](#)
- [IPv6 Support](#)

Distinctive Ring Tones

Distinctive ring tones allows certain incoming calls to trigger IP phones to play distinctive ring tones. The IP phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the IP phone strips out the URL or keyword parameter and maps it to the appropriate ring tone.

Note

If the caller already exists in the local directory, the ring tone assigned to the caller should be preferentially played.

Alert-Info headers in the following four formats:

Alert-Info: 127.0.0.1/Bellcore-drN (or Alert-Info: Bellcore-drN)

Alert-Info: ringtone-N (or Alert-Info: MyMelodyN)

Alert-Info: <URL>

Alert-Info: info=info text;x-line-id=0

- When the Alert-Info header contains the keyword "Bellcore-drN", the IP phone will play the Bellcore-drN (N=1, 2, 3, 4 or 5) ring tone if the parameter "features.alert_info_tone" is set to 1, or play the corresponding local ring tone (RingN.wav) in about ten seconds if the parameter "features.alert_info_tone" is set to 0.

Example:

Alert-Info: http://127.0.0.1/Bellcore-dr1

The following table identifies the different Bellcore ring tone patterns and cadences (These ring tones are designed for the BroadWorks server).

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	Nominal Duration (ms)	Maximum Duration (ms)
Bellcore-dr1 (standard)	1	Ringing	2s On	1800	2000	2200
		Silent	4s Off	3600	4000	4400
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Silent		315	400	525
		Ringing	Long	630	800	1025
		Silent		3475	4000	4400
Bellcore-dr3	3	Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Short	315	400	525

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	Nominal Duration (ms)	Maximum Duration (ms)
		Silent		145	200	525
		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

Note

"Bellcore-dr5" is a ring splash tone that reminds the user that the DND or Always Call Forward feature is enabled on the server side.

- When the Alert-Info header contains the keyword "ringtone-N" or "MyMelodyN", the IP phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) in about ten seconds if "N" is greater than 5 or less than 1.

Example:

Alert-Info: ringtone-2

Alert-Info: MyMelody2

The following table identifies the corresponding local ring tone:

Value	Ring Tone
1	Ring1.wav
2	Ring2.wav
3	Ring3.wav
4	Ring4.wav
5	Ring5.wav
N<1 or N>5	Ring1.wav

- When the Alert-Info header contains a remote URL, the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone if the parameter "account.X.alert_info_url_enable" is set to 1 (or the item called

"Distinctive Ring Tones" on the web user interface is Enabled), or play the preconfigured local ring tone in about ten seconds if the parameter "account.X.alert_info_url_enable" is set to 0 or if the IP phone fails to download the remote ring tone.

Example:

Alert-Info: http://192.168.0.12:8080/Custom.wav

- When the Alert-Info header contains an info text, the IP phone will map the text with the internal ringer text preconfigured on the IP phone, and then play the ring tone associated with the internal ringer text. If no internal ringer text maps, the IP phone will play the preconfigured local ring tone in about ten seconds.

Example:

Alert-Info: info=family;x-line-id=0

Auto Answer

If the Alert-Info header contains the following type of strings, the IP phone will answer incoming calls automatically without playing the ring tone:

- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)

Note

If the Alert-Info header contains multiple types of keywords, the IP phone will process the keywords in the following order:
AutoAnswer>URL>"Bellcore-drN/ringtone-N/MyMelodyN">info text.

Procedure

Distinctive ring tones can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure distinctive ring tones feature. Parameter: account.X.alert_info_url_enable
	y000000000037.cfg	Configure the internal ringer text and internal ringer file. Parameters: features.alert_info_tone distinctive_ring_tones.alert_info.X.text distinctive_ring_tones.alert_info.X.ringer
Local	Web User Interface	Configure distinctive ring tones feature. Navigate to:

		<p>http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</p> <p>Configure the internal ringer text and internal ringer file.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=setting-s-ring&q=load</p>
--	--	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.alert_info_url_enable (X = 1)	0 or 1	1
<p>Description:</p> <p>Enables or disables the IP phone to download the ring tone from the URL contained in the Alert-Info header.</p> <p>0-Disabled 1-Enabled</p> <p>Web User Interface:</p> <p>Account->Advanced->Distinctive Ring Tones</p> <p>Phone User Interface:</p> <p>None</p>		
features.alert_info_tone	0 or 1	0
<p>Description:</p> <p>Enables or disables the IP phone to map the keywords in the Alert-info header to the specified Bellcore ring tones.</p> <p>0-Disabled 1-Enabled</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
distinctive_ring_tones.alert_info.X.text (X ranges from 1 to 10)	String within 32 characters	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the internal ringer text to map the keywords contained in the Alert-Info header.</p> <p>Example: distinctive_ring_tones.alert_info.1.text = family</p> <p>Web User Interface: Settings->Ring->Internal Ringer Text</p> <p>Phone User Interface: None</p>		
distinctive_ring_tones.alert_info.X.ringer (X ranges from 1 to 10)	String within 32 characters	1
<p>Description: Configures the desired ring tones for each text. The value ranges from 1 to 5, the digit stands for the appropriate ring tone.</p> <p>1-Ring1.wav 2-Ring2.wav 3-Ring3.wav 4-Ring4.wav 5-Ring5.wav</p> <p>Web User Interface: Settings->Ring->Internal Ringer Text</p> <p>Phone User Interface: None</p>		

To configure distinctive ring tones via web user interface:

1. Click on **Account-> Advanced**.

2. Select the desired value from the pull-down list of **Distinctive Ring Tones**.

The screenshot shows the Yealink CP860 web interface with the 'Advanced' settings tab selected. The left sidebar contains links for Register, Basic, Codec, and Advanced. The main content area displays various configuration options with their current values and help icons. The 'Distinctive Ring Tones' option is highlighted with a red rectangular box. Below the settings are 'Confirm' and 'Cancel' buttons. A 'NOTE' section on the right states: 'Advanced: The Advanced parameters for administrator.'

Setting	Value
Keep Alive Type	Default
Keep Alive Interval(Seconds)	30
Local SIP Port	5062
RPort	Disabled
SIP Session Timer T1 (0.5~10s)	0.5
SIP Session Timer T2 (2~40s)	4
SIP Session Timer T4 (2.5~60s)	5
DTMF Type	RFC2833
Conference URI	
Early Media	Disabled
SIP Server Type	Default
Music Server URI	sip:moh@sp.com
Directed Call Pickup Code	
Group Call Pickup Code	
Distinctive Ring Tones	Enabled
Unregister When Reboot	Disabled

3. Click **Confirm** to accept the change.

To configure the internal ringer text and internal ringer file via web user interface:

1. Click on **Settings->Ring**.
2. Enter the keywords in the **Internal Ringer Text** fields.

3. Select the desired ring tones for each text from the pull-down lists of **Internal Ringer File**.

4. Click **Confirm** to accept the change.

Tones

When receiving a message, the IP phone will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the IP phone. The default tones used on IP phones are the US tone sets. Available tone sets for IP phones:

- Australia
- Austria
- Brazil
- Belgium
- China
- Czech
- Denmark
- Finland
- France
- Germany

- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States
- Chile
- Czech ETSI

Configured tones can be heard on the IP phone for the following conditions:

Condition	Description
Dial	When in the pre-dialing interface
Ring Back	Ring-back tone
Busy	When the callee is busy
Congestion	When the network is congested
Call Waiting	Call waiting tone
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail
Auto Answer	When automatically answering a call

Procedure

Tones can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the tones for the IP phone.</p> <p>Parameters:</p> <p>voice.tone.country</p> <p>voice.tone.dial</p> <p>voice.tone.ring</p> <p>voice.tone.busy</p> <p>voice.tone.congestion</p> <p>voice.tone.callwaiting</p> <p>voice.tone.dialrecall</p> <p>voice.tone.info</p> <p>voice.tone.stutter</p> <p>voice.tone.autoanswer</p>
Local	Web User Interface	<p>Configure the tones for the IP phone.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-tones&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.tone.country	Refer to the following content	Custom
<p>Description:</p> <p>Configures the country tone for the IP phone.</p> <p>Example:</p> <p>voice.tone.country = Custom</p> <p>Permitted Values:</p> <p>Custom, Australia, Austria, Brazil, Belgium, China, Czech, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States, Chile, Czech ETSI</p> <p>Web User Interface:</p> <p>Settings->Tones->Select Country</p>		

Parameters	Permitted Values	Default
Phone User Interface: None		
voice.tone.dial	String	Blank
Description: Customizes the dial tone. tonelist = element[,element] [,element]... Where element = [!] Freq1 [+ Freq2][+ Freq3][+ Freq4] / Duration Freq : the frequency of the tone (ranges from 200 to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone is comprised of at most four different frequencies. Duration : the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). If you want the IP phone to play tones once, add an exclamation mark "!" before tones (e.g., !250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). Note : It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Dial Phone User Interface: None		
voice.tone.ring	String	Blank
Description: Customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note : It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Ring Back Phone User Interface: None		
voice.tone.busy	String	Blank

Parameters	Permitted Values	Default
Description: Customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Busy Phone User Interface: None		
voice.tone.congestion	String	Blank
Description: Customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Congestion Phone User Interface: None		
voice.tone.callwaiting	String	Blank
Description: Customizes the call waiting tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Call Waiting Phone User Interface: None		
voice.tone.dialrecall	String	Blank

Parameters	Permitted Values	Default
Description: Customizes the call back tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Dial Recall Phone User Interface: None		
voice.tone.info	String	Blank
Description: Customizes the info tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Info Phone User Interface: None		
voice.tone.stutter	String	Blank
Description: Customizes the tone when the IP phone receives a voice mail. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". The default value is blank. Note: It works only if the parameter "voice.tone.country" is set to Custom. Web User Interface: Settings->Tones->Stutter Phone User Interface: None		
voice.tone.autoanswer	String	Blank

Parameters	Permitted Values	Default
<p>Description:</p> <p>Customizes the warning tone for auto answer.</p> <p>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".</p> <p>The default value is blank.</p> <p>Note: It works only if the parameter "voice.tone.country" is set to Custom.</p> <p>Web User Interface:</p> <p>Settings->Tones->Auto Answer</p> <p>Phone User Interface:</p> <p>None</p>		

To configure tones via web user interface:

1. Click on **Settings->Tones**.
2. Select the desired type from the pull-down list of **Select Country**.
If you select **Custom**, you can customize the tone for each condition of the IP phone.
3. Configure the tone for each condition of the IP phone.
If you leave the field blank, the IP phone will play default tones.

4. Click **Confirm** to accept the change.

Remote Phone Book

Remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the entries, and then display the

remote phone book entries on the phone user interface. IP phones support up to 5 remote phone books and 5000 entries. Remote phone book is customizable. For more information, refer to [Remote XML Phone Book](#) on page 331.

Sremote Name allows IP phones to search the entry names from the remote phone book for incoming/outgoing calls. Sremote Name Flash Time defines how often IP phones refresh the local cache of the remote phone book.

Procedure

Remote phone book can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Specify the access URL and the display name of the remote phone book.</p> <p>Parameters:</p> <p>remote_phonebook.data.X.url</p> <p>remote_phonebook.data.X.name</p> <p>Specify whether to query the entry name from the remote phone book for outgoing/incoming calls.</p> <p>Parameter:</p> <p>features.remote_phonebook.enable</p> <p>Specify how often the IP phone refreshes the local cache of the remote phone book.</p> <p>Parameter:</p> <p>features.remote_phonebook.flash_time</p>
Local	Web User Interface	<p>Specify the access URL of the remote phone book.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-remote&q=load</p> <p>Specify whether to query the entry name from the remote phone book for outgoing/incoming calls.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-remote&q=load</p> <p>Specify how often the IP phone refreshes the local cache of the remote phone book.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-remote&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
remote_phonebook.data.X.url (X ranges from 1 to 5)	URL within 511 characters	Blank
Description: Configures the access URL of the remote phone book. Example: remote_phonebook.data.1.url = http://192.168.1.20/Menu.xml Web User Interface: Directory->Remote Phone Book->Remote URL Phone User Interface: None		
remote_phonebook.data.X.name (X ranges from 1 to 5)	String within 99 characters	Blank
Description: Configures the display name of the remote phone book item. Example: remote_phonebook.data.1.name = yl01 Web User Interface: Directory->Remote Phone Book->Display Name Phone User Interface: None		
features.remote_phonebook.enable	0 or 1	0
Description: Enables or disables the IP phone to perform a remote phone book search for an incoming or outgoing call. 0-Disabled 1-Enabled Web User Interface: Directory->Remote Phone Book->Search Remote Phonebook Name Phone User Interface: None		

Parameters	Permitted Values	Default
features.remote_phonebook.flash_time	Integer from 120 to 2592000	21600
<p>Description:</p> <p>Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the IP phone will refresh the local cache of the remote phone book every 3600 seconds.</p> <p>Web User Interface:</p> <p>Directory->Remote Phone Book->Search Flash Time (Seconds)</p> <p>Phone User Interface:</p> <p>None</p>		

To specify the access URL of the remote phone book via web user interface:

1. Click on **Directory->Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.
3. Enter the name in the **Display Name** field.

The screenshot shows the Yealink CP860 web interface. The 'Directory' tab is selected, and the 'Remote Phone Book' sub-tab is active. A table with 3 columns (Index, Remote URL, Display Name) is shown. The first row (Index 1) has 'http://10.3.6.117:8080/phone.xml' in the Remote URL field and 'Sales1' in the Display Name field. Below the table, there are fields for 'Search Remote Phonebook Name' (set to 'Disabled') and 'Search Flash Time(Seconds)' (set to '21600'). A 'NOTE' box on the right states: 'Remote Phone Book. This feature allows you to download contact list from the server. Input the phonebook URL and rename the phone book.'

4. Click **Confirm** to accept the change.

To configure the remote phone book via web user interface:

1. Click on **Directory->Remote Phone Book**.
2. Select the desired value from the pull-down list of **Search Remote Phonebook Name**.

3. Enter the desired time in the **Search Flash Time (Seconds)** field.

The screenshot shows the Yealink CP860 web interface. The 'Directory' tab is selected. In the 'Remote Phone Book' section, the 'Search Remote Phonebook Name' dropdown is set to 'Enabled' and the 'Search Flash Time(Seconds)' field is set to '21600'. A red box highlights these two fields. The interface includes a sidebar with 'Local Directory', 'Remote Phone Book', 'Phone Call Info', 'LDAP', 'Multicast IP', and 'Setting'. The main area has a table with columns 'Index', 'Remote URL', and 'Display Name'. A 'NOTE' box on the right explains the Remote Phone Book feature.

4. Click **Confirm** to accept the change.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. IP phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using IP phones, therefore they do not have to maintain the local directory. Users can search and dial out from the LDAP directory and save LDAP entries to the local directory. LDAP entries displayed on the IP phone are read only, which cannot be added, edited or deleted by users. When an LDAP server is properly configured, the IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select the desired entry or group, and return the desired information.

Configurations on the IP phone limit the amount of displayed entries when querying from the LDAP server, and decide how the attributes are displayed and sorted.

You can assign a programable key to be an LDAP key, and press the LDAP key to enter the LDAP search screen when the IP phone is idle.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on IP phones:

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

For more information on LDAP, refer to *LDAP Phonebook on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

LDAP can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the LDAP feature. Parameters: ldap.enable ldap.name_filter ldap.number_filter ldap.host ldap.port ldap.base ldap.user ldap.password ldap.max_hits ldap.name_attr ldap.numb_attr ldap.display_name ldap.version
---------------------------	-------------------	---

		ldap.call_in_lookup ldap.ldap_sort Assign an LDAP key. Parameter: programablekey.X.type
Local	Web User Interface	Configure the LDAP feature. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=contacts-LDAP&q=load">http://<phoneIPAddress>/servlet?p=contacts-LDAP&q=load Assign an LDAP key. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=dsskey&model=2&q=load">http://<phoneIPAddress>/servlet?p=dsskey&model=2&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
ldap.enable	0 or 1	0
Description: Enables or disables LDAP feature on the IP phone. 0-Disabled 1-Enabled Web User Interface: Directory->LDAP->Enable LDAP Phone User Interface: None		
ldap.name_filter	String within 99 characters	Blank
Description: Configures the criteria for searching the LDAP contact name attributes. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition. Example: ldap.name_filter = ((cn=%)(sn=%)) When the name prefix of the cn or sn of the contact record matches the search criteria, the record will be displayed on the LCD screen.		

Parameters	Permitted Values	Default
Web User Interface: Directory->LDAP->LDAP Name Filter Phone User Interface: None		
ldap.number_filter	String within 99 characters	Blank
Description: Configures the criteria for searching the LDAP contact number attributes. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the entering string used as the prefix of the filter condition. Example: ldap.number_filter = ((telephoneNumber=%)(Mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, Mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the LCD screen. Web User Interface: Directory->LDAP->LDAP Number Filter Phone User Interface: None		
ldap.host	String within 99 characters	Blank
Description: Configures the IP address or domain name of the LDAP server. Example: ldap.host = 192.168.1.20 Web User Interface: Directory->LDAP->Server Address Phone User Interface: None		
ldap.port	Integer from 1 to 65535	389
Description: Configures the port of the LDAP server. Example: ldap.port = 389		

Parameters	Permitted Values	Default
Web User Interface: Directory->LDAP->Port Phone User Interface: None		
ldap.base	String within 99 characters	Blank
Description: Configures the LDAP search base which corresponds to the location of the LDAP phone book from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time. Example: ldap.base = dc=yealink,dc=cn Web User Interface: Directory->LDAP->Base Phone User Interface: None		
ldap.user	String within 99 characters	Blank
Description: Configures the user name used to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the user name to login the LDAP server. Example: ldap.user = cn=manager,dc=yealink,dc=cn Web User Interface: Directory->LDAP->Username Phone User Interface: None		
ldap.password	String within 99 characters	Blank
Description: Configures the password to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to login the LDAP server. Example:		

Parameters	Permitted Values	Default
ldap.password =secret Web User Interface: Directory->LDAP->Password Phone User Interface: None		
ldap.max_hits	Integer from 1 to 32000	50
Description: Configures the maximum number of search results to be returned by the LDAP server. If the value of the "Max.Hits" is blank, the LDAP server will return all searched results. Please note that a very large value of the "Max. Hits" will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth. Example: ldap.max_hits = 50 Web User Interface: Directory->LDAP->Max. Hits (1~32000) Phone User Interface: None		
ldap.name_attr	String within 99 characters	Blank
Description: Configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces. Example: ldap.name_attr = cn sn Web User Interface: Directory->LDAP->LDAP Name Attributes Phone User Interface: None		
ldap.numb_attr	String within 99 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes separated by spaces. Example: ldap.numb_attr = telephoneNumber Web User Interface: Directory->LDAP->LDAP Number Attributes Phone User Interface: None		
ldap.display_name	String within 99 characters	Blank
Description: Configures the display name of the contact record displayed on the LCD screen. The value must start with “%” symbol. Example: ldap.display_name = %cn The cn of the contact record is displayed on the LCD screen. Web User Interface: Directory->LDAP-> LDAP Display Name Phone User Interface: None		
ldap.version	2 or 3	3
Description: Configures the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. Web User Interface: Directory->LDAP-> Protocol Phone User Interface: None		
ldap.call_in_lookup	0 or 1	0

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to perform an LDAP search when receiving an incoming call. 0 -Disabled 1 -Enabled Web User Interface: Directory->LDAP->LDAP Lookup For Incoming Call Phone User Interface: None		
ldap.ldap_sort	0 or 1	0
Description: Enables or disables the IP phone to sort the search results in alphabetical order or numerical order. 0 -Disabled 1 -Enabled Web User Interface: Directory->LDAP->LDAP Sorting Results Phone User Interface: None		
programmablekey.X.type (X=1-6, 9, 13)	38	0
Description: Configures a programmable key as an LDAP key on the IP phone. The digit 38 stands for the key type LDAP . For more information on how to configure the programmable key, refer to Appendix C: Configuring Programmable Key on page 353. Example: programmablekey.2.type = 38 Web User Interface: DSSKey->Programmable Key->Type Phone User Interface: None		

To configure LDAP via web user interface:

1. Click on **Directory**->**LDAP**.
2. Select **Enabled** from the pull-down list of **Enable LDAP**.
3. Enter the values in the corresponding fields.
4. Select the desired values from the corresponding pull-down lists.

5. Click **Confirm** to accept the change.

To configure an LDAP key via web user interface:

1. Click on **DSSKey**->**Programmable Key**.
2. In the desired programmable key field, select **LDAP** from the pull-down list of **Type**.

3. Click **Confirm** to accept the change.

Message Waiting Indicator

Message Waiting Indicator (MWI) informs users of the number of messages waiting in their mailbox without calling the mailbox. IP phones support both audio and visual MWI

when receiving new voice messages.

IP phones support both solicited and unsolicited MWI. Unsolicited MWI is a server related feature.

IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes. For solicited MWI, you must enable MWI subscription feature on IP phones. IP phones support subscribing the MWI messages to the account or the voice mail number.

IP phones do not need to subscribe to message-summary updates. The server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure subscribe for MWI. Parameters: account.X.subscribe_mwi account.X.subscribe_mwi_expires account.X.subscribe_mwi_to_vm Configure subscribe MWI to voice mail. Parameter: voice_mail.number.X
Local	Web User Interface	Configure subscribe for MWI. Configure subscribe MWI to voice mail. Navigate to: <a href="http://<phoneIPAddress>/servlet?parameter=account-adv&q=load&acc=0">http://<phoneIPAddress>/servlet?parameter=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.subscribe_mwi (X = 1)	0 or 1	0
Description: Enables or disables the IP phone to subscribe the message waiting indicator. If it is set to 1 (Enabled), the IP phone will send a SUBSCRIBE message to the server for message-summary updates.		

Parameters	Permitted Values	Default
0-Disabled 1-Enabled Web User Interface: Account->Advanced->Subscribe for MWI Phone User Interface: None		
account.X.subscribe_mwi_expires (X = 1)	Integer from 0 to 84600	3600
Description: Configures MWI subscribe expiry time (in seconds). The IP phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the SUBSCRIBE dialog. Note: It works only if the parameter "account.X.subscribe_mwi" is set to 1 (Enabled). Web User Interface: Account->Advanced->MWI Subscription Period (Seconds) Phone User Interface: None		
account.X.subscribe_mwi_to_vm (X = 1)	0 or 1	0
Description: Enables or disables the IP phone to subscribe the message waiting indicator to the voice mail number. 0-Disabled 1-Enabled Note: It works only if the parameters "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured. Web User Interface: Account->Advanced->Subscribe MWI To Voice Mail Phone User Interface: None		
voice_mail.number.X (X = 1)	String within 99 characters	Blank
Description:		

Parameters	Permitted Values	Default
<p>Configures the voice mail number.</p> <p>Example:</p> <p>voice_mail.number.1 = 1234</p> <p>Note: It works only if the parameter “account.x.subscribe_mwi_to_vm” is set to 1 (Enabled).</p> <p>Web User Interface:</p> <p>Account->Advanced->Voice Mail</p> <p>Phone User Interface:</p> <p>None</p>		

To configure subscribe for MWI via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired value from the pull-down list of **Subscribe for MWI**.
3. Enter the period time in the **MWI Subscription Period (Seconds)** field.

The screenshot shows the Yealink CP860 web interface. The 'Account' tab is selected, and the 'Advanced' sub-tab is active. The 'Subscribe for MWI' dropdown menu is set to 'Enabled', and the 'MWI Subscription Period(Seconds)' text field contains the value '3600'. These two settings are highlighted with a red rectangular box. Other visible settings include 'Keep Alive Type' (Default), 'Keep Alive Interval(Seconds)' (30), 'Local SIP Port' (5062), 'RPort' (Disabled), 'SIP Session Timer T1' (0.5), 'SIP Session Timer T2' (4), 'SIP Session Timer T4' (5), 'DTMF Type' (RFC2833), 'DTMF Info Type' (DTMF-Relay), 'DTMF Payload Type(96~127)' (101), 'Retransmission' (Disabled), 'Subscribe MWI To Voice Mail' (Disabled), 'Voice Mail' (*88), 'Caller ID Source' (FROM), and 'Session Timer' (Disabled). A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.'

4. Click **Confirm** to accept the change.

The IP phone will subscribe to the account number for MWI service by default.

To configure subscribe MWI to voice mail via web user interface:

1. Click on **Account-> Advanced**.
2. Select the desired value from the pull-down list of **Subscribe MWI To Voice Mail**.

- Enter the desired voice number in the **Voice Mail** field.

The screenshot shows the Yealink CP860 web interface with the 'Advanced' settings tab selected. The 'Voice Mail' field is highlighted with a red box, showing the value '*88'. Other settings include Keep Alive Type (Default), Keep Alive Interval (30), Local SIP Port (5062), RPort (Disabled), SIP Session Timer T1 (0.5), SIP Session Timer T2 (4), SIP Session Timer T4 (5), DTMF Type (RFC2833), DTMF Info Type (DTMF-Relay), DTMF Payload Type (101), Retransmission (Disabled), Subscribe for MWI (Enabled), MWI Subscription Period (3600), and Caller ID Source (FROM).

- Click **Confirm** to accept the change.

Multicast Paging

Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the IP phone.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a configured multicast paging key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated IP phones. When the IP phone sends the RTP stream to a pre-configured multicast address, each IP phone that preconfigured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify a multicast codec for the IP phone to use for multicast RTP. Parameter: multicast.codec Assign a multicast paging key.
---------------------------	-------------------	--

		Parameters: programablekey.X.type programablekey.X.value.
Local	Web User Interface	Assign a multicast paging key. Navigate to: http://<phoneIPAddress>/servlet ?p=dsskey&model=2&q=load Specify a multicast codec for the IP phone to send the RTP stream. Navigate to: http://<phoneIPAddress>/servlet ?p=features-general&q=load

Details of the Configuration Parameter:

Parameters	Permitted Values	Default
multicast.codec	Refer to the following content	G722
Description: Configures the codec of multicast paging. Example: multicast.codec = G722 Permitted Values: PCMU, PCMA, G729, G722, Web User Interface: Features->General Information->Multicast Codec Phone User Interface: None		
programablekey.X.type (X=1-6, 9, 13)	24	0
Description: Configures a programmable key to be a multicast paging key on the IP phone. The digit 24 stands for the key type Multicast Paging . For more information on how to configure the programmable key, refer to Appendix C: Configuring Programmable Key on page 353. Example: programablekey.3.type = 24		

Parameters	Permitted Values	Default
Web User Interface: DSSKey->Programable Key->Programable KeyX->Type Phone User Interface: None		
programablekey.X.value (X=1-6, 9, 13)	String within 99 characters	blank
Description: Configures the multicast IP address and port number. Example: programablekey.3.value = 224.5.5.6:10008 Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. Web User Interface: DSSKey->Programable Key->Programable KeyX->Value Phone User Interface: None		

To configure a multicast paging key via web user interface:

1. Click on **DSSKey->Programable Key**.
2. In the desired programmable key field, select **Multicast Paging** from the pull-down list of **Type**.
3. Enter the multicast IP address and port number in the **Value** field.
The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

The screenshot shows the Yealink CP860 web interface. The 'DSSKey' tab is selected. On the left, 'Programable Key' is chosen. The main table lists keys: SoftKey 1-4, Up, Down, OK, and MUTE. The 'MUTE' key is highlighted with a red box. Its 'Type' is 'Multicast Paging' and its 'Value' is '224.5.6.20:10008'. A 'NOTE' panel on the right explains key types, events, and intercom functions.

4. Click **Confirm** to accept the change.

To configure a codec for multicast paging via web user interface:

1. Click on **Features ->General Information**.

2. Select the desired codec from the pull-down list of **Multicast Codec**.

The screenshot shows the Yealink CP860 web interface with the 'Features' tab selected. The 'General Information' section contains various settings. The 'Multicast Codec' is set to 'G722' and is highlighted with a red box. Other settings include 'Call Waiting' (Enabled), 'Call Waiting On Code' (empty), 'Call Waiting Off Code' (empty), 'Auto Redial' (Disabled), 'Auto Redial Interval (1~300s)' (10), 'Auto Redial Times (1~300)' (10), 'Key As Send' (#), 'DTMF Repetition' (3), 'Play Hold Tone Delay' (30), 'Allow IP Call' (Enable), 'IP Direct Auto Answer' (Disabled), 'Call List Show Number' (Disabled), 'Voice Mail Tone' (Enable), and 'DHCP Hostname' (CP860). A 'NOTE' section on the right provides information about 'Call Waiting', 'Key As Send', and 'Hotline Number'.

3. Click **Confirm** to accept the change.

Receiving RTP Stream

IP phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

Paging Barge

This parameter defines the priority of the voice call in progress, and decides how the IP phone handles the incoming multicast paging calls when there is already a voice call in progress. If the parameter is configured as disabled, all incoming multicast paging calls will be automatically ignored. If the parameter is the priority value, the incoming multicast paging calls with higher priority are automatically answered and the ones with lower priority are ignored.

Paging Priority Active

This parameter decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If the parameter is configured as disabled, the IP phone will automatically ignore all incoming multicast paging calls. If the parameter is configured as enabled, an incoming multicast paging call with higher priority is automatically answered, and the one with lower priority is ignored.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the listening multicast address.</p> <p>Parameters:</p> <p>multicast.listen_address.X.label</p> <p>multicast.listen_address.X.ip_address</p> <p>Configure the Paging Barge and Paging Priority Active features.</p> <p>Parameters:</p> <p>multicast.receive_priority.enable</p> <p>multicast.receive_priority.priority</p>
Local	Web User Interface	<p>Configure the listening multicast address.</p> <p>Configure the Paging Barge and Paging Priority Active features.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 10)	IP address:port	Blank
<p>Description:</p> <p>Configures the multicast address and port number that the IP phone listens to.</p> <p>Example:</p> <p>multicast.listen_address.1.ip_address = 224.5.6.20:10008</p> <p>Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.</p> <p>Web User Interface:</p> <p>Directory->Multicast IP->Listening Address</p> <p>Phone User Interface:</p> <p>None</p>		
multicast.listen_address.X.label (X ranges from 1 to 10)	String within 99 characters	Blank

Parameters	Permitted Values	Default
<p>Description: Configures the label to be displayed on the LCD screen when receiving the RTP multicast.</p> <p>Example: multicast.listen_address.1.label = Paging1</p> <p>Web User Interface: Directory->Multicast IP->Label</p> <p>Phone User Interface: None</p>		
multicast.receive_priority.enable	0 or 1	1
<p>Description: Enables or disables the IP phone to handle the incoming multicast paging calls when there is an active multicast paging call on the IP phone.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), the IP phone will answer the incoming multicast paging call with a higher priority and ignore that with a lower priority.</p> <p>Web User Interface: Directory->Multicast IP->Paging Priority Active</p> <p>Phone User Interface: None</p>		
multicast.receive_priority.priority	Integer from 0 to 10	10
<p>Description: Configures the priority of multicast paging calls. 1 is the highest priority, 10 is the lowest priority. If it is set to 0, all incoming multicast paging calls will be automatically ignored.</p> <p>Web User Interface: Directory->Multicast IP->Paging Barge</p> <p>Phone User Interface: None</p>		

To configure a listening multicast address via web user interface:

1. Click on **Directory->Multicast IP**.

2. Enter the listening multicast address and port number in the **Listening Address** field.

1 is the highest priority and 10 is the lowest priority.

3. Enter the label in the **Label** field.

The label will appear on the LCD screen when receiving the RTP multicast.

Yealink CP860

Status Account Network DSSKey Features Settings **Directory** Security

Local Directory
Remote Phone Book
Phone Call Info
LDAP
Multicast IP
Setting

Paging Barge: 10
Paging Priority Active: Enabled

IP Address	Listening Address	Label	Priority
1 IP Address	224.5.6.20:10008	paging1	1
2 IP Address			2
3 IP Address			3
4 IP Address			4
5 IP Address			5
6 IP Address			6
7 IP Address			7
8 IP Address			8
9 IP Address			9
10 IP Address			10

Confirm Cancel

NOTE
Multicast IP
The multicast IP parameters for administrator.

4. Click **Confirm** to accept the change.

To configure the paging barge and paging priority active features via web user interface:

1. Click on **Directory->Multicast IP**.
2. Select the desired value from the pull-down list of **Paging Barge**.
3. Select the desired value from the pull-down list of **Paging Priority Active**.

Yealink CP860

Status Account Network DSSKey Features Settings **Directory** Security

Local Directory
Remote Phone Book
Phone Call Info
LDAP
Multicast IP
Setting

Paging Barge: 10
Paging Priority Active: Enabled

IP Address	Listening Address	Label	Priority
1 IP Address	224.5.6.20:10008	paging1	1
2 IP Address			2
3 IP Address			3
4 IP Address			4
5 IP Address			5
6 IP Address			6
7 IP Address			7
8 IP Address			8
9 IP Address			9
10 IP Address			10

Confirm Cancel

NOTE
Multicast IP
The multicast IP parameters for administrator.

4. Click **Confirm** to accept the change.

Action URL

Action URL allows IP phones to interact with web server applications by sending an HTTP or HTTPS GET request. You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the pre-defined events (e.g., log on). The valid URL format is: `http(s)://IP address of the server/help.xml?`.

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs off the registered account.
Register Failed	When the IP phone fails to register an account.
Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.
Incoming Call	When the IP phone receives an incoming call.
Outgoing Call	When the IP phone places a call.
Established	When the IP phone establishes a call.
Terminated	When the IP phone terminates a call.
Open DND	When the IP phone enables the DND mode.
Close DND	When the IP phone disables the DND mode.
Open Always Forward	When the IP phone enables the always forward.
Close Always Forward	When the IP phone disables the always forward.
Open Busy Forward	When the IP phone enables the busy forward.
Close Busy Forward	When the IP phone disables the busy forward.
Open No Answer Forward	When the IP phone enables the no answer forward.
Close No Answer Forward	When the IP phone disables the no answer forward.
Transfer Call	When the IP phone transfers a call.
Blind Transfer	When the IP phone blind transfers a call.
Attended Transfer	When the IP phone performs the semi-attended/attended transfer.
Hold	When the IP phone places a call on hold.
UnHold	When the IP phone retrieves a hold call.
Mute	When the IP phone mutes a call.

Event	Description
UnMute	When the IP phone un-mutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the phone changes.
Forward Incoming Call	When the IP phone forwards an incoming call.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer New-In Call	When the IP phone answers a new call.
Transfer Finished	When the IP phone completes to transfer a call.
Transfer Failed	When the IP phone fails to transfer a call.
Idle to Busy	When the state of the IP phone changes from idle to busy.
Busy to Idle	When the state of phone changes from busy to idle.

An HTTP or HTTPS GET request may contain variable name and variable value, separated by “=”. Each variable value starts with \$ in the query part of the URL. The valid URL format is: `http(s)://IP address of server/help.xml?variable name=$variable value`. Variable name can be customized by users, while the variable value is pre-defined. For example, a URL “`http://192.168.1.10/help.xml?mac=$mac`” is specified for the event Mute, \$mac will be dynamically replaced with the MAC address of the phone when the IP phone mutes a call.

The following table lists the pre-defined variable values.

Variable Value	Description
\$mac	The MAC address of the phone
\$ip	The IP address of the phone
\$model	The IP phone model
\$firmware	The firmware version of the IP phone
\$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
\$local	The SIP URI of the caller when the IP phone places a

Variable Value	Description
	call. The SIP URI of the callee when the IP phone receives an incoming call.
\$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
\$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.
\$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.
\$call_id	The call-id of the active call.

Procedure

Action URL can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configure the action URL.</p> <p>Parameters:</p> <ul style="list-style-type: none"> action_url.setup_completed action_url.registered action_url.unregistered action_url.register_failed action_url.off_hook action_url.on_hook action_url.incoming_call action_url.outgoing_call action_url.call_established action_url.dnd_on action_url.dnd_off action_url.always_fwd_on action_url.always_fwd_off action_url.busy_fwd_on action_url.busy_fwd_off
---------------------------	-------------------	--

		action_url.no_answer_fwd_on action_url.no_answer_fwd_off action_url.transfer_call action_url.blind_transfer_call action_url.attended_transfer_call action_url.hold action_url.unhold action_url.mute action_url.unmute action_url.missed_call action_url.call_terminated action_url.busy_to_idle action_url.idle_to_busy action_url.ip_change action_url.forward_incoming_call action_url.reject_incoming_call action_url.answer_new_incoming_call action_url.transfer_finished action_url.transfer_failed
Local	Web User Interface	Configure the action URL. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=features-actionurl&q=load">http://<phoneIPAddress>/servlet?p=features-actionurl&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
action_url.setup_completed	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends after startup. The value format is: http(s)://IP address of server/help.xml? variable name=variable value. Valid variable values are: <ul style="list-style-type: none"> • \$mac • \$ip • \$model • \$firmware 		

Parameters	Permitted Values	Default
<ul style="list-style-type: none"> • \$active_url • \$active_user • \$active_host • \$local • \$remote • \$display_local • \$display_remote • \$call_id <p>Example: action_url.setup_completed = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Setup Completed</p>		
action_url.registered	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends after an account is registered.</p> <p>Example: action_url.registered = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Registered</p> <p>Phone User Interface: None</p>		
action_url.unregistered	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when an account is unregistered.</p> <p>Example: action_url.unregistered = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Unregistered</p> <p>Phone User Interface: None</p>		
action_url.register_failed	URL within 511 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when a register failed. Example: action_url.register_failed = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Register Failed Phone User Interface: None		
action_url.off_hook	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when off hook. Example: action_url.off_hook = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Off Hook Phone User Interface: None		
action_url.on_hook	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when on hook. Example: action_url.on_hook = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->On Hook Phone User Interface: None		
action_url.incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when receiving an incoming call. Example:		

Parameters	Permitted Values	Default
<p>action_url.incoming_call = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Incoming Call</p> <p>Phone User Interface: None</p>		
action_url.outgoing_call	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when placing a call.</p> <p>Example: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Outgoing Call</p> <p>Phone User Interface: None</p>		
action_url.call_established	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when establishing a call.</p> <p>Example: action_url.call_established = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Established</p> <p>Phone User Interface: None</p>		
action_url.dnd_on	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when DND feature is enabled.</p> <p>Example: action_url.dnd_on = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Open DND</p>		

Parameters	Permitted Values	Default
Phone User Interface: None		
action_url.dnd_off	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when DND feature is disabled. Example: action_url.dnd_off = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Close DND Phone User Interface: None		
action_url.always_fwd_on	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when always forward feature is enabled. Example: action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Open Always Forward Phone User Interface: None		
action_url.always_fwd_off	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when always forward feature is disabled. Example: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Close Always Forward Phone User Interface: None		

Parameters	Permitted Values	Default
action_url.busy_fwd_on	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when busy forward feature is enabled.</p> <p>Example: action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Open Busy Forward</p> <p>Phone User Interface: None</p>		
action_url.busy_fwd_off	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when busy forward feature is disabled.</p> <p>Example: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Close Busy Forward</p> <p>Phone User Interface: None</p>		
action_url.no_answer_fwd_on	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when no answer forward feature is enabled.</p> <p>Example: action_url.no_answer_fwd_on = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Open No Answer Forward</p> <p>Phone User Interface: None</p>		
action_url.no_answer_fwd_off	URL within 511 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when no answer forward feature is disabled. Example: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Close No Answer Forward Phone User Interface: None		
action_url.transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing a transfer. Example: action_url.transfer_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Transfer Call Phone User Interface: None		
action_url.blind_transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing a blind transfer. Example: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Blind Transfer Phone User Interface: None		
action_url.attended_transfer_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when performing an attended/semi-attended transfer.		

Parameters	Permitted Values	Default
Example: action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Attended Transfer Phone User Interface: None		
action_url.hold	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when placing a call on hold. Example: action_url.hold = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Hold Phone User Interface: None		
action_url.unhold	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when resuming a held call. Example: action_url.unhold = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->UnHold Phone User Interface: None		
action_url.mute	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when muting a call. Example: action_url.mute = http://192.168.0.20/help.xml?IP=\$ip Web User Interface:		

Parameters	Permitted Values	Default
Features->Action URL->Mute Phone User Interface: None		
action_url.unmute	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when un-muting a call. Example: action_url.unmute = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->UnMute Phone User Interface: None		
action_url.missed_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when missing a call. Example: action_url.missed_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Missed Call Phone User Interface: None		
action_url.call_terminated	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when terminating a call. Example: action_url.call_terminated = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Terminated Phone User Interface: None		

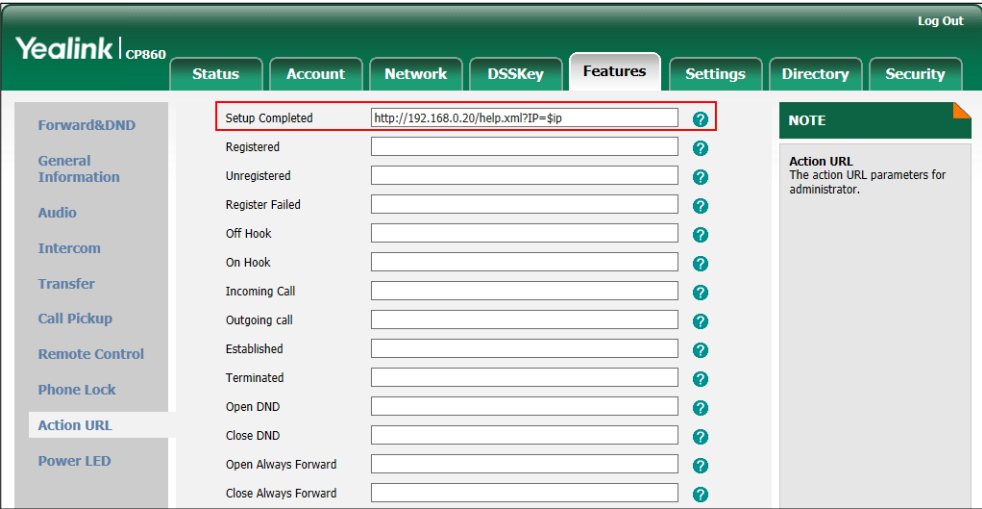
Parameters	Permitted Values	Default
action_url.busy_to_idle	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when changing the state of the IP phone from busy to idle.</p> <p>Example: action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Busy To Idle</p> <p>Phone User Interface: None</p>		
action_url.idle_to_busy	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when changing the state of the IP phone from idle to busy.</p> <p>Example: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Idle To Busy</p> <p>Phone User Interface: None</p>		
action_url.ip_change	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when changing the IP address of the IP phone.</p> <p>Example: action_url.ip_change = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->IP Changed</p> <p>Phone User Interface: None</p>		
action_url.forward_incoming_call	URL within 511 characters	Blank

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when forwarding an incoming call. Example: action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Forward Incoming Call Phone User Interface: None		
action_url.reject_incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when rejecting an incoming call. Example: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Reject Incoming Call Phone User Interface: None		
action_url.answer_new_incoming_call	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when answering a new incoming call. Example: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=\$ip Web User Interface: Features->Action URL->Answer New-In Call Phone User Interface: None		
action_url.transfer_finished	URL within 511 characters	Blank
Description: Configures the action URL the IP phone sends when completing a call transfer. Example:		

Parameters	Permitted Values	Default
<p>action_url.transfer_finished = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Transfer Finished</p> <p>Phone User Interface: None</p>		
action_url.transfer_failed	URL within 511 characters	Blank
<p>Description: Configures the action URL the IP phone sends when failing to transfer a call.</p> <p>Example: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=\$ip</p> <p>Web User Interface: Features->Action URL->Transfer Failed</p> <p>Phone User Interface: None</p>		

To configure action URL via web user interface:

1. Click on **Features->Action URL**.
2. Enter the action URLs in the corresponding fields.



The screenshot shows the Yealink CP860 web interface. The 'Features' tab is selected, and the 'Action URL' section is active. The 'Setup Completed' field is highlighted with a red box and contains the URL 'http://192.168.0.20/help.xml?IP=\$ip'. Other fields include Registered, Unregistered, Register Failed, Off Hook, On Hook, Incoming Call, Outgoing call, Established, Terminated, Open DND, Close DND, Open Always Forward, and Close Always Forward. A 'NOTE' box on the right states: 'Action URL. The action URL parameters for administrator.'

3. Click **Confirm** to accept the change.

Action URI

Opposite to action URL, action URI allows IP phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK message. A GET request may contain variable named as "key" and variable value, which are separated by "=". The valid URI format is:

http(s)://phone IP address/servlet?key=variable value.

The following table lists the pre-defined variable values.

Variable Value	Phone Action
OK	Press the OK key.
ENTER	Press the Enter soft key
F_TRANSFER	Transfers a call to another party.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease the volume.
MUTE	Mute a call.
F_HOLD	Place an active call on hold.
CANCEL	Return to a previous screen or cancel a call.
0-9/*/POUND	Press the keypad (0-9, * or #).
F_CONFERENCE	Press the Conference soft key.
F1-F4	Press the soft keys.
RD	Press the REDIAL key.
UP/DOWN	Press the navigation keys.
Reboot	Reboot the phone.
AutoP	Perform auto provisioning.
DNDOn	Activate the DND mode.
DNDOff	Deactivate the DND mode.
number=xxx&outgoing_uri=y	Place a call to xxx from SIP URI y.
OFFHOOK	Press the off-hook key.
ONHOOK	Press the on-hook key.
ANSWER	Answer a call.
Reset	Reset a phone.
ATrans=xxx	Perform a semi-attended/attended transfer to

Variable Value	Phone Action
BTrans=xxx	Perform a blind transfer to xxx.
CALLEND	End a call.

Note

The variable value is not applicable to all events. For example, the variable value "MUTE" is only applicable when the IP phone is during a call.

When authentication is required, you must enter "p=login&q=login&username=xxx&pwd=yyy&jumpto=URI&" before the variable "key". xxx refers to the login user name, and yyy refers to the login password.

For security reasons, IP phones do not receive and handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the specified IP address for the first time, the LCD screen prompts the message "Allow Remote Control?". You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address.

Procedure

Specify the trusted IP address for Action URI using the configuration files or locally.

Configuration File	y000000000037.cfg	Specify the trusted IP address(es) for sending the Action URI to the IP phone. Parameter: features.action_uri_limit_ip
Local	Web User Interface	Specify the trusted IP address(es) for sending the Action URI to the IP phone. Navigate to: http://<phoneIPAddress>/servlet?p=features-remotecontrol&q=load

Details of the Configuration Parameter:

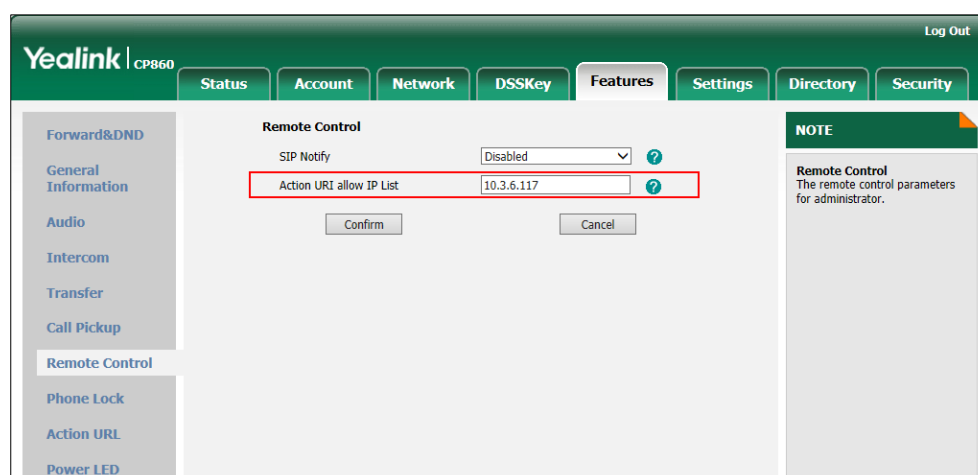
Parameter	Permitted Values	Default
features.action_uri_limit_ip	IP address or any	Blank
Description: Configures the address(es) from which Action URI will be accepted. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.* and the "*" stands for the values		

Parameter	Permitted Values	Default
0~255. For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255. If it is left blank, the IP phone cannot receive or handle any HTTP GET request. If it is set to "any", the IP phone will accept and handle HTTP GET requests from any IP address. Example: features.action_uri_limit_ip = any Web User Interface: Features->Remote Control->Action URI allow IP List Phone User Interface: None		

To configure the trusted IP address(es) for Action URI via web user interface:

1. Click on **Features->Remote Control**.
2. Enter the IP address or any in the **Action URI allow IP List** field.

Multiple IP addresses are separated by commas. If you enter "any" in this field, the IP phone can receive and handle GET requests from any IP address. If you leave the field blank, the IP phone cannot receive or handle any HTTP GET request.



3. Click **Confirm** to accept the change.

Server Redundancy

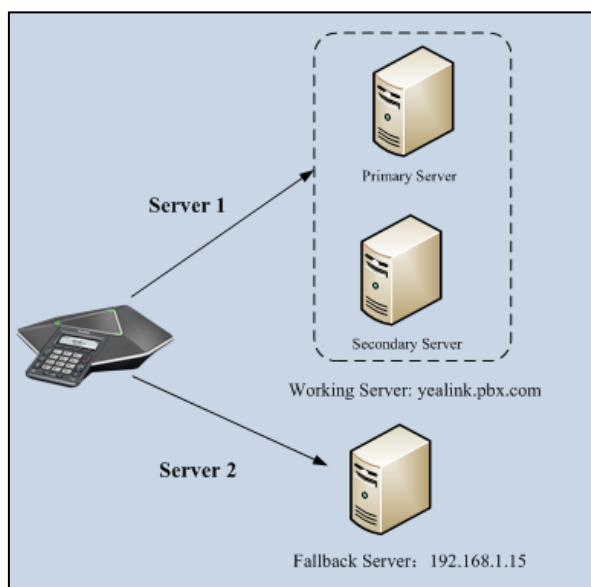
Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP phone and the server fails.

Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanisms from the primary to the secondary server.
- **Fallback:** In this mode, a second less featured call server (fallback server) with SIP capability takes over call control to provide basic calling capability, but without some advanced features (for example, shared lines, MWI) offered by the working server. IP phones support configuration of two SIP servers per SIP registration for fallback purpose.

Phone Configuration for Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how an IP phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate SIP servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example, yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple physical SIP servers for failover purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server is the highest priority server in a cluster of servers resolved by the DNS server. The secondary server backs up a primary server when the primary server fails and offers the same functionality as the primary server.

Fallback Server: Server 2 is configured with the address of the fallback server. For example, 192.168.1.15. A fallback server offers less functionality than the working server.

Phone Registration

Two registration methods for fallback mode:

- **Concurrent registration:** The IP phone registers to two SIP servers (working server and fallback server) at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some of the advanced features offered by the working server (default registration method).
- **Successive registration:** The IP phone only registers to one server at a time. The IP phone first registers to the working server. In a failure situation, the IP phone registers to the fallback server.

When registering to the working server, the IP phone must always register to the primary server first except in failover conditions. When the primary server registration is unavailable, the secondary server will serve as the working server.

For more information on server redundancy, refer to *Server Redundancy on Yealink IP Phones*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

Server redundancy can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure the server redundancy on the IP phone.</p> <p>Parameters:</p> <p>account.X.sip_server.Y.address</p> <p>account.X.sip_server.Y.port</p> <p>account.X.sip_server.Y.expires</p> <p>account.X.sip_server.Y.retry_counts</p> <p>Fallback Mode:</p> <p>account.X.fallback.redundancy_type</p> <p>account.X.fallback.timeout</p> <p>Failover Mode:</p> <p>account.X.sip_server.Y.fallback_mode</p> <p>account.X.sip_server.Y.fallback_timeout</p> <p>account.X.sip_server.Y.register_on_enable</p>
Local	Web User Interface	<p>Configure the server redundancy on the IP phone.</p> <p>Navigate to:</p> <p><a href="http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.address (X = 1, Y ranges from 1 to 2)	String within 256 characters	Blank
Description: Configures the IP address or domain name of the SIP server Y. Example: account.1.sip_server.1.address = yealink.pbx.com Web User Interface: Account->Register->SIP Server Y->Server Host Phone User Interface: None		
account.X.sip_server.Y.port (X = 1, Y ranges from 1 to 2)	Integer from 0 to 65535	5060
Description: Configures the port of the SIP server Y. Example: account.1.sip_server.1.port = 5060 Web User Interface: Account->Register->SIP Server Y->Port Phone User Interface: None		
account.X.sip_server.Y.expires (X = 1, Y ranges from 1 to 2)	Integer from 30 to 2147483647	3600
Description: Configures the registration expiration time (in seconds) of the SIP server Y. Example: account.1.sip_server.1.expires = 3600 Web User Interface: Account->Register->SIP Server Y->Server Expires Phone User Interface: None		

Parameters	Permitted Values	Default
account.X.sip_server.Y.retry_counts (X = 1, Y ranges from 1 to 2)	Integer from 0 to 20	3
Description: Configures the retry times for the IP phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y. Web User Interface: Account->Register->SIP Server Y->Server Retry Counts Phone User Interface: None		
account.X.fallback.redundancy_type (X = 1)	0 or 1	0
Description: Configures the registration mode for the IP phone in fallback mode. 0-Concurrent Registration 1-Successive Registration Web User Interface: None Phone User Interface: None		
account.X.fallback.timeout (X = 1)	Integer from 10 to 2147483647	120
Description: Configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request after the fallback server takes over call control. It is only applicable to the Successive Registration mode. Web User Interface: None Phone User Interface: None		
account.X.sip_server.Y.fallback_mode (X = 1, Y ranges from 1 to 2)	0, 1, 2 or 3	0

Parameters	Permitted Values	Default
Description: Configures the way in which the phone fails back to the primary server for call control in the failover mode. 0 -newRequests: all requests are sent to the primary server first, regardless of the last server that was used. 1 -DNSTTL: the IP phone will send requests to the last registered server first. If the time defined by DNSTTL on the registered server expires, the phone will retry to send requests to the primary server. 2 -registration: the IP phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server. 3 -duration: the IP phone will send requests to the last registered server first. If the time defined by the account.X.sip_server.Y.failback_timeout parameter expires, the phone will retry to send requests to the primary server. Web User Interface: None Phone User Interface: None		
account.X.sip_server.Y.failback_timeout (X = 1, Y ranges from 1 to 2)	0, 60 to 65535	3600
Description: Configures the time (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server when the parameter account.X.sip_server.Y.failback_mode is set to duration. If you set the parameter to 0, the IP phone will not send requests to the primary server until a failover event occurs with the current working server. Web User Interface: None Phone User Interface: None		
account.X.sip_server.Y.register_on_enable (X = 1, Y ranges from 1 to 2)	0 or 1	0
Description: Enables or disables the IP phone to register to the secondary server when sending requests to the secondary server in the failover mode. 0 -Disabled		

Parameters	Permitted Values	Default
1-Enabled		
Web User Interface:		
None		
Phone User Interface:		
None		

To configure server redundancy for fallback purpose via web user interface:

1. Click on **Account->Register**.
2. Configure registration parameters of the account in the corresponding fields.
3. Select the desired value from the pull-down list of **Transport**.
4. Configure parameters of SIP server 1 and SIP server 2 in the corresponding fields.

The screenshot displays the Yealink CP860 web interface for configuring a SIP account. The 'Register' tab is active, showing various registration parameters. The 'Transport' dropdown is set to 'UDP' and is highlighted with a red box. Below it, the 'SIP Server 1' and 'SIP Server 2' sections are also highlighted with red boxes, showing fields for Server Host, Server Expires, and Server Retry Counts. The 'SIP Server 1' section has values: 192.168.1.14, 3600, and 3. The 'SIP Server 2' section has values: 192.168.1.15, 3600, and 3. A 'NOTE' section on the right explains the fields. The bottom of the page shows 'Confirm' and 'Cancel' buttons.

5. Click **Confirm** to accept the change.

To configure server redundancy for failover purpose via web user interface:

1. Click on **Account->Register**.
2. Configure registration parameters of the account in the corresponding fields.
3. Select **DNS-NAPTR** from the pull-down list of **Transport**.

- Configure parameters of the SIP server 1 or SIP server 2 in the corresponding fields.

You must set the port of SIP server to 0 for NAPTR, SRV and A queries.

The screenshot shows the Yealink CP860 web interface with the 'Account' tab selected. The 'Register' section is active, showing various configuration fields. The 'Transport' field is set to 'DNS-NAPTR' and is highlighted with a red box. Below it, the 'SIP Server 1' section is also highlighted with a red box, showing 'Server Host' as 'yealink.pbx.com' and 'Port' as '0'. Other fields like 'Line Active', 'Label', 'Display Name', 'Register Name', 'User Name', 'Password', 'Enable Outbound Proxy Server', 'Outbound Proxy Server', 'NAT', and 'STUN Server' are also visible. A 'NOTE' section on the right provides additional information about the fields.

- Click **Confirm** to accept the change.

Note

If the outbound proxy server is required and the transport is set to DNS-NAPTR, you must set the port of outbound proxy server to 0 for NAPTR, SRV and A queries.

SIP Server Domain Name Resolution

If a domain name is configured for a SIP server, the IP address(es) associated with that domain name will be discovered through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs the NAPTR query for the SRV pointer and transport protocol (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.

If an explicit port (except 0) is specified and the transport type is set to DNS-NAPTR, A query will be performed only. If a SIP server port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.

The following details the procedures of DNS query for the IP phone to resolve the domain name (e.g., yealink.pbx.com) of working server into the IP address, port and transport protocol.

NAPTR (Naming Authority Pointer)

First, the IP phone sends the NAPTR query to get the SRV pointer and transport protocol.

Example of NAPTR records:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.yealink.pbx.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
order	Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is MORE preferred.
pref	Specify the preference for processing multiple NAPTR records with the same order value. Lower value is MORE preferred.
flags	The flag "s" means to perform an SRV lookup.
service	Specify the transport protocols supported by the domain server: SIP+D2U: SIP over UDP SIP+D2T: SIP over TCP SIP+D2S: SIP over SCTP SIPS+D2T: SIPS over TCP
regexp	Always empty for SIP services.
replacement	Specify a domain name for the next query.

The IP phone picks the first record, because its order of 90 is lower than 100. The pref parameter is unimportant as there is no other record with order 90. The flag "s" indicates performing the SRV query next. TCP will be used, targeted to a host determined by an SRV query of "_sip._tcp.yealink.pbx.com". If the flag of the NAPTR record returned is empty, the IP phone will perform the NAPTR query again according to the previous NAPTR query result.

SRV (Service Location Record)

The IP phone performs a SRV query on the record returned from the NAPTR for the host name and the port number. Example of SRV records:

	Priority	Weight	Port	Target
IN SRV	0	1	5060	server1.yealink.pbx.com
IN SRV	0	2	5060	server2.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
Priority	Specify preferential treatment for the specific host entry. Lower priority is MORE preferred.
Weight	When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Keep the same to load balance.
Port	Identify the port number to be used.
Target	Identify the actual host for an A query.

SRV query returns two records. The two SRV records point to different hosts and have the same priority 0. The weight of the second record is higher than the first one, so the second record will be picked first. The two records also contain a port "5060", the IP phone uses this port. If the Target is not a numeric IP address, the IP phone performs the A query. So in this case, the IP phone uses "server1.yealink.pbx.com" and "server2.yealink.pbx.com" for the A query.

A (Host IP Address)

The IP phone performs A query for the IP address of each target host name. Example of A records:

Server1.yealink.pbx.com IN A 192.168.1.13

Server2.yealink.pbx.com IN A 192.168.1.14

The IP phone picks the IP address "192.168.1.14" first.

Outgoing Call When the Working Server Connection Fails

When a user initiates a call, the IP phone will go through the following steps to connect the call:

1. Sends the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE, then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the IP phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection or the send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261.

If it is not the last server in the list, the maximum number of retries depends on the configured retry count.

Procedure

SIP Server Domain Name Resolution can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the transport type on the IP phone. Parameters: account.X.transport account.X.naptr_build
Local	Web User Interface	Configure the transport type on the IP phone. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.transport (X = 1)	Integer	0
Description: Configures the type of transport protocol. 0-UDP 1-TCP 2-TLS 3-DNS-NAPTR If the parameter is set to 3 (DNS-NAPTR) and no server port is given, the IP phone performs the DNS NAPTR and SRV queries for the service type and port. Web User Interface: Account->Register->Transport Phone User Interface: None		
account.X.naptr_build (X = 1)	0 or 1	0

Parameters	Permitted Values	Default
Description: Configures the way of SRV query for the IP phone to be performed when no result is returned from NAPTR query. 0 -SRV query using UDP only 1 -SRV query using UDP, TCP and TLS. Web User Interface: None Phone User Interface: None		

Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the SIP server is resolved to multiple IP addresses. If the IP phone is not configured with a DNS server, or the DNS query returns no result from a DNS server, you can configure a set of DNS NAPTR/SRV/A records into the IP phone. The IP phone will attempt to resolve the domain name of the SIP server with static DNS cache.

When the IP phone is configured with a DNS server, the IP phone will behave as follows to resolve domain name of the SIP server:

- The IP phone performs a DNS query to resolve the domain name from the DNS server.
- If the DNS query returns no results for the domain name, or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
- If the configured time interval is elapsed, the IP phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the IP phone will use the returned record and ignore the statically configured cache values.

When the IP phone is not configured with a DNS server, it will behave as follow:

- The IP phone attempts to resolve the domain name within the static DNS cache.
- The IP phone will always use the results returned from the static DNS cache.

IP phones can be configured to use static DNS cache preferentially. Static DNS cache is configurable on a per-line basis.

Procedure

Static DNS cache can be configured only using the configuration files.

Configuration File	<MAC>.cfg	<p>Configure NAPTR/SRV/A records.</p> <p>Parameters:</p> <p>account.X.dns_cache_naptr.Y.name account.X.dns_cache_naptr.Y.flags account.X.dns_cache_naptr.Y.order account.X.dns_cache_naptr.Y.preference account.X.dns_cache_naptr.Y.replace account.X.dns_cache_naptr.Y.service account.X.dns_cache_naptr.Y.ttl account.X.dns_cache_srv.Y.name account.X.dns_cache_srv.Y.port account.X.dns_cache_srv.Y.priority account.X.dns_cache_srv.Y.target account.X.dns_cache_srv.Y.weight account.X.dns_cache_srv.Y.ttl account.X.dns_cache_a.Y.name account.X.dns_cache_a.Y.ip account.X.dns_cache_a.Y.ttl</p> <p>Configure the IP phone whether to cache the additional DNS records.</p> <p>Parameter:</p> <p>account.X.dns_cache_type</p> <p>Configure the IP phone whether to use static DNS cache preferentially.</p> <p>Parameter:</p> <p>account.X.static_cache_pri</p>
---------------------------	-----------	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.dns_cache_naptr.Y.name (X= 1, Y ranges from 1 to 12)	String within 256 characters	Blank
<p>Description:</p> <p>Configures the domain name to which NAPTR record Y refers.</p> <p>Example:</p>		

Parameters	Permitted Values	Default
<p>account.1.dns_cache_naptr.1.name = yealink.pbx.com</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
<p>account.X.dns_cache_naptr.Y.flags (X= 1, Y ranges from 1 to 12)</p>	S, A, U or P	Blank
<p>Description:</p> <p>Configures the flag of NAPTR record Y. (Always “s” for SIP, which means to do an SRV lookup on whatever is in the replacement field).</p> <p>S-Do an SRV lookup next.</p> <p>A-Do an A lookup next.</p> <p>U-No need to do a DNS query next.</p> <p>P-Service customized by the user</p> <p>Example:</p> <p>account.1.dns_cache_naptr.1.flags = S</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
<p>account.X.dns_cache_naptr.Y.order (X= 1, Y ranges from 1 to 12)</p>	Integer from 0 to 65535	0
<p>Description:</p> <p>Configures the order of NAPTR record Y.</p> <p>NAPTR record with lower order is more preferred.</p> <p>Example:</p> <p>account.1.dns_cache_naptr.1.order = 90</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
<p>account.X.dns_cache_naptr.Y.preference</p>	Integer from 0 to 65535	0

Parameters	Permitted Values	Default
(X= 1, Y ranges from 1 to 12)		
Description: Configures the preference of NAPTR record Y. NAPTR record with lower preference is more preferred. Example: account.X.dns_cache_naptr.Y.preference = 50 Web User Interface: None Phone User Interface: None		
account.X.dns_cache_naptr.Y.replace (X= 1, Y ranges from 1 to 12)	Domain name	Blank
Description: Configures a domain name to be used for the next SRV query in NAPTR record Y. Example: account.1.dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com Web User Interface: None Phone User Interface: None		
account.X.dns_cache_naptr.Y.service (X= 1, Y ranges from 1 to 12)	String within 32 characters	Blank
Description: Configures the transport protocol available for the SIP server in NAPTR record Y. SIP+D2U: SIP over UDP SIP+D2T: SIP over TCP SIP+D2S: SIP over SCTP SIPS+D2T: SIPS over TCP Example: account.1.dns_cache_naptr.1.service = SIP+D2T Web User Interface: None		

Parameters	Permitted Values	Default
Phone User Interface: None		
account.X.dns_cache_naptr.Y.ttl (X= 1, Y ranges from 1 to 12)	Integer from 30 to 2147483647	300
Description: Configures the time interval (in seconds) that NAPTR record Y may be cached before the record should be consulted again. Example: account.1.dns_cache_naptr.1.ttl = 300 Web User Interface: None Phone User Interface: None		
account.X.dns_cache_srv.Y.name (X= 1, Y ranges from 1 to 12)	Domain name	Blank
Description: Configures the domain name in SRV record Y. Example: account.1.dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com Web User Interface: None Phone User Interface: None		
account.X.dns_cache_srv.Y.port (X= 1, Y ranges from 1 to 12)	Integer from 0 to 65535	0
Description: Configures the port to be used in SRV record Y. Example: account.1.dns_cache_srv.1.port = 5060 Web User Interface: None		

Parameters	Permitted Values	Default
Phone User Interface: None		
account.X.dns_cache_srv.Y.priority (X= 1, Y ranges from 1 to 12)	Integer from 0 to 65535	0
Description: Configures the priority for the target host in SRV record Y. Lower priority is more preferred. Web User Interface: None Phone User Interface: None		
account.X.dns_cache_srv.Y.target (X= 1, Y ranges from 1 to 12)	Domain name	Blank
Description: Configures the domain name of the target host for an A query in SRV record Y. Example: account.1.dns_cache_srv.1.target = server1.yealink.pbx.com Web User Interface: None Phone User Interface: None		
account.X.dns_cache_srv.Y.weight (X= 1, Y ranges from 1 to 12)	Domain name	0
Description: Configures the weight of the target host in SRV record Y. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred. Example: account.1.dns_cache_srv.1.weight = 1 Web User Interface: None Phone User Interface:		

Parameters	Permitted Values	Default
None		
account.X.dns_cache_srv.Y.ttl (X= 1, Y ranges from 1 to 12)	Integer from 30 to 2147483647	300
Description: Configures the time interval (in seconds) that SRV record Y may be cached before the record should be consulted again. Example: account.1.dns_cache_srv.1.ttl = 3600 Web User Interface: None Phone User Interface: None		
account.X.dns_cache_a.Y.name (X= 1, Y ranges from 1 to 12)	Domain name	Blank
Description: Configures the domain name in A record Y. Example: account.1.dns_cache_a.1.name = yealink.pbx.com Web User Interface: None Phone User Interface: None		
account.X.dns_cache_a.Y.ip (X= 1, Y ranges from 1 to 12)	IP address	Blank
Description: Configures the IP address that the domain name in A record Y maps to. Example: account.1.dns_cache_a.1.ip = 192.168.1.13 Web User Interface: None Phone User Interface: None		

Parameters	Permitted Values	Default
account.X.dns_cache_a.Y.ttl (X= 1, Y ranges from 1 to 12)	Integer from 30 to 2147483647	300
Description: Configures the time interval (in seconds) that A record Y may be cached before the record should be consulted again. Example: account.1.dns_cache_a.1.ttl = 300 Web User Interface: None Phone User Interface: None		
account.X.dns_cache_type (X = 1)	0, 1 or 2	1
Description: Configures whether the IP phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records. 0 -Perform real-time DNS query rather than using DNS cache. 1 -Use DNS cache, but do not cache the additional DNS records. 2 -Use DNS cache and cache the additional DNS records. Example: account.1.dns_cache_type = 1 Web User Interface: None Phone User Interface: None		
account.X.static_cache_pri (X = 1)	0 or 1	0
Description: Configures whether preferentially to use the static DNS cache for domain name resolution of the SIP server. 0 -Use domain name resolution from the DNS server preferentially 1 -Use static DNS cache preferentially Example:		

Parameters	Permitted Values	Default
account.1.static_cache_pri = 1 Web User Interface: None Phone User Interface: None		

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for IP phones:

- Capabilities Discovery -- allows LLDP-MED IP phones to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify IP phones which VLAN to use and QoS-related configuration for voice data. It provides a “plug and play” network environment.
- Power Management -- provides information related to how IP phones are powered, power priority, and how much power IP phones need.
- Inventory Management -- provides a means to effectively manage IP phones and their attributes such as model number, serial number and software revision.

TLVs supported by IP phones are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the phone.
	Port ID	The MAC address of the phone.
	Time To Live	Seconds until data unit expires. The default value is 60s.

TLV Type	TLV Name	Description
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the IP phone. The default value is "yealink".
	System Description	Description of the IP phone. The default value is "yealink".
	System Capabilities	The supported and enabled phone capabilities. The supported capabilities are Bridge, Telephone and Router. The enabled capabilities are Bridge and Telephone by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex and bit rate settings of the IP phone. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the IP phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of phone.

TLV Type	TLV Name	Description
	Inventory – Firmware Revision	Firmware revision of phone.
	Inventory – Software Revision	Software revision of phone.
	Inventory – Serial Number	Serial number of phone.
	Inventory – Manufacturer Name	Manufacturer name of phone. The default value is “yealink”.
	Inventory – Model Name	Model name of phone.
	Asset ID	Assertion identifier of phone. The default value is “asset”.

Procedure

LLDP can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure LLDP feature. Parameters: network.lldp.enable network.lldp.packet_interval
Local	Web User Interface	Configure LLDP feature. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network-adv&q=load">http://<phoneIPAddress>/servlet?p=network-adv&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.lldp.enable	0 or 1	1
Description: Enables or disables LLDP feature on the IP phone. 0 -Disabled 1 -Enabled Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->LLDP->Active		

Parameters	Permitted Values	Default
Phone User Interface: None		
network.lldp.packet_interval	Integer from 1 to 3600	60
Description: Configures the interval (in seconds) for the IP phone to broadcast the LLDP request. Note: If you change this parameter, the IP phone will reboot to make the change take effect. It works only if the parameter "network.lldp.enable" is set to 1 (Enabled). Web User Interface: Network->Advanced->LLDP->Packet Interval (1~3600s) Phone User Interface: None		

To configure LLDP via web user interface:

1. Click on **Network->Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired time interval in the **Packet Interval (1~3600s)** field.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected, and the 'Advanced' sub-tab is active. The 'LLDP' section is expanded, showing the following configuration:

- LLDP:** Active (Enabled), Packet Interval (1~3600s) (60)
- VLAN:** WAN Port (Active), VID (1-4094) (1), Priority (0), DHCP VLAN (Active), Option (132)
- Port Link:** WAN Port Link (Auto Negotiate)
- Voice QoS:** Voice QoS (0~63) (46), SIP QoS (0~63) (26)
- Local RTP Port:** Max RTP Port (1~65535) (11800), Min RTP Port (1~65535) (11780)

A red box highlights the 'Active' dropdown and the 'Packet Interval' field in the LLDP section. A 'NOTE' box on the right explains VLAN and QoS settings.

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
5. Click **OK** to reboot the phone.

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

The purpose of VLAN configurations on the IP phone is to insert tag with VLAN information to the packets generated by the IP phone. When VLAN is properly configured for the internet port on the IP phone, the IP phone will tag all packets from this port with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

In addition to manual configuration, the IP phone also supports automatic discovery of VLAN via LLDP or DHCP. The assignment takes effect in this order: assignment via LLDP, manual configuration, then assignment via DHCP.

VLAN Discovery via DHCP

IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

For more information on VLAN, refer to *VLAN Feature on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

VLAN can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure VLAN for the Internet port manually. Parameters: network.vlan.internet_port_enable network.vlan.internet_port_vid network.vlan.internet_port_priority Configure DHCP VLAN discovery feature. network.vlan.dhcp_enable network.vlan.dhcp_option
Local	Web User Interface	Configure VLAN for the Internet port. Configure DHCP VLAN discovery

		feature. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network-adv&q=load">http://<phoneIPAddress>/servlet? p=network-adv&q=load
	Phone User Interface	Configure VLAN for the Internet port.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vlan.internet_port_enable	0 or 1	0
Description: Enables or disables VLAN for the Internet (WAN) port. 0 -Disabled 1 -Enabled Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->VLAN->WAN Port->Active Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin)->Network->VLAN->WAN Port->VLAN Status		
network.vlan.internet_port_vid	Integer from 1 to 4094	1
Description: Configures VLAN ID for the Internet (WAN) port. Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->VLAN ->WAN Port->VID (1-4094) Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->VLAN ->WAN Port-> VID		
network.vlan.internet_port_priority	Integer from 0 to 7	0
Description: Configures VLAN priority for the Internet (WAN) port. 7 is the highest priority, 0 is the lowest priority.		

Parameters	Permitted Values	Default
<p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->VLAN ->WAN Port->Priority</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->VLAN ->WAN Port-> Priority</p>		
network.vlan.dhcp_enable	0 or 1	1
<p>Description: Enables or disables DHCP VLAN discovery feature on the IP phone.</p> <p>0-Disabled 1-Enabled</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->VLAN->DHCP VLAN->Active</p> <p>Phone User Interface: None</p>		
network.vlan.dhcp_option	Integer from 128 to 254	132
<p>Description: Configures the DHCP option from which the IP phone will obtain the VLAN settings. You can configure at most five DHCP options and separate them by commas.</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->VLAN->DHCP VLAN->Option</p> <p>Phone User Interface: None</p>		

To configure VLAN for Internet port via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **WAN Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.

4. Select the desired value (0-7) from the pull-down list of **Priority**.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Network' tab is selected. On the left, 'Basic' and 'Advanced' are listed, with 'Advanced' being the active view. The main content area is titled 'VLAN' and contains several configuration sections:

- LLDP**: Active (Enabled), Packet Interval (1~3600s) (60).
- VLAN**: WAN Port (Active, Enabled), VID (1-4094) (71), Priority (1). This section is highlighted with a red box.
- DHCP VLAN**: Active (Enabled), Option (132).
- Port Link**: WAN Port Link (Auto Negotiate).
- Voice QoS**: Voice QoS (0~63) (46), SIP QoS (0~63) (26).
- Local RTP Port**: Max RTP Port (1~65535) (11800), Min RTP Port (1~65535) (11780).
- SNMP**: Active (Disabled), Port (1~65535) (161), Trustring Address (empty).

On the right, a 'NOTE' section explains VLAN and QoS concepts. A 'Log Out' link is in the top right corner.

5. Click **Confirm** to accept the change.
A dialog box pops up to prompt reboot to make the settings effective.
6. Click **OK** to reboot the phone.

To configure the DHCP VLAN discovery via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **DHCP VLAN Active**.
3. Enter the desired option in the **Option** field.

The default option is 132.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected, and the 'VLAN' configuration page is displayed. Under the 'VLAN' section, the 'DHCP VLAN' is configured with 'Active' status, 'Enabled' for the 'Active' dropdown, and '132' for the 'Option' field. This section is highlighted with a red rectangle. Other visible settings include LLDP (Active, Enabled), WAN Port (Active, Enabled, VID 71, Priority 1), Port Link (Auto Negotiate), Voice QoS (Voice QoS 46, SIP QoS 26), Local RTP Port (Max 11800, Min 11780), and SNMP (Disabled, Port 161). A 'NOTE' box on the right provides definitions for VLAN, QoS, and Local RTP Port.

- Click **Confirm** to accept the change.

A dialog box pops up to prompt that settings will take effect after reboot.

- Click **OK** to reboot the phone.

To configure VLAN for Internet port via phone user interface:

- Press **Menu->Settings->Advanced Settings** (Default password: admin) **->Network->VLAN->WAN Port**.
- Press the ◀ or ▶ soft key to select the desired value from the **VLAN Status** field.
- Enter the VLAN ID (1-4094) in the **VID** field.
- Enter the priority value (0-7) in the **Priority** field.
- Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. VPN has become more prevalent due to the benefits of scalability, reliability, convenience and security. VPN provides remote offices or individual users with secure access to their organization's network. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together).

Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can be also classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

IP phones support SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities, designed to work with the TUN/TAP virtual networking interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection, while TUN simulates a network layer device and provides a virtual network segment. IP phones use OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the IP phone, the IP phone acts as a VPN client and uses the certificates to authenticate the VPN server.

To use VPN, the compressed package of VPN-related files should be uploaded to the IP phone in advance. The file format of the compressed package must be *.tar. The VPN-related files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information on how to package a TAR file, refer to *OpenVPN Feature on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

VPN can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the OpenVPN feature and upload a TAR file to the IP phone. Parameters: network.vpn_enable openvpn.url
	Web User Interface	Configure VPN feature and upload a TAR package to the IP phone. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network-adv&q=load">http://<phoneIPAddress>/servlet?p=network-adv&q=load
Local	Phone User Interface	Configure VPN feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.vpn_enable	0 or 1	0
Description: Enables or disables OpenVPN feature on the IP phone. 0 -Disabled 1 -Enabled Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->VPN->Active Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->VPN->VPN Active		
openvpn.url	URL within 511 characters	Blank
Description: Configures the access URL of the *.tar file for OpenVPN. Example: openvpn.url = http://192.168.10.25/OpenVPN.tar Web User Interface: Network->Advanced->VPN->Upload VPN Config Phone User Interface: None		

To upload the tar file to the phone and configure VPN via web user interface:

1. Click on **Network->Advanced**.
2. Click **Browse** to locate the TAR package from the local system.

3. Click **Upload** to upload the TAR file.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected. Under the 'VPN' section, the 'Active' dropdown is set to 'Enabled'. The 'Upload VPN Config' field contains the text 'C:\fakepath\OpenVPN.t', and there is an 'Upload' button next to it. A red box highlights this section. Other settings visible include LLDP (Active: Enabled), VLAN (WAN Port: Active, VID: 1, Priority: 0), and DHCP VLAN (Active: Enabled, Option: 132). A 'NOTE' section on the right explains VLAN and QoS. At the bottom, there are 'Confirm' and 'Cancel' buttons.

The web user interface prompts the message “Import config...”.

4. In the **VPN** block, select the desired value from the pull-down list of **Active**.
5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that settings will take effect after reboot.

6. Click **OK** to reboot the phone.

To configure VPN via phone user interface after uploading the tar file:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin) **->Network->VPN**.

2. Press to select the desired value from the **VPN Active** field.

You must upload the OpenVPN TAR file using configuration files or via web user interface in advance.

3. Press the **Save** soft key to accept the change.

The IP phone reboots automatically to make settings effective after a period of time.

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements. QoS guarantees are important for applications that require fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to

be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in the IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** – backwards compatible with IP precedence. Class Selector code points are of the form “xxx000”. The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** – the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** – defines a method by which BAs (Bandwidth Allocations) can be given different forwarding assurances.
- **Default PHB** – specifies that a packet marked with a DSCP value of “000000” gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth- and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic not to be delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. IP phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

SIP protocol is used for creating, modifying and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from IP phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

Procedure

DSCPs for voice packets and SIP packets can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the DSCPs for voice packets and SIP packets. Parameters: network.qos.rtplos network.qos.signallos
Local	Web User Interface	Configure the DSCPs for voice packets and SIP packets. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.qos.rtplos	Integer from 0 to 63	46
Description: Configures the DSCP for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->Voice QoS (0~63) Phone User Interface:		

Parameters	Permitted Values	Default
None		
network.qos.signalto	Integer from 0 to 63	26
<p>Description:</p> <p>Configures the DSCP for SIP packets.</p> <p>The default DSCP value for SIP packets is 26 (Assured Forwarding).</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Advanced->SIP QoS (0~63)</p> <p>Phone User Interface:</p> <p>None</p>		

To configure DSCPs for voice packets and SIP packets via web user interface:

1. Click on **Network->Advanced**.
2. Enter the desired value in the **Voice QoS (0~63)** field.
3. Enter the desired value in the **SIP QoS (0~63)** field.

The screenshot shows the Yealink CP860 web interface. The 'Network' tab is selected, and the 'Advanced' sub-tab is active. In the 'Voice QoS' section, the 'Voice QoS (0~63)' field is set to 46 and the 'SIP QoS (0~63)' field is set to 26. A red box highlights these two fields. Other settings visible include LLDP (Active, Enabled), VLAN (Active, Disabled), DHCP VLAN (Active, Enabled), Port Link (WAN Port Link, Auto Negotiate), Local RTP Port (Max RTP Port: 11800, Min RTP Port: 11780), and SNMP (Active, Disabled).

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
5. Click **OK** to reboot the phone.

Network Address Translation

Network Address Translation (NAT) is essentially a translation table that maps public IP address and port combinations to private ones. This reduces the need for a large number of public IP addresses. The NAT feature ensures security since each outgoing or incoming request must first go through a translation process. But in the VoIP environment, NAT breaks end-to-end connectivity.

NAT Traversal

NAT traversal is a general term for techniques that establish and maintain IP connections traversing NAT gateways, typically required for client-to-client networking applications, especially for VoIP deployments. STUN is one of the NAT traversal techniques supported by IP phones.

STUN (Simple Traversal of UDP over NATs)

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows applications to operate behind a NAT to discover the presence of the network address translator, and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to act as a STUN client, sending exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client.

Procedure

NAT traversal and STUN server can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure NAT traversal and STUN server on the IP phone. Parameters: account.X.nat.nat_traversal account.X.nat.stun_server account.X.nat.stun_port
Local	Web User Interface	Configure NAT traversal and STUN server on the IP phone. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.nat.nat_traversal (X = 1)	0 or 1	0
Description: Enables or disables the NAT traversal. 0-Disabled 1-Enabled Web User Interface: Account->Register->NAT Phone User Interface: None		
account.X.nat.stun_server (X = 1)	IP address or domain name	Blank
Description: Configures the IP address or the domain name of the STUN server. Example: account.1.nat.stun_server = 218.107.220.201 Web User Interface: Account->Register->STUN Server Phone User Interface: None		
account.X.nat.stun_port (X = 1)	Integer from 1024 to 65000	3478
Description: Configures the port of the STUN server. Example: account.1.nat.stun_port = 3478 Web User Interface: Account->Register->STUN Server->Port Phone User Interface: None		

To configure the NAT traversal and STUN server via web user interface:

1. Click on **Account**.
2. Select **STUN** from the pull-down list of **NAT**.
3. Enter the IP address or the domain name in the **STUN Server** field.

The screenshot shows the Yealink CP860 web interface with the 'Account' tab selected. The 'NAT' dropdown menu is set to 'STUN', and the 'STUN Server' field is highlighted with a red box. The 'STUN Server' field contains the IP address '192.168.1.30' and the 'Port' is set to '3478'. Other fields include 'Register Status' (Registered), 'Line Active' (Enabled), 'Label' (6006), 'Display Name' (6006), 'Register Name' (6006), 'User Name' (6006), 'Password' (*****), 'Enable Outbound Proxy Server' (Disabled), 'Outbound Proxy Server' (Port 5060), 'Transport' (UDP), 'SIP Server 1' (Server Host: 10.2.1.199, Port: 5060, Server Expires: 3600, Server Retry Counts: 3), and 'SIP Server 2' (Server Host: , Port: 5060, Server Expires: 3600, Server Retry Counts: 3). A 'NOTE' section on the right provides information about 'Display Name', 'Register Name', 'User Name', and 'NAT Traversal'.

4. Click **Confirm** to accept the change.

SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration, and can then be queried by the managing applications. The variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs).

IP phones only support SNMPv1 and SNMPv2. They act as SNMP clients, receiving requests from the SNMP server. The SNMP server may send requests from any available source port to the configured port on the client, while the client responds to the source port on the SNMP server. IP phones only support the GET request from the SNMP server.

The following table lists the basic object identifiers (OIDs) supported by IP phones:

MIB	OID	Description
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.1.0	The textual identification of the contact

MIB	OID	Description
		person for the IP phone, together with the contact information. For example, Sysadmin (root@localhost)
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.2.0	An administratively-assigned name for the IP phone. If the name is unknown, the value is a zero-length string.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.3.0	The physical location of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.4.0	The time (in milliseconds) since the network management portion of the system was last re-initialized.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.5.0	The firmware version of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.6.0	The hardware version of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.7.0	The IP phone's model.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.8.0	The MAC address of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.9.0	The IP address of the IP phone.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.10.0	The target version to which the current version is automatically updated. Format: MacVersion[*]ComVersion[*] For example, MacVersion[0.0.0.1]ComVersion[0.0.0.1]
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.11.0	The command of phone reboot. Format (XXXX is replaced by the IP address of phone): snmpset -v 2c XXXX public 37459.2.1.11.0 s reboot

Procedure

SNMP can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure SNMP on the IP phone. Parameters: network.snmp.enable network.snmp.port network.snmp.trust_ip
---------------------------	-------------------	--

Local	Web User Interface	Configure SNMP. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=network-adv&q=load">http://<phoneIPAddress>/servlet?p=network-adv&q=load
--------------	--------------------	---

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.snmp.enable	0 or 1	0
Description: Enables or disables SNMP feature on the IP phone. 0-Disabled 1-Enabled Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->SNMP->Active Phone User Interface: None		
network.snmp.port	1 to 65535	161
Description: Specifies the port used for SNMP communication. Example: network.snmp.port = 1008 Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Advanced->SNMP->Port (1~65535) Phone User Interface: None		
network.snmp.trust_ip	At most 255 characters	Blank
Description: Specifies the SNMP server addresses from which GET requests will be accepted. You can specify one or more addresses. Multiple addresses are separated by space.		

Parameters	Permitted Values	Default
<p>If it is set to "0.0.0.0", the IP phone can accept and handle GET requests from any IP address.</p> <p>If it is left blank, the IP phone cannot receive or handle any GET request.</p> <p>Example:</p> <p>network.snmp.trust_ip = 192.168.1.50 as.manager.com</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Advanced->SNMP->Trusted Address</p> <p>Phone User Interface:</p> <p>None</p>		

To configure SNMP via web user interface:

1. Click on **Network->Advanced**.
2. In the **SNMP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired port in the **Port** field.
4. Enter IP address(es) (IPv4 or IPv6) or domain name of the SNMP server in the **Trusted Address** field.

Multiple addresses are separated by space.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The 'Network' tab is selected, and the 'Advanced' sub-tab is active. The 'SNMP' configuration section is highlighted with a red box. It contains the following fields:

- Active:** A dropdown menu with 'Enabled' selected.
- Port (1~65535):** A text input field containing '161'.
- Trusted Address:** A text input field containing '0.0.0.0'.

Other visible configuration sections include:

- LLDP:** 'Active' (Enabled), 'Packet Interval (1~3600s)' (60).
- VLAN:** 'WAN Port' (Disabled), 'VID (1~4094)' (1), 'Priority' (0), 'DHCP VLAN' (Enabled), 'Option' (132).
- Local RTP Port:** 'Max RTP Port (1~65535)' (11800), 'Min RTP Port (1~65535)' (11780).
- Web Server:** 'HTTP' (Enabled), 'HTTP Port (1~65535)' (80), 'HTTPS' (Enabled), 'HTTPS Port (1~65535)' (443).

Buttons for 'Confirm' and 'Cancel' are at the bottom. A 'NOTE' sidebar on the right explains VLAN and QoS concepts.

5. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
6. Click **OK** to reboot the IP phone.

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN. The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the IP phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the IP phone provides credentials, such as user name and password, for the authenticator, and then the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the IP phone is allowed to access resources located on the protected side of the network.

IP phones support protocols EAP-MD5, EAP-TLS, PEAP-MSCHAPv2 and EAP-TTLS/EAP-MSCHAPv2 for 802.1X authentication.

For more information on 802.1X authentication, refer to *Yealink 802.1X Authentication*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

802.1X authentication can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the 802.1X authentication. Parameters: network.802_1x.mode network.802_1x.identity network.802_1x.md5_password network.802_1x.root_cert_url network.802_1x.client_cert_url
Local	Web User Interface	Configure the 802.1X authentication. Navigate to: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1X authentication.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.802_1x.mode	0, 1, 2, 3 or 4	0
<p>Description: Configures the 802.1x authentication method.</p> <p>0-Disabled 1-EAP-MD5 2-EAP-TLS 3-PEAP-MSCHAPv2 4-EAP-TTLS/EAP-MSCHAPv2</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->802.1x->802.1x Mode</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->802.1x Settings->802.1x Mode</p>		
network.802_1x.identity	String within 32 characters	Blank
<p>Description: Configures the user name for 802.1x authentication.</p> <p>Example: network.802_1x.identity = admin</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface: Network->Advanced->802.1x->Identity</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->802.1x Settings->802.1x Mode->Identity</p>		
network.802_1x.md5_password	String within 32 characters	Blank
<p>Description: Configures the password for 802.1x authentication.</p> <p>Example: network.802_1x.md5_password = admin123</p>		

Parameters	Permitted Values	Default
<p>Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is required for all 802.1x authentication methods except EAP-TLS.</p> <p>Web User Interface: Network->Advanced->802.1x->MD5 Password</p> <p>Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->802.1x Settings->MD5 Password</p>		
network.802_1x.root_cert_url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the CA certificate when the 802.1x authentication method is configured as EAP-TLS, PEAP-MSCHAPv2 or EAP-TTLS/EAP-MSCHAPv2.</p> <p>Example : network.802_1x.root_cert_url = http://192.168.1.10/ca.pem</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to EAP-TLS, PEAP-MSCHAPv2 and EAP-TTLS/EAP-MSCHAPv2 protocols. The format of the certificate must be *.pem, *.crt, *.cer or *.der.</p> <p>Web User Interface: Network->Advanced->802.1x->CA Certificates</p> <p>Phone User Interface: None</p>		
network.802_1x.client_cert_url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the device certificate when the 802.1x authentication method is configured as EAP-TLS.</p> <p>Example: network.802_1x.client_cert_url = http://192.168.1.10/ client.pem</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to the EAP-TLS protocol. The format of the certificate must be *.pem or *.cer.</p> <p>Web User Interface: Network->Advanced->802.1x->Device Certificates</p> <p>Phone User Interface: None</p>		

To configure the 802.1X via web user interface:

1. Click on **Network->Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **802.1x Mode**.
 - a) If you select **EAP-MD5**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **MD5 Password** field.

The screenshot shows the Yealink CP860 web interface with the 'Network' tab selected and the 'Advanced' sub-tab active. The '802.1x' configuration section is highlighted with a red box. The '802.1x Mode' dropdown is set to 'EAP-MD5'. The 'Identity' text field contains the value 'yealink'. The 'MD5 Password' text field is masked with dots. Below the '802.1x' section, there are fields for 'CA Certificates' and 'Device Certificates', each with an 'Upload' button and a 'Browse...' link. The 'VPN' section is also visible at the bottom of the configuration area.

- b) If you select **EAP-TLS**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Leave the **MD5 Password** field blank.
 - 3) In the **CA Certificates** field, click **Browse** to locate the desired CA certificate (*.pem, *.cert, *.cer or *.der) from your local system.
 - 4) In the **Device Certificates** field, click **Browse** to locate the desired client certificate (*.pem or *.cer) from your local system.

- 5) Click **Upload** to upload the certificates.

The screenshot shows the Yealink CP860 Network configuration page. The 'Network' tab is selected. The '802.1x' section is expanded, and the '802.1x Mode' is set to 'EAP-TLS'. The 'Identity' field contains 'yealink'. The 'MD5 Password' field is empty. The 'CA Certificates' field shows a file path 'C:\fakepath\ca.crt' and an 'Upload' button. The 'Device Certificates' field shows a file path 'C:\fakepath\client.pem' and an 'Upload' button. A red box highlights the 802.1x configuration section.

- c) If you select **PEAP-MSCHAPv2**:

- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the **MD5 Password** field.
- 3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem, *.crt, *.cer or *.der) from your local system.
- 4) Click **Upload** to upload the certificate.

The screenshot shows the Yealink CP860 Network configuration page. The 'Network' tab is selected. The '802.1x' section is expanded, and the '802.1x Mode' is set to 'PEAP-MSCHAPv2'. The 'Identity' field contains 'yealink'. The 'MD5 Password' field contains '*****'. The 'CA Certificates' field shows a file path 'C:\fakepath\ca.crt' and an 'Upload' button. The 'Device Certificates' field shows a file path 'C:\fakepath\client.pem' and an 'Upload' button. A red box highlights the 802.1x configuration section.

- d) If you select **EAP-TTLS/EAP-MSCHAPv2**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **MD5 Password** field.
 - 3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem, *.crt, *.cer or *.der) from your local system.
 - 4) Click **Upload** to upload the certificate.

The screenshot displays the Yealink CP860 web interface. The 'Network' tab is selected, and the '802.1x' configuration section is active. The '802.1x Mode' is set to 'EAP-TTLS/EAP-MSCHAPv2'. The 'Identity' field is filled with 'yealink', and the 'MD5 Password' field is masked with '*****'. The 'CA Certificates' field shows a file path 'C:\Vakepath\ca.crt' and an 'Upload' button. The 'Device Certificates' field also has an 'Upload' button. The page includes a sidebar with 'Basic' and 'Advanced' sections, and a 'NOTE' box on the right explaining VLAN, QoS, and Local RTP Port.

3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
4. Click **OK** to reboot the phone.

To configure the 802.1X via phone user interface after:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin)
->**Network->802.1x Settings**.
2. Press the ◀ or ▶ soft key to select the desired value from the **802.1x Mode** field.
 - a) If you select **EAP-MD5**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **MD5 Password** field.
 - b) If you select **EAP-TLS**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Leave the **MD5 Password** field blank.
 - c) If you select **PEAP-MSCHAPv2**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **MD5 Password** field.

- d) If you select **EAP-TLS/EAP-MSCHAPv2**:
 - 1) Enter the user name for authentication in the **Identity** field.
 - 2) Enter the password for authentication in the **MD5 Password** field.
 3. Click **Save** to accept the change.
- The IP phone reboots automatically to make the settings effective after a period of time.

TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

TR-069 is intended to support a variety of functionalities to manage a collection of CPEs, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software or firmware image management
- Status and performance monitoring
- Diagnostics

The following table provides a description of RPC methods supported by IP phones.

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.

RPC Method	Description
Download	<p>This method is used to cause the CPE to download a specified file from the designated location.</p> <p>File types supported by IP phones are:</p> <ul style="list-style-type: none"> • Firmware Image • Configuration File
Upload	<p>This method is used to cause the CPE to upload a specified file to the designated location.</p> <p>File types supported by IP phones are:</p> <ul style="list-style-type: none"> • Configuration File • Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

For more information on TR-069, refer to *Yealink TR-069 Technote*, available online:
<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Procedure

TR-069 can be configured using the configuration files or locally.

Configuration File	y0000000000037.cfg	<p>Configure the TR-069 feature.</p> <p>Parameters:</p> <p>managementserver.enable</p> <p>managementserver.username</p> <p>managementserver.password</p> <p>managementserver.url</p> <p>managementserver.connection_request_username</p> <p>managementserver.connection_request_password</p> <p>managementserver.periodic_inform_enable</p>
---------------------------	--------------------	--

		managementserver.periodic_inform_interval
Local	Web User Interface	<p>Configure the TR-069 feature.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-preference&q=load</p>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
managementserver.enable	0 or 1	0
<p>Description:</p> <p>Enables or disables TR-069 feature.</p> <p>0-Disabled 1-Enabled</p> <p>Web User Interface:</p> <p>Settings->TR069->Enable TR069</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.username	String within 128 characters	Blank
<p>Description:</p> <p>Configures the user name for the IP phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is required.</p> <p>Example:</p> <p>managementserver.username = user1</p> <p>Web User Interface:</p> <p>Settings->TR069->ACS Username</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.password	String within 64 characters	Blank
<p>Description:</p> <p>Configures the password for the IP phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is</p>		

Parameters	Permitted Values	Default
<p>required.</p> <p>Example:</p> <p>managementserver.password = pwd123</p> <p>Web User Interface:</p> <p>Settings->TR069->ACS Password</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.url	URL within 511 characters	Blank
<p>Description:</p> <p>Configures the access URL of the ACS (Auto Configuration Servers).</p> <p>Example:</p> <p>managementserver.url = http://192.168.1.20/acs/</p> <p>Web User Interface:</p> <p>Settings->TR069->ACS URL</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.connection_request_username	String within 128 characters	Blank
<p>Description:</p> <p>Configures the user name for the IP phone to authenticate the incoming connection requests.</p> <p>Example:</p> <p>managementserver.connection_request_username = accuser</p> <p>Web User Interface:</p> <p>Settings->TR069->Connection Request Username</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.connection_request_password	String within 64 characters	Blank
<p>Description:</p>		

Parameters	Permitted Values	Default
<p>Configures the password for the IP phone to authenticate the incoming connection requests.</p> <p>Example:</p> <p>managementserver.connection_request_password = acspwd</p> <p>Web User Interface:</p> <p>Settings->TR069->Connection Request Password</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.periodic_inform_enable	0 or 1	1
<p>Description:</p> <p>Enables or disables the IP phone to periodically report its configuration information to the ACS (Auto Configuration Servers).</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>Web User Interface:</p> <p>Settings->TR069->Enable Periodic Inform</p> <p>Phone User Interface:</p> <p>None</p>		
managementserver.periodic_inform_interval	Integer from 5 to 4294967295	60
<p>Description:</p> <p>Configures the interval (in seconds) for the IP phone to report its configuration to the ACS (Auto Configuration Servers).</p> <p>Web User Interface:</p> <p>Settings->TR069->Periodic Inform Interval (seconds)</p> <p>Phone User Interface:</p> <p>None</p>		

To configure TR-069 via web user interface:

1. Click on **Settings->TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the user name and password authenticated by the ACS in the **ACS Username** and **ACS Password** fields.

4. Enter the URL of the ACS in the **ACS URL** field.
5. Select the desired value from the pull-down list of **Enable Periodic Inform**.
6. Enter the desired time in the **Periodic Inform Interval (seconds)** field.
7. Enter the user name and password authenticated by the IP phone in the **Connection Request Username** and **Connection Request Password** fields.

8. Click **Confirm** to accept the change.

IPv6 Support

IPv6 is the next generation network layer protocol, designed as a replacement for the current IPv4 protocol. IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons. VoIP network based on IPv6 can ensure QoS, a set of service requirements to deliver performance guarantee while transporting traffic over the network.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the IP phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC):** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the IP phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the IP phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IP phone to configure itself with IPv6 address, as specified in RFC 4862.

Procedure

IPv6 can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the IPv6 address assignment method. Parameters: network.ip_address_mode network.ipv6_internet_port.type network.ipv6_internet_port.ip network.ipv6_prefix network.ipv6_internet_port.gateway network.ipv6_primary_dns network.ipv6_secondary_dns network.ipv6_static_dns_enable
Local	Web User Interface	Configure the IPv6 address assignment method. Navigate to: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure the IPv6 address assignment method.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.ip_address_mode	0, 1 or 2	0
Description: Configures the IP address mode. 0-IPv4 1-IPv6 2-IPv4&IPv6 Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Network->Basic->Internet Port->Mode (IPv4/IPv6) Phone User Interface: Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN		

Parameters	Permitted Values	Default
Port->IP Mode		
network.ipv6_internet_port.type	0 or 1	0
<p>Description:</p> <p>Configures the Internet (WAN) port type for IPv6 when the IP address mode is configured as IPv6 or IPv4&IPv6.</p> <p>0-DHCP</p> <p>1-Static IP Address</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin) ->Network->WAN Port->IPv6</p>		
network.ipv6_static_dns_enable	0 or 1	0
<p>Description:</p> <p>Enables or disables the IP phone to use manually configured static IPv6 DNS when Internet (WAN) port type for IPv6 is configured as DHCP.</p> <p>0-Disabled</p> <p>1-Enabled</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->IPv6 Static DNS</p> <p>Phone User Interface:</p> <p>None</p>		
network.ipv6_internet_port.ip	IPv6 address	Blank
<p>Description:</p> <p>Configures the IPv6 address when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address.</p> <p>Example:</p> <p>network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take</p>		

Parameters	Permitted Values	Default
<p>effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->Static IP Address->IP Address</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 Address</p>		
network.ipv6_prefix	Integer from 0 to 128	64
<p>Description:</p> <p>Configures the IPv6 prefix when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address.</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->Static IP Address->IPv6 Prefix (0~128)</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv6->Static IPv6 Client->Prefix</p>		
network.ipv6_internet_port.gateway	IPv6 address	Blank
<p>Description:</p> <p>Configures the IPv6 default gateway when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address.</p> <p>Example:</p> <p>network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->Static IP Address->Gateway</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv6-> Static IPv6 Client->Default Gateway</p>		
network.ipv6_primary_dns	IPv6 address	Blank

Parameters	Permitted Values	Default
<p>Description:</p> <p>Configures the primary IPv6 DNS server when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address.</p> <p>Example:</p> <p>network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->Static IP Address->Primary DNS</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv6->Static IPv6 Client->Primary DNS</p>		
network.ipv6_secondary_dns	IPv6 address	Blank
<p>Description:</p> <p>Configures the secondary IPv6 DNS server when the IP address mode is configured as IPv6 or IPv4&IPv6, and the Internet (WAN) port type for IPv6 is configured as Static IP Address.</p> <p>Example:</p> <p>network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Network->Basic->IPv6 Config->Static IP Address->Secondary DNS</p> <p>Phone User Interface:</p> <p>Menu->Settings->Advanced Settings (Default password: admin)->Network->WAN Port->IPv6->Static IPv6 Client ->Secondary DNS</p>		

To configure IPv6 address assignment method via web user interface:

1. Click on **Network->Basic**.
2. Select the desired address mode (IPv6 or IPv4&IPv6) from the pull-down list of **Mode (IPv4/IPv6)**.

3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP Address** radio box.
 - If you mark the **Static IP Address** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.

The screenshot shows the 'Network' configuration page for a Yealink CP860 device. The 'Internet Port' mode is set to 'IPv4 & IPv6'. Under 'IPv4 Config', 'DHCP' is selected. Under 'IPv6 Config', 'Static IP Address' is selected and highlighted with a red box. The fields for IPv6 Static IP are filled with: IP Address: 2005:1:1:1::12, IPv6 Prefix(0~128): 64, Gateway: 2005:1:1:1::1, IPv6 Static DNS: On, Primary DNS: 2005:1:1:1::24, and Secondary DNS: 2005:1:1:1::25. A 'NOTE' section on the right explains DHCP, Static IP Address, and PPPoE configurations.

- (Optional.) If you mark the **DHCP** radio box, you can configure the static DNS address in the corresponding fields.



The screenshot shows the same 'Network' configuration page. In this view, 'DHCP' is selected under 'IPv6 Config' and highlighted with a red box. The 'Static IP Address' option is unselected. The IPv6 Static DNS fields (On/Off, Primary DNS, Secondary DNS) are visible but not filled. The 'NOTE' section on the right remains the same.

4. Click **Confirm** to accept the change.

A dialog box pops up to prompt that the settings will take effect after reboot.

5. Click **OK** to reboot the phone.

To configure IPv6 address via phone user interface:

1. Press **Menu->Settings->Advanced Settings** (Default password: admin)
->Network->WAN Port.
2. Press the ◀ or ▶ soft key to select the desired address mode from the **IP Mode** field.
3. Press  to highlight **IPv6** and press the **Enter** soft key.
4. Press  to select the desired IPv6 address assignment method.

If you select the **Static IPv6 Client**, configure the IPv6 address and other configuration parameters in the corresponding fields.

5. Press the **Save** soft key to accept the change

The IP phone reboots automatically to make the settings effective after a period of time.

Configuring Audio Features

This chapter provides information for making configuration changes for the following audio features:

- [Audio Codecs](#)
- [Acoustic Clarity Technology](#)

Audio Codecs

CODEC is an abbreviation of COMpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The following table lists the audio codecs supported by CP860 IP conference phones:

Supported Audio Codecs	Default Audio Codecs
G722, PCMU, PCMA, G729, G723_53, G723_63, G726_16, G726_24, G726_32, G726_40, iLBC	G722, PCMU, PCMA, G729

The following table summarizes the supported audio codecs on IP phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16 KHz	20ms
PCMU	G.711	RFC 3551	64 Kbps	8 KHz	20ms
PCMA	G.711	RFC 3551	64 Kbps	8 KHz	20ms
G729	G.729	RFC 3551	8 Kbps	8 KHz	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms
G723_53/ G723_63	G.723.1	RFC 3951	5.3kbps 6.3kbps	8 Ksps	30ms
iLBC	iLBC	RFC 3952	13.33 Kbps	8 KHz	20ms 30ms

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
			15.2 Kbps		

Packetization Time

Ptime (Packetization Time) is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. You can also disable the ptime negotiation.

The attribute "rtptime" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

The corresponding attributes of the codec are listed as follows:

Codec	Configuration Methods	Priority	RTPmap
G722	Configuration Files Web User Interface	1	9
PCMU	Configuration Files Web User Interface	2	0
PCMA	Configuration Files Web User Interface	3	8
G729	Configuration Files Web User Interface	4	18
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102
G726-40	Configuration Files Web User Interface	0	105

Codec	Configuration Methods	Priority	RTPmap
iLBC	Configuration Files Web User Interface	4	106

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure the codecs to use.</p> <p>Parameters:</p> <p>account.X.codec.Y.enable</p> <p>account.X.codec.Y.payload_type</p> <p>Configure the priority and rtpmap for the enabled codec.</p> <p>Parameters:</p> <p>account.X.codec.Y.priority</p> <p>account.X.codec.Y.rtpmap</p> <p>Configure the display name of the codec.</p> <p>Parameter:</p> <p>account.X.codec.Y.display_name</p> <p>Configure the ptime.</p> <p>Parameter:</p> <p>account.X.ptime</p>
Local	Web User Interface	<p>Configure the codecs and adjust the priority of the enabled codecs.</p> <p><a href="http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0</p> <p>Configure the ptime.</p> <p>Navigate to:</p> <p><a href="http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0">http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</p>

Details of the Configuration Parameter:





Parameters	Permitted Values	Default
account.X.codec.Y.enable (X = 1, Y ranges from 1 to 11)	0 or 1	Refer to the following content

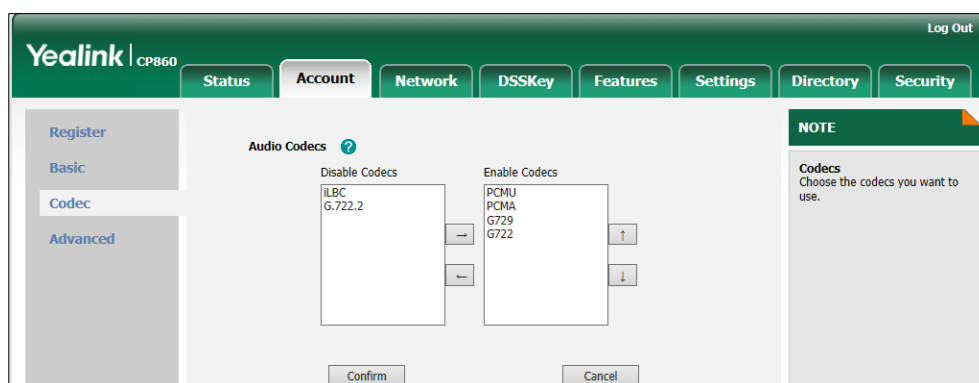
Parameters	Permitted Values	Default
<p>Description: Enables or disables the specified codec.</p> <p>0-Disabled 1-Enabled</p> <p>When Y=1, the default value is 1; When Y=2, the default value is 1; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0.</p> <p>Web User Interface: Account->Codec</p> <p>Phone User Interface: None</p>		
account.X.codec.Y.payload_type (X = 1, Y ranges from 1 to 11)	Refer to the following content	Refer to the following content
<p>Description: Configures the codec.</p> <p>Permitted Values: PCMU, PCMA, G729, G722, iLBC, AMR-WB</p> <p>Configures the codec.</p> <p>When Y=1, the default value is PCMU; When Y=2, the default value is PCMA; When Y=3, the default value is G723_53; When Y=4, the default value is G723_63; When Y=5, the default value is G729; When Y=6, the default value is G722; When Y=7, the default value is iLBC; When Y=8, the default value is G726-16;</p>		

Parameters	Permitted Values	Default
<p>When Y=9, the default value is G726-24; When Y=10, the default value is G726-32; When Y=11, the default value is G726-40.</p> <p>Example: account.1.codec.1.payload_type = PCMU</p> <p>Web User Interface: Account->Codec</p> <p>Phone User Interface: None</p>		
account.X.codec.Y.priority (X = 1, Y ranges from 1 to 11)	Integer from 0 to 11	Refer to the following content
<p>Description: Configures the priority of the enabled codec.</p> <p>When Y=1, the default value is 2; When Y=2, the default value is 3; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 4; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0.</p> <p>Web User Interface: Account->Codec</p> <p>Phone User Interface: None</p>		
account.X.codec.Y.rtpmap (X = 1, Y ranges from 1 to 11)	Integer from 0 to 127	Refer to the following content
<p>Description: Configures the rtpmap of the audio codec.</p> <p>When Y=1, the default value is 0;</p>		

Parameters	Permitted Values	Default
<p>When Y=2, the default value is 8; When Y=3, the default value is 4; When Y=4, the default value is 4; When Y=5, the default value is 18; When Y=6, the default value is 9; When Y=7, the default value is 106; When Y=8, the default value is 103; When Y=9, the default value is 104; When Y=10, the default value is 102; When Y=11, the default value is 105;</p> <p>Web User Interface: None</p> <p>Phone User Interface: None</p>		
account.X.codec.Y.display_name (X = 1, Y ranges from 1 to 11)	String within 99 characters	Blank
<p>Description: Configures the display name of the codec.</p> <p>Web User Interface: None</p> <p>Phone User Interface: None</p>		
account.X.ptime (X = 1)	0 (Disabled), 10, 20, 30, 40, 50 or 60	20
<p>Description: Configures the ptime (in milliseconds) for the codec.</p> <p>Example: account.1.ptime = 20</p> <p>Web User Interface: Account->Advanced->PTime (ms)</p> <p>Phone User Interface: None</p>		

To configure the codecs and adjust the priority of the enabled codecs on a per-line basis via web user interface:

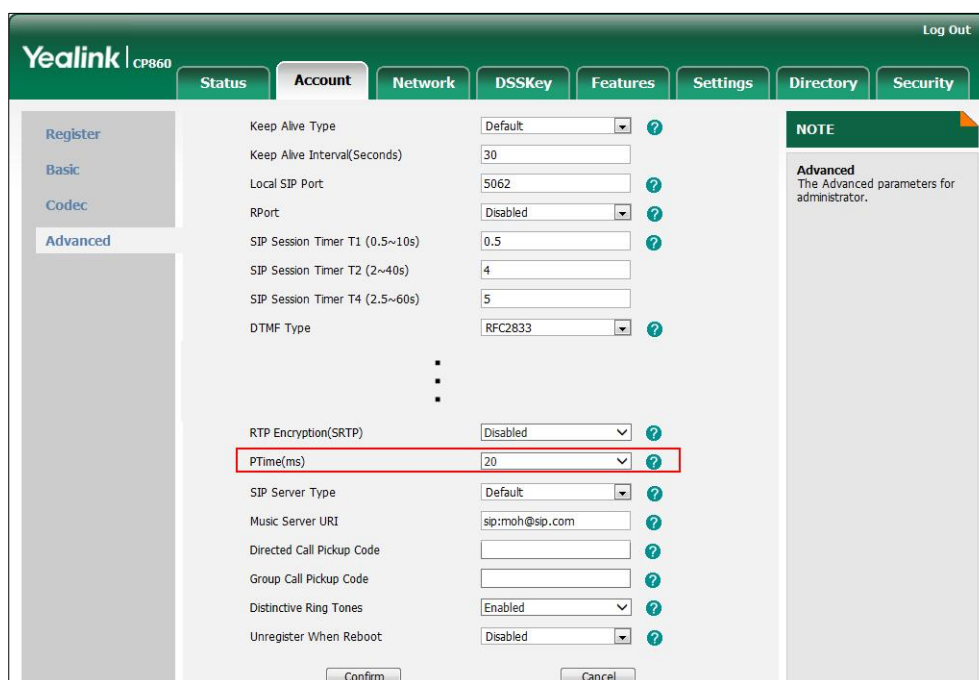
1. Click on **Account->Codec**.
2. Select the desired codec from the **Disable Codecs** column and click  .
The selected codec appears in the **Enable Codecs** column.
3. Repeat the step 2 to add more codecs to the **Enable Codecs** column.
4. Click  to remove the codec from the **Enable Codecs** column.
5. Click  or  to adjust the priority of the enabled codecs.



6. Click **Confirm** to accept the change.

To configure the Ptime via web user interface:

1. Click on **Account->Advanced**.
2. Select the desired value from the pull-down list of **PTime (ms)**.



3. Click **Confirm** to accept the change.

Acoustic Clarity Technology

Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) is used to reduce acoustic echo from a voice call to provide natural full-duplex communication patterns. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network.

Procedure

AEC can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure AEC. Parameter: voice.echo_cancellation
Local	Web User Interface	Configure AEC. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-voice&q=load">http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.echo_cancellation	0 or 1	1
Description: Enables or disables AEC (Acoustic Echo Canceller) feature on the IP phone. 0 -Disabled 1 -Enabled Web User Interface: Settings->Voice->Echo Cancellation->ECHO Phone User Interface: None		

To configure AEC via web user interface:

1. Click on **Settings->Voice**.

2. Select the desired value from the pull-down list of **ECHO**.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is selected. Under 'Echo Cancellation', the 'ECHO' dropdown is highlighted with a red box and set to 'Enabled'. Below it, 'VAD' is set to 'Disabled' and 'CNG' is set to 'Enabled'. The 'JITTER BUFFER' section has 'Type' set to 'Adaptive' (selected), 'Min Delay' set to 60, 'Max Delay' set to 300, and 'Normal' set to 120. There are 'Confirm' and 'Cancel' buttons at the bottom. A 'NOTE' section on the right explains VAD, CNG, and JITTER BUFFER.

3. Click **Confirm** to accept the change.

Background Noise Suppression

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

Automatic Gain Control

Automatic Gain Control (AGC) is applicable to hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in certain circumstances. This increases the effective user-phone radius and helps with the intelligibility of talkers.

Voice Activity Detection

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of "silence", VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and deactivate some processes during non-speech section of an audio session. VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

Procedure

VAD can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure VAD. Parameter:
---------------------------	-------------------	-------------------------------------

		voice.vad
Local	Web User Interface	Configure VAD. Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	0 or 1	0

Description:

Enables or disables VAD (Voice Activity Detection) feature on the IP phone.

0-Disabled

1-Enabled

Web User Interface:

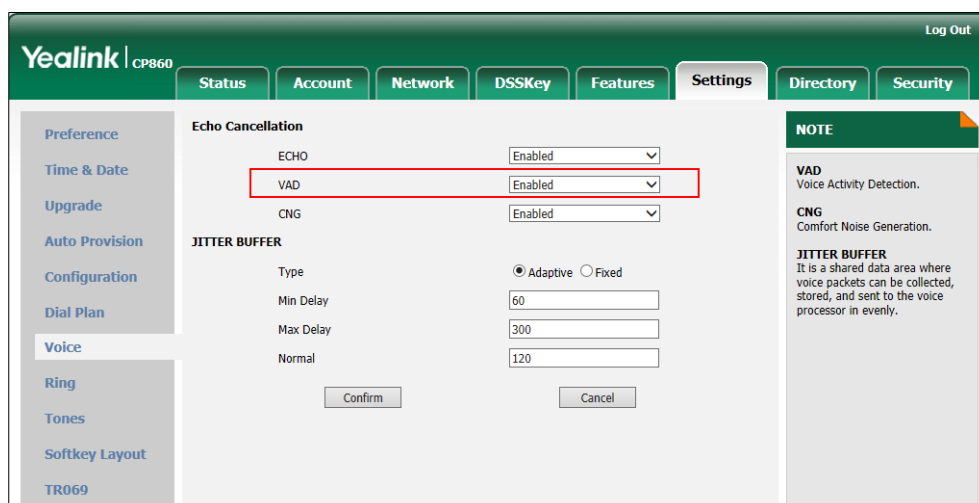
Settings->Voice->Echo Cancellation->VAD

Phone User Interface:

None

To configure VAD via web user interface:

1. Click on **Settings->Voice**.
2. Select the desired value from the pull-down list of **VAD**.



3. Click **Confirm** to accept the change.

Comfort Noise Generation

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation. It is a part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly responds when periods of silence occur and inserts artificial noise until voice activity resumes. The insertion of artificial noise gives the illusion of a constant transmission stream, so that background sound is consistent throughout the call and the listener does not think the line has released. The purpose of VAD and CNG is to maintain an acceptable perceived QoS while simultaneously keeping transmission costs and bandwidth usage as low as possible.

Procedure

CNG can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure CNG. Parameter: voice.cng
Local	Web User Interface	Configure CNG. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-voice&q=load">http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	0 or 1	1
Description: Enables or disables CNG (Comfortable Noise Generator) feature on the IP phone. 0-Disabled 1-Enabled Web User Interface: Settings->Voice->Echo Cancellation->CNG Phone User Interface: None		

To configure CNG via web user interface:

1. Click on **Settings->Voice**.

2. Select the desired value from the pull-down list of **CNG**.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings' (selected), 'Directory', and 'Security'. A left sidebar lists various settings categories like 'Preference', 'Time & Date', 'Upgrade', 'Auto Provision', 'Configuration', 'Dial Plan', 'Voice' (selected), 'Ring', 'Tones', 'Softkey Layout', and 'TR069'. The main content area is titled 'Echo Cancellation' and contains three dropdown menus: 'ECHO' (set to 'Enabled'), 'VAD' (set to 'Enabled'), and 'CNG' (set to 'Enabled', highlighted with a red box). Below this is the 'JITTER BUFFER' section with a 'Type' dropdown (set to 'Adaptive') and three input fields for 'Min Delay' (60), 'Max Delay' (300), and 'Normal' (120). 'Confirm' and 'Cancel' buttons are at the bottom. A right sidebar titled 'NOTE' provides definitions for 'VAD' (Voice Activity Detection), 'CNG' (Comfort Noise Generation), and 'JITTER BUFFER' (a shared data area for voice packets).

3. Click **Confirm** to accept the change.

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. IP phones support two types of jitter buffers: fixed and adaptive. A fixed jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on IP phones. An adaptive jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on IP phones.

Procedure

Jitter buffer can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. Parameters: voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
Local	Web User Interface	Configure the mode of jitter buffer and the delay time for

		jitter buffer. Navigate to: <a href="http://<phoneIPAddress>/servlet?<phoneIPAddress>=settings-voice&q=load">http://<phoneIPAddress>/servlet?<phoneIPAddress>=settings-voice&q=load
--	--	--

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.jib.adaptive	0 or 1	1
Description: Configures the type of jitter buffer. 0 -Fixed 1 -Adaptive Web User Interface: Settings->Voice->JITTER BUFFER->Type Phone User Interface: None		
voice.jib.min	Integer from 0 to 400	60
Description: Configures the minimum delay time (in milliseconds) of jitter buffer. Note: It works only if the parameter “voice.jib.adaptive” is set to 1 (Adaptive). Web User Interface: Settings->Voice->JITTER BUFFER->Min Delay Phone User Interface: None		
voice.jib.max	Integer from 0 to 400	300
Description: Configures the maximum delay time (in milliseconds) of jitter buffer. Note: It works only if the parameter “voice.jib.adaptive” is set to 1 (Adaptive). Web User Interface: Settings->Voice->JITTER BUFFER->Max Delay Phone User Interface: None		
voice.jib.normal	Integer from 0 to 400	120

Parameters	Permitted Values	Default
<p>Description:</p> <p>Configures the normal delay time (in milliseconds) of jitter buffer.</p> <p>Note: It works only if the parameter “voice.jib.adaptive” is set to 0 (Fixed).</p> <p>Web User Interface:</p> <p>Settings->Voice->JITTER BUFFER->Normal</p> <p>Phone User Interface:</p> <p>None</p>		

To configure Jitter Buffer via web user interface:

1. Click on **Settings->Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.
Valid values range from 0 to 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.
Valid values range from 0 to 300.
5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.
Valid values range from 0 to 300.

The screenshot shows the Yealink CP860 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'DSSKey', 'Features', 'Settings', 'Directory', and 'Security'. The left sidebar lists various settings categories: Preference, Time & Date, Upgrade, Auto Provision, Configuration, Dial Plan, Voice, Ring, Tones, Softkey Layout, and TR069. The main content area is titled 'JITTER BUFFER' and contains the following fields:

- Echo Cancellation:** ECHO (Enabled), VAD (Enabled), CNG (Enabled).
- JITTER BUFFER:**
 - Type:** Adaptive (selected) or Fixed.
 - Min Delay:** 60
 - Max Delay:** 300
 - Normal:** 120

At the bottom of the JITTER BUFFER section are 'Confirm' and 'Cancel' buttons. A red box highlights the JITTER BUFFER section. On the right side, there is a 'NOTE' section with the following text:

VAD
Voice Activity Detection.

CNG
Comfort Noise Generation.

JITTER BUFFER
It is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly.

6. Click **Confirm** to accept the change.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- [Transport Layer Security](#)
- [Secure Real-Time Transport Protocol](#)
- [Encrypting Configuration Files](#)

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

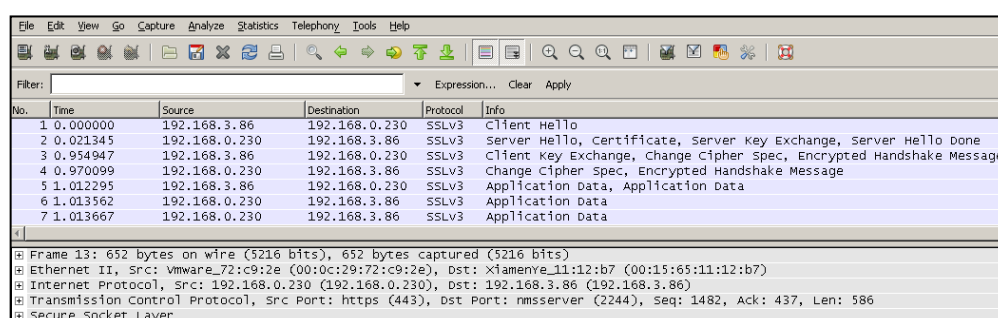
- **Symmetric encryption:** For symmetric encryption, the encryption key and the corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.
- **Asymmetric encryption:** For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

CP860 IP conference phones support TLS 1.0. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. CP860 IP conference phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA

- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:



The image shows a Wireshark packet capture of a TLS handshake. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.86	192.168.0.230	SSLV3	Client Hello
2	0.021345	192.168.0.230	192.168.3.86	SSLV3	Server Hello, Certificate, Server Key Exchange, Server Hello done
3	0.954947	192.168.3.86	192.168.0.230	SSLV3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4	0.970099	192.168.0.230	192.168.3.86	SSLV3	Change Cipher Spec, Encrypted Handshake Message
5	1.012295	192.168.3.86	192.168.0.230	SSLV3	Application Data, Application Data
6	1.013562	192.168.0.230	192.168.3.86	SSLV3	Application Data
7	1.013667	192.168.0.230	192.168.3.86	SSLV3	Application Data

Below the packet list, the details of Frame 13 are shown:

- Frame 13: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
- Ethernet II, Src: Vmware_72:c9:2e (00:0c:29:72:c9:2e), Dst: Xiamenye_11:12:b7 (00:15:65:11:12:b7)
- Internet Protocol, Src: 192.168.0.230 (192.168.0.230), Dst: 192.168.3.86 (192.168.3.86)
- Transmission Control Protocol, Src Port: https (443), Dst Port: nmsserver (2244), Seq: 1482, Ack: 437, Len: 586
- Secure Socket Layer

Step1: IP phone sends “Client Hello” message proposing SSL options.

Step2: Server responds with “Server Hello” message selecting the SSL options, sends its public key information in “Server Key Exchange” message and concludes its part of the

negotiation with “Server Hello Done” message.

Step3: The IP phone sends session key information (encrypted by server’s public key) in the “Client Key Exchange” message.

Step4: Server sends “Change Cipher Spec” message to activate the negotiated options for all future messages it will send.

IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon will appear on the LCD screen after the successful TLS negotiation.

Certificates

The IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate:** When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 30 built-in trusted certificates. You can upload up to 10 custom certificates to the IP phone. The format of the certificates must be *.pem, *.cer, *.crt and *.der.
- **Server Certificate:** When clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the IP phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer.
 - **A unique server certificate:** It is installed by default and is unique to an IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
 - **A generic server certificate:** It is installed by default and is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the IP phone may send a generic certificate for authentication.

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the IP phone accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server.

Note

For TLS feature, we use the terms trusted and server certificates. These are also known as CA and device certificates.

Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<MAC>.cfg	<p>Configure TLS.</p> <p>Parameter:</p> <p>account.X.transport</p>
	y000000000037.cfg	<p>Configure the trusted certificates feature.</p> <p>Parameters:</p> <p>security.trust_certificates</p> <p>security.ca_cert</p> <p>security.cn_validation</p> <p>Configure the server certificates feature.</p> <p>Parameters:</p> <p>security.dev_cert</p> <p>Upload the trusted certificates.</p> <p>Parameter:</p> <p>trusted_certificates.url</p> <p>Upload the server certificates.</p> <p>Parameter:</p> <p>server_certificates.url</p>
Local	Web User Interface	<p>Configure TLS.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0</p> <p>Configure the trusted certificates feature.</p> <p>Upload the trusted certificates.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=trusted-cert&q=load</p> <p>Configure the server certificates feature.</p> <p>Upload the server certificates.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet</p>

		et?p=server-cert&q=load
--	--	-------------------------

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.transport (X = 1)	Integer	0
Description: Configures the type of transport protocol. 0 -UDP 1 -TCP 2 -TLS 3 -DNS-NAPTR Web User Interface: Account->Register->Transport Phone User Interface: None		
security.trust_certificates	0 or 1	1
Description: Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list. 0 -Disabled 1 -Enabled If it is set to 1 (Enabled), the IP phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the IP phone will trust the server. If it is set to 0 (Disabled), the IP phone will trust the server no matter whether the certificate sent by the server is valid or not. Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Security->Trusted Certificates->Only Accept Trusted Certificates		
security.ca_cert	0, 1 or 2	2
Description: Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection.		

Parameters	Permitted Values	Default
0-Default certificates 1-Custom certificates 2-All certificates Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Security->Trusted Certificates->CA Certificates Phone User Interface: None		
security.cn_validation	0 or 1	0
Description: Enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. 0-Disabled 1-Enabled Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Security->Trusted Certificates->Common Name Validation Phone User Interface: None		
security.dev_cert	0 or 1	0
Description: Configures the type of the device certificates for the IP phone to send for TLS authentication. 0-Default certificates 1-Custom certificates Note: If you change this parameter, the IP phone will reboot to make the change take effect. Web User Interface: Security-> Server Certificates->Device Certificates Phone User Interface: None		

Parameters	Permitted Values	Default
trusted_certificates.url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server.</p> <p>Example: trusted_certificates.url = http://192.168.1.20/tc.crt</p> <p>Note: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.</p> <p>Web User Interface: Security->Trusted Certificates->Load trusted certificates file</p> <p>Phone User Interface: None</p>		
server_certificates.url	URL within 511 characters	Blank
<p>Description: Configures the access URL of the certificate the IP phone sends for authentication.</p> <p>Example: server_certificates.url = http://192.168.1.20/ca.pem</p> <p>Note: The certificate you want to upload must be in *.pem or *.cer format.</p> <p>Web User Interface: Security->Server Certificates->Load server cer file</p> <p>Phone User Interface: None</p>		

To configure the trusted certificates feature via web user interface:

1. Click on **Security->Trusted Certificates**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
3. Select the desired value from the pull-down list of **Common Name Validation**.

4. Select the desired value from the pull-down list of **CA Certificates**.

The screenshot shows the 'Trusted Certificates' page in the Yealink CP860 web interface. The 'CA Certificates' dropdown menu is highlighted with a red box, showing 'Default Certificates' selected. The page includes a table of certificates with columns for Index ID, Issued To, Issued By, Expiration, and Delete. Below the table is a 'Delete' button. The 'Import Trusted Certificates' section includes a 'Load trusted certificates file' input field, a 'Browse...' button, and an 'Upload' button. The 'Confirm' and 'Cancel' buttons are at the bottom.

5. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
6. Click **OK** to reboot the phone.

To configure TLS via web user interface:

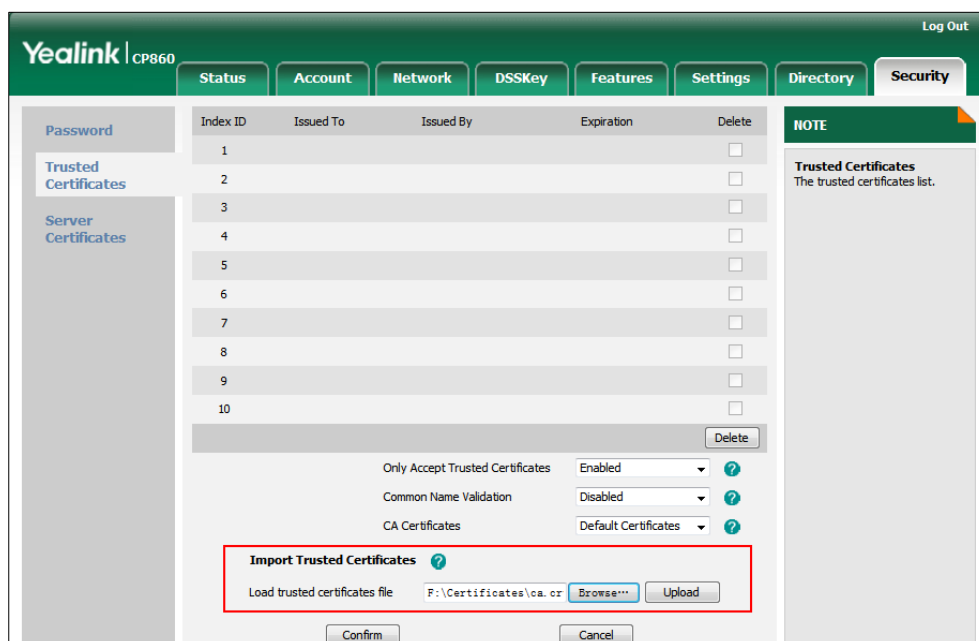
1. Click on **Account**.
2. Select **TLS** from the pull-down list of the **Transport**.

The screenshot shows the 'Account' settings page in the Yealink CP860 web interface. The 'Transport' dropdown menu is highlighted with a red box, showing 'TLS' selected. The page includes various configuration fields for SIP servers and NAT settings. The 'Register' section includes fields for Line Active, Label, Display Name, Register Name, User Name, Password, and Enable Outbound Proxy Server. The 'SIP Server 1' and 'SIP Server 2' sections include fields for Server Host, Server Expires, and Server Retry Counts. The 'NAT' section includes a 'NAT' dropdown and a 'STUN Server' field. The 'Confirm' and 'Cancel' buttons are at the bottom.

3. Click **Confirm** to accept the change.

To upload a trusted certificate via web user interface:

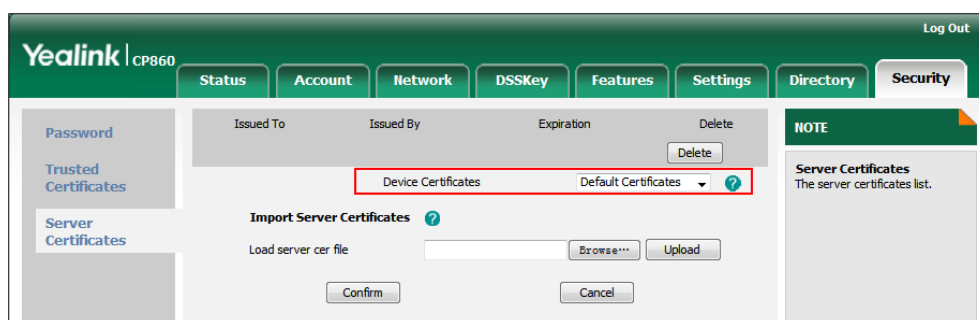
1. Click on **Security->Trusted Certificates**.
2. Click **Browse** to locate the certificate (*.pem, *.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

To configure the server certificates feature via web user interface:

1. Click on **Security->Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.

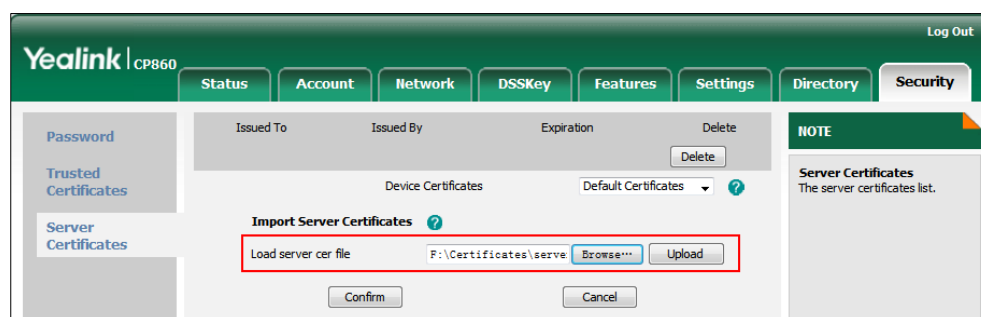


3. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after reboot.
4. Click **OK** to reboot the phone.

To upload a server certificate via web user interface:

1. Click on **Security->Server Certificates**.

- Click **Browse** to locate the certificate (*.pem or *.cer) from your local system.



- Click **Upload** to upload the certificate.

The dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait...".

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) encrypts RTP streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP simultaneously. When this feature is enabled on both phones, the encryption algorithm utilized for the session is negotiated between IP phones. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NzFINTUwZDk2OGVIOTc3YzNkYTkWZWVMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRiMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

When SRTP is enabled on both IP phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after successful negotiation.

Note

If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to [Transport Layer Security](#) on page 305.

Procedure

SRTP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure SRTP feature. Parameter: account.X.srtp_encryption
Local	Web User Interface	Configure SRTP feature. Navigate to: http://<phoneIPAddress>/servlet ?p=account-adv&q=load&acc= 0

Details of the Configuration Parameter:

Parameters	Permitted Values	Default
account.X.srtp_encryption (X = 1)	0, 1 or 2	0
Description: Configures whether to use voice encryption service. 0-Disabled		

Parameters	Permitted Values	Default
<p>1-Optional</p> <p>2-Compulsory</p> <p>If it is set to 1 (Optional), the IP phone will negotiate with the other IP phone what type of encryption to utilize for the session.</p> <p>If it is set to 2 (Compulsory), the IP phone is forced to use SRTP during a call.</p> <p>Web User Interface:</p> <p>Account->Advanced->RTP Encryption (SRTP)</p> <p>Phone User Interface:</p> <p>None</p>		

To configure SRTP via web user interface:

1. Click on **Account-> Advanced**.
2. Select the desired value from the pull-down list of **RTP Encryption (SRTP)**.

The screenshot shows the Yealink CP860 web interface. The 'Account' tab is selected, and the 'Advanced' sub-tab is active. The 'RTP Encryption(SRTP)' option is highlighted with a red box and set to 'Compulsory'. Other settings include Keep Alive Type (Default), Keep Alive Interval (30), Local SIP Port (5062), RPort (Disabled), SIP Session Timer T1 (0.5), SIP Session Timer T2 (4), SIP Session Timer T4 (5), DTMF Type (RFC2833), DTMF Info Type (DTMF-Relay), DTMF Payload Type (101), Retransmission (Disabled), Subscribe for MWI (Disabled), MWI Subscription Period (3600), Subscribe MWI To Voice Mail (Disabled), Voice Mail, Caller ID Source (FROM), Session Timer (Disabled), Session Expires (1800), Session Refresher (UAC), and Send user=phone (Disabled). A 'NOTE' box on the right states: 'Advanced: The Advanced parameters for administrator.'

3. Click **Confirm** to accept the change.

Encrypting Configuration Files

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (e.g., login passwords, registration information). Yealink supplies a configuration encryption tool for encrypting configuration files. The encryption tool encrypts plaintext y000000000037.cfg and <MAC>.cfg files (one by one or in batch) using 16-character symmetric keys (the

same or different keys for configuration files) and generates encrypted configuration files with the same file name as before. This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the IP phone, and generates new files named as <xx_Security>.enc (xx indicates the name of the configuration file, for example, y000000000037_Security.enc for y000000000037.cfg file). This tool generates another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

For a Microsoft Windows platform, you can use a Yealink-supplied encryption tool "Config_Encrypt_Tool.exe" to encrypt the y000000000037.cfg and <MAC>.cfg files respectively.

Note

Yealink also supplies a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to *Yealink Configuration Encryption Tool User Guide*.

For the security reasons, administrator should upload encrypted configuration files, y000000000037_Security.enc and/or <MAC_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP phone requests to download y000000000037.cfg file first. If the downloaded configuration file is encrypted, the IP phone will request to download y000000000037_Security.enc file (if enabled) and decrypt it into the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the IP phone decrypts y000000000037.cfg file using key2. After decryption, the IP phone resolves configuration files and updates configuration settings onto the IP phone system.

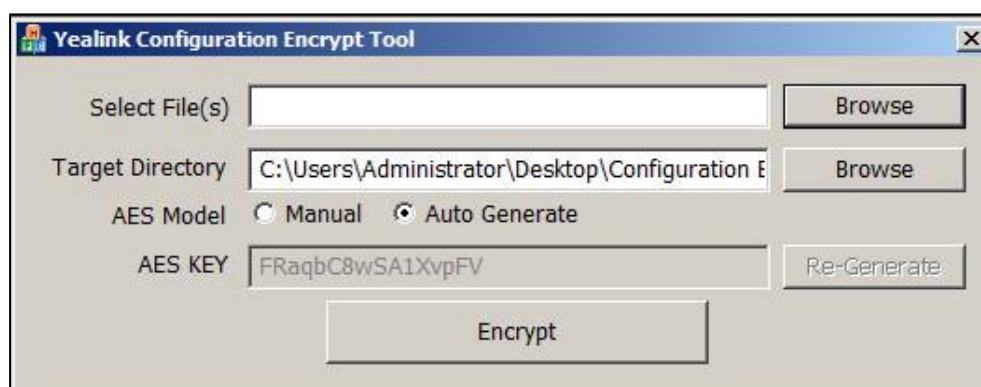
The way the IP phone processes the <MAC>.cfg file is the same to that of the y000000000037.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the y000000000037.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

The screenshot of the main page is shown as below:



When you start the application tool, a file folder named "Encrypted" is created

automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., y0000000000037.cfg) from your local system in the **Select File(s)** field.

To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select the next files.

3. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

The tool uses the file folder "Encrypted" as the target directory by default.

4. (Optional.) Mark the desired radio box in the **AES Model** field.

If you mark the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.

If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

Note

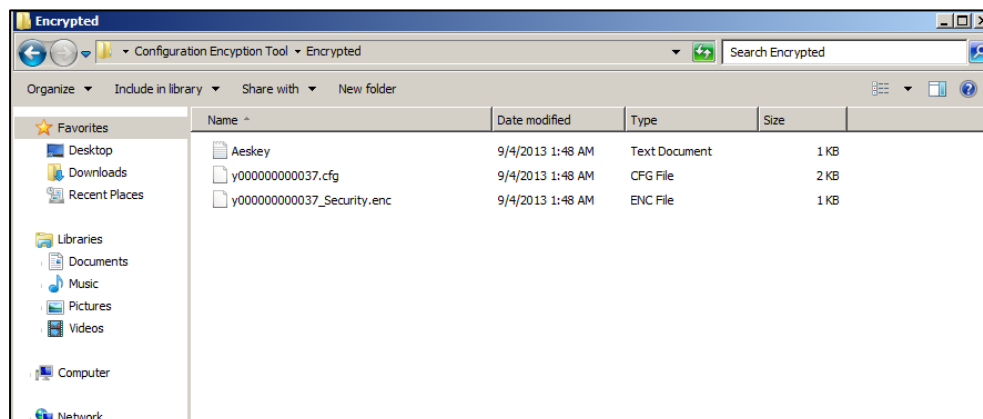
AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z.

5. Click **Encrypt** to encrypt the configuration file(s).



6. Click **OK**.

The target directory will be automatically opened. You can find the encrypted configuration file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).



Procedure

Encryption method and AES keys can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	Configure the decryption method and AES keys. Parameters: auto_provision.aes_key_in_file auto_provision.aes_key_16.com auto_provision.aes_key_16.mac auto_provision.update_file_mode
Local	Web User Interface	Configure the AES keys. Navigate to: <a href="http://<phoneIPAddress>/servlet?p=settings-autop&q=load">http://<phoneIPAddress>/servlet?p=settings-autop&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_provision.aes_key_in_file	0 or 1	0
Description: Enables or disables the IP phone to decrypt configuration files using the encrypted AES keys. 0-Disabled 1-Enabled		

Parameters	Permitted Values	Default
<p>If it is set to 1 (Enabled), the IP phone will download y000000000037_Security.enc and <MAC_Security>.enc files during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The IP phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3).</p> <p>If it is set to 0 (Disabled), the IP phone will decrypt the encrypted configuration files using plaintext AES keys configured on the IP phone.</p> <p>Web User Interface:</p> <p>None</p> <p>Phone User Interface:</p> <p>None</p>		
auto_provision.aes_key_16.com	16 characters	Blank
<p>Description:</p> <p>Configures the plaintext AES key for decrypting the Common CFG file.</p> <p>The valid characters contain: 0 ~ 9, A ~ Z, a ~ z.</p> <p>Example:</p> <p>auto_provision.aes_key_16.com = 0123456789abcdef</p> <p>Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p> <p>Web User Interface:</p> <p>Settings->Auto Provision->Common AES Key</p> <p>Phone User Interface:</p> <p>None</p>		
auto_provision.aes_key_16.mac	16 characters	Blank
<p>Description:</p> <p>Configures the plaintext AES key for decrypting the MAC-Oriented CFG file.</p> <p>The valid characters contain: 0 ~ 9, A ~ Z, a ~ z.</p> <p>Example:</p> <p>auto_provision.aes_key_16.mac = 0123456789abmins</p> <p>Note: It works only if the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled).</p> <p>Web User Interface:</p> <p>Settings->Auto Provision->MAC-Oriented AES Key</p>		

Parameters	Permitted Values	Default
Phone User Interface: None		
auto_provision.update_file_mode	0 or 1	0
Description: Enables or disables the IP phone to update encrypted configuration settings only during auto provisioning. 0-Disabled 1-Enabled Web User Interface: None Phone User Interface: None		

To configure the AES keys via web user interface:

1. Click on **Settings->Auto Provision**.
2. Enter the values in the **Common AES Key** and **MAC-Oriented AES Key** fields.

The screenshot displays the Yealink CP860 web interface. The 'Settings' tab is selected, and the 'Auto Provision' sub-tab is active. In the 'Auto Provision' section, the 'Common AES Key' and 'MAC-Oriented AES Key' fields are highlighted with a red rectangle. The 'Common AES Key' field contains a series of dots, and the 'MAC-Oriented AES Key' field also contains a series of dots. Other settings visible include 'PNP Active' (On), 'DHCP Active' (On), 'Custom Option(128~254)' (empty), 'DHCP Option Value' (yealink), 'Server URL' (empty), 'User Name' (empty), 'Password' (empty), 'Zero Active' (Disabled), 'Wait Time(0~100s)' (5), 'Power On' (On), 'Repeatedly' (Off), 'Interval(Minutes)' (1440), 'Weekly' (On), 'Time' (00:00:00), and 'Day of Week' (all days checked). A 'NOTE' box on the right states: 'Auto Provision: The auto provision parameters for administrator.'

3. Click **Confirm** to accept the change.

Resource Files

When configuring particular features, you may need to upload resource files (e.g., local contact directory, remote phone book) to the IP phone. The resources files can be local contact directory, remote phone book and so on. Ask Yealink field application engineer for resource file templates. If the resource file is to be used for all IP phones of the same model, the resource file access URL is best specified in the y0000000000037.cfg file. However, if you want to specify the desired phone to use the resource file, the access URL of resource file should be specified in the <MAC>.cfg file.

The names of the Yealink-supplied template file are (You can rename the filename as required):

Template File	File Name
Replace Rule Template	dialplan.xml
Dial-now Template	dialnow.xml
Softkey Layout Template	CallFailed.xml CallIn.xml Connecting.xml Dialing.xml RingBack.xml Talking.xml
Directory Template	favorite_setting.xml
Super Search Template	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.xml

This chapter provides the detailed information on how to customize the following resource files:

- [Replace Rule Template](#)
- [Dial-now Template](#)
- [Softkey Layout Template](#)
- [Directory Template](#)
- [Super Search Template](#)
- [Local Contact File](#)
- [Remote XML Phone Book](#)

Replace Rule Template

The replace rule template helps with the creation of multiple replace rules. After setup, place the replace rule file to the provisioning server and specify the access URL of the file in the configuration files.

When editing a replace rule template file, learn the following:

- `<DialRule>` indicates the start of the template file and `</DialRule>` indicates the end of the template file.
- Create replace rules between `<DialRule>` and `</DialRule>`.
- At most 100 replace rules can be added to the IP phone.
- The expression syntax in the replace rule template is the same as that introduced in the section [Dial Plan](#) on page 81.

Procedure

Use the following procedures to customize a replace rule template.

To customize a replace rule template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

```
<Data Prefix="" Replace="" />
```

Where:

`Prefix=""` specifies the numbers to be replaced.

`Replace=""` specifies the alternate string instead of what the user enters.

3. Specify the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a replace rule file:

```
<DialRule>

<Data Prefix="1" Replace="05928665234"/>

<Data Prefix="2(xx)" Replace="002$1"/>

<Data Prefix="5([6-9])(.)" Replace="3$2"/>

<Data Prefix="0(.)" Replace="9$1"/>

<Data Prefix="1009" Replace="05921009"/>

</DialRule>
```

Dial-now Template

The dial-now template helps with the creation of multiple dial-now rules. After setup, place the dial-now file to the provisioning server and specify the access URL of the file in the configuration files.

When editing a dial-now template, learn the following:

- `<DialNow>` indicates the start of a template and `</DialNow>` indicates the end of a template.
- Create dial-now rules between `<DialNow>` and `</DialNow>`.
- At most 100 dial-now rules can be added to the IP phone.
- The expression syntax in the dial-now rule template is the same as that introduced in the section [Dial Plan](#) on page 81.

Procedure

Use the following procedures to customize a dial-now template.

To customize a dial-now template:

1. Open the template file using an ASCII editor.
2. Add the following string to the template, each starting on a separate line:

```
<Data DialNowRule=""/>
```

Where:

`DialNowRule=""` specifies the dial-now rule.

3. Specify the values within double quotes.
4. Save the change and place this file to the provisioning server.

The following shows an example of a dial-now template:

```
<DialNow>
  <Data DialNowRule="1234"/>
  <Data DialNowRule="52[0-6]"/>
  <Data DialNowRule="xxxxxx"/>
</DialNow>
```

Softkey Layout Template

The softkey layout template allows assigning different soft key layouts to different call states. The call states include CallFailed, CallIn, Connecting, Dialing, RingBack and Talking. After setup, place the softkey layout file to the provisioning server and specify the access URL of the file in the configuration files.

When editing a softkey layout template, learn the following:

- `<Call States>` indicates the start of a template and `</Call States>` indicates the end of a template. For example, `<CallFailed></CallFailed>`.
- `<Disable>` indicates the start of the disabled soft key list and `</Disable>` indicates the end of the soft key list, the disabled soft keys are not displayed on the LCD screen.
- Create disabled soft keys between `<Disable>` and `</Disable>`.
- `<Enable>` indicates the start of the enabled soft key list and `</Enable>` indicates the end of the soft key list, the enabled soft keys are displayed on the LCD screen.
- Create enabled soft keys between `<Enable>` and `</Enable>`.
- `<Default>` indicates the start of the default soft key list and `</Default>` indicates the end of the default soft key list, the default soft keys are displayed on the LCD screen by default.

Procedure

Use the following procedures to customize a softkey layout template.

To customize a softkey layout template:

1. Open the template file using an ASCII editor.
2. For each soft key that you want to enable, add the following string to the file. Each starts on a separate line:

```
<Key Type=""/>
```

Where:

Key Type="" specifies the enabled soft key (This value cannot be blank).

For each disabled soft key and each default soft key that you want to add, add the same string introduced above.

3. Specify the values within double quotes.
4. Save the change and place this file to the provisioning server.

The following shows an example of the CallFailed template file:

```
<CallFailed>
  <Disable>
    <Key Type="Empty"/>
```

```

        <Key Type="Switch"/>
        <Key Type="Cancel"/>
    </Disable>
    <Enable>
        <Key Type="NewCall"/>
        <Key Type="Empty"/>
        <Key Type="Empty"/>
        <Key Type="Empty"/>
    </Enable>
    <Default>
        <Key Type="NewCall"/>
        <Key Type="Empty"/>
        <Key Type="Empty"/>
        <Key Type="Empty"/>
    </Default>
</CallFailed>

```

Directory Template

Directory provides easy access to frequently used lists. Users can access lists by pressing the Directory soft key when the IP phone is idle. The lists may contain Local Directory, History, Remote Phone Book and LDAP. You can add the desired list(s) to Directory using the supplied directory template. After setup, place the directory file to the provisioning server and specify the access URL of the file in the configuration files.

When editing a directory template, learn the following:

- `<root_favorite_set>` indicates the start of a template and `</root_favorite_set>` indicates the end of a template.
- The default display names of directory lists are Local Directory, History, Remote Phone Book and LDAP.
- When specifying the display priority of the directory list, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list for Directory, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a directory template.

Customizing a directory template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file. For example, you want to configure the local directory list, edit the following strings:

```
<item id_name="localdirectory" display_name="Local Directory" priority="1"
enable="1" />
```

Where:

`id_name=""` specifies the existing directory list ("localdirectory" for the local directory list). Do not edit this field.

`display_name=""` specifies the display name of the directory list. We recommend you do not edit this field.

`priority=""` specifies the display priority of the directory list.

`enable=""` enables or disables the directory list for Directory.

3. Edit the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a directory template:

```
<root_favorite_set>

  <item id_name="localdirectory" display_name="Local Directory"
priority="1" enable="1" />

  <item id_name="history" display_name="History" priority="2"
enable="0" />

  <item id_name="remotedirectory" display_name="Remote Phone Book"
priority="3" enable="0" />

  <item id_name="ldap" display_name="LDAP" priority="4" enable="0" />

</root_favorite_set>
```

Super Search Template

Search source list in dialing allows the IP phone to search for entries from the desired lists based on the entered string when in the pre-dialing screen, and then the user can select the desired entry to dial out quickly. The lists may contain Local Directory, History, Remote Phone Book and LDAP. You can configure the search source list in dialing using the supplied super search template (super_search.xml). After setup, place the super search file to the provisioning server and specify the access URL of the file in the configuration files.

When editing a super search template, learn the following:

- `<root_super_search>` indicates the start of a template and `</root_super_search>` indicates the end of a template.
- The default display names of directory lists are Local Directory, History, Remote Phone Book and LDAP.
- When specifying the priority of search results, the valid values are 1, 2, 3 and 4. 1 is the highest priority, 4 is the lowest.
- When enabling or disabling the desired directory list, the valid values are 0 and 1. 0 stands for Disabled, 1 stands for Enabled.

Procedure

Use the following procedures to customize a super search template.

Customizing a super search template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file. For example, you want to configure the local directory list, edit the following strings:

```
<item id_name="local_directory_search" display_name="Local Directory"
priority="1" enable="1" />
```

Where:

`id_name=""` specifies the directory list ("`local_directory_search`" for the local directory list). Do not edit this field.

`display_name=""` specifies the display name of the directory list. We recommend you do not edit this field.

`priority=""` specifies the priority of search results.

`enable=""` enables or disables the IP phone to search the directory list.

3. Edit the values within double quotes.
4. Place this file to the provisioning server.

The following shows an example of a super search template:

```
<root_super_search>

  <item id_name="local_directory_search" display_name="Local
Directory" priority="1" enable="1" />

  <item id_name="calllog_search" display_name="History" priority="2"
enable="1" />

  <item id_name="remote_directory_search" display_name="Remote Phone
Book" priority="3" enable="0" />

  <item id_name="ldap_search" display_name="LDAP" priority="4"
enable="0" />
```

</root_super_search>

Local Contact File

You can add contacts one by one on the IP phone directly. You can also add multiple contacts at a time and/or share contacts between IP phones using the local contact template file (Yealink-supplied template file is named as contact.xml). After setup, place the local contact file to the provisioning server, and specify the access URL of the file in the configuration files.

When editing a local contact file, learn the following:

- <root_contact> indicates the start of a contact list and </root_contact> indicates the end of a contact list.
- <root_group> indicates the start of a group list and </root_group> indicates the end of a group list.
- When specifying a ring tone for a contact or a group, the format of the value must be Auto (the first registered line), Resource:RingN.wav (the default system ring tone ranges from 1 to 5) or Custom:Name.wav (the custom ring tone).

Procedure

Use the following procedures to customize a local contact template file.

To customize a local contact file:

1. Open the template file using an ASCII editor.
2. For each group that you want to add, add the following string to the file. Each starts on a separate line:

```
<group display_name="" ring="" />
```

Where:

display_name="" specifies the name of the group.

ring="" specifies the desired ring tone for this group.

3. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

```
<contact display_name="" office_number="" mobile_number="" other_number=""  
ring="" group_id_name="" />
```

Where:

display_name="" specifies the name of the contact (This value cannot be blank or duplicated).

office_number = "" specifies the office number of the contact.

mobile_number="" specifies the mobile number of the contact.

other_number="" specifies the other number of the contact.

ring="" specifies the ring tone for this contact. If it is left blank, the ring tone of the contact will be specified as Auto.

group_id_name="" specifies the existing group you want to add the contact to.

4. Specify the values within double quotes.
5. Save the change and place this file to the provisioning server.

The following shows an example of a local contact file:

```
<root_group>
  <group display_name="Friend" ring="" />
  <group display_name="Family" ring="Resource:Ring1.wav" />
</root_group>
<root_contact>
  <contact display_name="John" office_number="1001"
mobile_number="12345678910" other_number="" ring="Auto"
group_id_name="All Contacts" />
  <contact display_name="Alice" office_number="1002" mobile_number=""
other_number="" ring="Resource:Ring2.wav" group_id_name="Friend" />
</root_contact>
```

Remote XML Phone Book

IP phones can access 5 remote phone books. You can customize the remote XML phone book for IP phones as required. You can also add multiple remote contacts at a time and/or share remote contacts between IP phones using the supplied template files (Menu.xml and Department.xml). The Menu.xml file defines departments of a remote phone book. The Department.xml file defines contact lists for a department, which is nested in Menu.xml file. After setup, place the files (Menu.xml and Department.xml) to the provisioning server, and specify the access URL of the file (Menu.xml) in the configuration files.

When creating a Menu.xml file, learn the following:

- <YealinkIPPhoneMenu> indicates the start of a remote phone book file and </YealinkIPPhoneMenu> indicates the end of a remote phone book file.
- Create the title of a remote phone book between <Title> and </Title>.
- <Menuitem> indicates the start of specifying a department file and </Menuitem> indicates the end of specifying a department file.
- <SoftKeyItem> indicates the start of specifying a XML file and </SoftKeyItem> indicates the end of specifying a XML file.

Procedure

Use the following procedures to customize an XML phone book.

To customize a Menu.xml file:

1. Open the template file using an ASCII editor.
2. For each department that you want to add, add the following strings to the file. Each starts on a separate line:

```
<MenuItem>
  <Name>Department1</Name>
  <URL>http://10.3.6.117:8080/Department1.xml</URL>
</MenuItem>
```

Where:

Specify the name of a department between <Name> and </Name>.

Specify the access URL of a department file between </URL> and </URL>.

3. For each XML file that you want to add, add the following strings to the file. Each starts on a separate line:

```
<SoftKeyItem>
  <Name>#</Name>
  <URL>http://10.3.6.128:8080/TextMenu.xml</URL>
</SoftKeyItem>
```

Where:

Specify the key between <Name> and </Name>.

Specify the access URL of a XML file between </URL> and </URL>.

4. Save the file and place this file to the provisioning server.

The following shows an example of a Menu.xml file:

```
<YealinkIPPhoneMenu>
  <Title>XiaMen Yealink</Title>
  <MenuItem>
    <Name>Department1</Name>
    <URL>http://10.3.6.117:8080/Department1.xml</URL>
  </MenuItem>
  <MenuItem>
    <Name>Department2</Name>
    <URL>http://10.3.6.117:8080/Department2.xml</URL>
  </MenuItem>
  <SoftKeyItem>
```

```
<Name>#</Name>  
<URL>http://10.3.6.117:8080/TextMenu</URL>  
</SoftKeyItem>  
</YealinkIPPhoneMenu>
```

When creating a Department.xml file, learn the following:

- `<YealinkIPPhoneDirectory>` indicates the start of a department file and `</YealinkIPPhoneDirectory>` indicates the end of a department file.
- Create contact lists for a department between `<DirectoryEntry>` and `</DirectoryEntry>`.

To customize a Department.xml file:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following strings to the file. Each starts on a separate line:

```
<Name>Mary</Name>  
<Telephone> 1001</Telephone>
```

Where:

Specify the contact name between `<Name>` and `</Name>`.

Specify the contact number between `<Telephone>` and `</Telephone>`.

3. Save the file and place this file to the provisioning server.

The following shows an example of a Department.xml file:

```
<YealinkIPPhoneDirectory>
  <DirectoryEntry>
    <Name>Jack</Name>
    <Telephone>1003</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>John</Name>
    <Telephone>1004</Telephone>
  </DirectoryEntry>
  <DirectoryEntry>
    <Name>Marry</Name>
    <Telephone>1005</Telephone>
  </DirectoryEntry>
</YealinkIPPhoneDirectory>
```

Note

Yealink supplies a phone book generation tool to quickly generate a remote XML phone book. For more information, refer to *Yealink Phonebook Generation Tool User Guide*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using CP860 IP conference phones.

Troubleshooting Methods

IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problems and fix them.

The following are helpful for better understanding and resolving the working status of the IP phone.

- [Viewing Log Files](#)
- [Capturing Packets](#)
- [Enabling the Watch Dog Feature](#)
- [Getting Information from Status Indicators](#)
- [Analyzing Configuration Files](#)

Viewing Log Files

If your IP phone encounters some problems, commonly the log files are needed. You can export the log files to a syslog server or the local system. You can also specify the severity level of the log to be reported to a log file. The default system log level is 3 (Changes to this parameter via web user interface require a reboot).

In the configuration files, you can use the following parameters to configure system log settings:

- **syslog.mode** – Specify the system log to be exported to a server or local system.
- **syslog.server** -- Specify the IP address or domain name of the syslog server to which the log will be exported.
- **syslog.log_level** -- Specify the system log level. The following lists the log level of events you can log:

0: system is unusable

1: action must be taken immediately

2: critical condition

3: error conditions

4: warning conditions

5: normal but significant condition

6: informational

Procedure

Log setting can be configured using the configuration files or locally.

Configuration File	y000000000037.cfg	<p>Configures the syslog mode.</p> <p>Parameters:</p> <p>syslog.mode</p> <p>Configures the IP address or domain name of the syslog server where to export the log files.</p> <p>Parameters:</p> <p>syslog.server</p> <p>Configures the severity level of the logs to be reported to a log file.</p> <p>Parameters:</p> <p>syslog.log_level</p>
Local	Web User Interface	<p>Configures the syslog mode.</p> <p>Configures the IP address or domain name of the syslog server where to export the log files.</p> <p>Configures the severity level of the logs to be reported to a log file.</p> <p>Navigate to:</p> <p>http://<phoneIPAddress>/servlet?p=settings-config&q=load</p>

Details of Configuration Parameters:

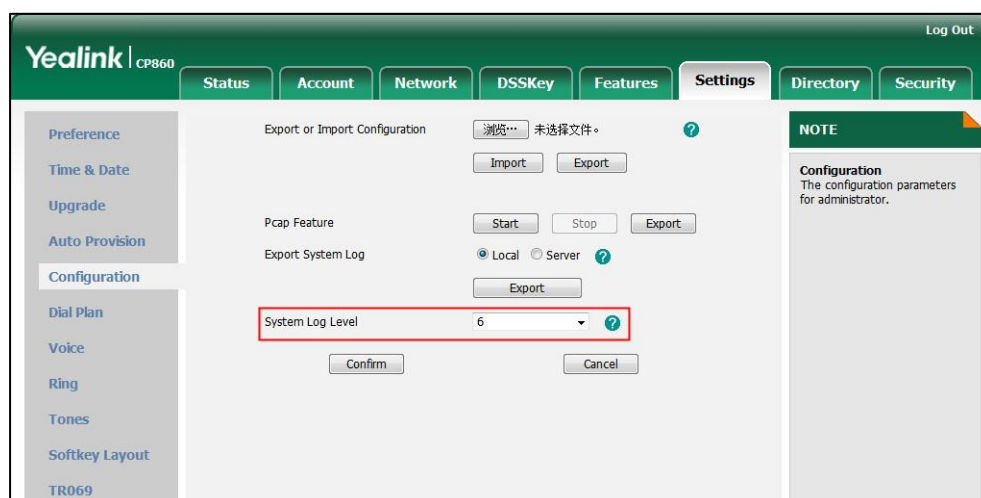
Parameters	Permitted Values	Default
syslog.mode	0 or 1	0
Description:		

Parameters	Permitted Values	Default
<p>Configures the IP phone to export log files to a syslog server or the local system.</p> <p>0-Local</p> <p>1-Server</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Settings->Configuration->Export System Log</p> <p>Phone User Interface:</p> <p>None</p>		
syslog.server	IP address or domain name	Blank
<p>Description:</p> <p>Configures the IP address or domain name of the syslog server when exporting log to the syslog server.</p> <p>Example:</p> <p>syslog.server = 192.168.1.50</p> <p>The log file will be automatically exported to the syslog server 192.168.1.50.</p> <p>Note: It works only if the parameter "syslog.mode" is set to 1 (Server). If you change this parameter, the IP phone will reboot to make the change take effect.</p> <p>Web User Interface:</p> <p>Settings->Configuration->Server Name</p> <p>Phone User Interface:</p> <p>None</p>		
syslog.log_level	Integer from 0 to 6	3
<p>Description:</p> <p>Configures the detail level of syslog information to be exported.</p> <p>0: system is unusable</p> <p>1: action must be taken immediately</p> <p>2: critical condition</p> <p>3: error conditions</p> <p>4: warning conditions</p> <p>5: normal but significant condition</p> <p>6: informational</p> <p>Note: If you change this parameter, the IP phone will reboot to make the change take effect.</p>		

Parameters	Permitted Values	Default
Web User Interface: Settings->Configuration->System Log Level Phone User Interface: None		

To configure the system log level via web user interface:

1. Click on **Settings->Configuration**.
2. Select **6** from the pull-down list of **System Log Level**.



3. Click **Confirm** to accept the change.
A dialog box pops up to prompt "Do you want to restart your machine?". The configuration will take effect after a reboot.
4. Click **OK** to reboot the phone.
After a reboot, the system log level is set as 6, the informational level.

Note Informational level may make some sensitive information accessible (e.g., password-dial number), we recommend that you reset the system log level to 3 after providing the syslog file.

To configure the phone to export the system log to a syslog server via web user interface:

1. Click on **Settings->Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.

3. Enter the IP address or domain name of the syslog server in the **Server Name** field.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is active, and the 'Export or Import Configuration' page is displayed. The 'Export System Log' section is highlighted with a red box. It shows the 'Server' radio button selected, and the 'Server Name' field contains the IP address '10.3.5.136'. The 'System Log Level' is set to '3'. There are 'Confirm' and 'Cancel' buttons at the bottom of the section.

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt "Do you want to restart your machine?". The configuration will take effect after a reboot.
5. Click **OK** to reboot the phone.
The system log will be exported successfully to the desired syslog server after a reboot.
6. Reproduce the issue.

To export a log file to the local system via web user interface:

1. Click on **Settings->Configuration**.
2. Mark the **Local** radio box in the **Export System Log** field.
3. Click **Export** to open file download window, and then save the file to your local system.

The screenshot shows the Yealink CP860 web interface. The 'Settings' tab is active, and the 'Export or Import Configuration' page is displayed. The 'Export System Log' section is highlighted with a red box. It shows the 'Local' radio button selected, and the 'Export' button is visible. The 'System Log Level' is set to '3'. There are 'Confirm' and 'Cancel' buttons at the bottom of the section.

The following figure shows a portion of a log file:

```

190 root      2856 S    /bin/sh /boot/script/netapp.sh
197 root      22484 S   /boot/bin/rtServer.exx
210 root      2856 S    /usr/sbin/telnetd
211 root      17448 S   /boot/bin/autoServer.exx
249 root      3440 S    ./sbin/lighttpd -f /phone/bin/lighttpd/config/lighttp
252 root      18924 S   /phone/www/WEB-INFO/bin/fcgiServer.exx
263 root      2856 S    /sbin/syslogd -S -O /tmp/log/0000000000000.log -s 200
275 root      2856 S    /bin/sh /phone/scripts/phoneapp.sh
276 root      6092 S    ./pcap.exx
291 root      140m S    /phone/bin/dskPhone.exx -qws
300 root          0 SW<   [ethTx/0]
301 root          0 SW<   [ethStatus/0]
309 root      5060 S    /boot/bin/lldpd
310 root      5572 S    /boot/bin/lldpd
357 root          0 DW    [hwthread]
358 root          0 DW    [hausioctl]
359 root          0 SW<   [frameProfiler]
360 root          0 DW<   [Cadence]
369 root      14016 S   /phone/bin/vaServer -q -w -m ANY=5
388 root      2920 S    /phone/bin/snmpd -c /etc/snmpd.conf
389 root      2856 S    /bin/sh /phone/scripts/sipapp.sh
396 root      41396 S N    /phone/bin/sipServer.exx
415 root      1628 S    /phone/bin/busybox udhcpc -b -i eth0 -a -s /boot/bin/
487 root      2856 S    sh -c cd /tmp;ifconfig >> log/0000000000000.log;ps >>
489 root      3180 R    ps
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End2
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() End.write 1024 bytes
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::write() Begin. size= 1;count=1024
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() Begin
Mar 12 03:32:58 fcgiServer.exx: HttpResponseImpl::commitHeader() End

```

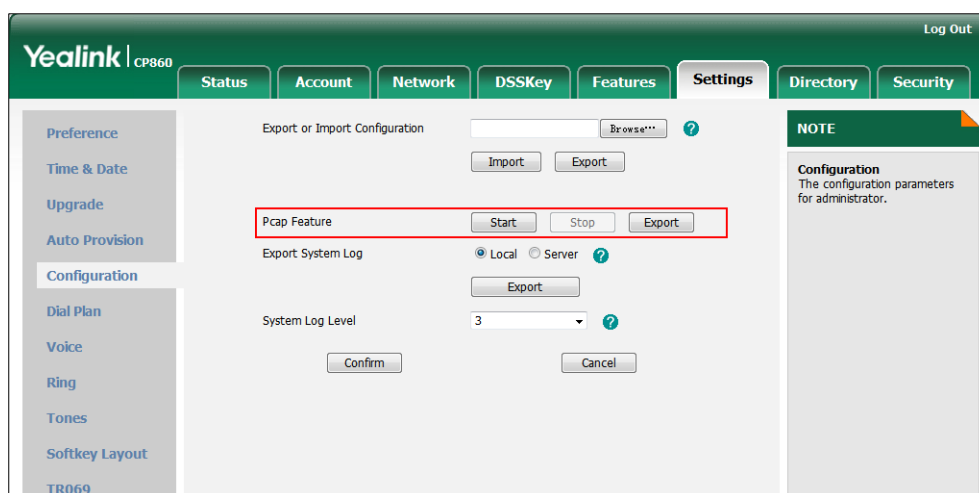
Capturing Packets

You can capture packets in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packets captured for troubleshooting purpose.

To capture packets via web user interface:

1. Click on **Settings->Configuration**.
2. Click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** to stop capturing.

- Click **Export** to open the file download window, and then save the file to your local system.



To capture packets using the Ethernet software:

Connect the Internet port of the IP phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Enabling the Watch Dog Feature

The IP phone provides a troubleshooting feature called “Watch Dog”, which helps you monitor the IP phone status and provides the ability to get stack traces from the last time the IP phone failed. If Watch Dog feature is enabled, the IP phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

You can use the “watch_dog.enable” parameter to configure watch dog in the configuration files.

Procedure

Watch Dog can be configured using the configuration files or locally.

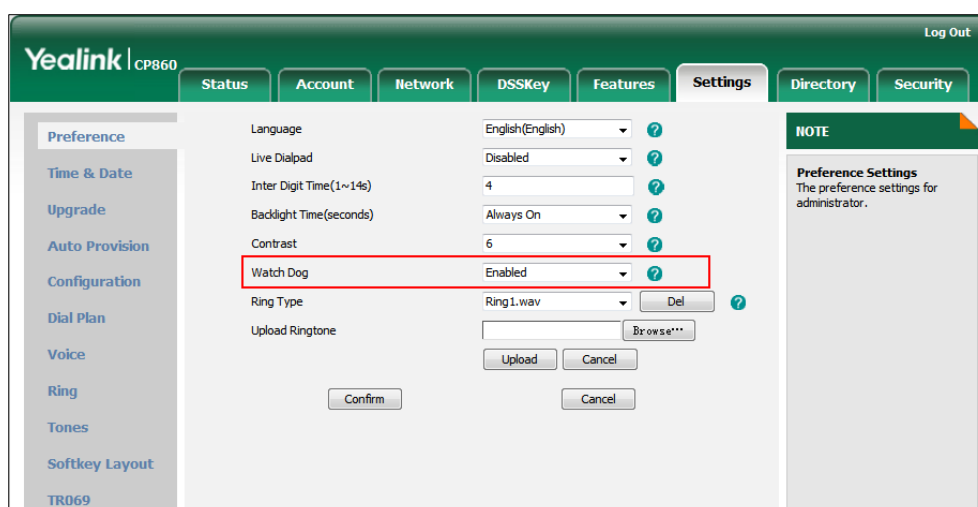
Configuration File	y000000000037.cfg	Configure Watch Dog feature. Parameter: watch_dog.enable
Local	Web User Interface	Configure Watch Dog feature. Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
watch_dog.enable	0 or 1	1
<p>Description : Enables or disables Watch Dog feature.</p> <p>0-Disabled 1-Enabled</p> <p>If it is set to 1 (Enabled), the IP phone will reboot automatically when the system is broken down.</p> <p>Web User Interface: Settings->Preference->Watch Dog</p> <p>Phone User Interface: None</p>		

To configure watch dog via web user interface:

1. Click on **Settings->Preference**.
2. Select the desired value from the pull-down list of **Watch Dog**.



3. Click **Confirm** to accept the change.

Getting Information from Status Indicators

Status indicators may consist of the indicator LEDs and the on-screen icon.

The following shows two examples of obtaining the IP phone information from status indicators on the CP860 IP conference phones:

- If a LINK failure of the IP phone is detected, a prompting message "Network

Unavailable” and the icon  will appear on the LCD screen.

- If an active call on the IP phone is muted, LED indicators illuminate solid red.

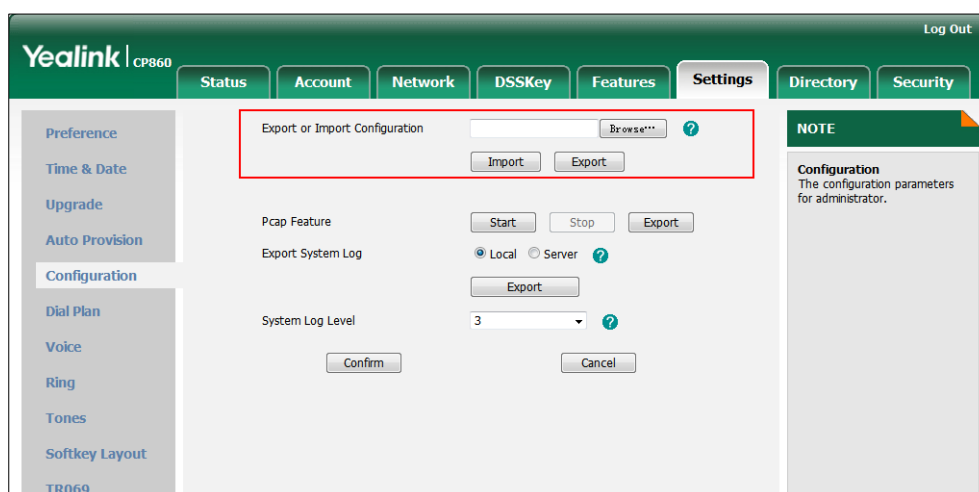
For more information on the icons, refer to [Reading Icons](#) on page 13.

Analyzing Configuration Files

Wrong configurations may have an impact on your phone use. You can export configuration file to check the current configuration of the IP phone and troubleshoot if necessary.

To export configuration file via web user interface:

1. Click on **Settings->Configuration**.
2. In the **Export or Import Configuration** block, click **Export** to open the file download window, and then save the file to your local system.



Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the IP phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

Why is the LCD screen blank?

Do one of the following:

- Ensure that the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone is plugged into a socket controlled by a switch that is on.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet.

- If your phone is PoE powered, ensure that you are using a PoE-compliant switch or hub.

Why doesn't the IP phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the IP phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

How do I find the basic information of the IP phone?

Press the OK key when the IP phone is idle to check the basic information (e.g., IP address, MAC address and firmware version).

Why doesn't the IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the Phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed and refreshed when upgrading firmware via web user interface.

Why doesn't the IP phone display time and date correctly?

Check if the IP phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

Why do I get poor sound quality during a call?

If you have poor sound quality/acoustics like intermittent voice, low volume, echo or other noise, the possible reasons could be:

- Users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause echo.
- Intermittent voice is mainly caused by packet loss, due to network congestion, and jitter, due to message recombination of transmission or receiving equipment (e.g., timeout handling, retransmission mechanism or buffer under run).
- Noisy equipment, such as a computer or a fan, may cause voice interference. Turn off any noisy equipment.

What is the difference between a remote phone book and a local phone book?

A remote phone book is placed on a server, while a local phone book is placed on the phone flash. A remote phone book can be used by everyone that can access the server, while a local phone book can only be used by a specific phone. A remote phone book is always used as a central phone book for a company; each employee can load it to obtain the real-time data from the same server.

What is the difference between user name, register name and display name?

Both user name and register name are defined by the server. User name identifies the account, while register name matched with a password is for authentication purposes. Display name is the caller ID that will be displayed on the callee's phone LCD screen. Server configurations may override the local ones.

How to reboot the IP phone remotely?

IP phones support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. When receiving a NOTIFY message with the parameter "reboot=true", the IP phone reboots immediately.

The message is formed as below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
```

```
From: sip:sipsak@<srchost>  
CSeq: 10 NOTIFY  
Call-ID: 1234@<srchost>  
Event: check-sync;reboot=true
```

Why does the IP phone use DOB format logo file instead of popular BMP, JPG and so on?

The IP phone only uses logo file in DOB format, as the DOB format file has a high compression ratio (the size of the uncompressed file compared to that of the compressed file) and can be stored in smaller space. Tools for converting BMP format to DOB format are available. For more information, refer to *Yealink_SIP-T2_Series_T19P_T4_Series_CP860_IP_Phones_Auto_Provisioning_Guide*, available online:

<http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

What will happen if I connect both PoE cable and power adapter?

Which has the higher priority?

IP phones use the PoE preferentially.

What is auto provisioning?

Auto provisioning refers to the update of IP phones, including update on configuration parameters, local phonebook, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

What is PnP?

Plug and Play (PnP) is a method for IP phones to acquire the provisioning server address. With PnP enabled, the IP phone broadcasts the PNP SUBSCRIBE message to obtain a provisioning server address during startup. Any SIP server recognizing the message will respond with the preconfigured provisioning server address, so the IP phone will be able to download the configuration files from the provisioning server. PnP depends on support from a SIP server.

Why doesn't the IP phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP phone model.
- The configuration may depend on support from a server.

What do "on code" and "off code" mean?

They are codes that the IP phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

For example, if you set the Always Forward on code to be *78 (may vary on different servers), and the target number to be 201. When you enable Always Forward on the IP phone, the IP phone sends *78201 to the server, and then the server will enable Always Forward feature on the server side, hence being able to get the right status of the extension.

Note

The use of anonymous call codes differ from that of other codes. For more information, refer to *Yealink_CP860_User_Guide*.

How to solve the IP conflict problem?

Do one of the following:

- Reset another available IP address for the IP phone.
- Check network configuration via phone user interface at the path **Menu->Settings->Advanced Settings->Network->WAN Port->IPv4 (or IPv6)**. If the Static IP is selected, select DHCP instead.

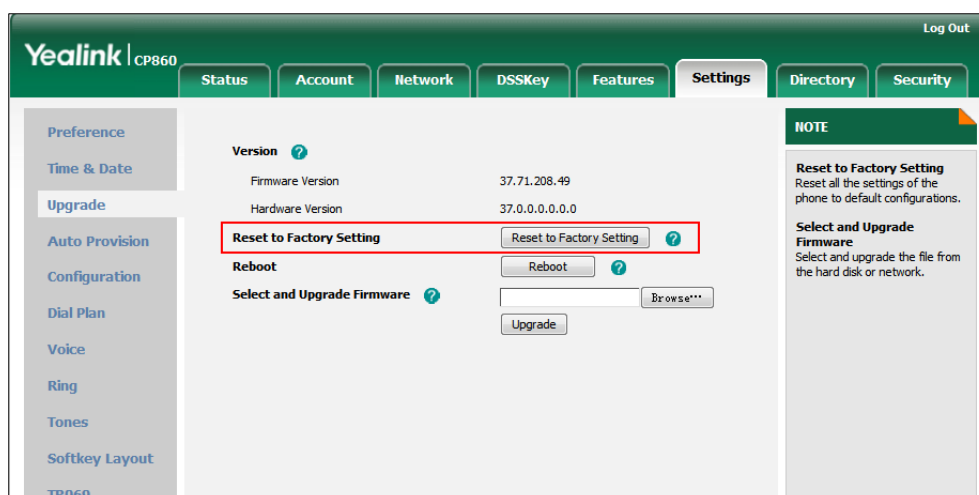
How to reset your phone to factory configurations?

Reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not resolve the problem. Note that all custom settings will be overwritten after resetting.

To reset your phone via web user interface:

1. Click on **Settings->Upgrade**.
2. Click **Reset to Factory Setting** in the **Reset to Factory Setting** field.

The web user interface prompts the message “Do you want to reset to factory?”.



3. Click **OK** to confirm the resetting.

The IP phone will be reset to factory successfully after startup.

Note

Reset of the phone may take a few minutes. Do not power off until the IP phone starts up successfully.

How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

Appendix

Appendix A: Glossary

802.1x — an IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN.

ACS (Auto Configuration server) — responsible for auto-configuration of the Central Processing Element (CPE).

Cryptographic Key — a piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

DHCP (Dynamic Host Configuration Protocol) — built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Option — can be configured for specific values and enabled for assignment and distribution to DHCP clients based on server, scope, class or client-specific levels.

DNS (Domain Name System) — a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) — only provides authentication of the EAP peer to the EAP server but not mutual authentication.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) — Provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2) — Provides for mutual authentication, but does not require a client certificate on the IP phone.

FAC (Feature Access Code) — special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol) — used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) — a widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers) — a non-profit professional association headquartered in New York City that is dedicated to advancing

technological innovation and excellence.

LAN (Local Area Network) — used to interconnects network devices in a limited area such as a home, school, computer laboratory, or office building.

MIB (Management Information Base) — a virtual database used for managing the entities in a communications network.

OID (Object Identifier) — assigned to an individual object within a MIB.

PNP (Plug and Play) — a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory) — a class of storage medium used in computers and other electronic devices.

RTP (Real-time Transport Protocol) — provides end-to-end service for real-time data.

TCP (Transmission Control Protocol) — a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol) — a protocol offers non-guaranteed datagram delivery.

URI (Uniform Resource Identifier) — a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator) — specifies the address of an Internet resource.

VLAN (Virtual LAN) — a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol) — a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network) — a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol) — which uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zone	Time Zone Name
– 11:00	Samoa
– 10:00	United States-Hawaii-Aleutian
– 10:00	United States-Alaska-Aleutian
– 09:00	United States-Alaska Time
– 08:00	Canada(Vancouver, Whitehorse)
– 08:00	Mexico(Tijuana, Mexicali)
– 08:00	United States-Pacific Time
– 07:00	Canada(Edmonton, Calgary)
– 07:00	Mexico(Mazatlan, Chihuahua)
– 07:00	United States-Mountain Time
– 07:00	United States-MST no DST
– 06:00	Canada-Manitoba(Winnipeg)
– 06:00	Chile(Easter Islands)
– 06:00	Mexico(Mexico City, Acapulco)
– 06:00	United States-Central Time
– 05:00	Bahamas(Nassau)
– 05:00	Canada(Montreal, Ottawa, Quebec)
– 05:00	Cuba(Havana)
– 05:00	United States-Eastern Time
– 04:30	Venezuela(Caracas)
– 04:00	Canada(Halifax, Saint John)
– 04:00	Chile(Santiago)
– 04:00	Paraguay(Asuncion)
– 04:00	United Kingdom-Bermuda(Bermuda)
– 04:00	United Kingdom(Falkland Islands)
– 04:00	Trinidad&Tobago
– 03:30	Canada-New Foundland(St.Johns)
– 03:00	Denmark-Greenland(Nuuk)
– 03:00	Argentina(Buenos Aires)
– 03:00	Brazil(no DST)
– 03:00	Brazil(DST)
– 02:00	Brazil(no DST)
– 01:00	Portugal(Azores)
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)

Time Zone	Time Zone Name
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Spain(Madrid)
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)

Time Zone	Time Zone Name
+04:30	Afghanistan
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+12:00	New Zealand(Wellington, Auckland)
+12:45	New Zealand(Chatham Islands)
+13:00	Tonga(Nukualofa)

Appendix C: Configuring Programmable Key

This appendix describes the programmable key parameters you can configure on IP phones. Programmable keys can be assigned with various key features. The CP860 IP phones support 8 programmable keys. The programmable key takes effect only if the IP phone is idle.

The parameters of the programmable key are detailed in the following:

Parameter- programmablekey.X.type (X=1-6, 9, 13)	Configuration File y000000000037.cfg
Description	Configures the key feature for the programmable key.

	Valid types are: <ul style="list-style-type: none"> • N/A • Forward • DND • Call Return • Intercom • XML Group • Multicast Paging • History • Menu • Status • LDAP • Prefix • Local Directory • Local Group • XML Directory • Keypad Lock • Directory
Format	Integer
Default Value	<p>when x=1, the default value is 28.</p> <p>when x=2, the default value is 61.</p> <p>when x=3, the default value is 5.</p> <p>when x=4, the default value is 30.</p> <p>when x=5, the default value is 28.</p> <p>when x=6, the default value is 0.</p> <p>when x=9, the default value is 33.</p> <p>when x=13, the default value is 0.</p>
Range	Valid values are: <p>0-N/A</p> <p>2-Forward</p> <p>5-DND</p> <p>7-Call Return</p> <p>14-Intercom</p> <p>22-XML Group</p> <p>24-Multicast Paging</p> <p>28-History</p> <p>30-Menu</p> <p>33-Status</p> <p>38-LDAP</p> <p>40-Prefix</p> <p>43-Local Directory</p>

	45-Local Group 47-XML Directory 50-Keypad Lock 61-Directory
Example	programablekey.1.type = 0

Parameter- programablekey.X.value (X=1-6, 9, 13)	Configuration File y000000000037.cfg
Description	Configures the value for some key features.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	When you assign the Prefix to the key, this parameter is used to add a specified prefix number before the dialed number. programablekey.1.value = 0592

Parameter- programablekey.X.label (X ranges from 1 to 4)	Configuration File y000000000037.cfg
Description	Configures the label displayed on the LCD screen for each soft key. This is an optional configuration.
Format	String
Default Value	Blank
Range	String within 99 characters
Example	programablekey.1.label = Dir

Parameter- programablekey.X.xml_phonebook (X=1-6, 9, 13)	Configuration File y000000000037.cfg
Description	Configures the desired group or remote phone book when multiple groups or remote phone books are configured on the IP phone.

	<p>This parameter is only applicable to Local Group/XML Group features.</p> <p>When the key feature is configured as Local Group, valid values are:</p> <p>0-All contacts</p> <p>1-First local group</p> <p>...</p> <p>48-Forty-eighth local group</p> <p>When the key feature is configured as XML Group (remote phone book), valid values are:</p> <p>0-First XML group</p> <p>1-Second XML group</p> <p>...</p> <p>4-Fifth XML group</p>
Format	Integer
Default Value	0
Range	0 to 48
Example	<p>Configures the second remote phone book.</p> <p>programablekey.1.xml_phonebook = 1</p>

Appendix D: SIP (Session Initiation Protocol)

This section describes how Yealink CP860 IP conference phones comply with the IETF definition of SIP as described in RFC 3261.

This section contains compliance information in the following:

- [RFC and Internet Draft Support](#)
- [SIP Request](#)
- [SIP Header](#)
- [SIP Responses](#)
- [SIP Session Description Protocol \(SDP\) Usage](#)

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 1889—RTP Media control
- RFC 2112—Multipart MIME
- RFC 2246—The TLS Protocol Version 1.0
- RFC 2327—SDP: Session Description Protocol
- RFC 2543—SIP: Session Initiation Protocol
- RFC 2616—Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2617—Http Authentication: Basic and Digest access authentication
- RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806—URLs for Telephone Calls
- RFC 2833—RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC2915—The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 3087—Control of Service Context using SIP Request-URI
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3266—Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310—HTTP Digest Authentication Using Authentication and Key Agreement (AKA)
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312—Integration of Resource Management and SIP
- RFC 3313—Private SIP Extensions for Media Authorization
- RFC 3323—A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324—Requirements for Network Asserted Identity
- RFC 3325—SIP Asserted Identity
- RFC 3326—The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3361—DHCP-for-IPv4 Option for SIP Servers
- RFC 3372—SIP for Telephones (SIP-T): Context and Architectures
- RFC 3420—Internet Media Type message/sipfrag

- RFC 3428—Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455—Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486—Compressing the Session Initiation Protocol (SIP)
- RFC 3489—STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3550—RTP , RTCP, IETF RFC 3550
- RFC 3556—Session Description Protocol (SDP) Bandwidth Modifiers for RTCP Bandwidth
- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666—SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680—SIP Event Package for Registrations
- RFC 3702—Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3890—A Transport Independent Bandwidth Modifier for the SDP
- RFC 3891—The Session Initiation Protocol (SIP) “Replaces” Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for SIP
- RFC 3960—Early Media and Ringing Tone Generation in SIP
- RFC3966—The tel URI for telephone number
- RFC 3968—The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 3969—The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4244—An Extension to the SIP for Request History Information

- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control - Conferencing for User Agents
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples
- RFC 5589—Session Initiation Protocol (SIP) Call Control - Transfer
- draft-levy-sip-diversion-04.txt—Diversion Indication in SIP
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents

To find the applicable Request for Comments (RFC) document, go to <http://www.ietf.org/rfc.html> and enter the RFC number.

SIP Request

The following SIP request messages are supported:

Method	Supported	Notes
REGISTER	Yes	
INVITE	Yes	Yealink CP860 IP conference phones support mid-call changes such as putting a call on hold as signaled by a new

Method	Supported	Notes
		INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

SIP Header

The following SIP request headers are supported:

Method	Supported	Notes
Accept	Yes	
Alert-Info	Yes	
Allow	Yes	
Allow-Events	Yes	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	
Diversion	Yes	

Method	Supported	Notes
Event	Yes	
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
Require	Yes	
Route	Yes	
RSeq	Yes	
Session-Expires	Yes	
Subscription-State	Yes	
Supported	Yes	
To	Yes	
User-Agent	Yes	
Via	Yes	

SIP Responses

The following SIP responses are supported:

1xx Response—Information Responses

1xx Response	Supported	Notes
--------------	-----------	-------

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
183 Session Progress	Yes	

2xx Response—Successful Responses

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Response—Redirection Responses

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	

4xx Response—Request Failure Responses

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	
410 Gone	No	

4xx Response	Supported	Notes
411 Length Required	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	Yes	
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
421 Extension Required	No	
423 Interval Too Brief	Yes	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

5xx Response—Server Failure Responses

5xx Response	Supported	Notes
500 Internal Server Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Gateway Timeout	No	
505 Version Not Supported	No	

6xx Response—Global Responses

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v—Protocol version	Yes
o—Owner/creator and session identifier	Yes
a—Media attribute	Yes
c—Connection information	Yes
m—Media name and transport address	Yes
s—Session name	Yes
t—Active time	Yes

Appendix E: SIP Call Flows

SIP uses six request methods:

- INVITE—Indicates a user is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the IP phone or the SIP server:

- SIP 1xx—Informational Responses

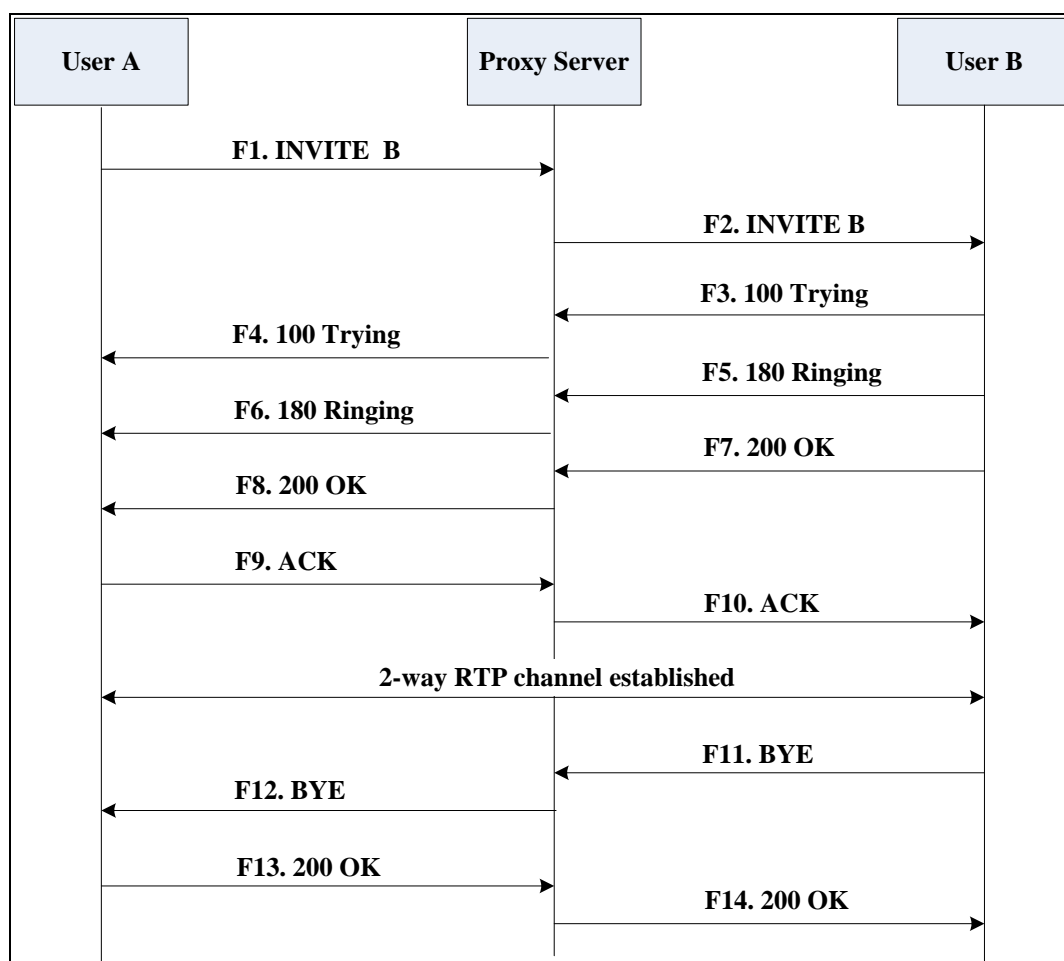
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B hangs up.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends a SIP INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.
F5	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.
F6	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.

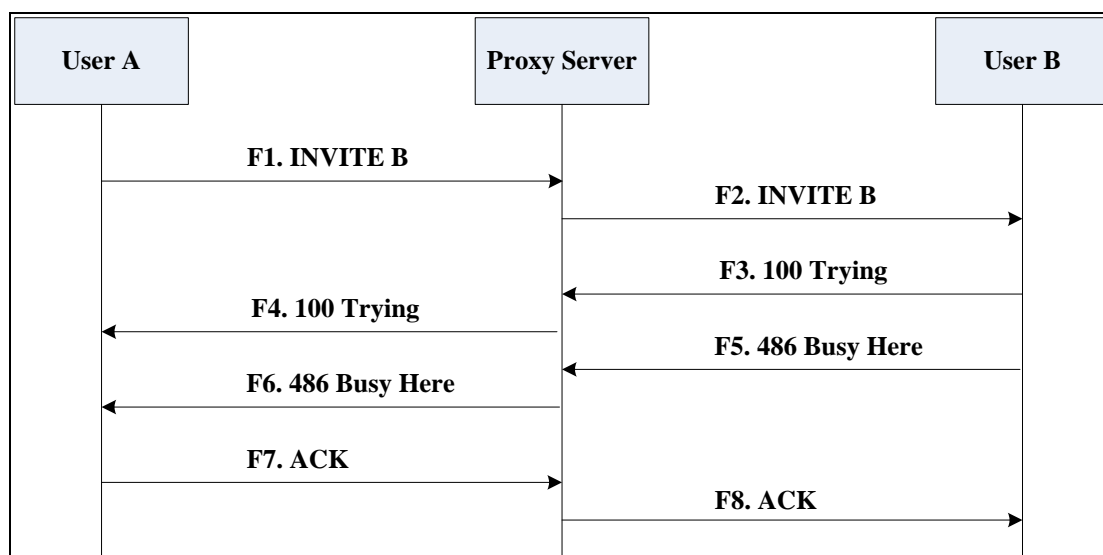
Step	Action	Description
F7	200 OK— User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F9	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F10	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F11	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F12	BYE—Proxy Server to User A	The proxy server forwards the SIP BYE request to User A to notify that User B wants to release the call.
F13	200 OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response indicates that User A has received the BYE request. The call session is now terminated.
F14	200 OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B to indicate that User A has received the BYE request. The call session is now terminated.

Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B is busy on the IP phone and unable or unwilling to take another call.
The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> The IP address of User B is inserted in the Request-URI field. User A is identified as the call session initiator in the From field. A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. The transaction number within a single call leg is identified in the CSeq field. The media capability User A is ready to receive is specified. The port on which User B is prepared to receive the RTP data

Step	Action	Description
		is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.
F5	486 Busy Here—User B to Proxy Server	User B sends a SIP 486 Busy Here response to the proxy server. The 486 Busy Here response is a client error response indicating that User B is successfully connected but User B is busy on the IP phone and unable or unwilling to take the call.
F6	486 Busy Here—Proxy Server to User A	The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The SIP ACK message indicates that User A has received the 486 Busy Here message.
F8	ACK—Proxy Server to User B	The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.

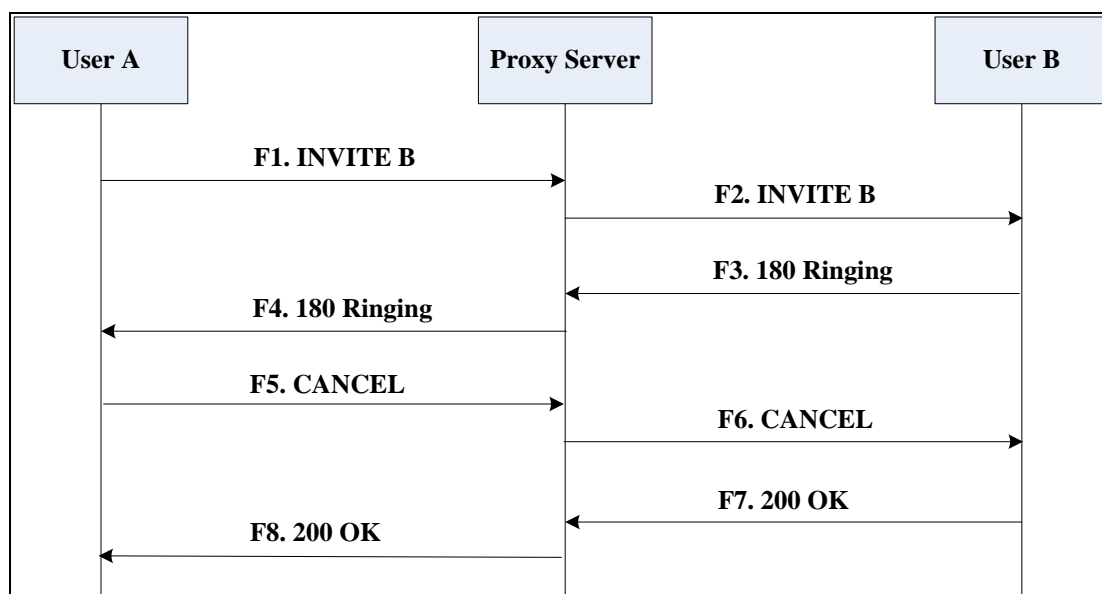
Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call caused by the called user's no answering. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B does not answer the call.
3. User A hangs up.

The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.

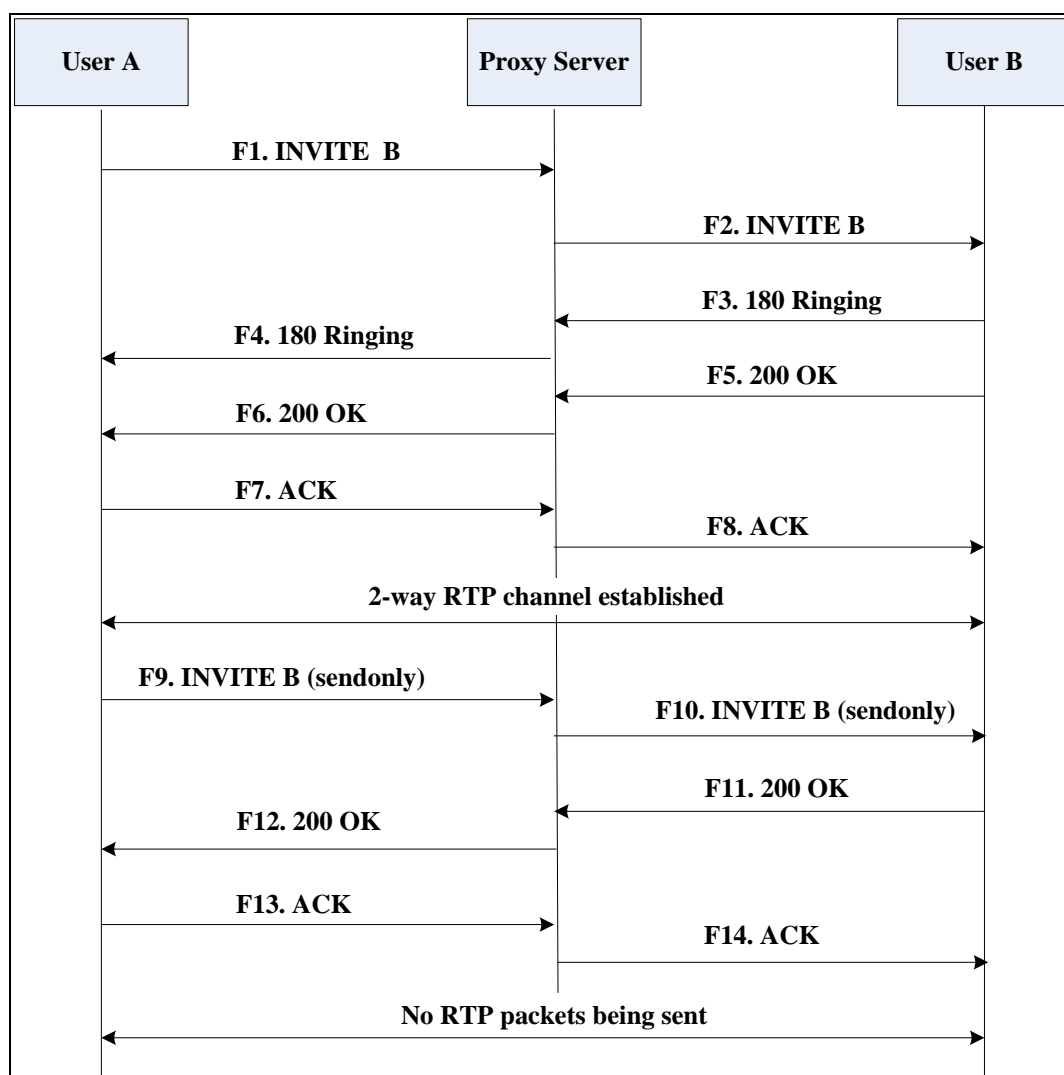
Step	Action	Description
		<ul style="list-style-type: none"> The transaction number within a single call leg is identified in the CSeq field. The media capability User A is ready to receive is specified. The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	CANCEL—User A to Proxy Server	User A sends a SIP CANCEL request to the proxy server after not receiving an appropriate response within the time allocated in the INVITE request. The SIP CANCEL request indicates that User A wants to disconnect the call.
F6	CANCEL—Proxy Server to User B	The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.
F7	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.

Successful Call Setup and Call Hold

The following figure illustrates a successful call setup and call hold. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

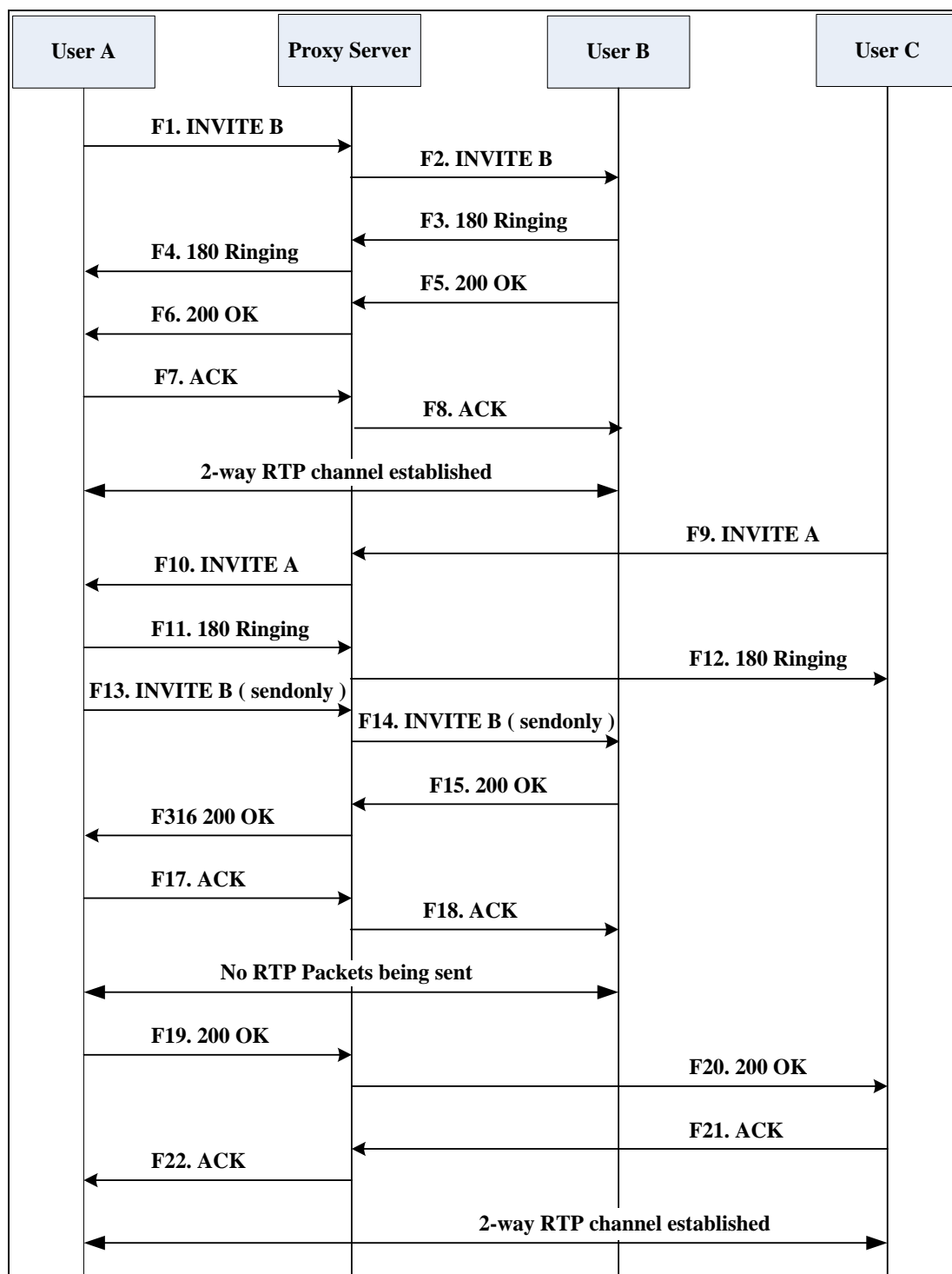
Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.

Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call, one of the participants receives and answers an incoming call from a third party. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User C calls User B.
4. User B accepts the call from User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User C to Proxy Server	<p>User C sends a SIP INVITE message to the proxy server. The INVITE request is an invitation to User A to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User A is inserted in the Request-URI field. • User C is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User C is ready to receive is specified. • The port on which User A is prepared to receive the RTP data is specified.
F10	INVITE—Proxy Server to User A	The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.
F11	180 Ringing—User A to Proxy Server	User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User C	The proxy server forwards the 180 Ringing response to User C. User C hears the ring-back tone indicating that User A is being alerted.

Step	Action	Description
F13	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F14	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK—User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.
F16	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F17	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F18	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F19	200 OK—User A to Proxy Server	User A sends a 200 OK response to the proxy server. The 200 OK response notifies that the connection has been made.
F20	200 OK—Proxy Server User C	The proxy server forwards the 200 OK message to User C.
F21	ACK—User C to Proxy Server	User C sends a SIP ACK to the proxy server. The ACK confirms that User C has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User A	The proxy server forwards the SIP ACK to User A to confirm that User C has received the 200 OK response.

Call Transfer without Consultation

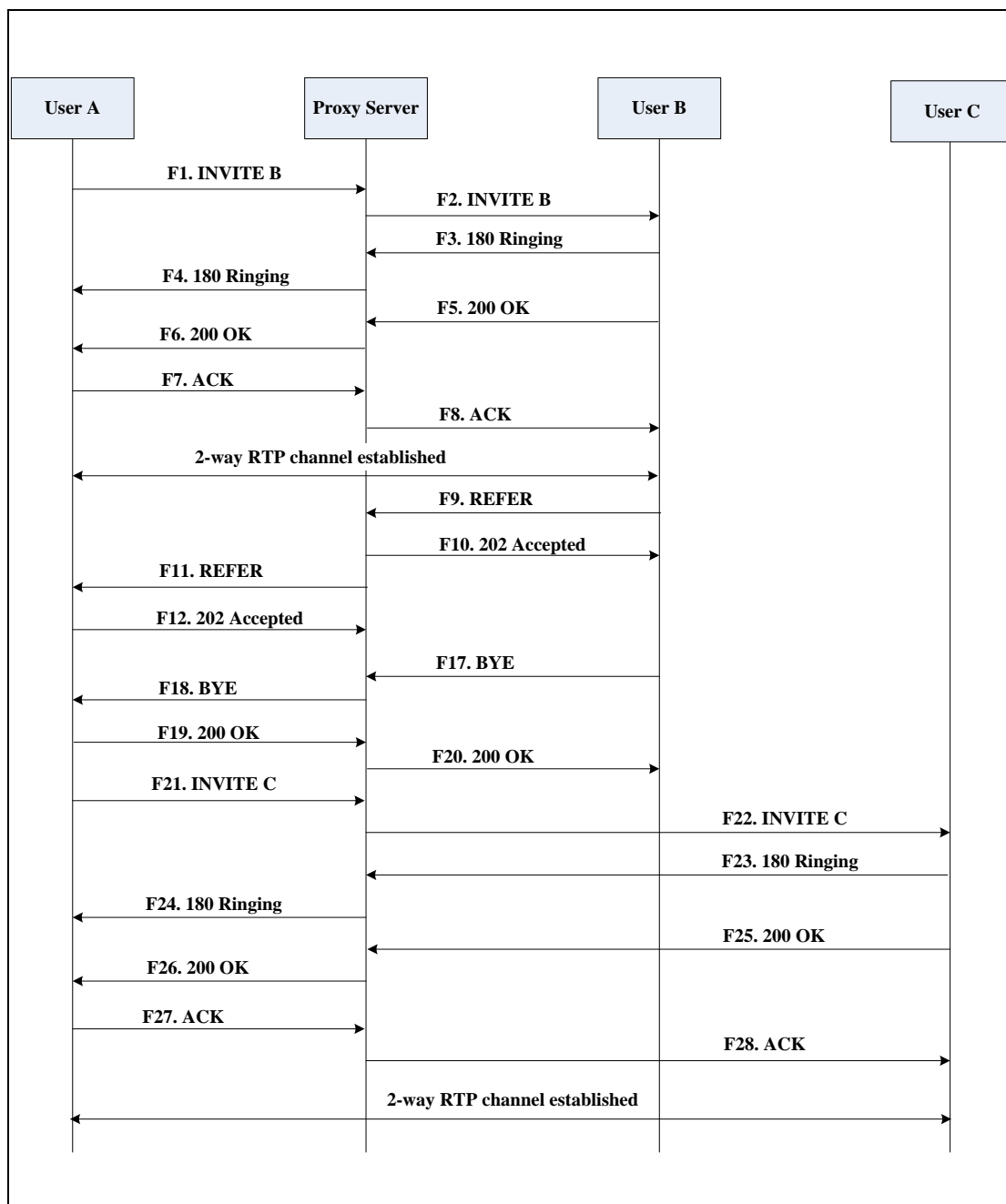
The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consultation. This is called a blind transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.

4. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to the proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	REFER—User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted—Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted response notifies User B that the proxy server has received the REFER message.
F11	REFER—Proxy Server to User A	The proxy server forwards the REFER message to User A.
F12	202 Accepted—User A to Proxy Server	User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.
F13	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F14	BYE—Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	200OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response confirms that User A has received the BYE request.
F16	200OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B.
F17	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A

Step	Action	Description
		requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

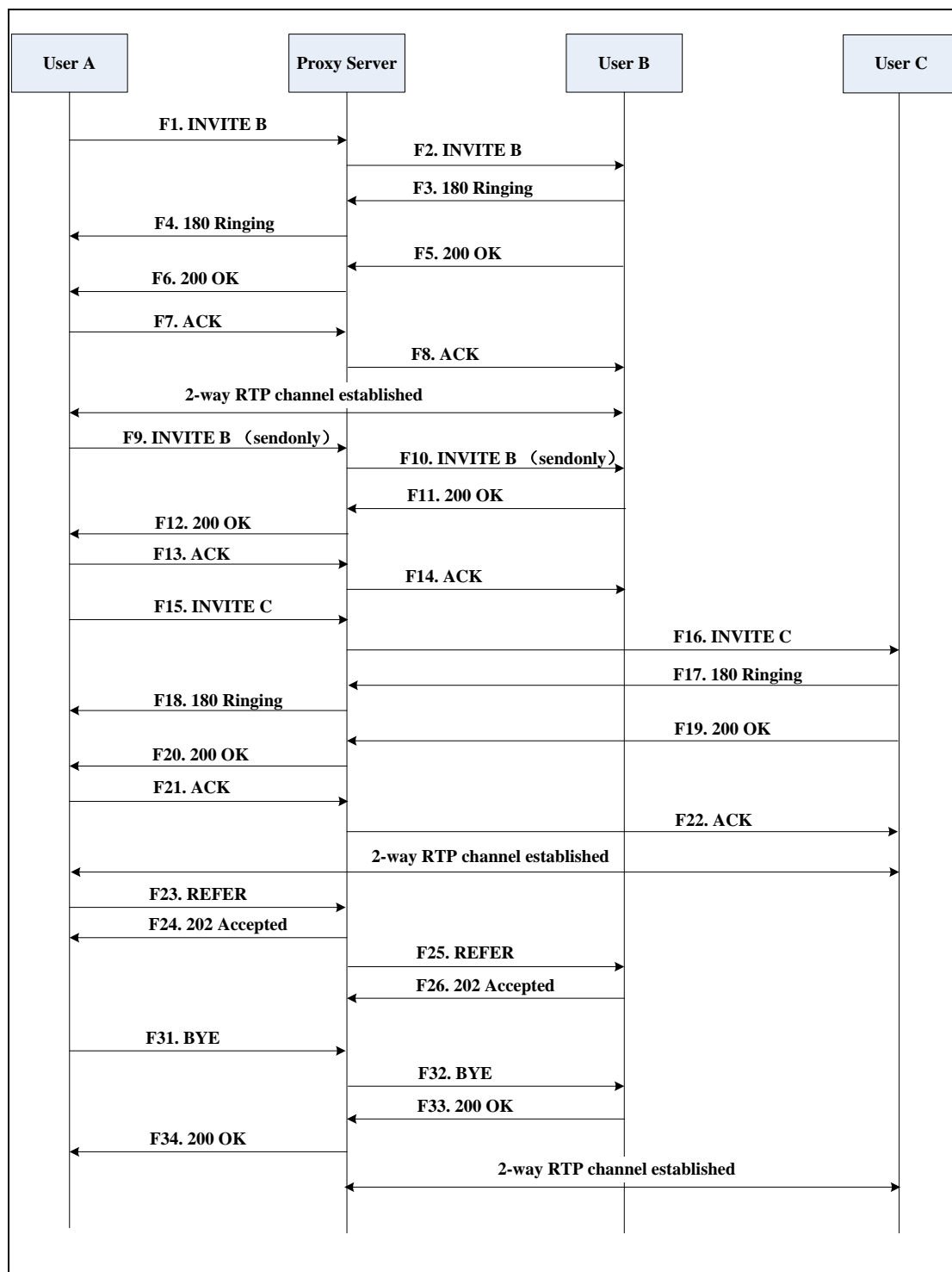
Call Transfer with Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A calls User C.
4. User C answers the call.

5. User A transfers the call to User C.
Call is established between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE was successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI in the To field to User C. The proxy server

Step	Action	Description
	C	sends the INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F23	REFER—User A to Proxy Server	User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.
F24	202 Accepted—Proxy Server to User A	The proxy server sends a SIP 202 Accepted response to User A. The 202 Accepted response notifies User A that the proxy server has received the REFER message.
F25	REFER—Proxy Server to User B	The proxy server forwards the REFER message to User B.
F26	202 Accepted—User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted

Step	Action	Description
		response indicates that User B accepts the transfer.
F27	BYE—User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE—Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

Always Call Forward

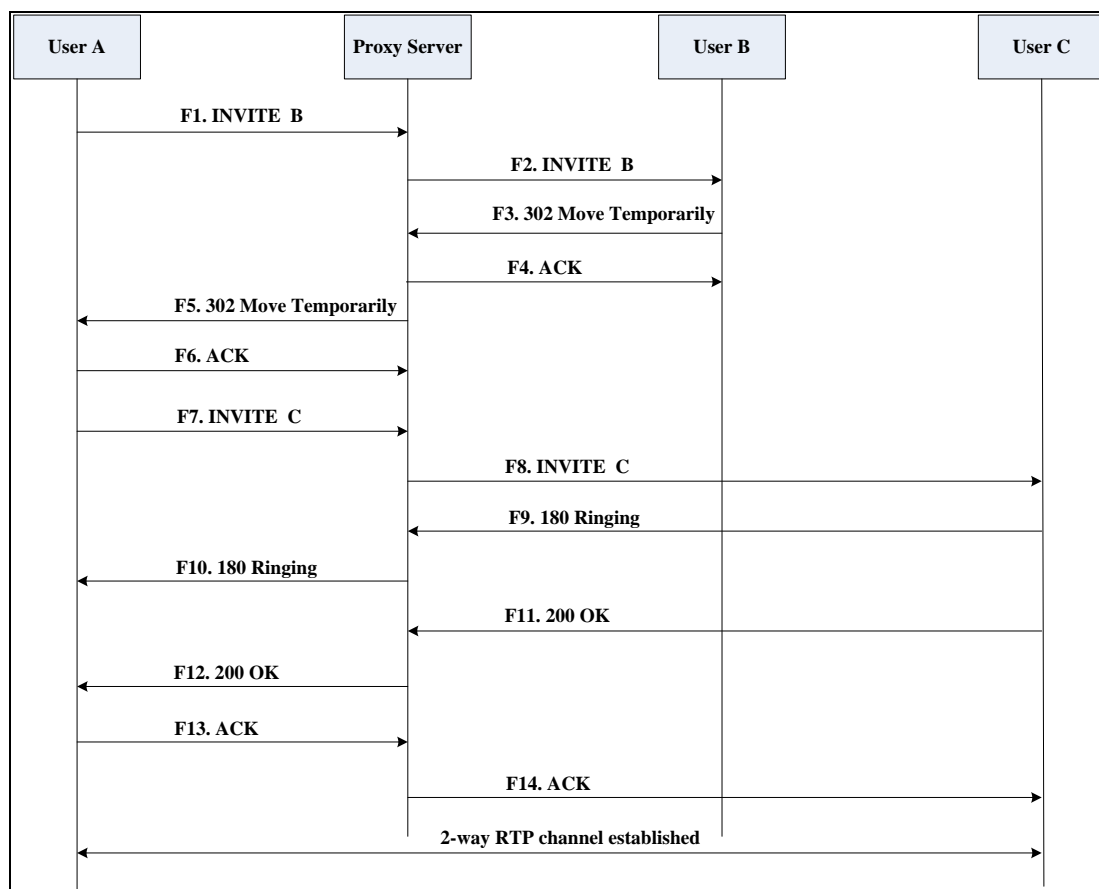
The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.

4. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of the User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F4	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.

Step	Action	Description
F7	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requested the call.
F8	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F9	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F10	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F11	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F12	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F13	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F14	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

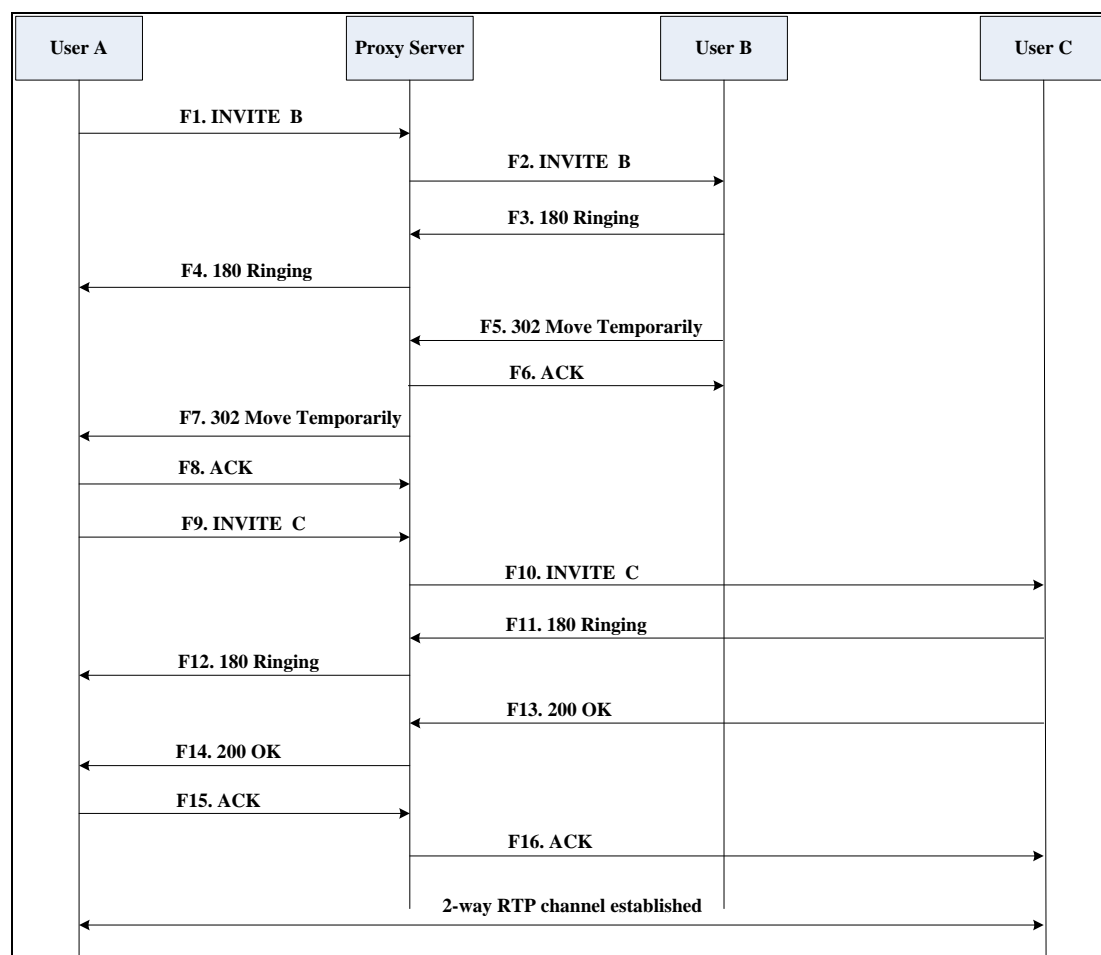
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C.

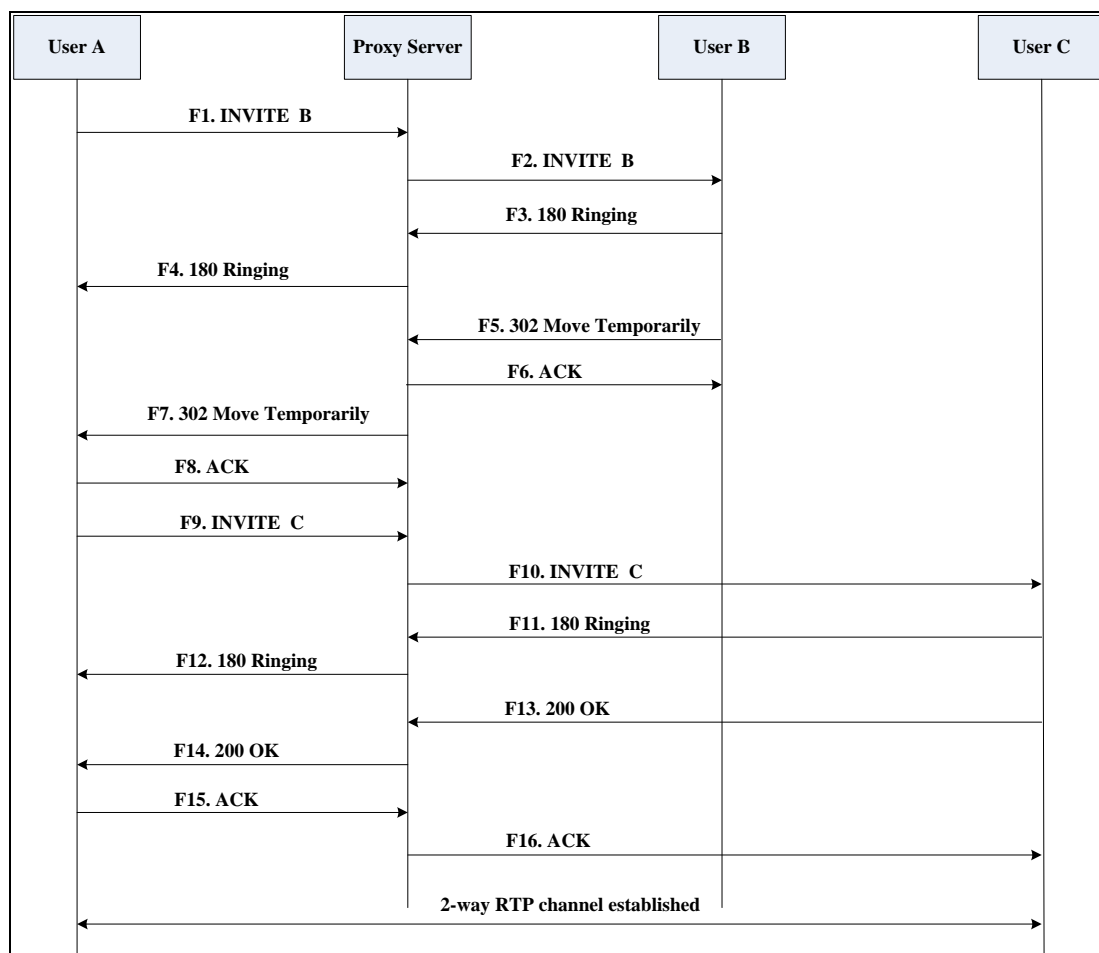
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily—User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK—Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the

Step	Action	Description
		ACK message.
F7	302 Move Temporarily—Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE—Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F15	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

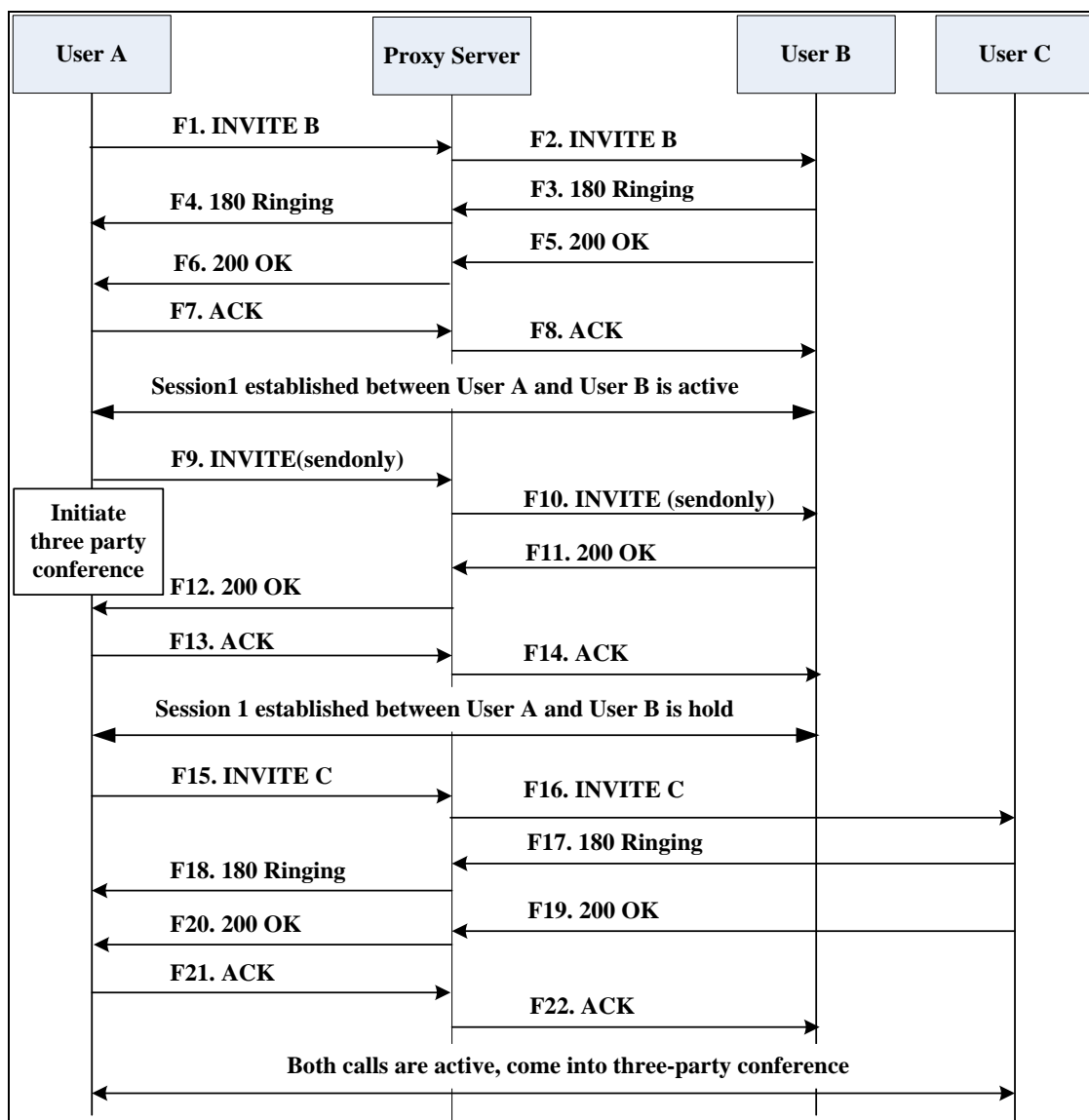
Call Conference

The following figure illustrates successful 3-way calling between Yealink CP860 IP conference phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A puts User B on hold.
4. User A calls User C.
5. User C answers the call.

6. User A mixes the RTP channels and establishes a conference between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	<p>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User A that User B is successfully put on hold.
F13	ACK—User A to Proxy Server	User A sends the ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User	The proxy server maps the SIP URI in the To field to User C. The proxy server

Step	Action	Description
	C	sends the SIP INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

Index

Numeric

- 180 Ring Workaround [126](#)
- 802.1x Authentication [268](#)

A

- About This Guide [v](#)
- Acoustic Echo Cancellation [298](#)
- Action URL [215](#)
- Action URI [230](#)
- Administrator Password [48](#)
- Always Forward [136](#)
- Analyzing the Configuration Files [343](#)
- Anonymous Call [112](#)
- Anonymous Call Rejection [116](#)
- Appendix [349](#)
- Appendix A: Glossary [349](#)
- Appendix B: Time Zones [351](#)
- Appendix C: Configuration Parameters [353](#)
- Appendix D: SIP [356](#)
- Appendix E: SIP Call Flows [364](#)
- Area Code [87](#)
- Attended Transfer [147](#)
- Audio Codecs [291](#)
- Auto Answer [109](#)
- Auto Redial [107](#)

B

- Backlight [42](#)
- Blind Transfer [147](#)
- Block Out [89](#)
- Busy Forward [136](#)
- Busy Tone Delay [123](#)

C

- Call Forward [136](#)
- Call Hold [131](#)

- Call Log [96](#)
- Call Return [160](#)
- Call Transfer [147](#)
- Call Waiting [103](#)
- Call Waiting Tone [103](#)
- Calling Line Identification Presentation [162](#)
- Connected Line Identification Presentation [164](#)
- Capturing Packets [340](#)
- Comfort Noise Generation [301](#)
- Configuration Files [15](#)
- Configuration Methods [14](#)
- Configuring Advanced features [179](#)
- Configuring Basic Features [39](#)
- Configuring Basic Network Parameters [18](#)
- Connecting the IP phone [7](#)
- Configuring Security Features [305](#)

D

- Dial Plan [81](#)
- Dial-now [84](#)
- Dial-now Template [325](#)
- Directory [93](#)
- Directed Call Pickup [153](#)
- Distinctive Ring Tones [180](#)
- Do Not Disturb (DND) [118](#)
- Documentations [v](#)
- DTMF [164](#)

E

- Early Media [126](#)
- Encrypting Configuration Files [316](#)
- Enabling the Watch Dog Feature [341](#)

G

- Getting Information from Status Indicators [342](#)
- Getting Started [7](#)
- Group Call Pickup [157](#)

H

H.323 [1](#)
Hotline [90](#)

I

In This Guide [v](#)
Index [403](#)
Initialization Process Overview [9](#)
Intercom [174](#)
IPv6 Support [283](#)

J

Jitter Buffer [302](#)

K

Key as Send [77](#)
Key Features of CP860 IP conference phones [4](#)

L

Language [66](#)
LDAP [196](#)
Live Dialpad [101](#)
LLDP [244](#)
Loading Language Packs [66](#)
Local Contact File [330](#)
Local Directory [99](#)
Logo Customization [70](#)

M

Message Waiting Indicator [204](#)
Missed Call Log [97](#)
Multicast Paging [208](#)
Music on Hold [131](#)

N

NAT Traversal [266](#)
Network Address Translation (NAT) [266](#)
Network Conference [150](#)
No Answer Forward [136](#)

P

Phone Lock [50](#)
Phone User Interface [15](#)
Physical Features of CP860 IP conference phones [4](#)
Product Overview [1](#)

Q

Quality of Service [262](#)

R

Reading Icons [13](#)
Remote Phone Book [192](#)
Remote XML Phonebook [331](#)
Replace Rule [82](#)
Replace Rule Template [324](#)
Return Message When DND [119](#)
Return Code When Refuse [124](#)
RFC and Internet Draft Support [357](#)

S

Search Source List in Dialing [94](#)
Semi-attended Transfer [147](#)
Server Redundancy [232](#)
Session Timer [136](#)
SIP [1](#)
SIP Components [2](#)
SIP Header [360](#)
SIP Request [359](#)
SIP Responses [361](#)
SIP IP Phone Models [3](#)
SIP Session Description Protocol Usage [364](#)
SIP Session Timer [129](#)
Softkey Layout [72](#)
Specifying the Language to Use [67](#)
SRTP [314](#)
STUN Server [266](#)
Suppressing DTMF Display [169](#)

T

Table of Contents [vii](#)
Time and Date [54](#)

Transfer on Conference Hang Up [152](#)
Transfer via DTMF [172](#)
Transport Layer Security (TLS) [305](#)
Troubleshooting [335](#)
Troubleshooting Methods [335](#)
Troubleshooting Solutions [343](#)
TR-069 Device Management [278](#)

U

Upgrading Firmware [32](#)
Use Outbound Proxy in Dialog [128](#)
User Agent Client (UAC) [2](#)
User Agent Server (UAS) [3](#)
User Password [46](#)

V

Verifying Startup [13](#)
Viewing Log Files [335](#)
VLAN [255](#)
Voice Activity Detection [299](#)
VoIP Principle [1](#)
VPN [259](#)

W

Web Server Type [43](#)
Web User Interface [15](#)