



VC Series Video Conferencing System Administrator Guide

Copyright

Copyright © 2016 YEALINK NETWORK TECHNOLOGY

Copyright © 2016 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 via the media, Yealink Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file for private use only and 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 USE 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.

You can find the CE and FCC information from the label on the back of the Codec.

CE Mark Warning

This device marked with the CE mark is in compliance with radio equipment and telecommunications terminal equipment directive 1999/5/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.
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 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. WEEE must not be regarded as unsorted municipal waste and must be collected and disposed of separately by a competent authority.

Customer Feedback

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

About This Guide

The VC400/VC120 video conferencing system represents a new generation of full high-definition video conferencing launched by Yealink. It features, in addition to a high-definition audio-visual experience, flexible compatibility, easy deployment and intelligent network adaptation. With high product standards, it is an ideal choice for SMEs. The VC400/VC120 video conferencing system allows branch offices, as well as branch and head offices, to communicate flexibly and cooperate efficiently.

The guide is intended for administrators who need to configure, customize, manage, and troubleshoot the video conferencing system properly, rather than for end-users. It provides details on the functionality and configuration of the Yealink VCS system.

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

Documentations

This guide covers the VC400/VC120 video conferencing system. In addition to the administrator guide, the following related documentations are available:

- Quick Start Guide, which describes how to assemble the system and configure basic network features on the system.
- User Guides, which describe how to configure and use basic features available on the systems.
- Video Conference Room Deployment Solution, which describes the conference room layout requirements and how to deploy the systems.
- Network Deployment Solution, which describes how to deploy network for your systems.

You can download the above documentations from Yealink website:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>

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

Firmware

Common reasons for updating firmware include fixing bugs or adding features to the device. You can download the latest firmware for your product online:

<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>

For more information on how to upgrade the system firmware, refer to [Upgrading Firmware](#) on page 209.

In This Guide

This administrator guide includes the following chapters:

- Chapter 1, "[System Overview](#)" describes system components, icons and Indicator LEDs.
- Chapter 2, "[Getting Started](#)" describes how to install and start up the system and configuration methods.
- Chapter 3, "[Configuring Network](#)" describes how to configure network features on the system.
- Chapter 4, "[Configuring Call Preferences](#)" describes how to configure call preferences on the system.
- Chapter 5, "[Configuring System Settings](#)" describes how to configure basic, audio and video features on the system.
- Chapter 6, "[System Management](#)" describes how to manage system contacts and call history.
- Chapter 7, "[Configuring Security Features](#)" describes how to configure security features on the system.
- Chapter 8, "[System Maintenance](#)" describes how to upgrade system firmware and reset the system.
- Chapter 9, "[Troubleshooting](#)" describes how to troubleshoot the system and provides some common troubleshooting solutions.

Summary of Changes

This section describes the changes to this guide for each release and guide version.

Changes for Release 20, Guide Version 20.6

The following sections are new for this version:

- [Firmware](#) on page v
- [Physical Features of Yealink VCS System](#) on page 2
- [VCM60 Video Conferencing Wireless Microphone](#) on page 12
- [VCM30 Video Conferencing Microphone Array](#) on page 22
- [Remote Control Battery Safety Information](#) on page 40
- [Static DNS](#) on page 53

- [STUN](#) on page 83
- [Keep Alive](#) on page 87
- [Rport](#) on page 88
- [DTMF](#) on page 108
- [Video Codecs](#) on page 114
- [Ringback Timeout](#) on page 124
- [Auto Refuse Timeout](#) on page 125
- [URI Call Mode](#) on page 126
- [Meeting Password](#) on page 143
- [Meeting Whitelist](#) on page 144
- [License](#) on page 182

Major updates have occurred to the following sections:

- [Packaging Contents](#) on page 3
- [VCC18 HD Camera](#) on page 8
- [VCR10 Remote Control](#) on page 25
- [LED Instructions](#) on page 30
- [System Installation](#) on page 35
- [VLAN](#) on page 59
- [Configuring the System for Use with a Firewall or NAT](#) on page 75
- [H.460 Firewall Traversal](#) on page 89
- [Configuring SIP Settings](#) on page 99
- [Audio Setting](#) on page 145
- [Dual-Stream Protocol](#) on page 151
- [Camera Control Protocol](#) on page 160
- [Dual Screen](#) on page 179
- [H.235](#) on page 203
- [Capturing Packets](#) on page 220

Table of Contents

About This Guide V

Documentations	v
Firmware	v
In This Guide	vi
Summary of Changes	vi
Changes for Release 20, Guide Version 20.6	vi

Table of Contents ix

System Overview 1

VoIP Principles	1
Physical Features of Yealink VCS System.....	2
Packaging Contents.....	3
Optional Accessory.....	6
System Component Instructions	6
VC400/VC120 Codec	6
VCC18 HD Camera	8
VCP40 Video Conferencing Phone.....	10
VCM60 Video Conferencing Wireless Microphone.....	12
VCM30 Video Conferencing Microphone Array	22
VCR10 Remote Control.....	25
Icon Instructions	27
Icons on Display Device.....	27
Icons on the VCP40 Video Conferencing Phone	29
LED Instructions	30
User Interfaces.....	32
Remote Control	32
Web User Interface	32

Getting Started..... 35

System Installation.....	35
Installing the VC400 Video Conferencing System	36
Installing the VC120 Video Conferencing Endpoint	36
Installing the Camera	38
Installing Batteries in the Remote Control	40
Connecting the CPE80 Expansion Microphone	40

Powering the System On and Off	41
System Initialization	42
System Startup	42
Setup Wizard	43
Enabling Communication with Other Systems	47
Placing a Test Call from the Yealink VCS System	47

Configuring Network 49

Preparing the Network	49
Configuring LAN Properties	50
DHCP	50
Configuring Network Settings Manually	54
Configuring Network Speed and Duplex Mode	57
VLAN	59
LLDP	60
Manual Configuration for VLAN	63
DHCP VLAN	65
802.1X Authentication	66
H.323 Tunneling	71
Configuring the System for Use with a Firewall or NAT	75
Reserved Ports	75
Network Address Translation	78
H.460 Firewall Traversal	89
Intelligent Firewall Traversal	91
Quality of Service	92
VPN	95

Configuring Call Preferences 99

Configuring SIP Settings	99
SIP Account	99
SIP IP Call	102
Configuring H.323 Settings	104
DTMF	108
Methods of Transmitting DTMF Digit	109
Codecs	113
Audio Codecs	113
Video Codecs	114
Call Protocol	116
Do Not Disturb	117
Auto Answer	119
Call Match	120
History Record	121
Bandwidth	122

Ringback Timeout	124
Auto Refuse Timeout	125
URI Call Mode.....	126
Configuring System Settings	129
General Setting.....	129
Site Name.....	129
Backlight of the VCP40 Video Conferencing Phone	130
Language	131
Date & Time.....	132
Automatic Sleep Time	139
Hide IP Address.....	140
Relog Offtime	141
Key Tone	142
Meeting Password	143
Meeting Whitelist	144
Audio Setting	145
Audio Output Device	145
Audio Input Device.....	147
Adjusting MTU of Video Packets.....	150
Dual-Stream Protocol.....	151
Mix Sending.....	154
Configuring Camera Settings.....	154
Far-end Camera Control.....	159
Camera Control Protocol	160
Tones	163
System Management.....	167
Local Directory	167
LDAP	172
Call History.....	176
Search Source List in Dialing	178
Dual Screen.....	179
VC400 Screen Layout	179
VC120 Screen Layout	181
License	182
Device Type License.....	182
8-Way Conference License	183
Configuring Security Features.....	187
User Mode	187
Administrator Password.....	188

Web Server Type.....	190
Transport Layer Security	192
Secure Real-Time Transport Protocol	200
H.235	203
Attack Defense in Public Network	204
Abnormal Call Answering.....	205
Configuring Safe Mode Call.....	206
System Maintenance	209
Upgrading Firmware	209
Importing/Exporting Configuration	210
Resetting to Factory	211
SNMP.....	212
Troubleshooting	217
Troubleshooting Methods	217
Viewing Log Files.....	217
Capturing Packets	220
Getting Information from Status Indicators	223
Analyzing Configuration Files	223
Viewing Call Statistics.....	224
Using Diagnostic Methods.....	224
Troubleshooting Solutions	226
General Issues	226
Camera Issues.....	228
Video & Audio Issues.....	229
System Maintenance	231
Appendix	233
Appendix A: Time Zones	233
Appendix B: Trusted Certificates	235
Index	237

System Overview

This chapter contains the following information about VC400/VC120 video conferencing system:

- [VoIP Principles](#)
- [Physical Features of Yealink VCS System](#)
- [Packaging Contents](#)
- [System Component Instructions](#)
- [Icon Instructions](#)
- [LED Instructions](#)
- [User Interfaces](#)

VoIP Principles

VoIP

VoIP (Voice over Internet Protocol) is a technology that uses 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 system. 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.

Physical Features of Yealink VCS System

Video conferencing systems are in the overall network topology, which are designed to interoperate with other compatible equipment, including application servers, media servers, internet-working gateways, and other systems.

In order to operate systems in your network successfully, the systems must meet the following requirements:

- A working IP network is established.
- VoIP gateway is configured for SIP or H.323, and H.323 gatekeeper is configured for H.323.
- The latest (or compatible) firmware of system is available.
- A call server is active and configured to receive and send SIP/H.323 messages.



The VC400 and the VC120 have same physical interfaces, camera parameters and video resolutions.

VC400/VC120 Codec Interface

- 2 x HDMI
- 1x DVI

- 1x VGA
- 1xVCS phone port(RJ-45)
- 1x10/100/1000M Ethernet
- 1 x Line-in (3.5mm)
- 1 x Line-out (3.5mm)
- 2 x USB2.0 port
- 1 x power port
- Others: 1 x power key, 1 x security lock slot, 1 x reset slot

Full-HD Camera

- 1920x1080 video resolution
- Up to 18x optical zoom PTZ camera
- Pan range: $\pm 100^\circ$
- Tilt range: $\pm 30^\circ$
- Up to 10 preset positions
- Beauty shot feature

Video Resolution

- Full-HD 1080P at 30fps (1920x1080), from 1Mbps
- 720P (1280x720), from 512Kbps
- W448P (768 x 448), WQVGA (400 x 240)
- 4CIF (704x576), CIF (352 x 288)

Packaging Contents

The following items are included in your package. If you find anything missing, contact your system administrator.

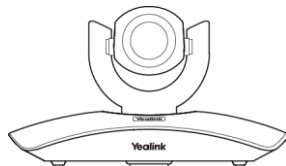
Note

We recommend that you use the accessories provided or approved by Yealink. The use of unapproved third-party accessories may result in reduced performance.

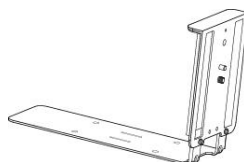
- **VC400/VC120 Codec**






- **VCC18 HD Camera**



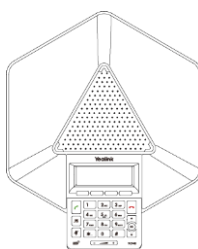
- **L-Bracket (for installing the camera)**



- **Camera Mounting Accessories**

Expansion bolts		× 4
Screws(Specificaiton: T4×30)		× 4
Screws(Specificaiton: M3×8)		× 2

- **VCP40 Video Conferencing Phone**



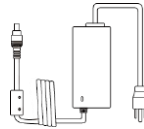
- **VCR10 Remote Control**



- 2 AAA Batteries



- Power Adapter



- Cables (for VC400)



DVI Cable



VGA Cable



HDMI Cables X 2



3.5mm Audio Cable



Ethernet Cable
(2m)



Ethernet Cable
(7.5m)

- Cables (for VC120)



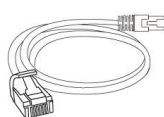
DVI Cable



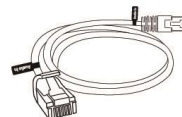
VGA Cable



HDMI Cable

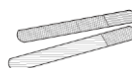


Ethernet Cable
(2m)

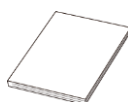


Ethernet Cable
(7.5m)

- Cable Ties (7 for VC400, 5 for VC120)



- **Quick Start Guide**



Check the list before installation. If you find anything missing, contact your system administrator.

Optional Accessory

The following item is an optional accessory for the VC400/VC120 system. You can buy it separately if necessary.

The CPE80 expansion microphone is used for expanding the audio pickup range.

- **CPE80 Expansion Microphone**



System Component Instructions

Before installing and using the VC400/VC120 video conferencing system, you need to be familiar with the following system components, including:

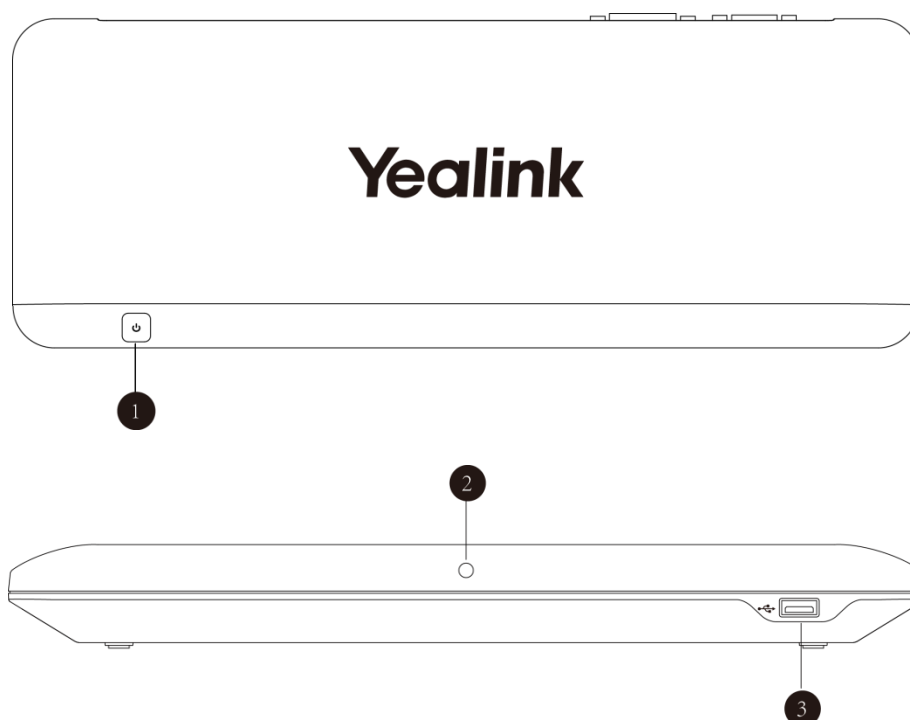
- [VC400/VC120 Codec](#)
- [VCC18 HD Camera](#)
- [VCP40 Video Conferencing Phone](#)
- [VCM60 Video Conferencing Wireless Microphone](#)
- [VCM30 Video Conferencing Microphone Array](#)
- [VCR10 Remote Control](#)

VC400/VC120 Codec

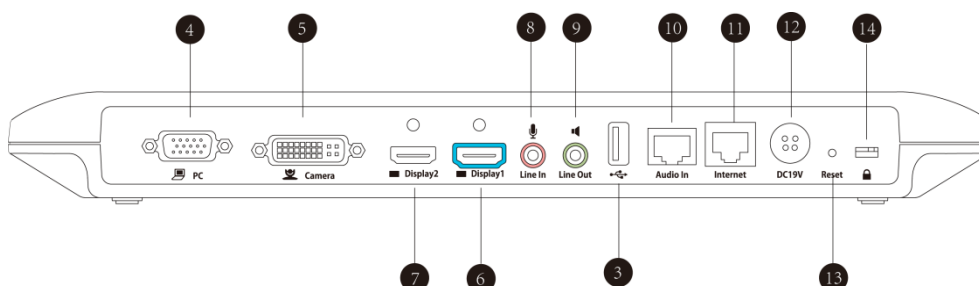
VC400/VC120 codec supports 1080P full HD video. It supports both H. 323 and SIP protocols and can connect to a mainstream video conferencing system.

Strong audio/video processing ability, rich interfaces, compatibility with different display devices and adaptive resolution make it easy to use.

VC400/VC120 codec front panel



VC400/VC120 codec back panel



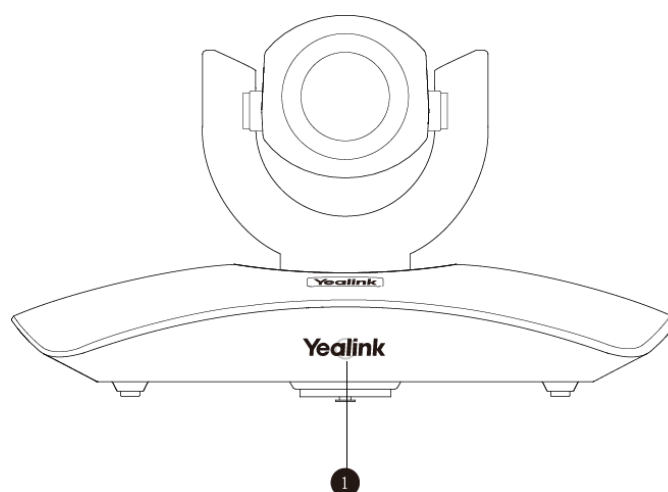
	Port Name	Description
①	Power Button	Powers the system on or off.
②	LED Indicator	Indicates the system statuses. For more information, refer to
③	USB	Inserts a USB flash drive to one of the two USB ports for storing screenshots and recording videos. Note: If two USB flash drives are connected, only the latter one can be identified.
④	PC	Connects to a PC for sharing documents or videos during a call.
⑤	Camera	Connects to a camera.
⑥	Display1	Connects to a display device for displaying video images. When connecting only one display device, Display1

	Port Name	Description
		port on the VC400/VC120 codec is the only available port.
⑦	Display2	Connects to secondary display device for displaying video images.
⑧	Line In	Connects to an audio input device using an audio cable (3.5mm).
⑨	Line Out	Connects to an audio output device using an audio cable (3.5mm).
⑩	Audio In	Connects to the VCP40 video conferencing phone.
⑪	Internet	Connects to the network device.
⑫	DC19V	Connects to the power source via a power adapter.
⑬	Reset Key	Resets the system to factory defaults.
⑭	Security Slot	Allows you to connect a universal security cable to VC400/VC120 codec, so you can lock it down. The system cannot be removed when it is locked.

VCC18 HD Camera

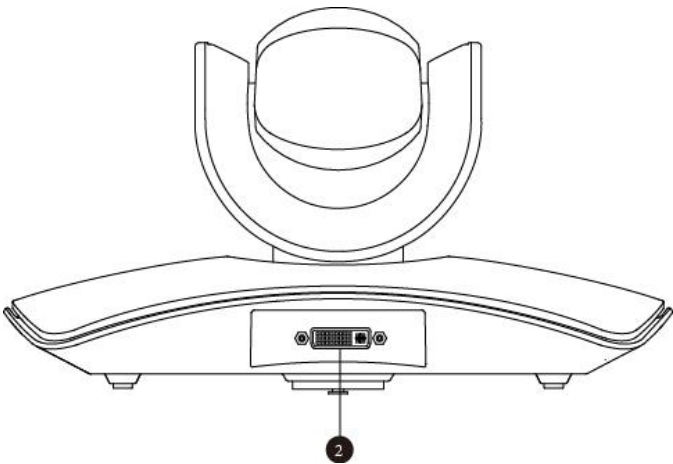
The VCC18 HD camera supports 18x optical zoom, white balance and automatic gain. Exceptionally clear images can bring you an immersive experience.

The front of VCC18 HD camera



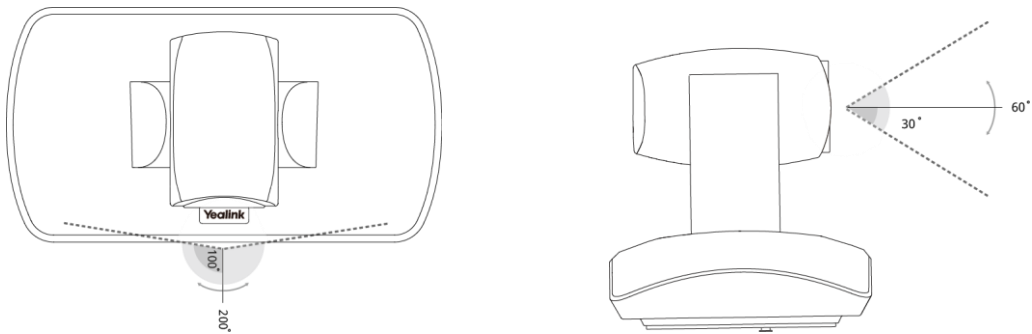
	Port Name	Description
①	LED Indicator	Indicates different system statuses. For more information, refer to LED Instructions on page 30.

The back of VCC18 HD camera



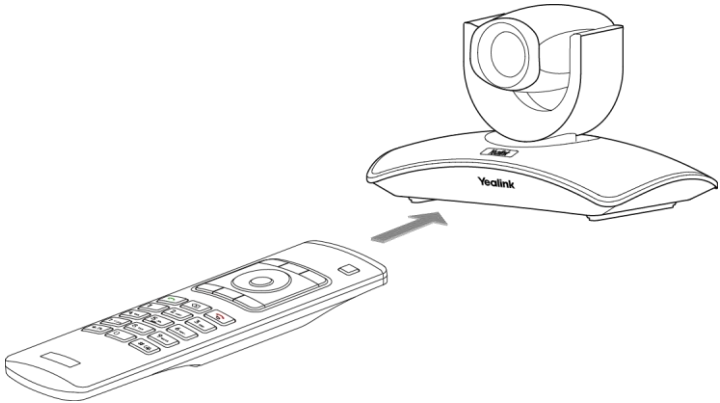
	Port Name	Description
②	Camera	Connects to the Camera port on the VC400/VC120 codec using a DVI cable.

You can use the remote control to adjust the position or focus of the camera. The VCC18 camera can be panned (± 100 degrees range), tilted (± 30 degrees range).



Infrared Sensor

The infrared sensor is located within the Yealink logo. Aim the remote control at the camera IR sensor to operate the unit.

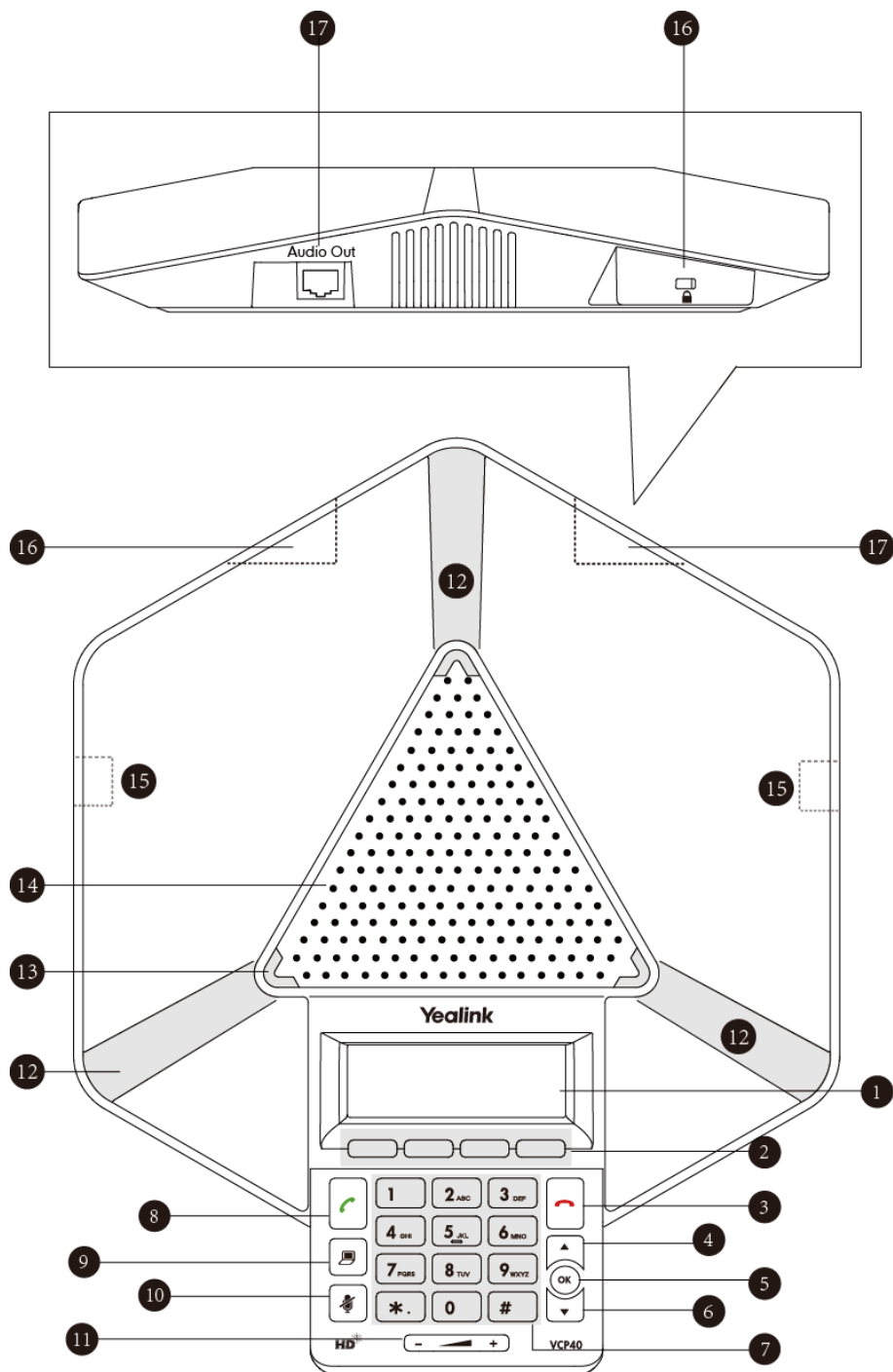


Note Avoid physically turn camera while system is powered on to prevent permanent damaging the camera. Always use the remote control to pan and tilt the camera head.





VCP40 Video Conferencing Phone

The VCP40 video conferencing phone can be used as the speakerphone and microphone for the system. It supports 360-degree audio pickup at a radius of up to 3 meters to achieve ultra-HD voice.

You can place calls, answer calls or view directory and call history on the VCP40 phone.



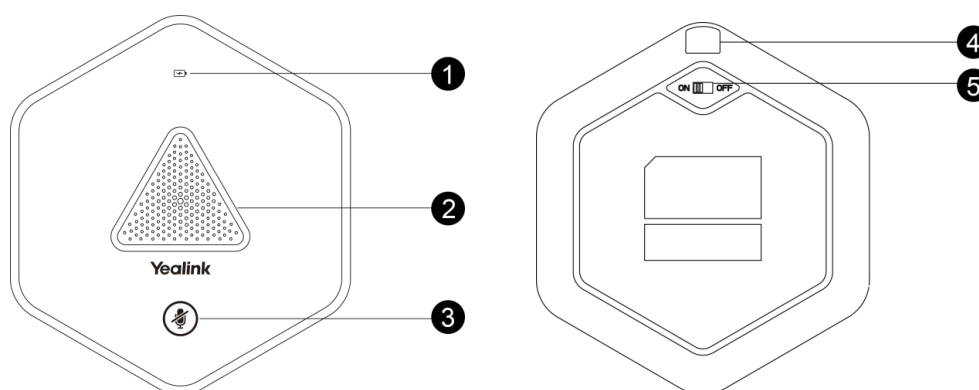
System component instructions for the VCP40 phone are:

	Item	Description
①	LCD Screen	Shows information about calls, messages, soft keys, time, date and other relevant data: <ul style="list-style-type: none"> • Call information—call duration • Icons (for example, ) • Missed call information • Time and date
②	Soft Keys	Label automatically to identify their context-sensitive features.
③	On-hook Key	Rejects or ends a call or returns to the previous screen.
④		Scrolls upwards through the displayed information.
⑤		Enters list or answers incoming calls.
⑥		Scrolls downwards through the displayed information.
⑦	Keypad	Provides the digits and special characters ". " "*" "#".
⑧	Off-hook Key	Initiates a call or answers a call.
⑨	Presentation Key	Enables or disables presentation.
⑩	Mute Key	Toggles mute feature.
⑪	Volume Key	Adjusts the volume of the speakerphone and ringer.
⑫	Microphone	Picks up voice.
⑬	LED Indicators	Indicates phone and call statuses.
⑭	Speakerphone	Provides ringer and hands-free (speakerphone) audio output.
⑮	MIC Port	Connects to a CPE80 expansion microphone to one of two MIC ports.
⑯	Security Slot	Allows you to connect a universal security cable to your phone, so you can lock it down. The phone cannot be removed when it is locked.
⑰	Audio Out Port	Connects to the VCP40 phone using the 7.5m Ethernet cable labeled Audio in. Provides the power supply for the VCP40 phone.

VCM60 Video Conferencing Wireless Microphone

The VCM60 is a video conferencing wireless microphone which can work as the audio input device for VC120 video conferencing endpoint. It supports 360-degree audio pickup at a radius of up to 2 meters. There are a mute button and a battery indicator LED on its top. You can mute or unmute the VCM60 by tapping the mute button.

There is a power switch on its bottom. You can turn off this switch if the VCM60 is not in use for a long period of time.

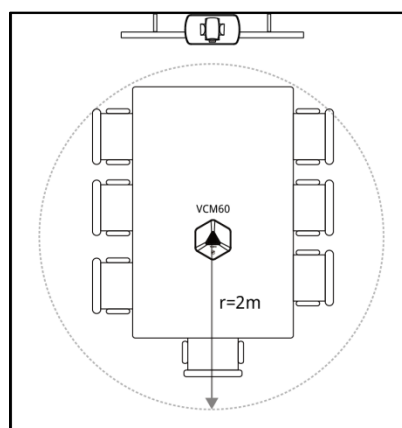


	Name	Description
①	Battery Indicator LED	Indicates the battery information. For more information on the battery Indicator LED, refer to LED Instructions on page 30.
②	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 2 meters.
③	Mute Button	<ul style="list-style-type: none"> Mutes or unmutes the VCM60. For more information on the mute indicator LED, refer to LED Instructions on page 30. Activates the VCM60 to search the dongle when it is in the offline standby mode. For more information, refer to Standby Mode on page 30. Enters registration mode. For more information, refer to Registering and Deregistering the VCM60 on page 17.
④	Charging Interface	Connects the VCM60 to a power adapter or a computer's USB port using a USB cable to charge the VCM60.
⑤	Switch	Turns on or off the VCM60.

Placing the VCM60

The VCM60 has a rubber pads on its base to prevent it from sliding. You can place the VCM60 on a conference table. Do the following to ensure optimal voice quality:

- For registering to the dongle successfully, make sure the VCM60 video conferencing wireless microphone is less than 30 meters distant from the dongle.
- Place the VCM60 on a stable surface and keep it away from obstacles so that it can effectively pick up sounds.



Turning On or Off the VCM60

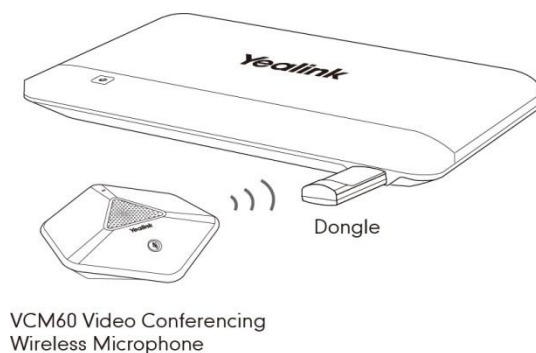
There is a power switch on the bottom of the VCM60. Turn on the power switch to start the VCM60. After the VCM60 starts, it registers with the paired dongle automatically. You can turn off this switch if the VCM60 is not in use for a long period of time.


Connecting VCM60 to the Video Conferencing Endpoint

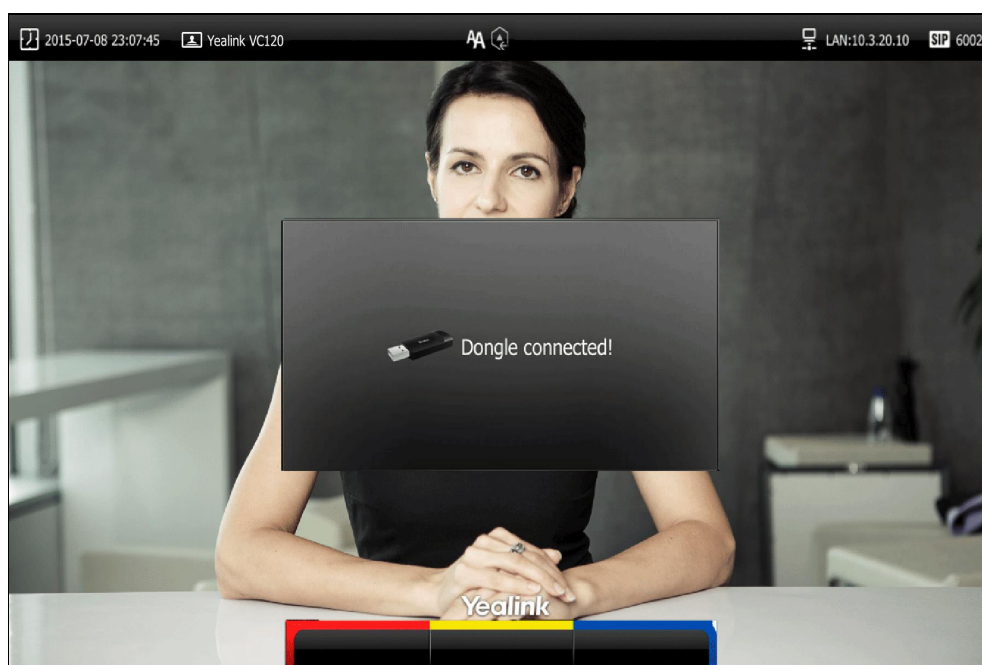
To ensure good voice quality, VCM60 video conferencing wireless microphone can be connected to the VC120 video conferencing endpoint to work as the audio input device.

To connect the VCM60 to the VC120 video conferencing endpoint, do the following:




1. Connect the dongle to one of the USB ports on the VC120 codec.

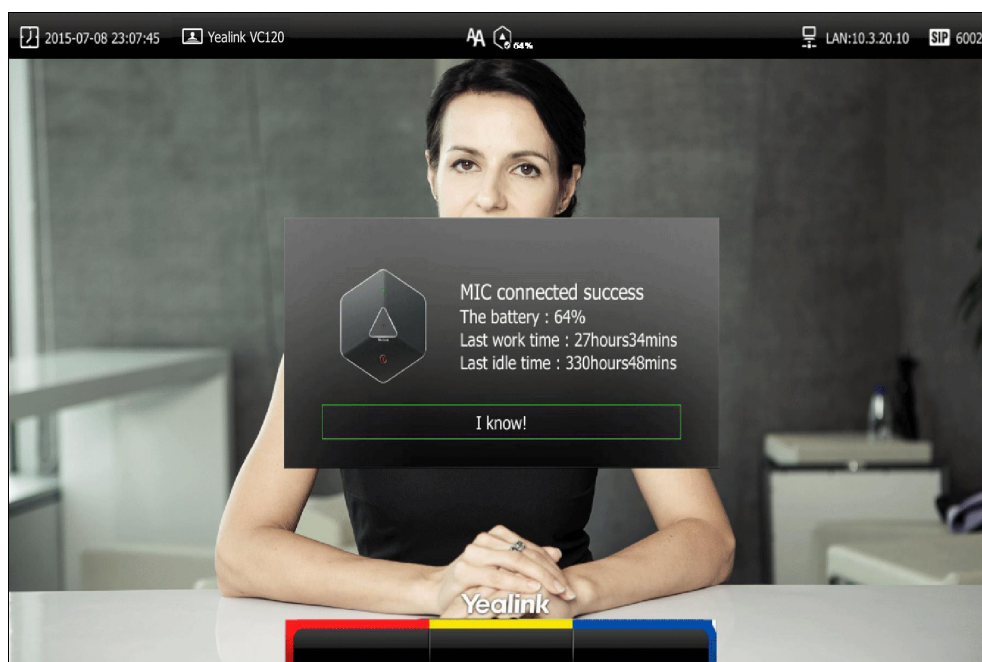


The display device prompts "Dongle connected!", and the  (unregistered) icon appears on the status bar.




2. Turn on the VCM60.

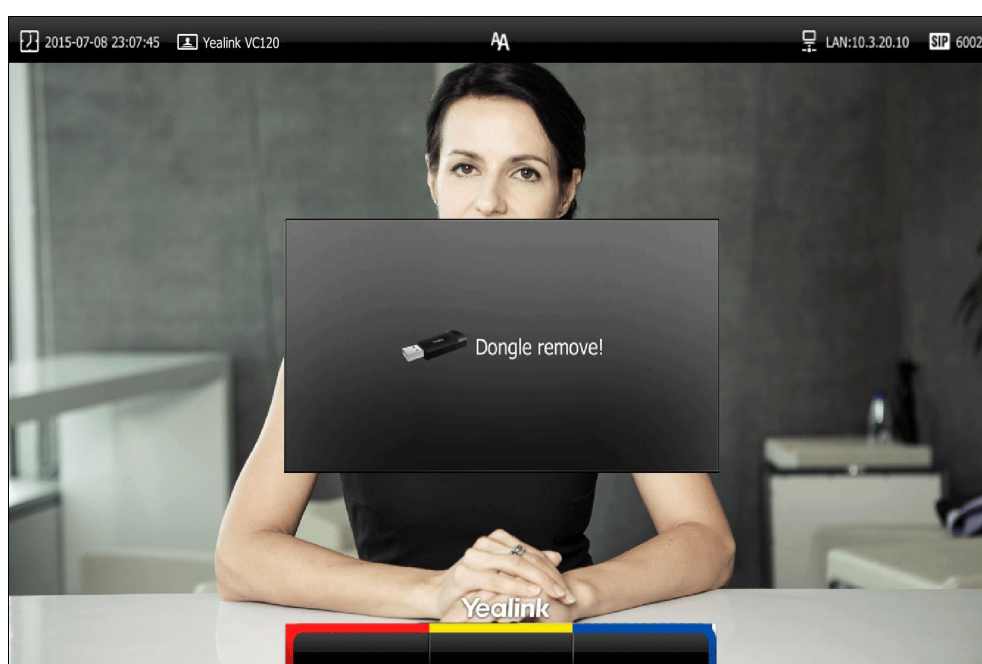
The VCM60 registers with the dongle automatically. If successful, the  (unregistered) icon will change to  (registered). Current capacity appears on the right side of the  icon. When the standby time is less than 1 hour, please charge the VCM60. For more information, refer to [Charging the VCM60](#) on page 19.



To remove the VCM60 from the VC120 video conferencing endpoint, do the following:

1. Remove the dongle from the VC120 codec.

The display device prompts "Dongle remove!". And the icon  disappears from the status bar.



Standby Mode

The VCM60 supports two standby modes: online standby and offline standby.

Online standby:

- When registering with dongle successfully, the VCM60 enters online standby mode and the mute indicator LED changes to green and is in breathing state.

Offline standby:



- If VC120 video conferencing endpoint encounters poor signal, wireless interference or is powered off, the VCM60 may lose connection with the dongle. In this case, the VCM60 will search the dongle again, and the mute indicator LED fast flashes green. If dongle cannot be searched in 2 minutes, the VCM60 will enter offline standby mode automatically and the mute indicator LED slowly flashes orange.
- When the VCM60 is in offline standby mode, you need to tap the mute button to activate VCM60 to search dongle again and the mute indicator LED fast flashes green.

Muting or Unmuting the VCM60



There is a mute button on the top of the VCM6. If VCM60 works as the audio input device of the VC120 video conferencing endpoint, you can mute or unmute it in the following scenarios:

- If you do not want to have your voice broadcast during a call, you can tap the mute button to mute the VCM60.
- If you want to speak again during a call, you can tap mute button to unmute the VCM60.

To mute the VCM60 during a call:

1. Tap  again to mute the call.
The mute indicator LED illuminates solid red. And the  mute icon appears on the local video image.

To unmute the VCM60 during a call:

1. Tap  again to unmute the call.
The mute indicator LED illuminates solid green. And the  mute icon disappears from the local video image.

Viewing VCM60 Information

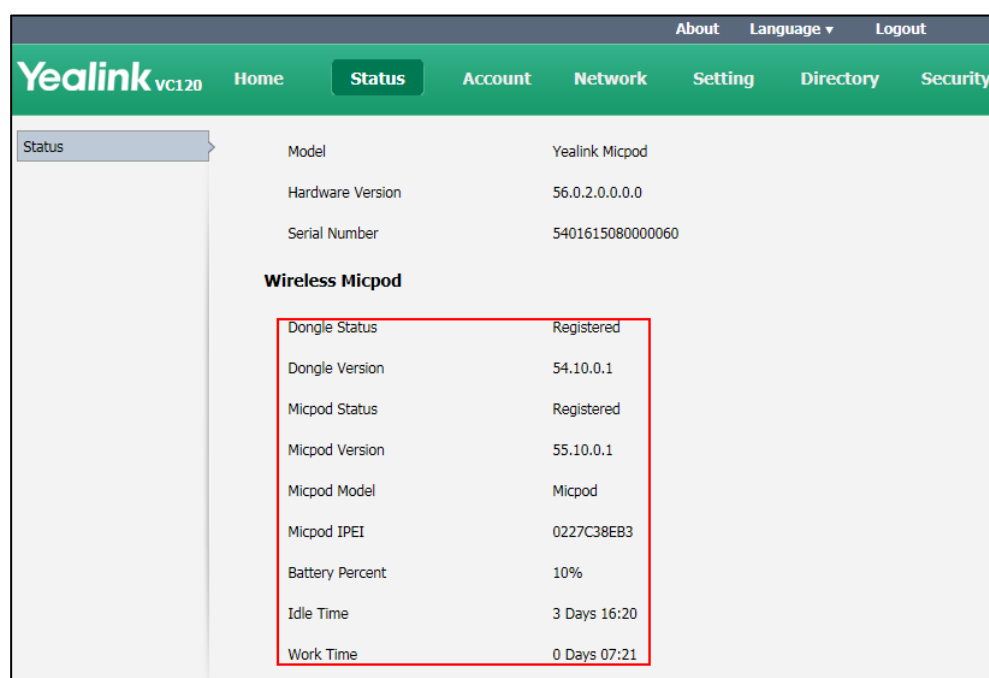
When the dongle is connected to the USB port of the VC120 codec, you can view VCM60 status via the remote control or web user interface.

Available information of VCM60 includes:

- Dongle status
- Dongle Version
- Micpod Status
- Micpod Version
- Micpod Model
- Micpod IPEI
- Battery percent
- Idle Time (estimated standby time)
- Work Time(estimated working time)

To view the VCM60 information via web user interface:

1. Click on **Status**.



To view the VCM60 information via the remote control:

1. Select **Menu->Status->Wireless Micpod**.

Registering and Deregistering the VCM60

The VCM60 video conferencing wireless microphone and dongle are automatically “paired” at the factory. But In following cases, you may need to deregister or register the VCM60 video conferencing wireless microphone manually.

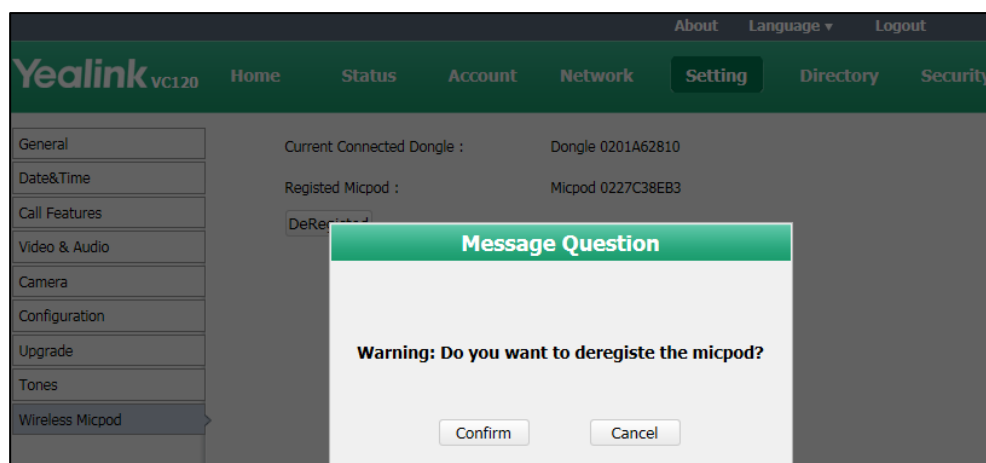
- The device is broken, new VCM60 or new dongle need to be re-paired.

- VCM60 and dongle need to be paired during the production.

You can only register and deregister the VCM60 via web user interface. The web user interface will display the model and product ID of the dongle and video conferencing wireless microphone.

To deregister the VCM60 via web user interface:

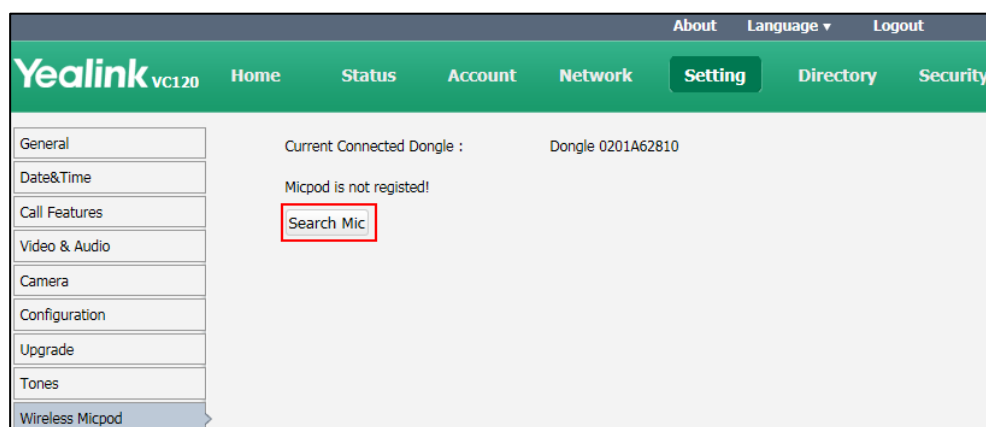
1. Click on **Setting->Wireless Micpod**.
2. Click **DeRegistered**.



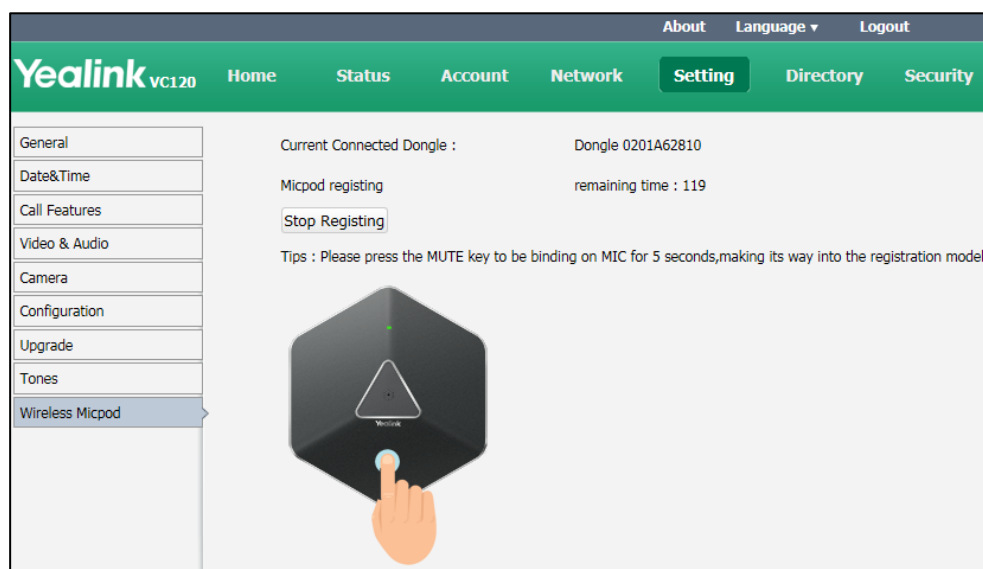
3. Click **Confirm** to deregister the video conferencing wireless microphone.
The paired information will be cleared. The VCM60 video conferencing wireless microphone will enter offline standby mode and the mute indicator LED slowly flashes orange.

To register the VCM60 via web user interface:

1. Click on **Setting->Wireless Micpod**.
2. Click **Search Mic**.




The web user interface starts 120-second countdown for pairing the dongle and video conferencing wireless microphone.



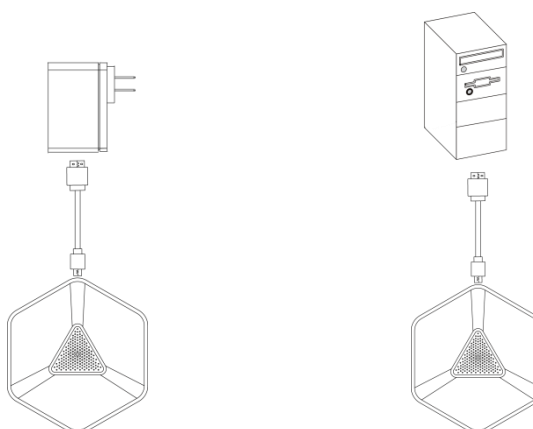
3. Tap and hold the mute button on the VCM60 video conferencing wireless microphone for 5 seconds until the mute indicator LED flashes orange.


The VCM60 video conferencing wireless microphone and the dongle will be paired automatically. If this fails, the VCM60 will exit registration mode in 2 minutes.

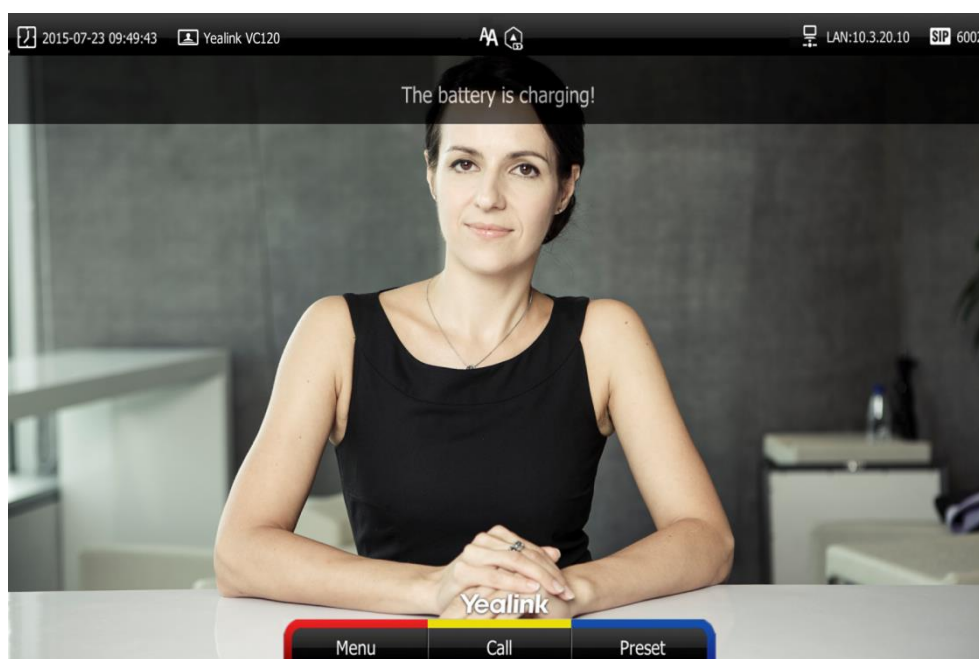
Charging the VCM60

When the standby time of the VCM60 is less than 1 hour (the battery indicator LED flashes red), the  icon appears on the status bar, and the display device prompts "The battery of wireless micpod is too low, please charge it in time!" every 15 minutes.

To charge the VCM60, connect it to a power adapter or a computer using the supplied USB cable.



The VPM60 can work normally during charging. If you charge the VCM60 when it is working, the display device prompts "The battery is charging!", and the  (charging) icon appears on the status bar.



During charging, the battery LED indicator will flash green. And it will illuminate solid green when the battery capacity reaches 100%.

VCM60 Working Frequency

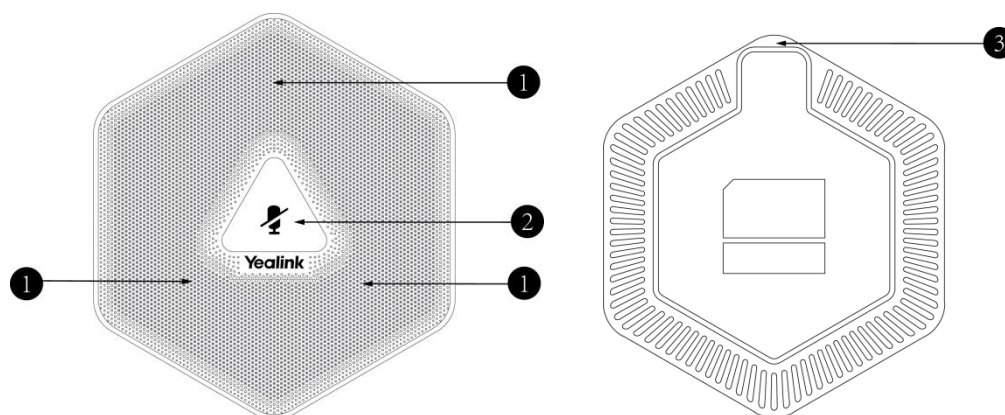
For reference, the Frequency/Channels of VCM60 used in each Region are tabulated below:

Freq (MHz)	RF Carrier Index (DECT tester Numbering)						
	EU	Taiwan	US	LA	Korea	Brazil	Japan
1881.792	9	9					
1883.520	8	8					
1885.248	7	7					
1886.976	6	6					
1888.704	5	5					
1890.432	4	4					
1892.160	3	3					
1893.888	2	2					
1895.616	1						4(F1)
1897.344	0						3(F2)

Freq (MHz)	RF Carrier Index (DECT tester Numbering)						
	EU	Taiwan	US	LA	Korea	Brazil	Japan
1899.072							2(F3)
1900.800							1(F4)
1902.528							0(F5)
1904.256							
1905.984							
1907.712							
1909.440							
1911.168						4	
1912.896				9		3	
1914.624				8		2	
1916.352				7		1	
1918.080				6		0	
1919.808				5			
1921.536			4	4			
1923.264			3	3			
1924.992			2	2			
1926.720			1	1			
1928.448			0	0			
1787.616					8		
1789.344					7		
1791.072					6		

VCM30 Video Conferencing Microphone Array

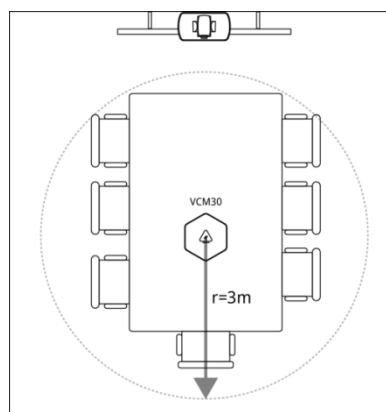
The VCM30 is a video conferencing microphone array which can work as the audio input device for VC120 video conferencing endpoint. It has 3 built-in microphones which support 360-degree audio pickup at a radius of up to 3 meters. There is a mute button on its top. You can mute or unmute the VCM30 by tapping the mute button during a call.



	Name	Description
①	Built-in Microphones	Support 360-degree audio pickup at a radius of up to 3 meters.
②	Mute Button	Mutes or unmutes the VCM30. For more information on the mute indicator LED, refer to LED Instructions on page 30.
③	Audio Out Port	Connects to the Audio In port of VC120 codec using the 7.5m Ethernet cable labeled Audio In. Provides the power supply for the VCM30.

Placing the VCM30

The VCM30 has a rubber pads on its base to prevent it from sliding. You can place the VCM30 on a stable surface and keep it away from obstacles so that it can effectively pick up sounds.





Muting or Unmuting the VCM30

There is a mute button at the top of the VCM30. You can mute or unmute it in the following scenarios:


- If you do not want to have your voice broadcast during a call, you can tap the mute button to mute the VCM30.
- If you want to speak again during a call, you can tap mute button to unmute the VCM30.


To mute the VCM30 during a call:

1. Tap  to mute the call.

The mute indicator LED illuminates solid red. And the  mute icon appears on the local video image.

To unmute the VCM30 during a call:

1. Tap  again to unmute the call.

The mute indicator LED illuminates solid green. And the  mute icon disappears from the local video image.

Viewing VCM30 Information

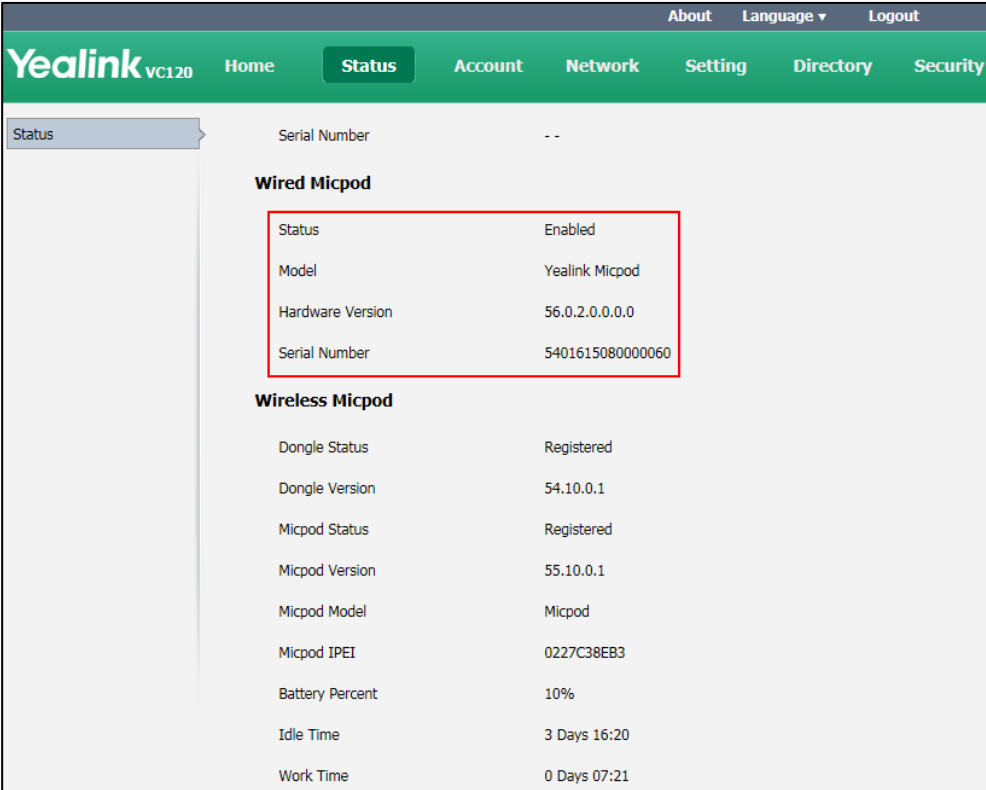
When the VCM30 is connected to the Audio In port of VC120 codec, you can view VCM30 status via the remote control or web user interface.

Available information of VCM30 includes:

- Status
- Model
- Hardware Version
- Serial Number

To view the VCM30 information via web user interface

1. Click **Status**.



The screenshot shows the Yealink VC120 web interface. The top navigation bar includes links for About, Language, and Logout. The main navigation bar has links for Home, Status, Account, Network, Setting, Directory, and Security. The 'Status' menu item is selected in the left sidebar. The main content area displays the 'Wired Micpod' status, which is highlighted with a red box. Below it, the 'Wireless Micpod' status is shown.

Serial Number	
--	

Wired Micpod

Status	Enabled
Model	Yealink Micpod
Hardware Version	56.0.2.0.0.0.0
Serial Number	5401615080000060

Wireless Micpod

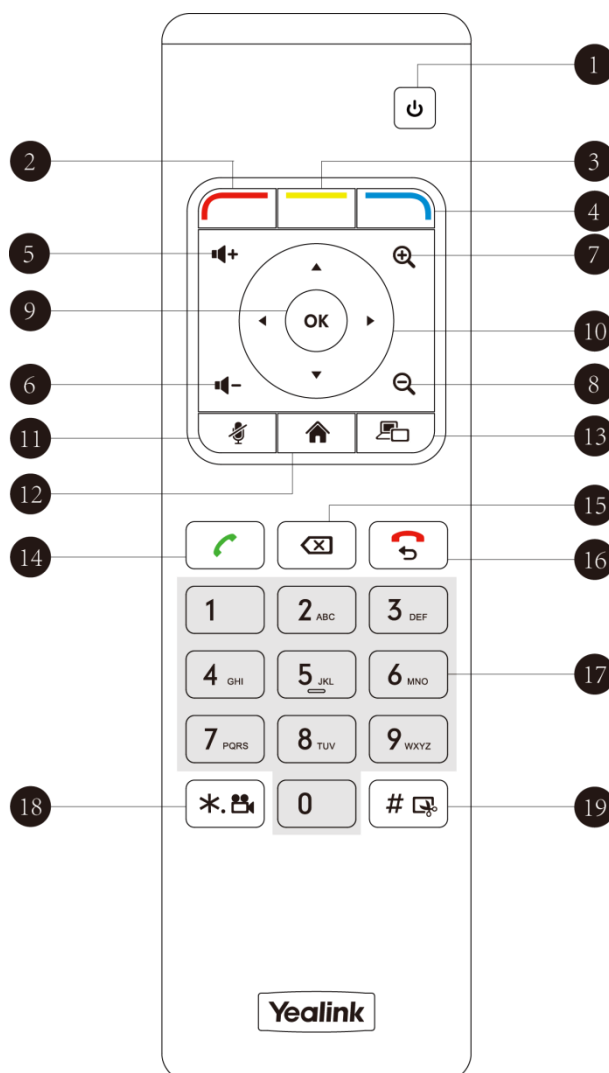
Dongle Status	Registered
Dongle Version	54.10.0.1
Micpod Status	Registered
Micpod Version	55.10.0.1
Micpod Model	Micpod
Micpod IPEI	0227C38EB3
Battery Percent	10%
Idle Time	3 Days 16:20
Work Time	0 Days 07:21

To view the VCM30 information via the remote control:

1. Select **Menu->Status->Wired Micpod**.

VCR10 Remote Control

VCR10 remote control is compact, and has definite function zoning. Users can organize conferences easily using infrared signals.



Hardware components of the remote control:

	Item	Description
①	Sleep Key	Puts the system to sleep or wakes the system up.
②	Red Shortcut Key	Located at the bottom left of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to enter the main menu screen and corresponds to the Menu soft key.
③	Yellow Shortcut Key	Located at the bottom center of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to enter the pre-dialing screen, and corresponds to the Call soft key.














	Item	Description
④	Blue Shortcut Key	Located at the bottom right of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to save and check the camera preset position, and corresponds to the Preset soft key.
⑤	Vol+	Increases the system volume.
⑥	Vol-	Decreases the system volume.
⑦	Zoom out Key	<ul style="list-style-type: none"> Decreases the camera zoom or the captured image magnifications. Behaves as page up in a multiple page list.
⑧	Zoom in Key	<ul style="list-style-type: none"> Increases the camera zoom or the captured image magnifications. Behaves as page up in a multiple page list.
⑨	OK Key	Confirms actions or answers incoming calls.
⑩	Navigation Key	<ul style="list-style-type: none"> In the menu screen, press ◀ or ▶ to switch menus, press ▲ or ▼ to select items. In the idle screen, pan and tilt the camera to adjust the viewing angle.
⑪	Mute Key	Toggles the mute feature.
⑫	Home Key	<ul style="list-style-type: none"> Returns to the idle screen when in the menu screen. Enters the pre-dialing screen during a call.
⑬	Video Source Key	Switches the input source between Camera, Camera-PC, or PC.
⑭	Off-hook Key	<ul style="list-style-type: none"> Enters the pre-dialing screen. Places a call. Answers a call.
⑮	Delete key	Deletes one character at a time.
⑯	On-hook Key	<ul style="list-style-type: none"> Ends a call or exits from a conference call. Returns to the previous screen when not in a call.
⑰	Keypad	<ul style="list-style-type: none"> Enters digits. Enters the pre-dialing screen.





















	Item	Description
		<ul style="list-style-type: none"> Stores the preset position of the camera.
⑱	Video Recording Key	<ul style="list-style-type: none"> Generates a special characters “.”. Starts/Stops recording video.
⑲	Snapshot Key	<ul style="list-style-type: none"> Generates a pound key (#). Captures the image from the camera.


Icon Instructions

Icons on Display Device

Icons appearing on the display device are described in the following table:
















Icon	Description
 (flashing)	Network is disconnected
	Network is available
	Packet loss
 (flashing)	VCP40 video conferencing phone is not connected
 (flashing)	Camera is not connected
	SIP account is registered
	H.323 account is registered
	Lowercase letters input mode of the on-screen keyboard
	Uppercase letters input mode of the on-screen keyboard
	Character input mode of the on-screen keyboard
	Auto answer
	Missed calls
	Volume is 0

Icon	Description
	Do not disturb
	Do not disturb during a call
	Call mute
	Call encryption
	The content of the local camera
	Focus content
	Camera position
	Record a video
	Dialed calls
	Received calls
	Missed calls
	Dongle is connected to the USB port of the VC120 codec, while the VCM60 is unregistered
	Dongle is connected to the USB port of the VC120 codec, and the VCM60 is registered
	The VCM60 is charging
	The standby time of VCM60 is less than one hour
	Dual screen mode
	Dual video sources (when a PC is connected to the PC port on the VC400/VC120 codec)
	A USB flash drive is inserted to the USB port on the VC400/VC120 codec
	Local contact
	Conference contact (not applicable to VC120)

Icon	Description
	VPN is enabled

Icons on the VCP40 Video Conferencing Phone

Icons appearing on the VCP40 LCD screen are described in the following table:

Icon	Description
 (Flashing)	Network is unavailable
	SIP account is registered (the icon flashes when the SIP account is not registered successfully)
	H.323 account is registered (the icon flashes when the H.323 account is not registered successfully)
	Auto answer
	Do not disturb
	Call is muted
	Volume is 0
	A USB flash drive is inserted into the port on the VC400/VC120 codec
	Record a video
	Local contact
	Conference contact (not applicable to VC120)
	Conference call
	Received calls
	Dialed calls
	Missed calls

LED Instructions

Indicator LED on the VC400/VC120 codec:

LED Status	Description
Solid green	The VC400/VC120 codec is powered on. The VC400/VC120 codec is upgrading firmware.
Solid red	The VC400/VC120 codec is in sleep mode.
Solid orange	System exception (e.g., network unavailable, update failure).
Off	The VC400/VC120 codec is powered off, is not connected to the power adapter.

Indicator LED on the camera:

LED Status	Description
Solid green	The camera is properly connected to the VC400/VC120 codec, and the VC400/VC120 codec is powered on.
Solid red	The VC400/VC120 codec is in sleep mode.
Flashing green	Press the key on the remote control.
Off	The camera is not connected properly to the VC400/VC120 codec, or the VC400/VC120 codec is powered off.

Indicator LED on the VCP40:

LED Status	Description
Solid red	The phone is initializing. The VCP40 is muted when the VC400 is during a call.
Flashing red	The phone is ringing.
Solid green	The phone is placing a call. There is an active call on the phone.
Off	The phone is idle. The phone is not connected to the VC400/VC120 codec correctly.

Indicator LED of the Internet port on the VC400/VC120 codec:

LED Status	Description
Indicator LED on the left is off.	Network is not connected.
Indicator LED on the left is solid green.	Network is connected.
Indicator LED on the right is flashing yellow.	Sending and receiving data.

Battery indicator LED on the VCM60 video conferencing wireless microphone:

LED Status	Description
Solid green	The VCM60 is turned on within the first 5 seconds. The battery capacity reaches 100% during charging.
Flashing red	The battery capacity can maintain less than 1 hour.
Flashing green	The VCM60 is charging.
Off	Other status.

Mute indicator LED on the VCM60 video conferencing wireless microphone (When the VCM60 is working as the audio input device of VC120):

LED Status	Description
Fast flashing green	The VCM60 is searching the dongle.
Green and in breathing state	The VCM60 registers with the dongle, and then enters the online standby mode.
Solid green	The VC120 is placing a call. The VC120 is in a call.
Solid red	The VC120 is muted during a call.
Fast flashing orange	The VCM60 enters registration mode.
Slowly flashing orange	The VCM60 fails to search the dongle, and then enters the offline standby mode.
Off	The VCM60 is turned off. The VCM60 runs out of battery.

Mute Indicator LED on the VCM30 video conferencing microphone array:

LED Status	Description
Solid red	The VCM30 is muted when the VC120 is during a call.
Flashing red	The VC120 is ringing.
Solid green	The VCM30 is connected to the VC120 codec within the first 5 seconds. The VC120 is placing a call. The VCM30 is unmuted when the VC120 is during a call.
Off	The VCM30 is not connected to the VC120 codec. The VCM30 is idle.

User Interfaces

There are two ways to customize the configurations of your system:

- [Remote Control](#)
- [Web User Interface](#)

The following describes how to configure the VC400/VC120 video conferencing system via the two methods above.

Detailed operation steps will be introduced in the feature section.

Remote Control

You can use the remote control and display device to configure and use the VC400/VC120 video conferencing system.

For more information on the function of each key on the remote control, refer to [Remote Control](#) on page 32. The Advanced option is only accessible to the user with the administrator's permission. The default administrator password is "0000".

Web User Interface

You can customize your system via web user interface. To access the web user interface, you need to know the user name and the administrator's password. The default user name is "admin" (case-sensitive), and the default password is "0000". You can also access the web user interface with user credential, which is disabled by default. For more information on how to enable the user credential, refer to [User Mode](#) on page 187.

The system uses the HTTPS protocol to access the web user interface by default. For more information on the access protocol for web user interface access, refer to [Web Server Type](#) on page 190.

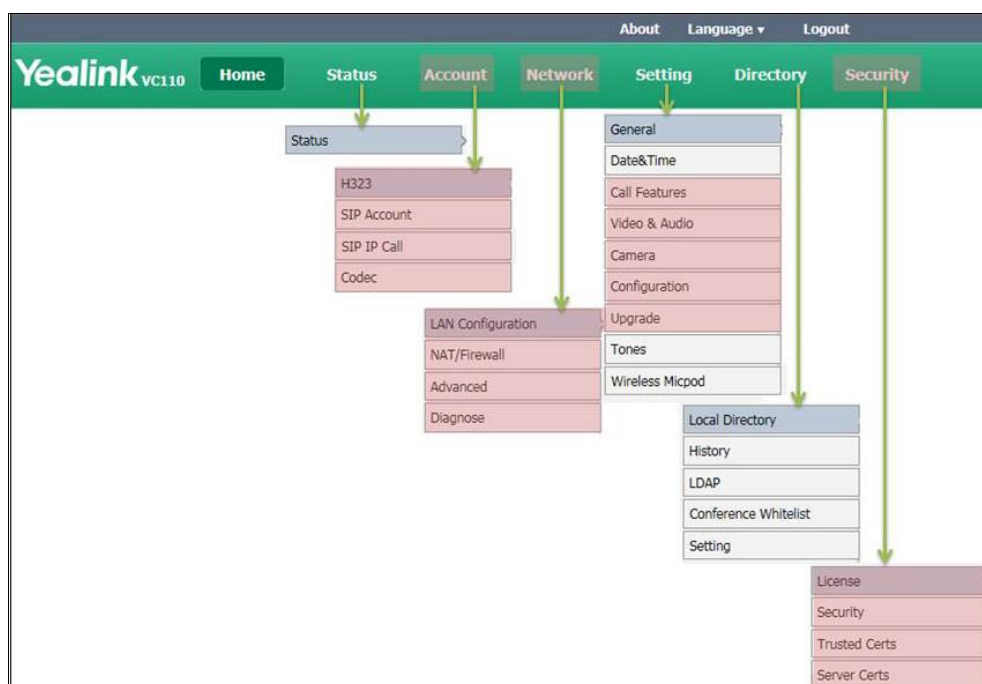
Log into the web user interface of the system:

1. Enter the IP address (e.g.192.168.0.10) in the address bar of a web browser on your computer, and then press the **Enter** key.
2. Enter the administrator user name and password.
3. Click **Login**.

After you log into the web user interface successfully, you can click **Logout** on the top right corner of the web interface to log out.

Administrator has full permission to access every menu in the web user interface. User can log into the web user interface with user credentials.

The web structure tree of VC400 is shown as below, (the red highlight is hidden for users with user credentials):



You can monitor or place calls via web user interface. You can do the following in the **Home** page.

- Placing or ending calls
- Viewing remote and nearby sites
- Enabling the mute mode or the DND mode for a call
- Changing the video input source
- Adjusting the position and focus of the camera
- Saving the camera preset
- Capturing the video images

Note

Although the web user interface is used to initiate the call, it is the video conferencing system that is used for the call. It is not the PC running the web user interface.

Getting Started

This chapter provides basic information and installation instructions for Yealink VCS systems in the following sections:

- [System Installation](#)
- [Powering the System On and Off](#)
- [System Initialization](#)
- [System Startup](#)
- [Setup Wizard](#)
- [Enabling Communication with Other Systems](#)
- [Placing a Test Call from the Yealink VCS System](#)

System Installation

Placing the System

Do not place the camera facing a window or other bright light. Ensure sufficient space to connect the cables. Ensure all participants are facing both the display device and the camera at the same time by putting camera and display device together.

System Components Installation

This section introduces the following:

- Installing the VC400 video conferencing system
- Installing the VC120 video conferencing endpoint
- Installing the camera
- Installing batteries in the remote control
- Connecting the CPE80 expansion microphone

Note

Up to two display devices can be connected to the VC400/VC120 codec. Because the display device is not included in the package, you need to purchase it separately if required. Ensure that the purchased display device supports HDMI input.

When connecting just one display device to the VC400/VC120 codec, Display1 port is the only available port. If dual screen mode is required, you can connect secondary display device to the Display2 port.

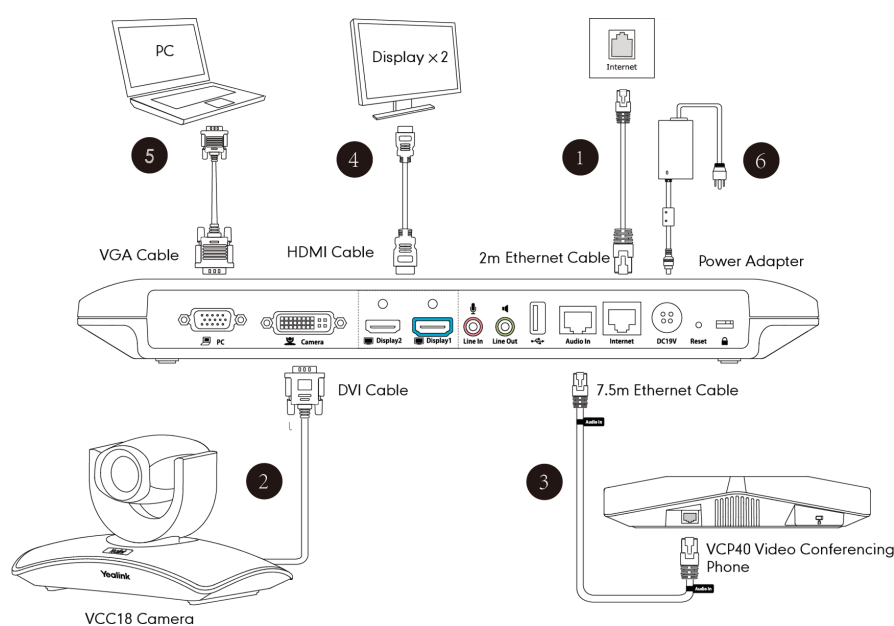
Because the DVI cable is tailor-made, please use the Yealink-supplied DVI cable.

To prevent shock damage, do not connect the power adapter and turn on the power before connecting all system components.

Installing the VC400 Video Conferencing System

Do the following:

1. Connect the Internet port on the VC400 codec to a switch/hub device port with the supplied 2m Ethernet cable.
2. Locate the Camera port on the back of the VC400 codec, and connect it to the Camera port of the camera with the supplied DVI cable.
3. Connect the Audio In port on the VC400 codec to the Audio Out port on VCP40 video conferencing phone with the 7.5m Ethernet cable labeled Audio in.
4. Locate the Display1 port on the VC400 codec, and connect it to the HDMI port on the display device with the supplied HDMI cable (Make sure the display device is powered on)
5. (Optional.) Locate the VGA output port on the PC and connect it to the PC port on the VC400 codec with the supplied VGA cable for sharing content.
6. Connect the DC19V port on the VC400 codec to an AC power outlet with the supplied power adapter and power cord.

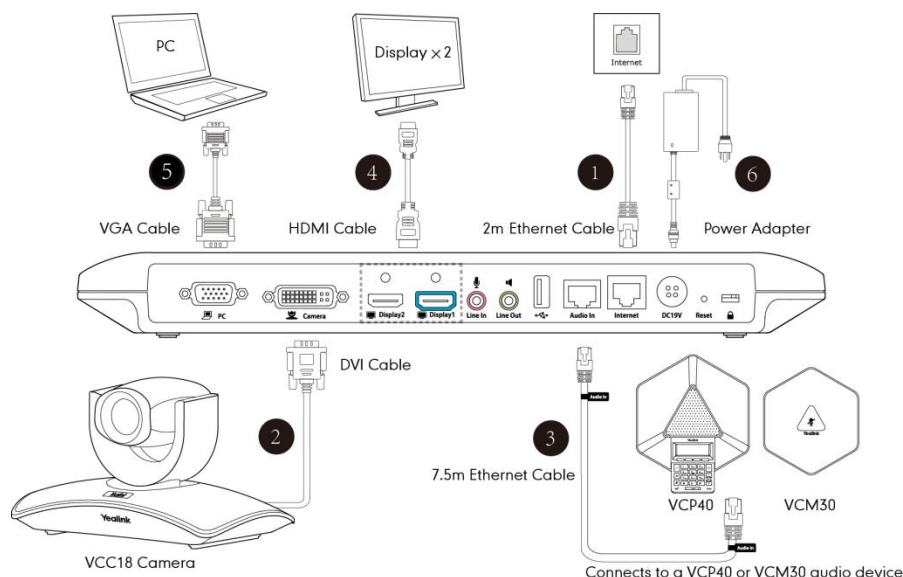


Installing the VC120 Video Conferencing Endpoint

Do the following:

1. Connect the Internet port of the VC120 codec to a switch/hub device port with the supplied 2m Ethernet cable.
2. Locate the Camera port on the back of the VC120 codec, and connect it to the Camera port on the camera with the supplied DVI cable.

3. (Optional) Locate the Audio In port of the VC120 codec, do one of the following:
 - Connect it to the Audio Out port on the VCP40 video conferencing phone with the 7.5m Ethernet cable that labeled Audio In.
 - Connect it to the Audio Out port on the VCM30 video conferencing microphone array with the 7.5m Ethernet cable that labeled Audio In.
4. Locate the Display1 port on the VC120 codec, and connect it to the HDMI port on the display device with the supplied HDMI cable (Make sure the display device is powered on)
5. (Optional.) Locate the VGA output port on the PC and connect it to the PC port on the VC120 codec with the supplied VGA cable for sharing content.
6. Connect the DC19V port on the VC120 codec to an AC power outlet with the supplied power adapter and power cord.



Note

The VC400/VC120 should be used with Yealink original power adapter (19V/3.42A) only. The use of the third-party power adapter may cause the damage to the system.

You can fasten all cables with cable ties after all devices are connected.

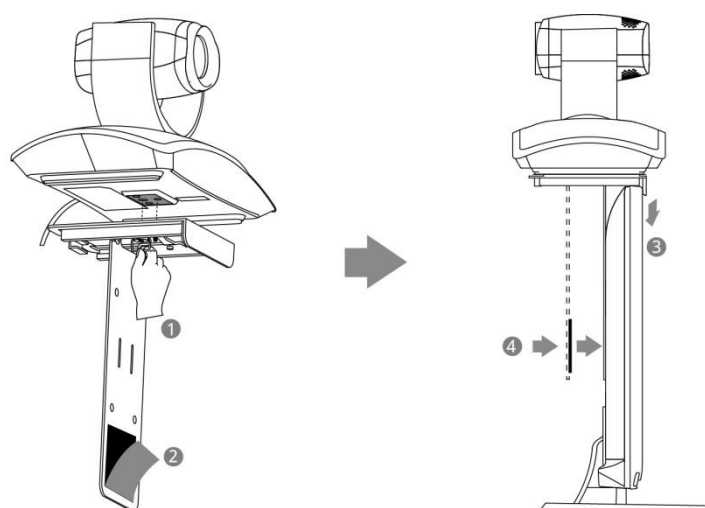


Installing the Camera

You can mount the camera on to the TV or a wall based on your actual needs.

a) Mounting the Camera on the TV

When the thickness of your TV is between 35-120 mm, you can mount the camera on to your TV.



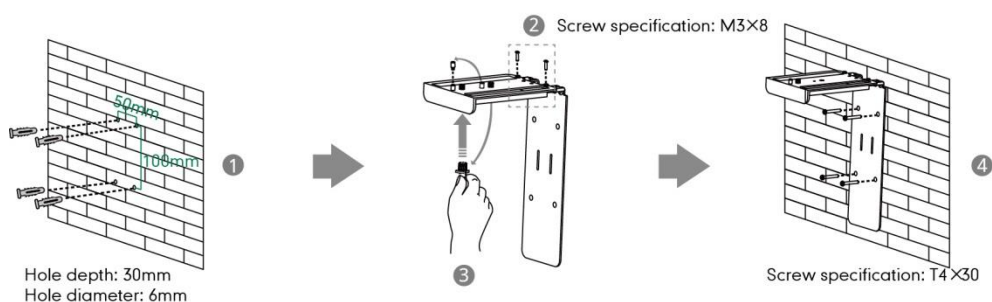
Do the following:

1. Lock the camera to the L-bracket.
2. Remove the protection of the Velcro.
3. Put the L-bracket on the top of the TV.
4. Adjust the L-bracket to ensure close adhesion to the back of the TV.

b) Mounting the camera on to a wall

You can also mount the camera on to a wall. The recommended height for camera positioning is 1.5m-1.8m above the ground.

Do the following:

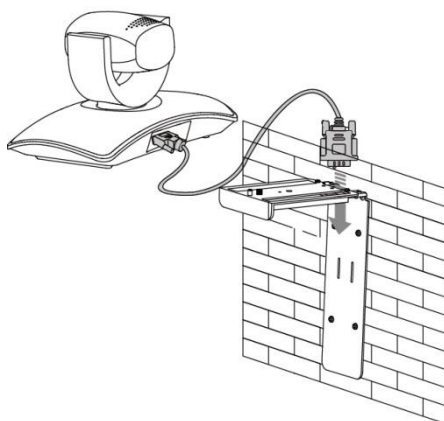


1. Punch holes in the wall and then insert the expansion bolts.

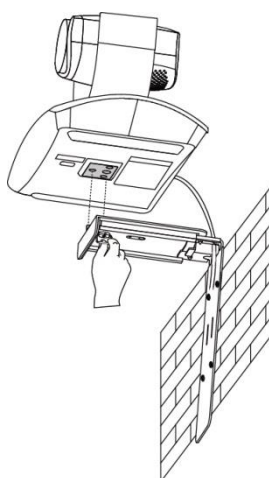
Installation location for the expansion bolts and punching requirement are shown

above.

2. Lock the L-bracket with the M3×8 screws.
3. Adjust the screws position and manually lock them.
4. Lock the L-bracket to the wall with T4×30 screws.
5. Connect one end of the DVI cable to the camera and put the other end of the cable through the L-bracket.



6. Lock the camera to the L-bracket, and then connect the other end of the DVI cable to the VC400/VC120 codec.



Installing Batteries in the Remote Control

Do the following:

1. Open the battery cover on the back of the remote control.
2. Insert the batteries with the correct polarity.
3. Replace the battery cover.



Remote Control Battery Safety Information

- Never make wrong polarity connection when charging and discharging battery packs.
- Avoid crushing, puncturing, or putting a high degree of pressure on any battery, as this can cause an internal short-circuit, resulting in overheating.
- Remove the batteries if they are not in use for long period of time. Battery leakage and corrosion can damage the remote control, dispose batteries safely.
- Do not dispose used batteries in domestic waste. Dispose batteries at special collection points or return to stores if applies.
- Do not dispose batteries in a fire.

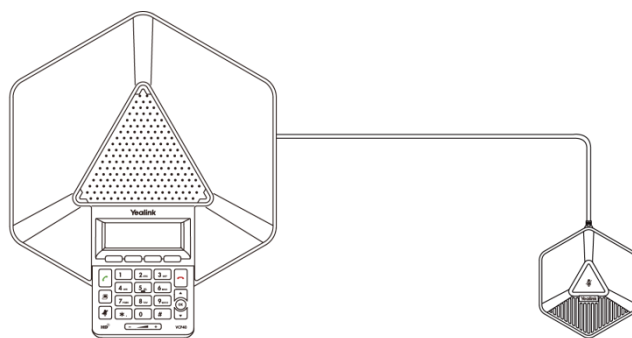
Connecting the CPE80 Expansion Microphone

If your video conferencing room is large, you can add an extra CPE80 expansion microphone to the MIC port on the VCP40 phone to expand the audio range of the conference phone. VCP40 phone has two MIC ports. This allows you to connect a CPE80 expansion microphone to one of the ports, depending on the location of the speaker.

CPE80 is a directional microphone. It supports 120-degree audio pickup range. Always ensure that the speaker faces the expansion microphone.

To connect the expansion microphone:

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



VCP40 Video Conferencing Phone

CPE80 Expansion Microphone

Note


Up to two expansion microphones can be connected to a VCP40 conference phone.

Powering the System On and Off

Note




Caution! To avoid corrupting the system, you should always power off the system using the power button on the VC400/VC120 codec. After turning the power off in this way, wait at least 15 seconds before you unplug the power adapter from the VC400/VC120 codec. This helps to ensure that the system powers off correctly.

To power on the system:

After all components are connected, press  on the VC400/VC120 codec. The indicator LED on the VC400/VC120 codec then illuminates solid green.

To power off the system:

Do one of the following:

- Long press  on the VC400/VC120 codec.
- Short press  on the VC400/VC120 codec, the display device will prompt "Press the power button to turn off the system. Press any button on remote control to cancel". Press  again to power off the system or press any button on the remote control to cancel.

System Initialization

Once you have power on the system, it will begin its initialization process.

During the initialization process, the following events take place:

Loading the ROM file

The ROM file sits in the flash memory of the system. Systems come from the factory with a ROM file preloaded. During initialization, systems run a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If the system is connected to a switch, the switch will notify the system about the VLAN information defined on the switch.

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The system is capable of querying a DHCP server. DHCP is enabled on the system by default. The following network settings 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 settings of the system manually if any of them are not provided by the DHCP server. For more information on configuring network settings manually, refer to [Configuring Network Settings Manually](#) on page 54.

System Startup

After the initializing process, the system will complete startup by cycling the following steps:

1. The LED indicator on the VC400/VC120 codec illuminates solid green.
2. The LED indicator on the camera illuminates solid green.
3. The display device displays the boot up screen.
4. The camera pans to the middle position automatically.
5. The display device displays the setup wizard (when you first start up or reset the system, the display device will display the setup wizard)

For more information on how to complete the setup wizard, refer to [Setup Wizard](#) on page 43.

6. After completing the setup wizard, the display device displays the main screen.
The main screen displays the following:

- Time and date
- System IP address and site name
- Status icon
- Soft key labels
- Video image

7. The VCP40 conferencing phone starts up normally. The phone's LCD screen displays the site name, status icon, soft keys, time and date.

If the system has successfully passed through these steps, it starts up correctly and is ready for use.

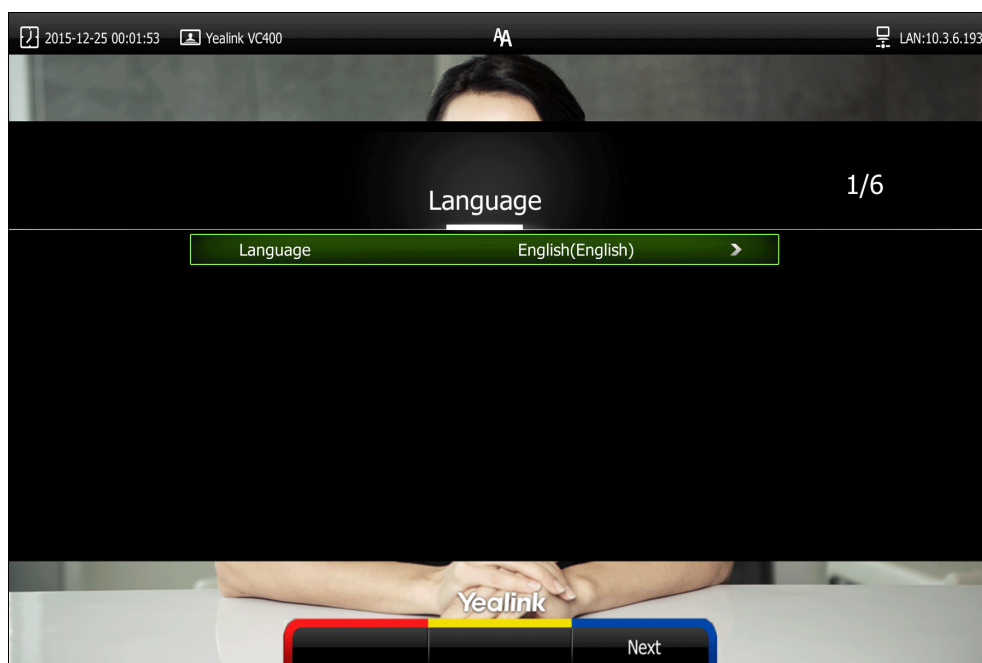
Setup Wizard


When you first start up or reset the system, the display device will display the setup wizard.

To complete the setup wizard via the remote control:

1. Set the language displayed on the display device.

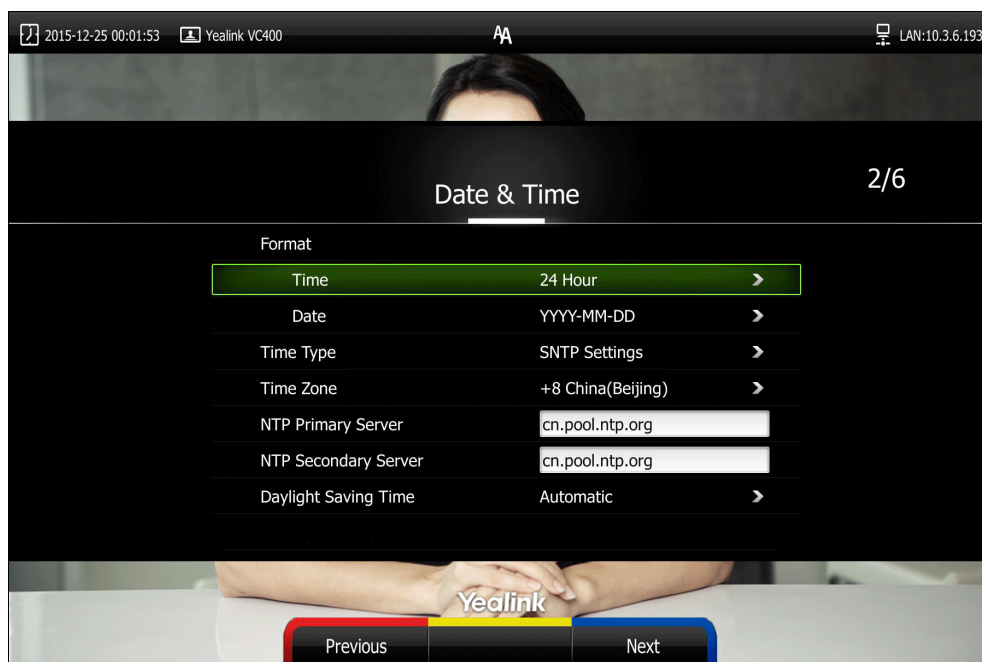
The default language is English.





2. Press  (Next soft key) to continue.
3. Set the date and time (e.g., set the time zone, time format, date format and the type of the daylight saving time).

The system obtains the time and date from the NTP server automatically by default.

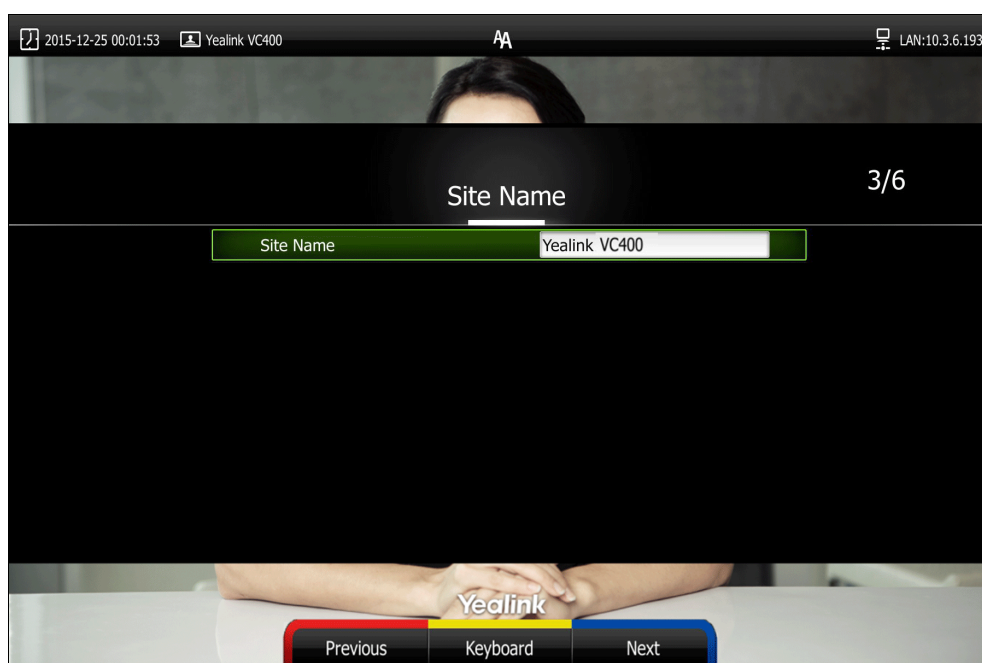
You can also configure the time and date manually. For more information, refer to [Date & Time](#) on page 132.





- Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.

- Edit the site name.

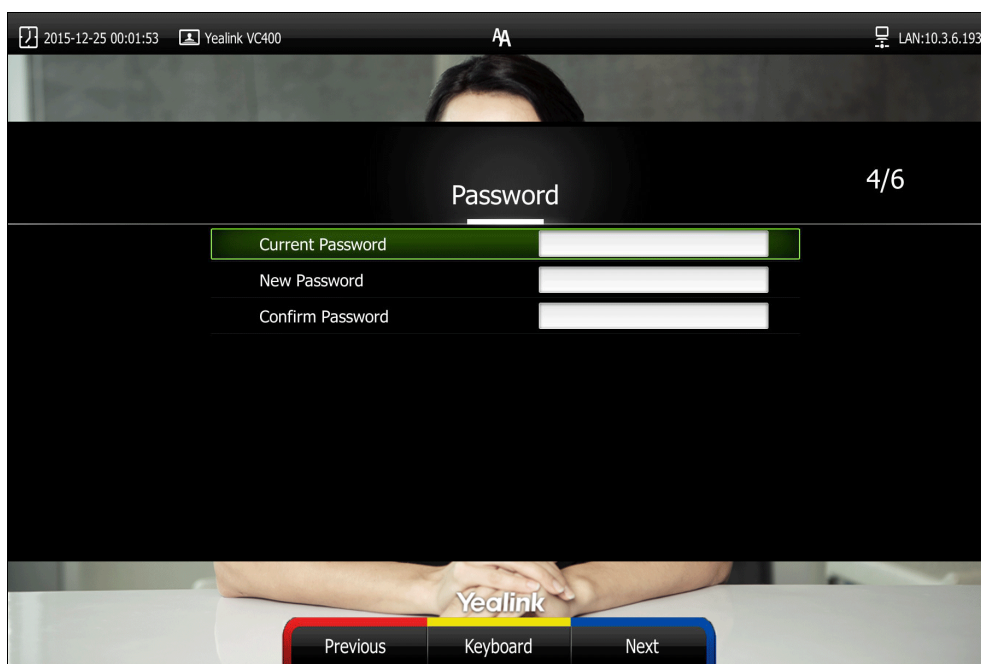
The default site name is "Yealink VC400" or "Yealink VC120".



- Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.



- Change the administrator password.

The default administrator password is “0000”. For security reasons, the administrator should change the default administrator password as soon as possible.

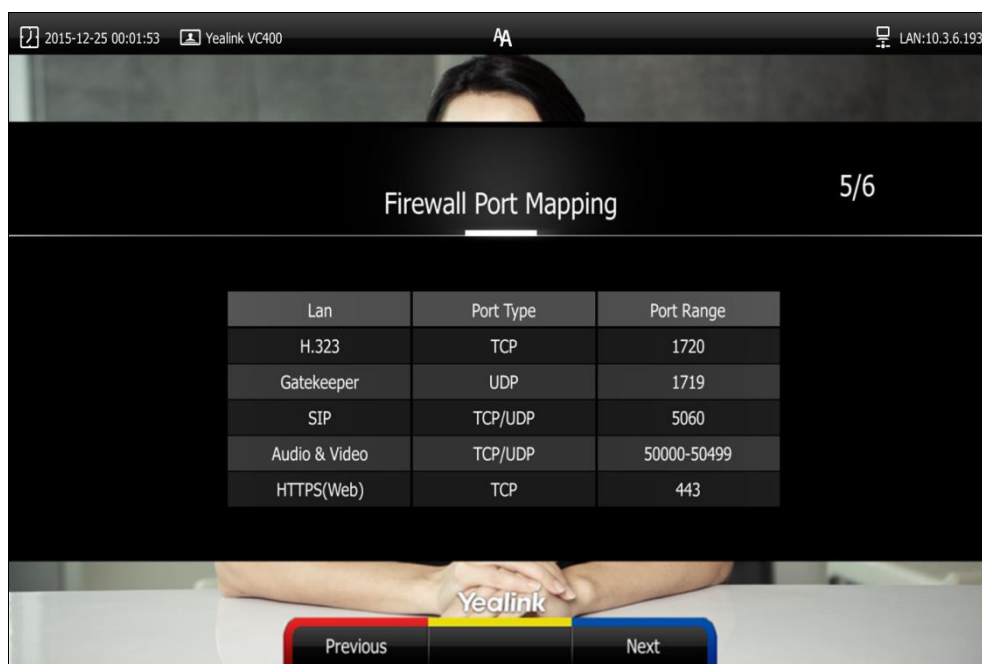
**Note**



Do remember the new administrator password or keep a copy of the password in a safe place. If you forget the password, you will need to reset the system to the factory settings, and then reset the password or use the default password “0000”.

For more information, refer to [Resetting to Factory](#) on page 211.

8. Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.


The display device displays firewall port mapping information.



9. Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.
10. Configure network settings.

The phone will try to contact a DHCP server in your network to obtain network parameters by default. If you uncheck the DHCP checkbox, you will then need to configure network settings manually. For more information, refer to [Configuring LAN Properties](#) on page 50.



11. Press  (**Complete** soft key) to complete the setup wizard.

Enabling Communication with Other Systems

- If you use Network Address Translation (NAT) to assign a public IP address to your VC400/VC120 system for communication with devices outside your private network, you must enable NAT on your VC400/VC120 system before placing calls. For more information, refer to [Network Address Translation](#) on page 78.
- If your VC400/VC120 system communicates with other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the VC400/VC120 system through the reserved ports specified in [Reserved Ports](#) on page 75. And the required ports specified in [Configuring the System for Use with a Firewall or NAT](#) on page 75. Users placing calls through a firewall to system may experience one-way audio or video if the firewall is not properly configured.
- If you are using Session Initiation Protocol (SIP) servers in your environment to place calls using the SIP protocol, refer to [Configuring SIP Settings](#) on page 99.
- If you are using H.323 gatekeepers in your environment and want to place calls using a name or extension with the H.323 protocol, refer to [Configuring H.323 Settings](#) on page 104.

Placing a Test Call from the Yealink VCS System

Yealink Demo1 to Yealink Demo3 are three default contacts stored in the local directory. You can place a test call to the default contact, and the test call will be routed to the Yealink demo video conferencing system. Yealink demo contacts can help users to test quickly whether the system is normal after installation.

Configuring Network

This chapter provides information on how to configure network settings for the system. Proper network settings allow the system work efficiently in your network environment.

This chapter provides the following sections:

- [Preparing the Network](#)
- [Configuring LAN Properties](#)
- [Configuring Network Speed and Duplex Mode](#)
- [VLAN](#)
- [802.1X Authentication](#)
- [H.323 Tunneling](#)
- [Configuring the System for Use with a Firewall or NAT](#)
- [91Intelligent Firewall Traversal](#)
- [Quality of Service](#)
- [VPN](#)

Preparing the Network

Before you begin configuring the network options, you must make sure your network is ready for video conferencing.

The following table lists the network information you need to obtain from the network administrator when preparing your network.

Type	Network Information
Type of system	DHCP
	Static IP Address <ul style="list-style-type: none">• IP address• Subnet mask• Gateway
DNS Server	IP address of DNS server
Call Protocol	Register information of SIP account
	Register information of H.323 account
802.1X	Authentication information

Configuring LAN Properties

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. The system complies with the DHCP specifications documented in RFC 2131. DHCP by default, which allows the system connected to the network to become operational by obtaining IP addresses and additional network parameters from the DHCP server.

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 system to the network. The system broadcasts DISCOVER messages to request network information carried in DHCP options. The DHCP server responds with the specific values in the corresponding options.

The following table lists the common DHCP options supported by the system.

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

Parameter	DHCP Option	Description
Address		client's subnet.
Network Time Protocol Servers	42	Specifies a list of the NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identifies the vendor-specific information.
Vendor Class Identifier	60	Identifies the vendor type.
TFTP Server Name	66	Identifies a TFTP server when the 'name' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identifies 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>.

To make the system gather network settings via DHCP options, you need to contact your network administrator to configure the DHCP server properly.

DHCP feature parameters on the system are described below:

Parameter	Description	Configuration Method
DHCP	Enables or disables the system to obtain network settings from the DHCP server. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Host Name	Configures the host name of the system. Default: Blank Note: When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12. Host name is optional, so it is not	Web User Interface

Parameter	Description	Configuration Method
	<p>a mandatory configuration item. For more information, contact your network administrator.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	

To configure DHCP via web user interface:

1. Click on **Network->LAN Configuration**.
2. In the **IP Config** block, mark the **DHCP** radio box.
3. (Optional.)Enter the host name of the system in the **Host Name** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network (selected), Setting, Directory, and Security. On the left, there's a sidebar with LAN Configuration, NAT/Firewall, Advanced, and Diagnose. The main content area shows the LAN Configuration page. The DHCP radio button is selected, and the Host Name field is filled with 'VC400'. Below this, there's a table showing port configurations.

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Audio&Video media stream port	TCP/UDP	50000-50499
Web management port (optional)	TCP	443

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **Confirm** to reboot the system immediately.

To configure DHCP via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**LAN Configuration**.
2. Check the **DHCP** checkbox.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Static DNS

Even though DHCP is enabled, you can manually configure the static DNS address(es).

Parameters of static DNS on the system are described below:

Parameter	Description	Configuration Method
Static DNS	<p>Triggers the static DNS feature to on or off.</p> <p>Default: Off</p> <p>Note: If it is set to Off, the system will use the IPv4 DNS obtained from DHCP.</p> <p>If it is set to On, the system will use manually configured static IPv4 DNS.</p> <p>It only works if the value of the "IP Config" is set to DHCP. If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Primary DNS	<p>Configures the primary IPv4 DNS server.</p> <p>Default: Blank</p> <p>Note: It only works if the value of the "Static DNS" is set to On. If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Secondary DNS	<p>Configures the secondary IPv4 DNS server.</p> <p>Default: Blank</p> <p>Note: It only works if the value of the "Static DNS" is set to On. If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>

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

1. Click on **Network->LAN Configuration**.
2. In the **IP Config** block, mark the **DHCP** radio box.

3. In the **Static DNS** block, mark the **On** radio box.
4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Audio&Video media stream port	TCP/UDP	50000-50499
Web management port (optional)	TCP	443

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

To configure static DNS when DHCP is used via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**LAN Configuration**.
2. Check the **DHCP** checkbox.
3. Check the **Static DNS** checkbox.
4. Enter the desired values in the **DNS Primary Server** and **DNS Secondary Server** fields respectively.
5. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
6. Select **OK** to reboot the system immediately.

Configuring Network Settings Manually

If DHCP is disabled or the system cannot obtain network settings from the DHCP server, you need to configure them manually.

The following parameters should be configured for systems to establish network connectivity:

- **IP Address:** Configure the system to use the assigned IP address.
- **Subnet Mask:** Enter the subnet mask address when the system does not automatically obtain the subnet mask.
- **Gateway:** A gateway is a network point that works as an entrance to another network.
- **Primary DNS /Secondary DNS:** Domain Name System (DNS) servers translates domain names (for example: www.example.com), which can be easily memorized by humans, to the numerical IP addresses (192.168.1.15) needed for the purpose of computer services and devices worldwide.

Network parameters need to be configured manually on the system are described below.

Parameter	Description	Configuration Method
Static IP	Enables or disables the system to use manually configured network settings. Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
IP Address	Configures the IP address assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Subnet Mask	Configures the subnet mask assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Gateway	Configures the gateway assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Primary DNS	Configures the primary DNS server assigned to the system.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	
Secondary DNS	Configures the secondary DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure network settings manually via web user interface:

1. Click on **Network->LAN Configuration**.
2. In the **IP Config** block, mark the **Static IP** radio box.
3. Enter the IP address, subnet mask, default gateway, primary DNS and secondary DNS in the corresponding fields.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (highlighted), 'Setting', 'Directory', and 'Security'. On the left, a sidebar shows 'LAN Configuration' (selected), 'NAT/Firewall', 'Advanced', and 'Diagnose'. The main content area shows the 'LAN Configuration' page with two radio buttons: 'DHCP' and 'Static IP' (selected). Below the radio buttons, there are input fields for 'IP Address' (10.3.6.193), 'Subnet Mask' (255.255.255.0), 'Gateway' (10.3.6.254), 'Static DNS' (On/Off), 'Primary DNS' (192.168.1.166), 'Secondary DNS' (192.168.1.167), and 'Host Name' (VC400). A table at the bottom lists port configurations:

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Audio&Video media stream port	TCP/UDP	50000-50499
Web management port (optional)	TCP	443

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **Confirm** to reboot the system immediately.

To configure network settings manually via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**LAN Configuration**.
2. Uncheck the **DHCP** checkbox.
3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **DNS Primary Server** and **DNS Secondary Server** fields respectively.
4. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
5. Select **OK** to reboot the system immediately.

Configuring Network Speed and Duplex Mode

You can configure the network speed and duplex mode the system uses. The network speed and duplex mode you select for the system must be supported by the switch. The network speeds and duplex modes supported by the system are:

- Auto
- 10 Mb/s Half Duplex
- 100 Mb/s Half Duplex
- 10 Mb/s Full Duplex
- 100 Mb/s Full Duplex
- 1000 Mb/s Full Duplex

Auto is configured on the system by default.

Auto

Auto means that the switch will negotiate the network speed and duplex mode for the systems 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 systems.

Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one system can send data on the line, but not receive data simultaneously.

Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one system can send data on the line while also receiving data.

Parameter of network speed feature on the system is described below:

Parameter	Description	Configuration Method
Network Speed	<p>Specifies the network speed and duplex mode for the system to use.</p> <p>Default: Auto</p> <p>Note: If Auto is selected, the network speed and duplex mode will be negotiated by the switch automatically.</p> <p>The network speed and duplex mode you select must be supported by the switch.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface

To configure the network speed via web user interface:

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

2. Select the desired value from the pull-down list of **Network Speed**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is divided into several sections: **SNMP** (Active: Disabled, Port: 161, Trusted Address: empty), **Web Server** (HTTP: Enabled, HTTP Port: 80, HTTPS: Enabled, HTTPS Port: 443), **802.1x** (802.1x Mode: Disabled, Identity: empty, MD5 Password: masked, CA Certificates: empty with Browse... and Upload buttons, Device Certificates: empty with Browse... and Upload buttons), and **VPN** (Active: Disabled, Upload VPN Config: empty with Browse... and Upload buttons). At the bottom, the **Speed** section is highlighted with a red box, showing 'Network Speed' set to '100Mb/s Half Duplex M'. At the very bottom are 'Confirm' and 'Cancel' buttons.

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

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

4. Click **Confirm** to reboot the system immediately.

VLAN

VLAN (Virtual Local Area Network) is used to divide a physical network logically into several broadcast domains. VLAN membership is configurable 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 system is to insert a tag with VLAN information to the packets generated by the system. When VLAN is configured on the system properly, the system will tag all packets with the VLAN ID. The switch receives

and forwards the tagged packets to the corresponding VLAN according to the tag's VLAN ID, as described in IEEE Std 802.3.

In addition to manual configuration, the system also supports automatic VLAN discovery via LLDP or DHCP. The assignment takes effect in the following order: assignment via LLDP, manual configuration, then assignment via DHCP.

For more information on VLAN, refer to [VLAN Feature on Yealink IP Phones](#).

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the system 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 the system:

- Capabilities Discovery -- allows LLDP-MED system to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify the system 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 the system is powered, power priority, and how much power the system needs.
- Inventory Management -- provides a means to effectively manage the system and its attributes, such as model number, serial number and software revision.

TLVs supported by the system are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the system.
	Port ID	The MAC address of the system.
	Time To Live	Seconds until data unit expires. The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the system.

TLV Type	TLV Name	Description
		The default value is "VCS".
	System Description	Description of the system. Description includes firmware version of the system.
	System Capabilities	The supported and enabled system capabilities. The Telephone capability is supported and enabled 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 mode and network speed settings of the system. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 1000BASE-T (full duplex mode) 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 system 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 the system.
	Inventory – Firmware Revision	Firmware revision of the system.
	Inventory –	Software revision of the system.

TLV Type	TLV Name	Description
	Software Revision	
	Inventory – Serial Number	Serial number of the system.
	Inventory – Manufacturer Name	Manufacturer name of the system. The default value is "Yealink".
	Inventory – Model Name	Model name of the system. The default value is "VCS".
	Asset ID	Assertion identifier of the system.

Parameters of LLDP feature on the system are described below.

Parameter	Description	Configuration Method
LLDP->Active	Enables or disables LLDP feature on the system. Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Packet Interval(1-3600s)	Configures the interval (in seconds) for the system to send LLDP requests. Default: 60 Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

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**.

- Enter the desired time interval in the **Packet Interval (1-3600s)** field.

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

To configure LLDP via the remote control:

- Select **Menu->Advanced** (default password: 0000) -> **Advanced Network**.
- In the **LLDP** block, check the **Active** checkbox.
- Enter the desired value in the **Packet Interval (1-3600s)** field.
- Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
- Select **OK** to reboot the system immediately.

Manual Configuration for VLAN

VLAN is disabled on systems by default. You can configure VLAN manually. Before configuring VLAN on the systems, you need to obtain the VLAN ID from your network administrator.

Parameters of manual VLAN on the system are described below.

Parameter	Description	Configuration Method
Internet Port->Active	<p>Enables or disables VLAN for the Internet (WAN) port.</p> <p>Default: Disabled</p> <p>Note: If you change this parameter, the system will reboot</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	to make the change take effect.	
VID(1-4094)	Configures VLAN ID for the Internet (WAN) port. Default: 1 Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Priority	Configures VLAN priority for the Internet (WAN) port. Valid values: 0-7 7 is the highest priority, 0 is the lowest priority. Default: 0 Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

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 **Internet 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 VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, a sidebar shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is titled 'LLDP' and 'VLAN'. Under 'VLAN', the 'Internet Port' section is highlighted with a red box, containing three fields: 'Active' (dropdown menu set to 'Enabled'), 'VID(1-4094)' (text input field with '1'), and 'Priority' (dropdown menu set to '0'). Below this, the 'DHCP VLAN' section shows 'Active' (dropdown menu set to 'Enabled') and 'Option' (text input field with '132').

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

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

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

To configure VLAN via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **VLAN** block, check the **Active** checkbox.
3. Enter the VLAN ID in the **VID(1-4094)** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change.

The display device prompts "Reboot now?".

6. Select **OK** to reboot the system immediately.

DHCP VLAN

The system supports VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the system will examine the 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](#).

Parameters of VLAN feature on the system are described below.

Parameter	Description	Configuration Method
DHCP VLAN->Active	Enables or disables the DHCP VLAN discovery feature on the system. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Option	Configures the DHCP option from which the system obtains the VLAN settings. You can configure at most five DHCP options and separate them by commas. Valid Values: 128-254 Default: 132 Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

To configure 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 VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main navigation bar has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, a sidebar menu shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is divided into sections: 'LLDP' (Active: Disabled, Packet Interval: 60), 'VLAN' (Internet Port: Active: Disabled, VID: 1, Priority: 0), and 'DHCP VLAN' (Active: Enabled, Option: 132). The 'DHCP VLAN' section is highlighted with a red rectangular box. Below it is the 'QoS' section with Audio Priority: 63, Video Priority: 34, and Data Priority: 63.

4. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after a reboot.
5. Click **Confirm** to reboot the system immediately.

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 system that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the system provides credentials, such as user name and default password, for the authenticator. The authenticator then forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the system is allowed to access resources located on the protected side of the network.

The system supports the authentication 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](#).

802.1X feature parameters on the system are described below:

Parameter	Description	Configuration Method
802.1x Mode	<p>Specifies the 802.1x authentication mode.</p> <ul style="list-style-type: none"> • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 <p>Default: Disabled</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Identity	<p>Configures the user name for 802.1x authentication.</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
MD5 Password	<p>Configures the password for 802.1x authentication.</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
CA Certificates	<p>Configures the access URL of the CA certificate when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPV2 or EAP-TTLS/EAP-MSCHAPV2.</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
Device Certificates	<p>Configures the access URL of the device certificate when the 802.1x authentication mode is</p>	Web User Interface

Parameter	Description	Configuration Method
	configured as EAP-TLS. Note: If you change this parameter, the system will reboot to make the change take effect.	

To configure 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 **Mode 802.1x**.
 - 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 VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network (selected), Setting, Directory, and Security. On the left, a sidebar shows LAN Configuration, NAT/Firewall, Advanced (selected), and Diagnose. The main content area is titled 'SNMP' and 'Web Server'. The '802.1x' section is highlighted with a red box and contains the following fields:

- 802.1x Mode:** A dropdown menu set to 'EAP-MD5'.
- Identity:** A text field containing 'yealink'.
- MD5 Password:** A text field with masked characters (dots).

Below the 802.1x section, there are two rows for certificates:

- CA Certificates:** A text field followed by 'Browse...' and 'Upload' buttons.
- Device Certificates:** A text field followed by 'Browse...' and 'Upload' buttons.

- 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, *.crt, *.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 VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network (selected), Setting, Directory, and Security. On the left, a sidebar lists configuration options: LAN Configuration, NAT/Firewall, Advanced (selected), and Diagnose. The main content area is titled 'SNMP' and 'Web Server'. The '802.1x' section is highlighted with a red box and contains the following fields:

- 802.1x Mode:** A dropdown menu set to 'EAP-TLS'.
- Identity:** A text input field containing 'yealink'.
- MD5 Password:** A text input field with masked characters (dots).
- CA Certificates:** A text input field containing 'C:\fakepath\ca.crt', with 'Browse...' and 'Upload' buttons to its right.
- Device Certificates:** A text input field containing 'C:\fakepath\client.pem', with 'Browse...' and 'Upload' buttons to its right.

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 VC400 web interface. The 'Network' tab is active, and the 'Advanced' sub-tab under 'LAN Configuration' is selected. The '802.1x' configuration section is highlighted with a red border. It includes the following fields and options:

- 802.1x Mode:** A dropdown menu set to 'PEAP-MSCHAPv2'.
- Identity:** A text input field containing 'yealink'.
- MD5 Password:** A text input field with masked characters (dots).
- CA Certificates:** A text input field containing 'C:\fakepath\ca.crt', accompanied by 'Browse...' and 'Upload' buttons.
- Device Certificates:** An empty text input field, accompanied by 'Browse...' and 'Upload' buttons.

- 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 shows the Yealink VC400 web interface. The left sidebar has a menu with 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area has tabs for 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. Under the 'Network' tab, there are sections for 'SNMP' and 'Web Server'. The '802.1x' section is highlighted with a red box. It contains the following fields and buttons:

- 802.1x Mode:** A dropdown menu set to 'EAP-TTLS/EAP-MSCHA'.
- Identity:** A text field containing 'yealink'.
- MD5 Password:** A text field with masked characters (dots).
- CA Certificates:** A text field containing 'C:\fakepath\ca.crt', followed by 'Browse...' and 'Upload' buttons.
- Device Certificates:** A text field, followed by 'Browse...' and 'Upload' buttons.

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

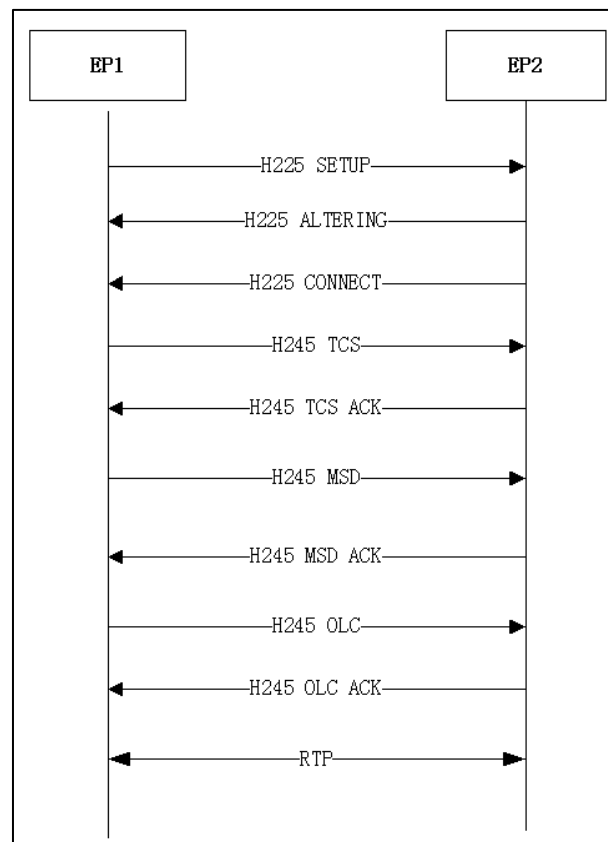
To configure the 802.1X via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **Advanced Network**.
2. Select the desired mode from the pull-down list of **802.1x Mode**.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

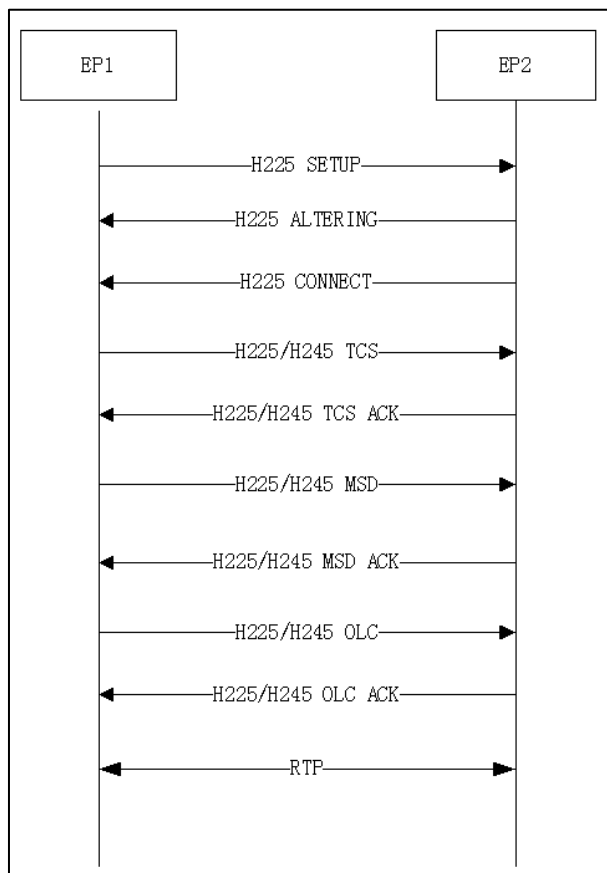
H.323 Tunneling

The H.245 protocol is a control protocol that manages the media sessions. It is a part of the H.323 protocol suite. The H.245 protocol is used primarily to negotiate the master-slave relationship between communicating systems. The H.245 messages can be encapsulated and carried between H.225 controlled system within H.225 messages. This way of "piggy-backing" an H.245 message to the H.225 message is referred to as H.323 Tunneling. The tunneling feature relies on H.225 system-to-system connectivity (via TCP) to pass H.245 messages, and uses the H.225 communication channel without creating a separate TCP socket connection (per H.323 call) for media control.

If H.323 tunneling feature is disabled, the setup processes of an H.323 call are shown below:



If H.323 tunneling feature is enabled on both sites, the setup processes of an H.323 call are shown below:



The parameter of the H.323 tunneling feature on the system is described below:

Parameter	Description	Configuration Method
H.323 Tunneling	Enables or disables the H.323 tunneling on the system. Default: Disabled	Remote Control Web User Interface

To configure H.323 tunneling via web user interface:

1. Click on **Account->H323**.

2. Select the desired value from the pull-down list of **H.323 Tunneling**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. Below this is a green header with 'Yealink VC400' and tabs for 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is selected. On the left, a sidebar menu has 'H323' selected. The main content area displays various configuration settings for H.323. A red rectangle highlights the 'H.323 Tunneling' dropdown menu, which is currently set to 'Enabled'. Other settings include 'Register Status' (Registered), 'H.323 Protocol' (Enabled), 'H.323 Account' (Enabled), 'H.323 Name' (9000), 'H.323 Extension' (9000), 'Gatekeeper Mode' (Manual), 'Gatekeeper IP Address 1' (10.2.1.43) with Port 1719, 'Gatekeeper IP Address 2' (empty) with Port 1719, 'Gatekeeper Authentication' (Disabled), 'Gatekeeper Username' (empty), 'Gatekeeper Password' (masked), 'H.460 Active' (Disabled), 'H.323 Tunneling' (Enabled), 'H.235 Encryption' (Disabled), and 'Protocol Monitor Port' (1720).

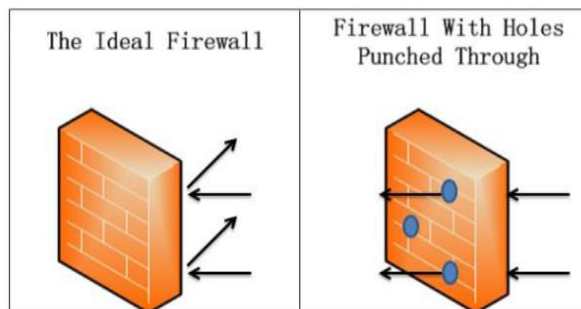
3. Click **Confirm** to accept the change.

To configure H.323 tunneling via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **H.323**.
2. Check the **H.323 Tunneling** checkbox.
3. Press the **Save** soft key to accept the change.

Configuring the System for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with video conferencing equipment, you must configure the firewall to allow incoming and outgoing traffic to the VC400/VC120 system through the reserved ports. Users placing calls through a firewall to system may experience one-way audio or video if the firewall is not properly configured.



You must configure your firewall to allow incoming and outgoing traffic through the following ports:

Description	Port Range	Port Type
H.323 register/call request	1719	UDP
H.323 call setup	1720	TCP
SIP (default transport protocol)	5060	UDP
SIP (when selecting the TCP transport protocol)	5060	TCP
SIP (when selecting the TLS transport protocol)	5061	TCP
Reserved ports on the system. For more information, refer to Reserved Ports on page 75.	50000-50499 (default range)	TCP/UDP
HTTPS (Optional)	443	TCP

Reserved Ports

By default, the system communicates through TCP and UDP ports in the 50000 - 54999 range for video, voice, presentations, and camera control. The system uses only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type

of call: video or voice.

The following tables identify the number of ports required per connection by protocol and the type of call.

Required ports for an H.323 two-way call:

Call Type	Number of Required Ports
Video	8 UDP ports (6 if presentation is disabled) 2 TCP ports
Voice	2 UDP ports 2 TCP ports
Each additional video participant requires 8 UDP ports and 2 TCP ports.	
Each additional audio participant requires 2 UDP ports and 2 TCP ports.	

Required ports for a SIP two-way call:

Call Type	Number of Required Ports
Video	8 UDP ports (6 if presentation is disabled)
Voice	2 UDP ports
Each additional video participant requires 8 UDP ports.	
Each additional audio participant requires 2 UDP ports.	

The following table lists the number of UDP and TCP ports needed for the video conferencing system. This information can help you to determine the range of port number to be entered in the **Reserved Port** field.

System	Maximum Connections	Required Ports for an H.323 Call		Required Ports for a SIP Call	
Basic version of VC400	Four-way video call and a presentation and a voice call	26 UDP 8 TCP	50000-50025 50000-50007	26 UDP	50000-50025
Upgraded version of VC400	Eight-way video call and a presentation and a voice call	58 UDP 16 TCP	50000-50057 50000-50015	58 UDP	50000-50057
VC120	Two-way video call and a presentation and a voice call	10 UDP 4 TCP	50000-50009 50000-50003	10 UDP	50000-50009

Parameters for reserved ports on the system are described below:

Parameter	Description	Configuration Method
UDP Port Scope	<p>Configures the range of the UDP ports.</p> <p>Valid values: 1-65535</p> <p>Default range: 50000-50499</p> <p>Note: SIP and H.323 calls share the configured ports.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
TCP Port Scope	<p>Configures the range of the TCP ports.</p> <p>Valid values: 1-65535</p> <p>Default range: 50000-50499</p> <p>Note: SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure reserved ports via web user interface:

1. Click on **Network->NAT/Firewall**.
2. In the **Reserve Port** block, configure the UDP port range in the **UDP Port Scope** field.

3. In the **Reserve Port** block, configure the TCP port range in the **TCP Port Scope** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', 'NAT/Firewall' (selected), 'Advanced', and 'Diagnose'. The main content area is titled 'NAT Configuration' and includes sections for 'NAT Configuration', 'Stun Config', 'Reserve Port', and 'Intelligent Firewall Traversal'. The 'Reserve Port' section is highlighted with a red box, showing 'UDP Port Scope' and 'TCP Port Scope' both set to '50000 ~ 50499'.

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

A dialog box pops up to prompt that the settings will be implemented after a reboot.

5. Click **Confirm** to reboot the system immediately.

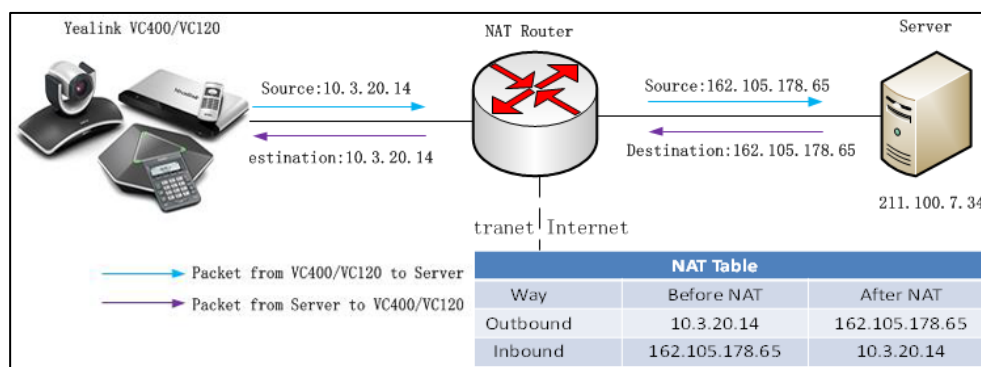
To configure reserved ports via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **NAT/Firewall**.
2. In the **Reserved** block, configure the range of the UDP ports and TCP ports.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Network Address Translation

NAT device usually connects two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses. NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address.

Multiple solutions for NAT traversal are available, for example, application layer gateway (ALG), simple traversal of UDP through NAT (STUN), and H.460 firewall traversal.



Static NAT

If NAT/Firewall devices do not support the ALG, VC400/VC120 must be configured with the static NAT.

Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address while the mapped-to address is the real host IP address.

If your system is connected to a LAN that uses a NAT, you need to configure NAT Public IP Address so that your system can communicate to WAN.

Note

If H.460 firewall traversal is enabled on the system, the system will automatically ignore the static NAT settings for H.323 calls. For more information on H.460 firewall traversal, refer to [H.460 Firewall Traversal](#) on page 89.

Static NAT feature parameters on the system are described below:

Parameter	Description	Configuration Method
Static NAT	<p>Specifies the static NAT type.</p> <ul style="list-style-type: none"> Disabled—the system does not use the NAT feature. Manual—the system uses the manually configured NAT public address. Auto—the system obtains the NAT public address from the Yealink-supplied server. 	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	Default: Disabled	
NAT Public IP Address	<ul style="list-style-type: none"> Displays the NAT public address automatically obtained from the Yealink-supplied server if the static NAT is set to Auto. Configures the NAT public address for the system if the static NAT is set to Manual. 	Remote Control Web User Interface
Route Traversal	<p>Configures the route traversal type.</p> <ul style="list-style-type: none"> Auto—NAT works only when making a call to public network or receiving a call from the public network. Compulsory—NAT works when you are in multi-level intranet network to solve the one-way audio or video problem. <p>Default: Auto</p>	Web User Interface
NAT_Traversal	<p>Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately.</p> <ul style="list-style-type: none"> Disabled STUN StaticNat <p>Default: Disabled</p> <p>Note: Static NAT works only if this parameter is set to StaticNat.</p>	Remote Control Web User Interface

To configure static NAT via web user interface:

1. Click on **Network->NAT/Firewall**.
2. Select the desired value from the pull-down list of **Static NAT**.
3. Configure the NAT public address in the **NAT Public IP Address** field if **Manual** is selected from the pull-down list of **Static NAT**.

4. If multi-level intranet network has deployed in your environment, and you experience the one-way audio or video problem, select **Compulsory** from the pull-down list of **Route Traversal** to solve this problem.

The screenshot displays the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. Below this, a green header bar contains the Yealink logo and navigation tabs: Home, Status, Account, Network (highlighted), Setting, Directory, and Security. On the left side, a sidebar menu lists LAN Configuration, NAT/Firewall (selected), Advanced, and Diagnose. The main content area is titled 'NAT Configuration' and contains several sections: 'Static NAT' with a dropdown menu set to 'Auto'; 'NAT Public IP Address' with a text field containing '117.28.234.34'; 'Route Traversal' with a dropdown menu set to 'Compulsory'; 'Stun Config' with 'Active' set to 'Disabled', 'Stun Server' as an empty field, and 'STUN Port' as '3478'; 'Reserve Port' with 'UDP Port Scope' and 'TCP Port Scope' both set to '50000 ~ 50499'; and 'Intelligent Firewall Traversal' with a dropdown menu set to 'On'. A red rectangular box highlights the 'Static NAT', 'NAT Public IP Address', and 'Route Traversal' settings.

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

To configure Static NAT for SIP account via web user interface:

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

2. Select **StaticNat** from the pull-down list of **NAT_Traversal**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account' (selected), 'SIP IP Call', and 'Codec'. The main content area displays various settings for the selected 'SIP Account'. The 'NAT_Traversal' dropdown menu is highlighted with a red box and set to 'StaticNat'. Other settings include 'SIP Account' (Enabled), 'Register Name', 'User Name', 'Password', 'Server Host', 'Port' (5060), 'Enable Outbound Proxy Server' (Disabled), 'Outbound Proxy Server', 'Port' (5060), 'Transport' (UDP), 'Server Expires' (3600), 'SRTP' (Disabled), 'DTMF Type' (SIP INFO), 'DTMF Info Type' (DTMF), 'DTMF Payload Type (96~127)' (101), and 'Keep Alive Interval' (30).

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

To configure Static NAT for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select **StaticNat** from the pull-down list of **NAT_Traversal**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account', 'SIP IP Call' (selected), and 'Codec'. The main content area displays various settings for the selected 'SIP IP Call'. The 'NAT_Traversal' dropdown menu is highlighted with a red box and set to 'StaticNat'. Other settings include 'Transport' (TCP), 'SRTP' (Disabled), 'DTMF Type' (SIP INFO), 'DTMF Info Type' (DTMF), 'DTMF Payload Type (96~127)' (101), 'RPort' (Enabled), 'BFCP' (Enabled), and 'FECC(SIP)' (Enabled).

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

To configure static NAT via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **NAT/Firewall**.
2. Select the desired value from the pull-down list of **Type**.
3. Configure the NAT public address in the **Public IP Address** field if **Manual Settings** is

selected from the pull-down list of **Type**.

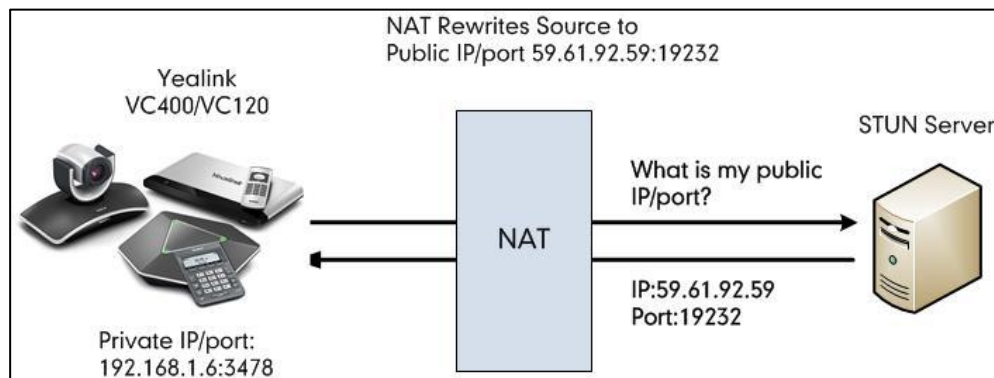
4. Press the **Save** soft key to accept the change.

To configure static NAT for SIP IP call via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **SIP IP Call**.
2. Select **StaticNat** from the pull-down list of **NAT_Traversal**.
3. Press the **Save** soft key to accept the change.

STUN

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 entities behind a NAT to first discover the presence of a NAT and the type of NAT (for more information on the NAT types, refer to [NAT Types](#) on page 86.) 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 work as a STUN client, to send 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. For more information, refer to [RFC3489](#).



Capturing packets after you enable the STUN feature, you can find that the VC400/VC120 sends Binding Request to the STUN server, and then mapped IP address and port is placed in the Binding Response: Binding Success Response
MAPPED-ADDRESS: 59.61.92.59:19232.

No.	Time	Source	Destination	Protocol	Length	Info
444	18.711349	192.168.1.6	218.107.220.74	STUN	98	Binding Request
447	18.711349	218.107.220.74	192.168.1.6	STUN	98	Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232

STUN feature parameters on the system are described below:

Parameter	Description	Configuration Method
Active	Enables or disables the STUN	Remote Control

Parameter	Description	Configuration Method
	(Simple Traversal of UDP over NATs) feature on the system. Default: Disabled	Web User Interface
STUN Server	Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. Default: Blank	Remote Control Web User Interface
STUN Port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. Default: 3478	Remote Control Web User Interface
NAT_Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. <ul style="list-style-type: none">• Disabled• STUN• StaticNat Default: Disabled Note: STUN works only if this parameter is set to STUN.	Remote Control Web User Interface

To configure STUN server via web user interface:

1. Click on **Network->NAT/Firewall**.
2. In the **Stun Config** block, select the desired value from the pull-down list of **Active**.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.

- Enter the port of the STUN server in the **Port** field.

The screenshot shows the Yealink VC400 web interface. The 'Network' tab is selected. In the left sidebar, 'NAT/Firewall' is highlighted. The main content area shows the 'NAT Configuration' section. Under 'Stun Config', the 'Active' checkbox is checked, 'Stun Server' is set to '218.107.220.201', and 'STUN Port' is set to '3478'. The 'Reserve Port' section shows 'UDP Port Scope' and 'TCP Port Scope' both set to '50000 ~ 50499'. The 'Intelligent Firewall Traversal' section shows 'Intelligent Firewall Traversal' set to 'On'.

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

To configure STUN for SIP account via web user interface:

- Click on **Account->SIP Account**.
- Select **STUN** from the pull-down list of **NAT_Traversal**.

The screenshot shows the Yealink VC400 web interface. The 'Account' tab is selected. In the left sidebar, 'SIP Account' is highlighted. The main content area shows the 'SIP Account' configuration page. The 'NAT_Traversal' dropdown menu is highlighted, showing 'STUN' selected.

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

To configure STUN for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select **STUN** from the pull-down list of **NAT_Traversal**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account', 'SIP IP Call' (selected), and 'Codec'. The main content area displays various settings for SIP IP Call, including Transport (TCP), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT_Traversal (STUN, highlighted with a red box), RPort (Enabled), BFCP (Enabled), and FECC(SIP) (Enabled).

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

To configure STUN server via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **NAT/Firewall**.
2. Check the **STUN Active** checkbox.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
4. Enter the port of the STUN server in the **Port** field.
5. Press the **Save** soft key to accept the change.

To configure STUN server for SIP IP call via the remote control:

4. Select **Menu->Advanced** (default password: 0000) -> **SIP IP Call**.
5. Select **STUN** from the pull-down list of **NAT_Traversal**.
6. Press the **Save** soft key to accept the change.

NAT Types

Full Cone:

A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Restricted Cone:

A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

Port Restricted Cone:

A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

Symmetric:

A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

Keep Alive

The system can send keep-alive packets to NAT device for keeping the communication port open.

The keep alive interval parameter on the system is described below:

Parameter	Description	Configuration Method
Keep Alive Interval	Configures the keep-alive interval (in seconds) that the system sends to the NAT device to keep the communication port open. So that NAT can continue to function for SIP account. Default: 30	Web User Interface

To configure the keep-alive interval via web user interface:

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

- Enter the keep alive interval in the **Keep Alive Interval** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account' (selected), 'SIP IP Call', and 'Codec'. The main content area displays various configuration fields for the SIP account. The 'Keep Alive Interval' field is highlighted with a red box and contains the value '30'. Other fields include Register Name (9000), User Name (9000), Password (masked), Server Host (10.2.1.48), Port (5060), Enable Outbound Proxy Server (Disabled), Outbound Proxy Server, Transport (UDP), Server Expires (3600), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT_Traversal (STUN), RPort (Enabled), and BFCP (Disabled).

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

Rport

Rport in [RFC 3581](#), allows a client to request that the server sends the response back to the source port from which the request came. Rport feature depends on support from a SIP server.

The rport parameter on the system is described below:

Parameter	Description	Configuration Method
RPort	Enables or disables NAT Rport feature. You can configure it for the SIP account or SIP IP call separately. Default: Enabled	Web User Interface

To configure rport feature for SIP account via web user interface:

- Click on **Account->SIP Account**.

2. Select the desired value from the pull-down list of **RPort**.

The screenshot shows the Yealink VC400 web interface with the 'Account' tab selected. The left sidebar lists 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The main content area displays various configuration fields for the SIP Account. The 'RPort' field, located near the bottom, is a dropdown menu currently set to 'Enabled' and is highlighted with a red rectangular box. Other fields include Register Name (9000), User Name (9000), Password (masked), Server Host (10.2.1.48), Port (5060), Enable Outbound Proxy Server (Disabled), Outbound Proxy Server, Transport (UDP), Server Expires (3600), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT_Traversal (STUN), Keep Alive Interval (30), and BFCP (Disabled).

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

To configure rport feature for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select the desired value from the pull-down list of **RPort**.

The screenshot shows the Yealink VC400 web interface with the 'SIP IP Call' tab selected under the 'Account' section. The left sidebar lists 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The main content area displays configuration fields for SIP IP Call. The 'RPort' field, located near the bottom, is a dropdown menu currently set to 'Enabled' and is highlighted with a red rectangular box. Other fields include Transport (TCP), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT_Traversal (Disabled), BFCP (Enabled), and FECC(SIP) (Enabled).

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

H.460 Firewall Traversal

H. 323 includes signal based on TCP, while the STUN solution cannot realize the NAT traversal of TCP. Before the emergence of H.460, Enterprises have their own firewall/NAT

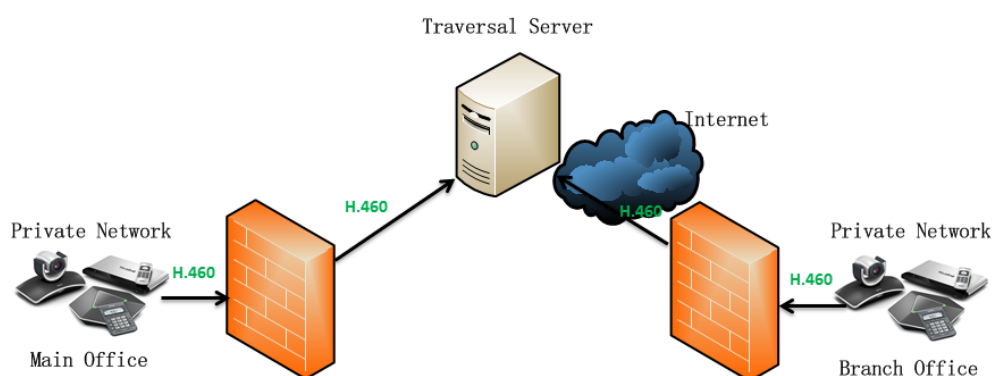
traversal solutions, which are incompatible with each other. Therefore, IP communication between enterprises is difficult. H.460 resolves the compatibility problem.

H.460 enables H.323 signaling and media to traverse firewall. H.460 is a set of extensions to the ITU H.323 standard that include methods to traverse firewalls. Devices that use H.460, implement a set of security policies that a firewall is configurable to accept. Therefore using H.460, video conferencing system can communicate across a firewall. You can configure the system to use standard-based H.460.18 and H.460.19 firewall traversal, which allows the system to establish IP connections across firewalls more easily.

The H.460.18 deals with signaling. The H.460.18 solution perpetually hunts in order to open pinholes from the internal network to the external one. Without using the H.460.18 solution, which permits the gatekeeper to open a connection, the external device could not communicate with internal device, because the firewall would obstruct its attempt to setup a call. H.460.19 extends H.323 by defining the NAT/firewall mechanism for media. In addition, H.460.19 provides a solution for opening RTP and RTCP pinholes and a method for maintaining them using a keep-alive mechanism.

To use H.460, you need to deploy a Traversal Server (TS) at public network.

The following illustration shows how a H.460 traversal server works between two enterprise locations.



The H.460 firewall traversal parameter is described below:

Parameter	Description	Configuration Method
H.460 Active	Enables or disables H.460 firewall traversal feature on the system. Default: Disabled	Remote Control Web User Interface

To configure H.460 firewall traversal via web user interface:

1. Click on **Account->H323**.

2. Select the desired value from the pull-down list of **H.460 Active**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. Below this is a green header with tabs for Home, Status, Account, Network, Setting, Directory, and Security. The 'Account' tab is selected. On the left, a sidebar lists configuration categories: H323, SIP Account, SIP IP Call, and Codec. The main content area displays the H.323 configuration settings. A red rectangle highlights the 'H.460 Active' dropdown menu, which is currently set to 'Disabled'. Other visible settings include Register Status (Registered), H.323 Protocol (Enabled), H.323 Account (Enabled), H.323 Name (9000), H.323 Extension (9000), Gatekeeper Mode (Manual), Gatekeeper IP Address 1 (10.2.1.43), Gatekeeper IP Address 2 (empty), Gatekeeper Authentication (Disabled), Gatekeeper Username (empty), Gatekeeper Password (masked with dots), H.323 Tunneling (Disabled), H.235 Encryption (Disabled), and Protocol Monitor Port (1720).

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

To configure H.460 firewall traversal via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **H.323**.
2. Check the **H.460 Active** checkbox.
3. Press the **Save** soft key to accept the change.

Intelligent Firewall Traversal

The video conferencing system can provide efficiency and continuous communication for both the head office and a branch office.

In some cases, the head office is in the WAN and lacks a VPN network, while the branch office is in the LAN, and no port mapping is configured on its firewall. You can enable the intelligent firewall traversal feature, so that the head office can share content with branch office, or control the camera of branch office.

The intelligent firewall traversal parameter is described below:

Parameter	Description	Configuration Method
Intelligent Firewall Traversal	Enables or disables the intelligent firewall traversal feature on the system. Default: Disabled	Web User Interface

To configure intelligent firewall traversal via web user interface:

1. Click on **Network->NAT/Firewall**.
2. Select the desired value from the pull-down list of **Intelligent Firewall Traversal**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network, Setting, Directory, and Security. The left sidebar shows a tree view with LAN Configuration, NAT/Firewall (selected), Advanced, and Diagnose. The main content area is titled 'NAT Configuration' and contains several sections: NAT Configuration (Static NAT: Disabled, NAT Public IP Address: empty, Route Traversal: Auto), Stun Config (Active: Disabled, Stun Server: empty, STUN Port: 3478), Reserve Port (UDP Port Scope: 50000 ~ 50499, TCP Port Scope: 50000 ~ 50499), and Intelligent Firewall Traversal (Intelligent Firewall Traversal: On). The 'Intelligent Firewall Traversal' dropdown menu is highlighted with a red box.

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

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network. This allows the transport of traffic with special requirements. QoS guarantees are important for applications that require a 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 a 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 delivery, 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 is 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, with regard to guaranteeing how that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice, video and data packets are given priority over other kinds of network traffic. Yealink video conferencing systems support the DiffServ model of QoS. DSCPs for voice, video and data packets that can be specified respectively.

Voice QoS

To make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

Video QoS

To ensure acceptable visual quality for video, video packets emanated from the system should be configured with a high transmission priority.

Data QoS

To ensure good call quality, data packets (e.g., SIP signaling and H.225 call signaling) emanated from the system should be configured with a high transmission priority.

QoS feature parameters on the system are described below.

Parameter	Description	Configuration Method
Audio Priority	<p>Specifies the DSCP value for voice packets.</p> <p>Valid Values: 0-63</p> <p>Default: 63</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Video Priority	<p>Specifies the DSCP value for video packets.</p> <p>Valid Values: 0-63</p> <p>Default: 34</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Data Priority	<p>Specifies the DSCP value for data packets.</p> <p>Valid Values: 0-63</p> <p>Default: 63</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure QoS via web user interface:

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

2. In the **QoS** block, enter the desired values in the corresponding fields.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area displays various network settings:

- LLDP**: Active (Disabled), Packet Interval(1-3600s) (60).
- VLAN**: Internet Port (Disabled), VID(1-4094) (1), Priority (0).
- DHCP VLAN**: Active (Enabled), Option (132).
- QoS** (highlighted with a red box): Audio Priority (63), Video Priority (34), Data Priority (63).
- MTU**: Video MTU (1500).

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

To configure QoS via the remote control:

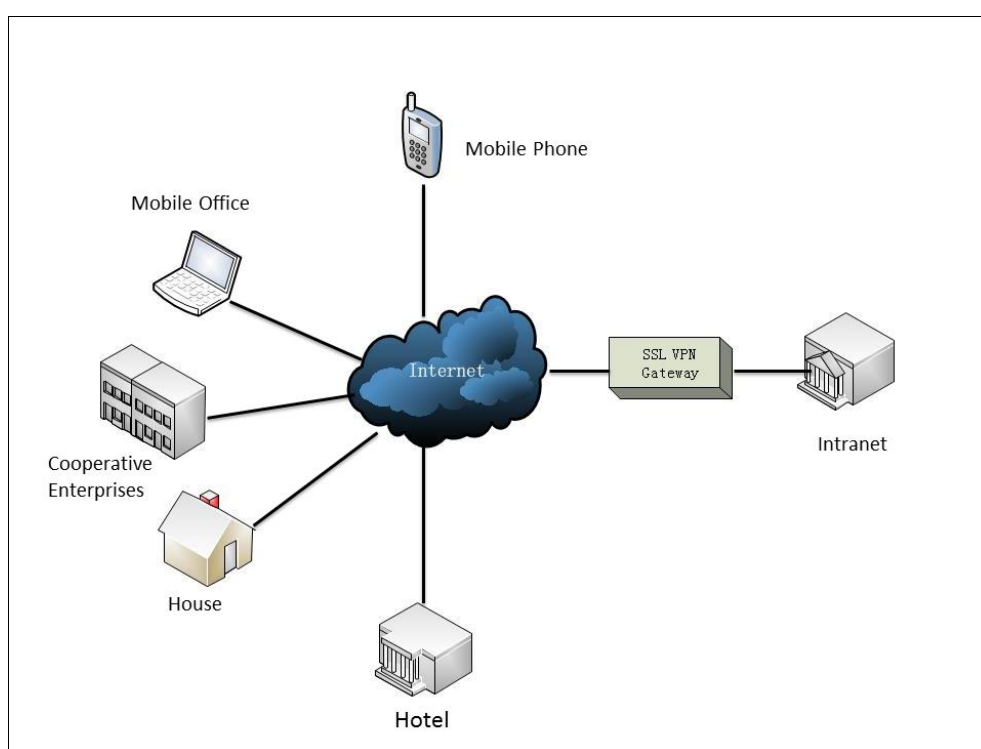
1. Select **Menu->Advanced** (default password: 0000) -> **Advanced Network**.
2. In the **Diffserv QoS** block, enter the desired values in the corresponding fields.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructures, 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 also be classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

The system supports 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 and is designed 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. The system uses OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel system must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the system, the system 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 system 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, refer to [OpenVPN Feature on Yealink IP Phones](#).

VPN feature parameters on the system are described below.

Parameter	Description	Configuration Method
VPN->Active	Enables or disables VPN feature on the system.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: Disabled Note: You need to upload the compressed package of VPN-related files to the system first before enabling the VPN feature. If you change this parameter, the system will reboot to make the change take effect.	
Upload VPN Config	Uploads the compressed package of VPN-related files (*.tar) to the system.	Web User Interface

To configure VPN via web user interface:

1. Click on **Network->Advanced**.
2. In the **VPN** block, click **Browse** to locate the VPN file (*.tar) from your local system.
3. Click **Upload** to upload the file to the system.
4. Select the desired value from the pull-down list of **Active**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, a sidebar shows 'LAN Configuration' with sub-items: 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is divided into sections: 'SNMP' (Active: Disabled, Port: 161, Trusted Address: empty), 'Web Server' (HTTP: Enabled, HTTP Port: 80, HTTPS: Enabled, HTTPS Port: 443), and '802.1x' (802.1x Mode: Disabled, Identity: empty, MD5 Password: empty, CA Certificates: empty, Device Certificates: empty). At the bottom, the 'VPN' section is highlighted with a red box. It contains 'Active' (Enabled) and 'Upload VPN Config' (C:\fakepath\openvpn.tar) with 'Browse...' and 'Upload' buttons.

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

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

6. Click **Confirm** to reboot the system immediately.

To configure VPN via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**Advanced Network**.
2. Check the **VPN** checkbox.
3. Press the **Save** soft key to accept the change.

The display device prompts "Reboot now?".

4. Select **OK** to reboot the system immediately.

Configuring Call Preferences

This chapter provides information on how to configure system's call preferences (e.g., call protocol and network bandwidth).

This chapter provides the following sections:

- [Configuring SIP Settings](#)
- [Configuring H.323 Settings](#)
- [DTMF](#)
- [Codecs](#)
- [Call Protocol](#)
- [Do Not Disturb](#)
- [Auto Answer](#)
- [Call Match](#)
- [History Record](#)
- [Bandwidth](#)
- [Ringback Timeout](#)
- [Auto Refuse Timeout](#)
- [URI Call Mode](#)

Configuring SIP Settings

Yealink VC400/VC120 video conferencing system support Session Initiation Protocol (SIP).

If your server supports SIP, you can use SIP to establish calls.

SIP Account

To establish calls using SIP, you can configure a SIP account for the system.

SIP account parameters on the system are described below:

Parameter	Description	Configuration Method
SIP Protocol	Enables or disables the SIP protocol. Default: Enabled. Note: Only when it is set to Enabled, can SIP account be	Remote Control Web User Interface

Parameter	Description	Configuration Method
	registered.	
SIP Account	Enables or disables the SIP account. Default: Enabled	Remote Control Web User Interface
Register Name	Configures the user name of the SIP account for register authentication. Default: Blank	Remote Control Web User Interface
User Name	Specifies the user name to use for authentication when registering with a SIP server. Default: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the user name used to authenticate the system to the SIP server. Default: Blank	Remote Control Web User Interface
Server Host	Configures the IP address or domain name of the SIP server for the SIP account. Default: Blank	Remote Control Web User Interface
Enable Outbound Proxy Server	Enables or disables the system to send requests of the SIP account to the outbound proxy server. Default: Disabled	Remote Control Web User Interface
Outbound Proxy Server	Configures the IP address or domain name of the outbound proxy server for the SIP account. Valid values: Integer from 1 to 65535. Default: it is configurable only when the Outbound Proxy Server is enabled.	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP account. <ul style="list-style-type: none"> UDP—provides best-effort transport via UDP for SIP 	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<p>signaling.</p> <ul style="list-style-type: none"> • TCP—provides reliable transport via TCP for SIP signaling. • TLS—provides secure communication of SIP signaling. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. <p>Default: UDP</p> <p>Note: TLS is available only when the system is registered with a SIP server that supports TLS.</p>	
Server Expires	<p>Configures the registration expiration time (in seconds) of the SIP server for SIP account.</p> <p>Default: 3600s</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure SIP account via web user interface:

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

2. Configure the SIP account settings.

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

After successful registration, the display device displays **SIP**, and the LCD screen of the VCP40 phone displays **SIP**.

To configure SIP account via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **SIP Account**.
2. Configure the SIP account settings.
3. Press the **Save** soft key to accept the change.

After successful registration, the display device displays **SIP**, and the LCD screen of the VCP40 phone displays **SIP**.

SIP IP Call

When making an IP call using the SIP protocol, the system doesn't support the TLS transport protocol. So configuration parameters of SIP IP call are divided from the SIP account. You can configure SIP IP call separately.

SIP IP call parameters on the system are described below:

Parameter	Description	Configuration Method
SIP Protocol	Enables or disables the SIP protocol. Default: Enabled.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Note: When it is set to Enabled on both sites, the VC400/VC120 can call the far site by dialing an IP address directly.	
Transport	Configures the type of transport protocol for the SIP IP call. <ul style="list-style-type: none"> UDP—provides best-effort transport via UDP for SIP signaling. TCP—provides reliable transport via TCP for SIP signaling. DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: TCP	Remote Control Web User Interface

To configure SIP IP call via web user interface:

1. Click on **Account->SIP Account**.
2. Select **Enabled** from the pull-down list of **SIP Protocol**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account' (selected), 'SIP IP Call', and 'Codec'. The main content area displays the 'SIP Account' configuration. The 'Register Status' is 'Registered'. The 'SIP Protocol' dropdown is highlighted with a red box and set to 'Enabled'. Other fields include 'SIP Account' (Enabled), 'Register Name' (9000), 'User Name' (9000), 'Password' (masked), 'Server Host' (10.2.1.48), 'Port' (5060), 'Enable Outbound Proxy Server' (Disabled), 'Outbound Proxy Server' (empty), 'Port' (5060), 'Transport' (UDP), 'Server Expires' (3600), 'SRTP' (Disabled), 'DTMF Type' (SIP INFO), 'DTMF Info Type' (DTMF), and 'DTMF Payload Type (96~127)' (101).

3. Click **SIP IP Call**.

4. Select the desired value from the pull-down list of **Transport**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. Below it, a green bar contains 'Yealink VC400' and tabs for 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is active. On the left, a sidebar lists 'H323', 'SIP Account', 'SIP IP Call' (selected), and 'Codec'. The main content area displays various SIP settings. The 'Transport' dropdown is highlighted with a red rectangle and shows 'TCP'. Other settings include SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT Traversal (Disabled), RPort (Enabled), BFCP (Enabled), and FECC(SIP) (Enabled).

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

To configure SIP IP call via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **SIP Account**.
2. Mark the **On** radio box in the **SIP Protocol** field.
3. Press the **Save** soft key to accept the change.
4. Press the **Back** soft key to return to the Advanced menu.
5. Select **SIP IP Call**, and then press **OK**.
6. Select the desired value from the pull-down list of **Transport**.
7. Press the **Save** soft key to accept the change.

Configuring H.323 Settings

Yealink VC400/VC120 video conferencing systems support H.323 protocol. If your network uses a gatekeeper, you can register an H.323 account for the system, and specify its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

SIP settings parameters on the system are described below:

Parameter	Description	Configuration Method
H.323 Protocol	<p>Enables or disables the H.323 protocol.</p> <p>Default: Enabled.</p> <p>Note: Only when it is set to Enabled, can H.323 account be registered. When it is set to Enabled on both sites, the VC400/VC120 can call the far</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	site by dialing an IP address directly.	
H.323 Account	<p>Enables or disables the H.323 account.</p> <p>Default: Enabled</p> <p>If it is set to disabled, the system cannot place or receive calls with the H.323 protocol.</p>	<p>Remote Control</p> <p>Web User Interface</p>
H.323 Name	<p>Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both system are registered to a gatekeeper.</p> <p>Default: blank</p>	<p>Remote Control</p> <p>Web User Interface</p>
H.323 Extension	<p>Specifies the extension that gatekeepers and gateways use to identify this system.</p> <p>Default: blank</p> <p>Note: Users can place point-to-point calls using the extension if both systems are registered with a gatekeeper.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Gatekeeper ID	<p>Configures the gatekeeper ID.</p> <p>Note: This is set only when required by the gatekeeper. For example, for configurations with multiple gatekeepers. The gatekeeper ID must match the one configured on the gatekeeper. Do not configure this parameter if the gatekeeper does not require it, as this may result in failure to register with the gatekeeper.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Gatekeeper Mode	<p>Configures the gatekeeper mode.</p> <ul style="list-style-type: none"> • Disabled—the system does not use a 	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>gatekeeper.</p> <ul style="list-style-type: none"> Auto—the system automatically discovers a gatekeeper. Manual—specify the IP address and port for the gatekeeper manually. <p>Default: Disabled</p>	
Gatekeeper IP Address 1	Configures the IP address of the primary gatekeeper.	Remote Control Web User Interface
Gatekeeper IP Address 2	Configures the IP address of the secondary gatekeeper.	Remote Control Web User Interface
Gatekeeper Authentication	<p>Enables or disables support for gatekeeper authentication.</p> <p>Default: Disabled</p> <p>Note: When Gatekeeper Authentication is enabled, the gatekeeper ensures that only trusted H.323 systems are allowed to access the gatekeeper.</p>	Remote Control Web User Interface
Gatekeeper Username	<p>Specifies the user name for authentication with gatekeeper.</p> <p>Default: blank</p>	Remote Control Web User Interface
Gatekeeper Password	<p>Specifies the password for authentication with gatekeeper.</p> <p>Default: blank</p>	Remote Control Web User Interface
H.460 Active	<p>Enables or disables H.460 firewall traversal feature on the system.</p> <p>Default: Disabled</p> <p>For more information, refer to H.460 Firewall Traversal on page 89.</p>	Remote Control Web User Interface
H.323 Tunneling	Enables or disables the H.323	Remote Control

Parameter	Description	Configuration Method
	tunneling on the system. Default: Disabled For more information, refer to H.323 Tunneling on page 71.	Web User Interface
H.235 Encryption	Specifies the H.235 type for the H.323 account. <ul style="list-style-type: none">• Disabled—do not use H.235 in H.235 calls.• Optional—negotiate with the far site whether to use H.235 for media encryption in H.323 calls.• Compulsory—compulsory use H.235 for media encryption in H.323 calls. Default: Disabled For more information, refer to H.235 on page 203.	Web User Interface
Protocol Monitor Port	Specifies the port for the H.323 protocol. Default 1720. Note: It is only applicable to IP call.	Web User Interface

To configure H.323 account via web user interface:

1. Click on **Account->H323**.

2. Configure the H.323 account settings.

Setting	Value
Register Status	Registered
H323 Protocol	Enabled
H.323 Account	Enabled
H.323 Name	9000
H.323 Extension	9000
Gatekeeper Mode	Manual
Gatekeeper IP Address 1	10.2.1.43
Gatekeeper IP Address 2	
Gatekeeper Authentication	Disabled
Gatekeeper Username	
Gatekeeper Password	*****
H.460 Active	Disabled
H.323 Tunneling	Disabled
H235 Encryption	Disabled
Protocol Monitor Port	1720

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

After successful registration, the display device displays **H323** , and the LCD screen of the VCP40 phone displays **H323** .

To configure H.323 account via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**H323**.
2. Configure the H.323 account settings.
3. Press the **Save** soft key to accept the change.

After successful registration, the display device displays **H323** , and the LCD screen of the VCP40 phone displays **H323** .

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 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

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits:

- **RFC2833** -- DTMF digits are transmitted by RTP Events compliant to RFC2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages.

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 for. The payload type for 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 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.

DTMF parameters for SIP protocol on the system are described below:

Parameter	Description	Configuration Method
DTMF Type	<p>Configures the DTMF type. You can configure it for the SIP account or SIP IP call separately.</p> <ul style="list-style-type: none"> INBAND—DTMF digits are transmitted in the voice band. RFC2833—DTMF digits are transmitted by RTP Events compliant to RFC2833. SIP INFO—DTMF digits are transmitted by the SIP INFO messages. RFC2833+ SIP INFO—DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages. <p>Default: INBAND</p>	<p>Remote Control</p> <p>Web User Interface</p>
DTMF Info Type	<p>Configures the DTMF info type when DTMF type is set to SIP INFO or RFC2833+SIP INFO. You can configure it for the SIP account or SIP IP call separately.</p> <ul style="list-style-type: none"> DTMF-Relay DTMF Telephone-Event <p>Default: DTMF</p>	<p>Remote Control</p> <p>Web User Interface</p>
DTMF Payload Type (96~127)	<p>Configures the value of DTMF payload. You can configure it for the SIP account or SIP IP call separately.</p> <p>Default: 101</p>	<p>Web User Interface</p>

To configure DTMF type for SIP account via web user interface:

1. Click on **Account->SIP Account**.
2. Select the desired value from the pull-down list of **DTMF Type**.

If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

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

The screenshot shows the Yealink VC400 web interface with the 'Account' tab selected. The left sidebar has 'SIP Account' highlighted. The main content area shows various configuration fields. A red box highlights the following fields:

DTMF Type	SIP INFO
DTMF Info Type	DTMF
DTMF Payload Type (96~127)	101

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

To configure DTMF type for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select the desired value from the pull-down list of **DTMF Type**.

If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

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

The screenshot shows the Yealink VC400 web interface with the 'Account' tab selected. The left sidebar has 'SIP IP Call' highlighted. The main content area shows various configuration fields. A red box highlights the following fields:

DTMF Type	SIP INFO
DTMF Info Type	DTMF
DTMF Payload Type (96~127)	101

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

DTMF parameters for H.323 protocol on the system are described below:

Parameter	Description	Configuration Method
DTMF Type	<p>Configures the DTMF type for H.323 protocol.</p> <ul style="list-style-type: none"> INBAND—DTMF digits are transmitted in the voice band. Auto—the system automatically negotiates the way (Inband, RFC2833 or SIP INFO) to transfer DTMF digits. <p>Default: INBAND</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure DTMF type for H.323 via web user interface:

- Click on **Account->H.323**.
- Select the desired value from the pull-down list of **DTMF Type**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar shows 'H323' selected, with sub-items 'SIP Account', 'SIP IP Call', and 'Codec'. The main content area displays the 'H.323 Account' configuration page. The 'DTMF Type' dropdown menu is highlighted with a red box and is set to 'INBAND'. Other visible settings include 'H.323 Name' (9000), 'H.323 Extension' (9000), 'Gatekeeper Mode' (Manual), 'Gatekeeper IP Address 1' (10.2.1.43), 'Gatekeeper IP Address 2' (empty), 'Gatekeeper Authentication' (Disabled), 'Gatekeeper Username' (empty), 'Gatekeeper Password' (masked), 'H.460 Active' (Disabled), 'H.323 Tunneling' (Disabled), 'H.235 Encryption' (Disabled), 'Protocol Monitor Port' (1720), 'H.239' (Enabled), and 'FECC(H.323)' (Enabled).

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

Codecs

CODEC is an abbreviation of COmpress-DECompress, and is 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/video signal with a minimum number of bits while retaining quality. This can effectively reduce the frame size and the bandwidth required for audio/video transmission.

Audio Codecs

The audio codec that the system uses to establish a call should be supported by the server. When placing a call, the system will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.



The following table summarizes the supported audio codecs on the system:



Codec	Algorithm	Bit Rate	Sample Rate	Reference
G.722.1c	G.722.1	48 Kbps	32 Ksps	RFC 5577
G.722.1c		32 Kbps	32 Ksps	RFC 5577
G.722.1c		24 Kbps	32 Ksps	RFC 5577
G.722.1	G.722.1	24 Kbps	16 or 32 Ksps	RFC 5577
G722	G.722	64 Kbps	16 Ksps	RFC 3551
PCMU	G.711	64 Kbps	8 Ksps	RFC 3551
PCMA	G.711	64 Kbps	8 Ksps	RFC 3551

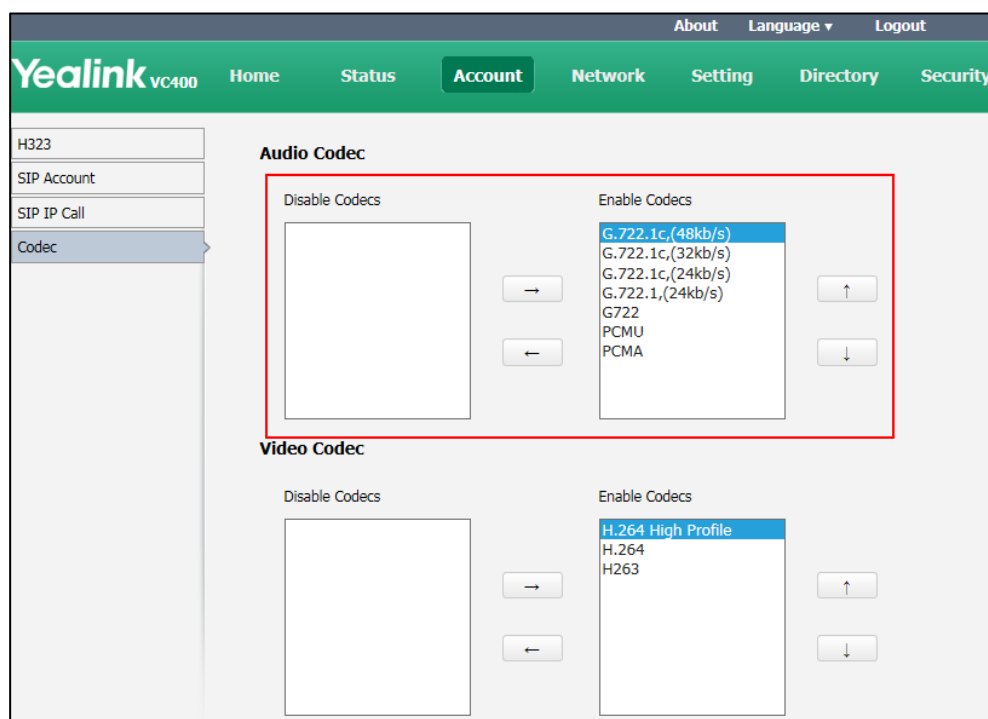
Audio codecs parameters on the system are described below:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the enabled audio codecs for the system to use. Note: All support audio codecs are enabled on the system by default.	Web User Interface
Disable Codecs	Specifies the disabled audio codecs for the system not to use.	Web User Interface

To configure audio codecs via web user interface:

1. Click on **Account->Codec**.
2. Select the desired codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click  or  to disable or enable the selected codec.

4. Select the desired audio codec from the Enable Codecs column, and click  or  to adjust the priority of the selected audio codecs.



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

Video Codecs

The video codec that the system uses to establish a call should be supported by the server. When placing a call, the system will offer the enabled video codec list to the server and then use the video codec negotiated with the called party according to the priority.





The following table summarizes the supported video codecs on the system:

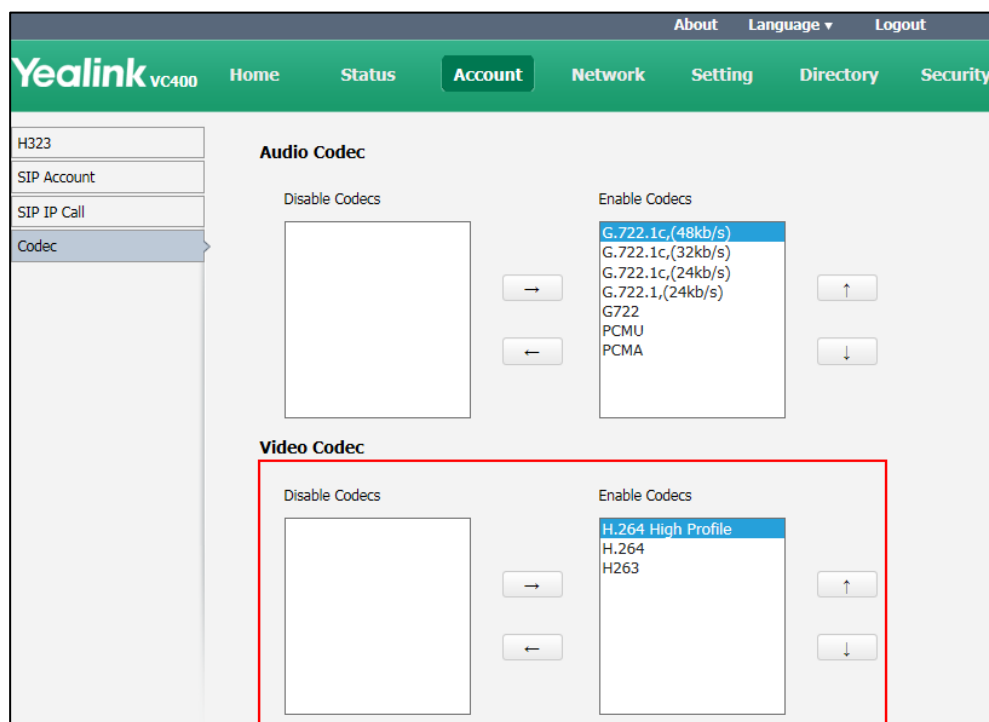
Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.264 High Profile	H264/90000	90 kbps to 2048 kbps	5 fps to 30 fps	Tx: WQVGA,360P, 448P, 540P, 720P, 1080P
H.264	H264/90000			Rx: Conventional Size Below 1080P
H.263	H263/90000			Tx: CIF, 4CIF RX: QCIF, CIF, 4CIF

Video codecs parameters on the system are described below:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the enabled video codecs for the system to use. Note: All support video codecs are enabled on the system by default.	Web User Interface
Disable Codecs	Specifies the disabled video codecs for the system not to use.	Web User Interface

To configure video codecs via web user interface:

1. Click on **Account->Codec**.
2. Select the desired video codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click  or  to disable or enable the selected video codec.
4. Select the desired video codec from the Enable Codecs column, and click  or  to adjust the priority of the selected video codecs.



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

Call Protocol

The system supports SIP and H.323 protocols for incoming and outgoing calls. H.323 is commonly used to communicate to other video conferencing system. SIP is commonly used to communicate with other VoIP devices. The default call protocol on the system is Auto. The system preferentially uses the H.323 protocol to place calls. If there is no available H.323 account on the system, the system will switch to the SIP protocol for placing calls. You can specify the desired protocol for the system to place calls. Ensure the remote system supports the same protocol.

The call protocol parameter on the system is described below:

Parameter	Description	Configuration Method
Call Protocol	<p>Specifies the desired call protocol for placing calls.</p> <ul style="list-style-type: none">• Auto—the system automatically uses the available call protocol.• SIP—the system uses the SIP protocol for placing calls.• H.323—the system uses H.323 protocol for placing calls. <p>Default: Auto</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure call protocol via web user interface:

1. Click on **Setting->Call Features**.

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

The screenshot shows the Yealink VC400 web interface. The 'Setting' tab is active. On the left sidebar, 'Call Features' is selected. The main content area displays various settings with their current values in dropdown menus:

- DND: Disabled
- Auto Answer: Enabled
- Auto Answer Mute: Enabled
- Auto Answer Multiway: Disabled
- Call Match: Enabled
- History Record: Enabled
- Call Protocol: Auto** (highlighted with a red box)
- Uplink Bandwidth: Auto
- Downlink Bandwidth: Auto
- Abnormal call answering: IP Call Answer
- Safe mode call: Disabled
- Ringback Timeout(30-240): 200
- Auto Refuse Timeout(30-240): 120
- URI Call Mode: SIP IP Call

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

To configure call protocol via the remote control:

1. Select **Menu->Call Features ->Call Protocol**.
2. Select the desired value from the pull-down list of **Call Protocol**.
3. Press the **Save** soft key to accept the change.

Do Not Disturb

Do not Disturb allows the system to reject all incoming calls automatically. You can activate the DND mode for the system when it is idle, and the DND mode will be deactivated after the system places a call. You can also activate the DND mode for the system during a call, and the DND mode will be deactivated after the system ends the call.

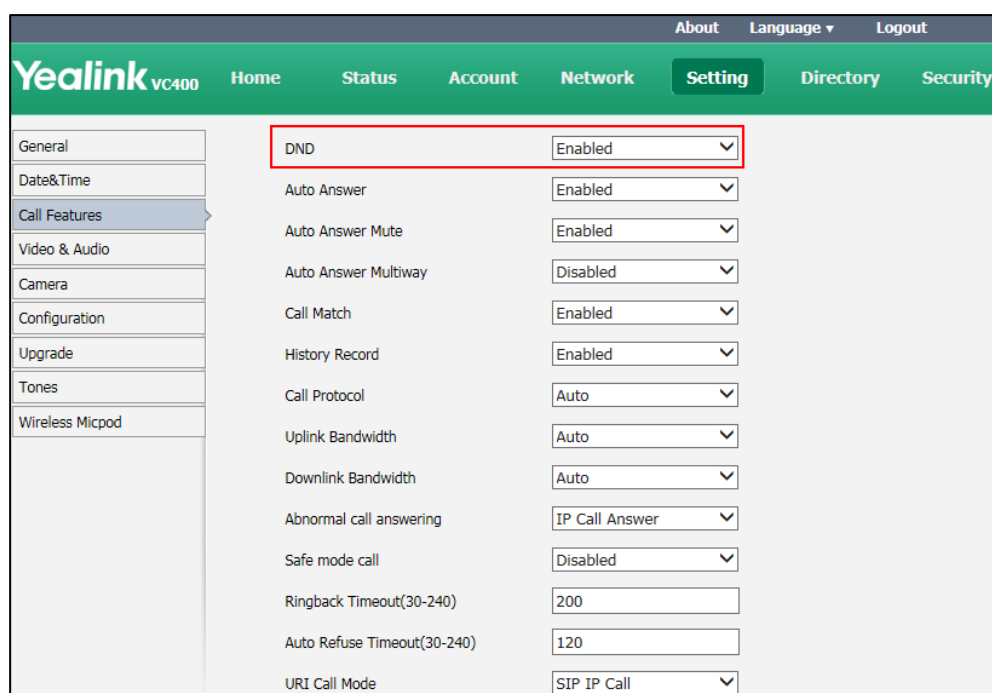
The DND parameter on the system is described below:

Parameter	Description	Configuration Method
DND	Enables or disables DND mode on the system. Default: Disabled	Remote Control Web User Interface


To configure DND via web user interface:

1. Click on **Setting->Call Features**.

2. Select the desired value from the pull-down list of **DND**.




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

If **Enabled** is selected, the display device will display , and the LCD screen of the VCP40 phone will display **DND**.


To configure DND via the remote control:

1. Select **Menu->Call Features**.
2. Check the **DND** checkbox.
3. Press the **Save** soft key to accept the change.

The display device will display , and the LCD screen of the VCP40 phone will display **DND**.


To configure DND during a call via web user interface:

1. Click **Home**.
2. Check the **DND** checkbox.

The display device will display , and the LCD screen of the VCP40 phone will display **DND**.

To configure DND during a call via the remote control:

1. Press the **More** soft key.
2. Check the **DND** checkbox.
3. Press the **Back** soft key to exit the **More** window.

The display device will display , and the LCD screen of the VCP40 phone will display **DND**.

Auto Answer

The auto answer feature allows the system to answer incoming calls automatically. The auto answer mute feature allows the system to turn off the microphone when an incoming call is answered automatically. The auto answer mute feature is available only when the auto answer feature is enabled. The auto answer multiway feature allows the system to answer new incoming calls automatically during an active call.

Auto answer parameters on the system are described below:

Parameter	Description	Configuration Method
Auto Answer	Enables or disables the auto answer feature on the system. Default: Enabled	Remote Control Web User Interface
Auto Answer Mute	Enables or disables the auto answer mute feature on the system. Default: Enabled Auto answer mute feature is configurable only when the auto answer is enabled.	Remote Control Web User Interface
Auto Answer Multiway	Enables or disables the auto answer multiday feature on the system. Default: Disabled The auto answer multiway feature is available only when the auto answer is enabled.	Remote Control Web User Interface

To configure auto answer via web user interface:

1. Click on **Setting->Call Features**.
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**.

- Select the desired value from the pull-down list of **Auto Answer Multiway**.

The screenshot shows the Yealink VC400 web interface. The 'Setting' tab is selected. On the left sidebar, 'Call Features' is highlighted. The main content area shows various settings. A red box highlights the 'Auto Answer', 'Auto Answer Mute', and 'Auto Answer Multiway' settings. 'Auto Answer' is set to 'Enabled', 'Auto Answer Mute' is set to 'Enabled', and 'Auto Answer Multiway' is set to 'Disabled'.

Setting	Value
DND	Disabled
Auto Answer	Enabled
Auto Answer Mute	Enabled
Auto Answer Multiway	Disabled
Call Match	Enabled
History Record	Enabled
Call Protocol	Auto
Uplink Bandwidth	Auto
Downlink Bandwidth	Auto
Abnormal call answering	IP Call Answer
Safe mode call	Disabled
Ringback Timeout(30-240)	200
Auto Refuse Timeout(30-240)	120
URI Call Mode	SIP IP Call

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

If **Enabled** is selected, the display device will display **AA**, and the LCD screen of the VCP40 phone will display **AA**.

To configure auto answer via the remote control:

- Select **Menu->Call Features**.
- Check the **Auto Answer** checkbox.
- Check the **Auto Answer Mute** checkbox.
- Check the **Auto Answer Multiway** checkbox.
- Press the **Save** soft key to accept the change.

The display device will display **AA**, and the LCD screen of the VCP40 phone will display **AA**.

Call Match

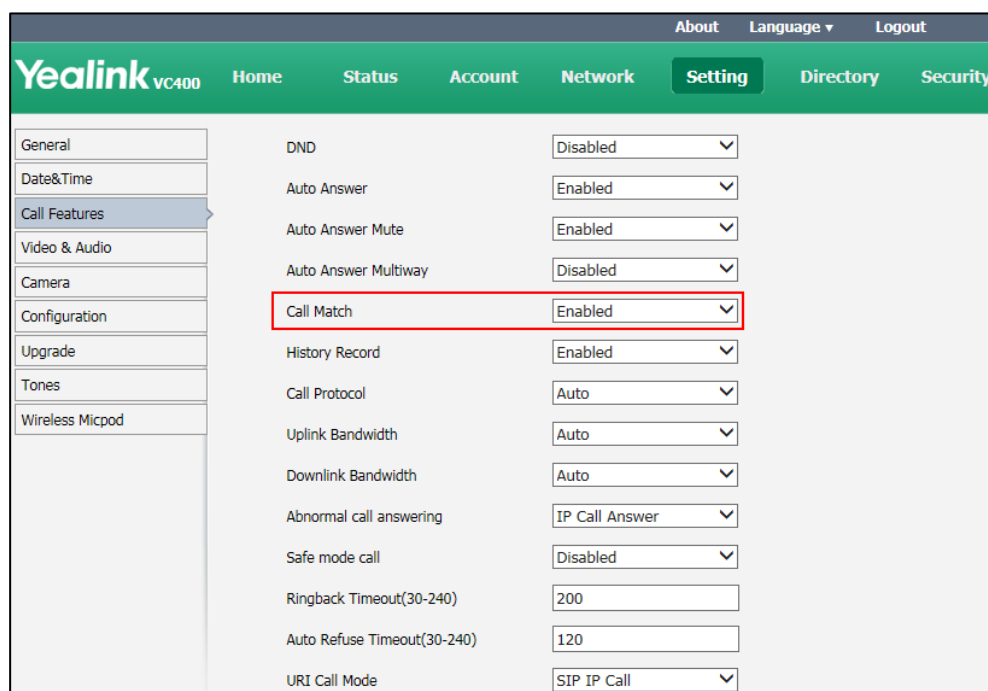
The call match feature allows the system to search entries automatically from the search source list based on the entered string. Once matched, the results will be displayed on the screen. If no list is added to the search source list, the system will not perform a search even if call match is enabled. For more information on how to search source list in dialing, refer to [Search Source List in Dialing](#) on page 178.

Parameter of call match on the system is described below:

Parameter	Description	Configuration Method
Call Match	Enables or disables the call match feature on the system. Default: Enabled	Remote Control Web User Interface

To configure call match via web user interface:

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



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

To configure call match via the remote control:

1. Select **Menu->Call Features**.
2. Check the **Call Match** checkbox.
3. Press the **Save** soft key to accept the change.

History Record

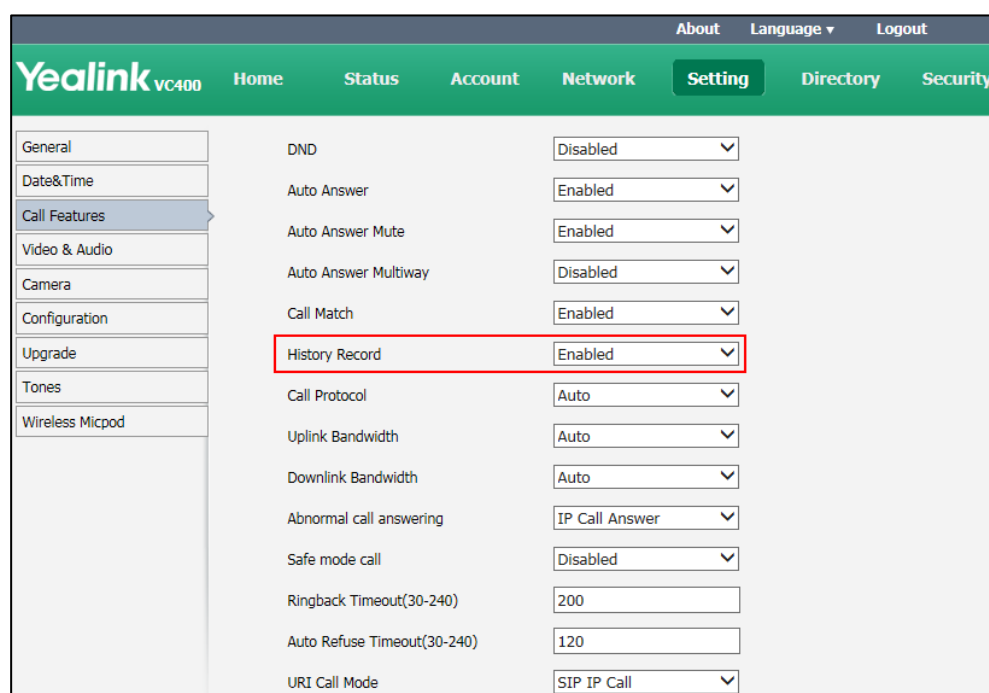
The system maintains a local call history, which contains call information such as remote party identification, time and date, and call duration (call duration is only listed on the web user interface). Users can manage call history list via the remote control, web user interface and VCP40 phone. To save call history, you must enable the history record feature on the system in advance. If history record feature is disabled, the system will not save call log and prompt the missed call.

The history record parameter on the system is described below:

Parameter	Description	Configuration Method
History Record	Enables or disables the history record feature on the system. Default: Enabled	Remote Control Web User Interface

To configure history record via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **History Record**.



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

To configure history record via the remote control:

1. Select **Menu->Call Features**.
2. Check the **History Record** checkbox.
3. Press the **Save** soft key to accept the change.

Bandwidth

The system automatically detects the available bandwidth for call connection by default. The VC400/VC120 supports connecting to other devices with different bandwidth. If a device with lower bandwidth joins a call, the video quality will stay the same or will not reduce a lot. You can specify the uplink and downlink bandwidths for the system to achieve the best result. Uplink bandwidth is the max bandwidth of outgoing calls, and downlink bandwidth is the max bandwidth of incoming calls. The

configurable bandwidths on the system are: 256 kb/s, 384 kb/s, 512 kb/s, 640 kb/s, 768 kb/s, 1024 kb/s, 1280 kb/s, 1500 kb/s, 2000 kb/s, 3000 kb/s, 4000 kb/s, 5000 kb/s, 6000 kb/s. The specified value of the uplink bandwidth becomes the maximum value that users can select from the pull-down list of Bandwidth in the dial screen.

Note

The actual resolution depends on the performance of the far site, and is affected by the quality of the communication channel.

Bandwidth settings parameters on the system are described below:

Parameter	Description	Configuration Method
Uplink Bandwidth	Specifies the maximum transmitting bandwidth for the system. Default: Auto If Auto is selected, the system will select the appropriate uplink bandwidth automatically.	Remote Control Web User Interface
Downlink Bandwidth	Specifies the maximum receiving bandwidth for the system. Default: Auto If Auto is selected, the system will select the appropriate downlink bandwidth automatically.	Remote Control Web User Interface

To configure bandwidth settings via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **Uplink Bandwidth**.

3. Select the desired value from the pull-down list of **Downlink Bandwidth**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features (highlighted), Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area shows the 'Call Features' settings. A red box highlights the 'Uplink Bandwidth' and 'Downlink Bandwidth' settings, both of which are set to 'Auto'. Other settings visible include DND (Disabled), Auto Answer (Enabled), Auto Answer Mute (Enabled), Auto Answer Multiway (Disabled), Call Match (Enabled), History Record (Enabled), Call Protocol (Auto), Abnormal call answering (IP Call Answer), Safe mode call (Disabled), Ringback Timeout(30-240) (200), Auto Refuse Timeout(30-240) (120), and URI Call Mode (SIP IP Call).

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

To configure bandwidth settings via the remote control:

1. Select **Menu->Call Features->Bandwidth Settings**.
2. Select the desired value from the pull-down list of **Uplink Bandwidth**.
3. Select the desired value from the pull-down list of **Downlink Bandwidth**.
4. Press the **Save** soft key to accept the change.

Ringback Timeout

Ringback timeout defines a specific period of time within which the video conferencing system will cancel the dialing if the call is not answered.

The ringback timeout parameter on the system is described below:

Parameter	Description	Configuration Method
Ringback Timeout (30-240)	<p>Configures the duration time (in seconds) in the ringback state.</p> <p>Default: 200</p> <p>If it is set to 200, the system will cancel the dialing if the call is not answered within 200s.</p>	Web User Interface

To configure ringback timeout via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **Ringback Timeout(30-240)**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists configuration categories: General, Date&Time, Call Features (highlighted), Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area displays various settings with their current values in dropdown menus:

- DND: Disabled
- Auto Answer: Enabled
- Auto Answer Mute: Enabled
- Auto Answer Multiway: Disabled
- Call Match: Enabled
- History Record: Enabled
- Call Protocol: Auto
- Uplink Bandwidth: Auto
- Downlink Bandwidth: Auto
- Abnormal call answering: IP Call Answer
- Safe mode call: Disabled
- Ringback Timeout(30-240): 200** (highlighted with a red box)
- Auto Refuse Timeout(30-240): 120
- URI Call Mode: SIP IP Call

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

Auto Refuse Timeout

Auto refuse timeout defines a specific period of time within which the video conferencing system will stop ringing if the call is not answered.

The auto refuse timeout parameters on the system are described below:

Parameter	Description	Configuration Method
Auto Refuse Timeout (30-240)	<p>Configures the duration time (in seconds) in the ringing state.</p> <p>Default: 120</p> <p>If it is set to 120, the system will stop ringing if the call is not answered within 120s.</p>	Web User Interface

To configure auto refuse timeout via web user interface:

1. Click on **Setting->Call Features**.

2. Select the desired value from the pull-down list of **Auto Refuse Timeout (30-240)**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features (highlighted), Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area displays a list of settings under the 'Call Features' section. The 'Auto Refuse Timeout(30-240)' setting is highlighted with a red box, showing a value of 120. Other settings include DND (Disabled), Auto Answer (Enabled), Auto Answer Mute (Enabled), Auto Answer Multiway (Disabled), Call Match (Enabled), History Record (Enabled), Call Protocol (Auto), Uplink Bandwidth (Auto), Downlink Bandwidth (Auto), Abnormal call answering (IP Call Answer), Safe mode call (Disabled), Ringback Timeout(30-240) (200), and URI Call Mode (SIP IP Call).

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

URI Call Mode

If the far site registers an URI address, near site can use SIP IP call or SIP account to connect to the far site.

The URI call mode parameters on the system are described below:

Parameter	Description	Configuration Method
URI Call Mode	<p>Configures the URI call mode.</p> <ul style="list-style-type: none"> SIP IP Call—when dialing the URI of the far site, the system actually uses SIP IP address to establish a connection. SIP Account—when dialing the URI of the far site, the system uses SIP account to establish a connection. The outbound proxy server should be configured before dialing. <p>Default: SIP IP Call</p>	Web User Interface

To configure the URI call mode via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **URI Call Mode**.

The screenshot displays the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists configuration categories: 'General', 'Date&Time', 'Call Features' (selected), 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', 'Tones', and 'Wireless Micpod'. The main content area shows various settings with their current values in dropdown menus:

Setting	Value
DND	Disabled
Auto Answer	Enabled
Auto Answer Mute	Enabled
Auto Answer Multiway	Disabled
Call Match	Enabled
History Record	Enabled
Call Protocol	Auto
Uplink Bandwidth	Auto
Downlink Bandwidth	Auto
Abnormal call answering	IP Call Answer
Safe mode call	Disabled
Ringback Timeout(30-240)	200
Auto Refuse Timeout(30-240)	120
URI Call Mode	SIP IP Call

The 'URI Call Mode' setting is highlighted with a red rectangle, and its dropdown menu is open, showing 'SIP IP Call' as the selected option.

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

Configuring System Settings

This chapter provides information for making configuration changes for the system, such as language, time and date, backlight of the VCP40 video conferencing phone, video&audio setting and camera setting:

Topics include:

- [General Setting](#)
- [Audio Setting](#)
- [Adjusting MTU of Video Packets](#)
- [Dual-Stream Protocol](#)
- [Mix Sending](#)
- [Configuring Camera Settings](#)
- [Far-end Camera Control](#)
- [Camera Control Protocol](#)
- [Tones](#)

General Setting

Site Name

When the system is idle, the site name is displayed on the status bar of display device and VCP40 phone. When H.323 or SIP protocol is enabled, you can make an IP address call to the far site, the site name will be displayed on the display device of the far site. Site name can consist of letters, numbers or special characters. You can configure the site name of the system via the remote control or web user interface.

The site name parameter is described below:

Parameter	Description	Configuration Method
Site Name	Configures the site name of the system. Valid values: String within 64 characters Default: For VC400: Yealink VC400 For VC120: Yealink VC120	Remote Control Web User Interface

To configure the site name via web user interface:

1. Click on **Setting**->**General**.
2. Edit the site name in the **Site Name** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. Below this is a green header with the Yealink VC400 logo and a menu with Home, Status, Account, Network, Setting (highlighted), Directory, and Security. On the left, a sidebar lists various settings categories: General (selected), Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'General Information' and contains several configuration fields. The 'Site Name' field is highlighted with a red rectangular box and currently displays 'Yealink VC400'. Other fields include 'Automatic Sleep Time' (set to 10 Min), 'Backlight Time' (set to Always On), 'Hide IP Address' (set to Disabled), 'ReLogOffTime(1-1000min)' (set to 5), 'Key Tone' (set to On), 'Meeting Password' (set to Off), and a 'Password' field.

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

The LCD screen of the display device and VCP40 will display the changed site name.

To configure the site name via the remote control:

1. Select **Menu**->**Basic**.
2. Edit the site name in the **Site Name** field.
3. Press the **Save** soft key to accept the change.

The LCD screen of the display device and VCP40 will display the changed site name.

Backlight of the VCP40 Video Conferencing Phone

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 phone is inactive.

You can configure the backlight time in the following formats:

- **Always On:** Backlight is turned on permanently.
- **15 s, 30 s, 1 Min, 2 Min, 5 Min, 10 Min, 30 Min:** Backlight is turned off when the phone is inactive after a preset period of time. It is automatically turned on if the status of the phone changes or any key is pressed.

The backlight parameter on VCP40 phone is described below:

Parameter	Description	Configuration Method
Backlight Time	Configure the backlight time of the VCP40 phone. Default: Always On	Web User Interface

To configure the backlight of the VCP40 phone via web user interface:

1. Click on **Setting->General**.
2. Select the desired value from the pull-down list of **Backlight Time**.

The screenshot shows the Yealink VCP40 web user interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network, Setting (selected), Directory, and Security. On the left, a sidebar lists various settings categories: General (selected), Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'General Information' and contains several settings: Site Name (Yealink VC400), Automatic Sleep Time (10 Min), Backlight Time (Always On, highlighted with a red box), Hide IP Address (Disabled), ReLogOffTime (5), Key Tone (On), Meeting Password (Off), and Password. The 'Backlight Time' dropdown menu is currently set to 'Always On'.

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

Language

The default language of the LCD screen of the display device and the VCP40 is English, and you can change it via the remote control. The VCP40 phone will detect and use the same language as the display device.

The default language of the web user interface is English. You can change the web user interface language for web user interface.

The available languages for system are English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian and Czech.

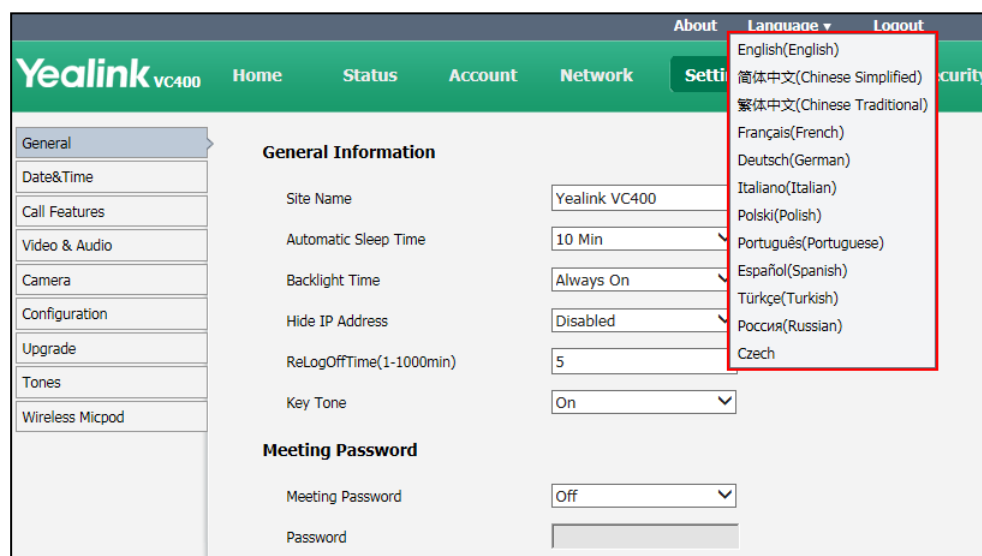
The language parameters on the system are described below:

Parameter	Description	Configuration Method
Language	Specifies the language for the web user interface	Web User Interface
Language	Specifies the language for the	Remote Control

Parameter	Description	Configuration Method
	LCD screen of the display device and the VCP40 phone. Default: English	

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

1. Click **Language** at the top of the web page.
2. Select the desired language from the pull-down list of **Language**.



To specify the language for the display device via the remote control:

1. Select **Menu->Basic**.
2. Select the desired language from the pull-down list of **Language**.
3. Press the **Save** soft key to accept the change.

Date & Time

Time and date are displayed on the idle screen of the display device and the VCP40 phone. Time and date are synced automatically from the NTP server by default. The default NTP server is cn.pool.ntp.org. The NTP server is configurable manually or obtained by DHCP via DHCP Option 42. The phone will use the NTP server obtained by DHCP preferentially. If the system cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date 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 the system 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 DST at various times, details vary by location. DST can be adjusted automatically from the time zone configuration. Typically, there is no need to change this setting.

DST parameters are described below:

Parameter	Description	Configuration Method
DHCP Time	Enables or disables the system to update time with the offset time obtained from the DHCP server. Default: Disabled Note: it is only available to GMT 0.	Web User Interface
Time Zone	Configures the time zone. Default: +8 China (Beijing)	Remote Control Web User Interface
Primary Server/NTP Primary Server	Configures the primary NTP server. Default: cn.pool.ntp.org	Remote Control Web User Interface
Secondary Server/NTP Secondary Server	Configures the secondary NTP server. Default: cn.pool.ntp.org	Remote Control Web User Interface
Synchronism (15~86400s)	Configures the interval (in minutes) for the system to synchronize time and date with NTP server. Default: 1000.	Web User Interface
Daylight Saving Time	Configures the Daylight Saving Time (DST) type. The available types for the system are: <ul style="list-style-type: none">Disabled-not use DST.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<ul style="list-style-type: none"> • Enabled-use DST. You can manually configure the start time, end time and offset according to your needs. • Automatic-use DST. DST will be configured automatically. You do not need to manually configure the start time, end time and offset. <p>Default: Automatic</p>	
Fixed Type	<p>Configures the DST calculation methods.</p> <ul style="list-style-type: none"> • By Date- specifies the month, day and hour to be the DST start /end date. • By Week- specifies the month, week, day and hour the DST start /end date. <p>Note: It only works if the value of Daylight Saving Time is set to Enabled.</p>	Web User Interface
Start Date	<p>When the DST calculation method is set to By Date. Configures the time to start DST.</p> <p>Note: It only works if the value of the Daylight Saving Time is set to Enabled.</p>	Web User Interface
End Date	<p>When the DST calculation method is set to By Date. Configures the time to end DST.</p> <p>Note: It only works if the value</p>	Web User Interface

Parameter	Description	Configuration Method
	of the Daylight Saving Time is set to Enabled.	
DST Start Month	When the DST calculation method is set to By Week . Configures the time to start DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Start Day of Week		
DST Start Day of Week Last in Month		
Start Hour of Day		
DST Stop Month	When the DST calculation method is set to By Week . Configures the time to end DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Stop Day of Week		
DST Stop Day of Week Last in Month		
End Hour of Day		
Offset(minutes)	Configures the DST offset time (in minutes). Valid values: -300 to +300. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
Time Type	Configures the DST time type. <ul style="list-style-type: none"> SNTP: obtain the time and date from the NTP server automatically. Manual Time: configure the time and date manually. Default: SNTP	Remote Control Web User Interface
Time Format/ Time	Configures the time format. <ul style="list-style-type: none"> Hour12 Hour24 Default: Hour 24	Remote Control Web User Interface
Date Format/Date	Configures the date format.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<ul style="list-style-type: none"> WWW MMM DD DD-MMM-YY YYYY-MM-DD DD/MM/YYYY MM/DD/YY DD MMM YYYY WWW DD MMM <p>Default: YYYY-MM-DD</p>	

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

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

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network, Setting (selected), Directory, and Security. On the left, a sidebar lists various settings categories: General, Date&Time (selected), Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'Date & Time' and contains several configuration fields. A red box highlights the 'Fixed Type' section, which includes the 'DST By Date' radio button (selected), the 'Start Date' (Month 6, Day 28, Hour 10), the 'End Date' (Month 11, Day 30, Hour 10), and the 'Offset(minutes)' field (10). Other fields include 'DHCP Time' (Disabled), 'Time Zone' (+8 China(Beijing)), 'Primary Server' (cn.pool.ntp.org), 'Secondary Server' (cn.pool.ntp.org), 'Synchronism (15~86400s)' (1000), 'Daylight Saving Time' (Enabled), 'Time Type' (SNTP), 'Time Format' (Hour 24), and 'Date Format' (YYYY-MM-DD).

- 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 Yealink VC400 web interface. The 'Setting' tab is selected, and the 'Date&Time' sub-tab is active in the left sidebar. The main content area displays various system settings. A red rectangular box highlights the 'Fixed Type' section, which includes the following fields:

- Fixed Type:** Radio buttons for 'DST By Date' and 'DST By Week' (selected).
- DST Start Month:** Dropdown menu set to 'January'.
- DST Start Day of Week:** Dropdown menu set to 'Sunday'.
- DST Start Day of Week Last in Month:** Dropdown menu set to 'First In Month'.
- Start Hour of Day:** Empty text input field.
- DST Stop Month:** Dropdown menu set to 'January'.
- DST Stop Day of Week:** Dropdown menu set to 'Sunday'.
- DST Stop Day of Week Last in Month:** Dropdown menu set to 'First In Month'.
- End Hour of Day:** Empty text input field.
- Offset(minutes):** Text input field containing the value '10'.

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 **Setting->Date & Time**.
2. Select **Manual Time** from the pull-down list of **Time Type**.
3. Enter the current date in the **Date** field.
4. Enter the current time in the **Time** field.
5. Select the desired value from the pull-down list of **Time Format**.
6. Select the desired value from the pull-down list of **Date Format**.

The screenshot shows the Yealink VC400 web interface. The 'Setting' tab is selected, and the 'Date & Time' sub-tab is active in the left sidebar. The main content area displays the 'Date & Time' settings. A red rectangular box highlights the 'Manual Time' section, which includes the following fields:

- DHCP Time:** Dropdown menu set to 'Enabled'.
- Time Type:** Dropdown menu set to 'Manual Time'.
- Date:** Fields for Year (2015), Month (12), and Day (26).
- Time:** Fields for Hour (9), Minute (36), and Second (40).
- Time Format:** Dropdown menu set to 'Hour 24'.
- Date Format:** Dropdown menu set to 'YYYY-MM-DD'.

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

To configure the time and date format via the remote control:

- Select **Menu->Basic->Date & Time**.
- Configure the desired values.
- Press the **Save** soft key to accept the change.

The time and date displayed on the LCD screen of the display device and VCP40 phone will change accordingly.

Automatic Sleep Time

The system will enter the sleep mode automatically when it has been inactive for a period of time (the default time is 10 minutes). When the system is in sleep mode, it can still accept incoming calls. The display device will prompt "No Signal", and the LCD screen of the VCP40 phone prompts "Sleeping Press any key to resume". You can press any key on the remote control or the VCP40 phone to wake the system up. When receiving a call, the system will be woken up automatically.

You can change the automatic sleep time via the remote control or web user interface. You can also press the sleep key on the remote control to make the system sleep immediately.

The automatic sleep time is described below:

Parameter	Description	Configuration Method
Automatic Sleep Time	<p>Configures the inactive time (in minutes) before the system enters sleep mode.</p> <p>Default: 10 Min</p> <p>Note: During setup wizard, the automatic sleep time feature is disabled automatically. To protect the display device, you should configure the automatic sleep time immediately.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure the automatic sleep time via web user interface:

- Click on **Setting->General**.

2. Select desired value from the pull-down list of **Automatic Sleep Time**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists 'General' (selected), 'Date&Time', 'Call Features', 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', 'Tones', and 'Wireless Micpod'. The main content area is titled 'General Information' and contains the following settings:

- Site Name: Yealink VC400
- Automatic Sleep Time: 10 Min** (highlighted with a red box)
- Backlight Time: Always On
- Hide IP Address: Disabled
- ReLogOffTime(1-1000min): 5
- Key Tone: On

Below this is the 'Meeting Password' section:

- Meeting Password: Off
- Password: (empty field)

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

To configure the automatic sleep time via the remote control:

1. Select **Menu->Basic**.
2. Select desired value from the pull-down list of **Automatic Sleep Time**.
3. Press the **Save** soft key to accept the change.

Hide IP Address

When the system is idle, the display device displays shortcut keys and status bar. The status bar displays time and date, site name, IP address, SIP and H.323 account (when SIP and H.323 account are registered). You can hide the system IP address.

The hide IP address parameter is described below:

Parameter	Description	Configuration Method
Hide IP Address	Enables or disables the system to hide IP address. Default: Disabled	Web User Interface

To enable the hide IP address feature via web user interface:

1. Click on **Setting->General**.

2. Select **Enabled** from the pull-down list of **Hide IP Address**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The 'General Information' section is active, showing fields for Site Name (Yealink VC400), Automatic Sleep Time (10 Min), Backlight Time (Always On), Hide IP Address (Enabled, highlighted with a red box), ReLogOffTime(1-1000min) (5), Key Tone (On), Meeting Password (Off), and Password.

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

The IP address is hidden from the status bar of the display device.

ReLog Offtime

The system will log out of the web user interface automatically after being inactive for a period of time (default: 5 minutes). You need to re-enter the user name and password to login. You can only configure the relog offtime via web user interface.

The relog offtime parameter is described below:

Parameter	Description	Configuration Method
ReLogOffTime (1-1000min)	Configures the inactive time (in minutes) before the system logs out of the web user interface automatically. Default: 5	Web User Interface

To configure the relog offtime via web user interface:

1. Click on **Setting->General**.

2. Enter the desired time in the **ReLogOffTime (1-1000min)** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. Below this is a green header with the Yealink VC400 logo and tabs for Home, Status, Account, Network, Setting (selected), Directory, and Security. On the left, a sidebar lists various settings categories: General (selected), Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'General Information' and contains several settings: Site Name (Yealink VC400), Automatic Sleep Time (10 Min), Backlight Time (Always On), Hide IP Address (Disabled), ReLogOffTime(1-1000min) (5, highlighted with a red box), Key Tone (On), Meeting Password (Off), and a Password field.

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

Key Tone

You can enable the key tone feature for the system to make a keyboard click sound effect (key tone) when pressing any key on the remote control. If you disable this feature or system ringer volume is adjusted to 0, the system will not play a key tone when you press any key on the remote control.

Key tone is configurable via the remote control or web user interface.

The key tone parameter is described below:

Parameter	Description	Configuration Method
Key Tone	Enables or disables the key tone. Default: On	Remote Control Web User Interface

To configure the key tone via web user interface:

1. Click on **Setting->General**.

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

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The 'General Information' section is active, displaying several configuration fields: Site Name (Yealink VC400), Automatic Sleep Time (10 Min), Backlight Time (Always On), Hide IP Address (Enabled), ReLogOffTime(1-1000min) (5), and Key Tone (On, highlighted with a red box). Below this is the 'Meeting Password' section, which includes a 'Meeting Password' dropdown (set to Off) and a 'Password' input field.

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

To configure the key tone via the remote control:

1. Select **Menu->Basic**.
2. Mark the radio box in the **Key Tone** field.
3. Press the **Save** soft key to accept the change.

Meeting Password

Meeting password is used to manage the incoming calls. If you enable this feature, only the people who know the meeting password can dial your system. If your system is idle, meeting password can prevent people from dialing your system. If your system is during a call or conducting a conference call, meeting password can prevent unauthorized people from joining.

Meeting password is configurable via the remote control or web user interface.

Note

You can add specified users to the meeting whitelist. Users in the whitelist can dial your system without meeting password. For more information on meeting whitelist, refer to [Meeting Whitelist](#) on page 144.

The meeting password parameters are described below:

Parameter	Description	Configuration Method
Meeting Password	Enable or disable the meeting password feature. Default: Off	Remote Control Web User Interface

Parameter	Description	Configuration Method
Password	Configures the meeting password. Default: blank	Remote Control Web User Interface

To configure the meeting password via web user interface:

1. Click on **Setting->General**.
2. Select the desired value from the **Meeting Password** pull-down list.
3. Enter the desired value in the **Password** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists 'General' (selected), 'Date&Time', 'Call Features', 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', 'Tones', and 'Wireless Micpod'. The main content area is titled 'General Information' and contains several settings: Site Name (Yealink VC400), Automatic Sleep Time (10 Min), Backlight Time (Always On), Hide IP Address (Enabled), ReLogOffTime(1-1000min) (5), and Key Tone (On). Below these is the 'Meeting Password' section, which is highlighted with a red box. It contains a 'Meeting Password' dropdown menu set to 'On' and a 'Password' text field containing '123'.

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

To configure the meeting password via the remote control:

1. Select **Menu->Basic->Meeting Password**.
2. Check the **Meeting Password** checkbox.
3. Enter the meeting password in the **Password** field.
4. Press the **Save** soft key to accept the change.

People can press **IP##meeting password** or **meeting password@IP** to dial your system or join your conference call. For example: your IP address is 10.3.6.201 and you set 123 as your meeting password. People should press **10.3.6.201##123** or **123@10.3.6.201** to dial your system or join your conference call. If people call you without a meeting password or with a wrong meeting password, the call will fail.

Meeting Whitelist

You can add the IP, account or domain name of the remote system to the meeting whitelist. Users in the whitelist can dial your VC400/VC120 or join your conference call directly without meeting password even if you have enabled the meeting password

feature. VC400 /VC120 supports up to 100 whitelist records. Meeting whitelist is configurable via web user interface only.

To add the meeting whitelist numbers via web user interface:

1. Click on **Directory->Meeting Whitelist**.
2. Enter the user's IP, account or domain name in the **Meeting White Number List** field.

Meeting White Number List	Operator
10.3.6.157	+ Add

3. Click **Add**.
4. Repeat step 2-3 to add more numbers to the whitelist.

To delete the meeting whitelist numbers via web user interface:

1. Click on **Directory -> Meeting Whitelist**.
2. Click **Delete** beside the numbers that you want to delete.

Meeting White Number List	Operator
	+ Add
10.3.6.157	- Delete
10.3.6.159	- Delete

The web user interface prompts the message "Warning: Are you sure delete the white number?".

3. Click **Confirm**.

Audio Setting

Audio Output Device

The system supports the following audio output devices:

- Auto
- VCS Phone
- HDMI

- **Line Output**

By default, the system automatically selects the audio output devices with highest priority. The priority is: VCS Phone>HDMI>Line Output. If the audio output device with highest priority is removed from the codec, the system will select the next highest priority device.

You can also specify the desired audio output device via the remote control or the web user interface.

The audio output device parameter is described below:

Parameter	Description	Configuration Method
Audio Output	<p>Specifies the audio output device for the system.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • Auto - selects the audio output device with highest priority. • HDMI - selects the built-in speakerphone of the display device. • Line Output - selects the speakerphone connected to the Line Out port on the VC400/VC120 codec. • VCS Phone - selects the VCP40 phone. <p>Default: Auto</p> <p>If VCS Phone is selected as the audio output device manually or automatically, the audio input device must be VCS Phone or Line In+VCS Phone.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure the audio output device feature via web user interface:

1. Click on **Setting->Video & Audio**.

2. Select the desired value from the pull-down list of **Audio Output**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. Below this is a green header with the Yealink logo and navigation tabs: Home, Status, Account, Network, Setting (highlighted), Directory, and Security. On the left is a sidebar menu with options: General, Date&Time, Call Features, Video & Audio (highlighted), Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'Audio Settings' and contains several sections: 'Audio Input' with a dropdown set to 'Auto(Line Input + VCS)', 'Audio Output' with a dropdown set to 'Auto(VCS Phone)' (highlighted with a red box), 'Presentation' with a 'Mix' dropdown set to 'On', and 'Far-end Camera Control' with three dropdowns: 'Far Control Near Camera' set to 'Enabled', 'Far Set of Camera Presets' set to 'Disabled', and 'Far Move to Camera Presets' set to 'Disabled'.

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

To configure the automatic sleep time via the remote control:

1. Select **Menu->Video & Audio->Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Output**.
3. Press the **Save** soft key to accept the change.

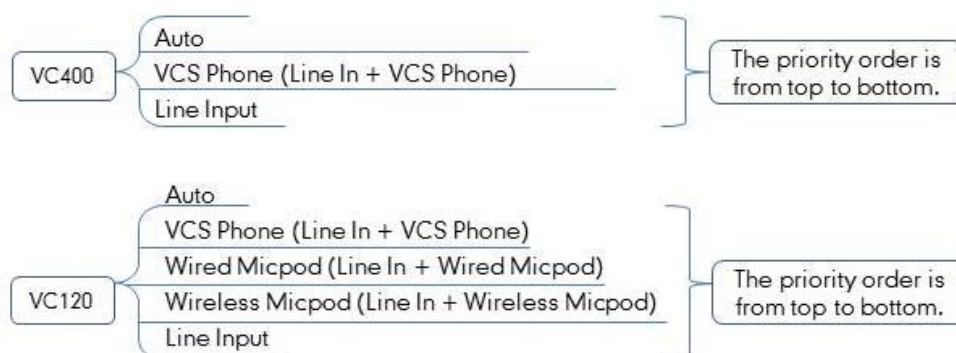
Audio Input Device

The system supports the following audio input devices:

- **Auto** (select the audio input device with highest priority)
- **VCS Phone** (VCP40 phone)
- **Wired Micpod** (VCM30)
- **Wireless Micpod** (VCM60)
- **Line Input** (microphone connected to the Line In port on the VC400/VC120 codec)
- **Line In + VCS Phone**
- **Line In + Wired Micpod**
- **Line In + Wireless Micpod**

By default, the VC400/VC120 automatically selects the audio input devices with highest priority. "Device" and "Line In + Other device" options have the same priority. For example: "VCS Phone" and "Line In + VCS Phone" have the same priority.

The priority of audio input device is:



You can also specify the desired audio input device via the remote control or the web user interface.

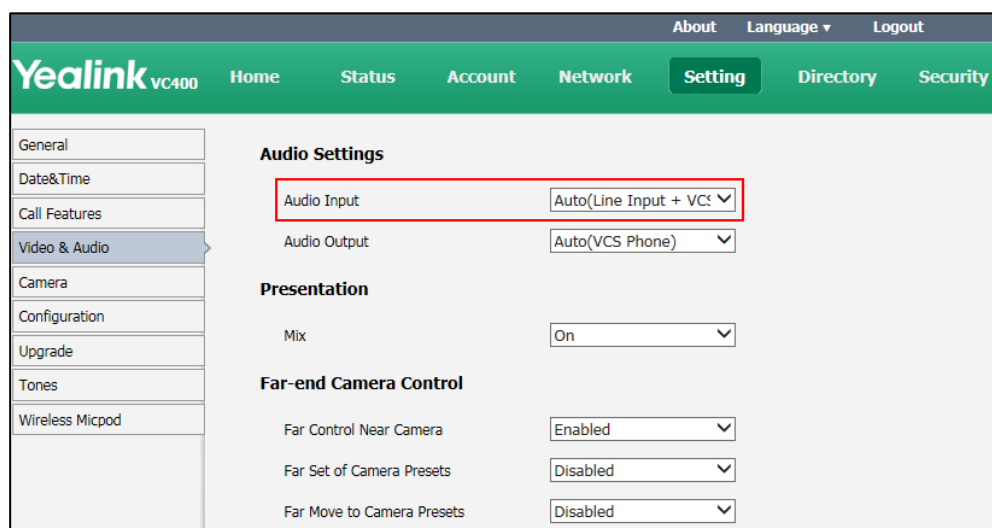
The audio output device parameter is described below:

Parameter	Description	Configuration Method
Audio Input	<p>Specifies the audio input device for the VC400/VC120.</p> <p>Valid values:</p> <ul style="list-style-type: none"> Auto- selects the audio input device with highest priority. VCS Phone- selects the VCP40 phone. Wired Micpod- selects the VCM30 video conferencing microphone array Wireless Micpod -selects the VCM60 video conferencing wireless microphone. Line Input- selects the microphone connected to the Line In port on the VC400/VC120 codec. Line In +VCS Phone- selects microphone connected to the Line In port on the codec and VCP40 phone. Line In + Wired Micpod - selects microphone connected to the Line In port on the codec and VCM30 video conferencing 	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>microphone array.</p> <ul style="list-style-type: none"> Line In + Wireless Micpod- selects the microphone connected to the Line In port on the codec and VCM60 video conferencing wireless microphone. <p>Default: Auto.</p> <p>If “Line Input” is selected as the audio input device, the near site will not play sound from the Line Input device.</p> <p>If “Line Input” is selected as an auxiliary audio input, which means that “Line In + Other device” is selected as the audio input device, the near site will play sound from the Line Input device. (For example: during a video training for main office and branch office, both offices need to hear the video sound).</p>	

To configure the audio input device via web user interface:

1. Click on **Setting->Video & Audio**.
2. Select the desired value from the pull-down list of **Audio Input**.



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

To configure the audio input device via the remote control:

1. Select **Menu->Video & Audio->Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Input**.
3. Press the **Save** soft key to accept the change.

Adjusting MTU of Video Packets

Video packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped. This results in poor quality video at the receiving device. You can set the maximum MTU size of the video packets sent by the system. The default value is 1500 bytes. Specify the MTU size used in calls based on the network bandwidth settings. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small, increase the MTU.

The MTU parameter on the system is described below.

Parameter	Description	Configuration Method
Video MTU	<p>Specifies the maximum MTU size (in bytes) of video packets sent by the system.</p> <p>Valid Values: Integer from 1000 to 1500</p> <p>Default: 1500</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure MTU via web user interface:

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

2. In the **MTU** block, enter the desired value in the **Video MTU** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is divided into sections: 'Internet Port' (Active: Disabled, VID: 1, Priority: 0), 'DHCP VLAN' (Active: Enabled, Option: 132), 'QoS' (Audio Priority: 63, Video Priority: 34, Data Priority: 63), and 'MTU' (Video MTU: 1500). The 'Video MTU' field is highlighted with a red rectangle.

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

To configure MTU via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **Advanced Network**.
2. Enter the desired value in the **Video MTU(1000-1500)** field.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Dual-Stream Protocol

To enhance the process of communicating with others over video, the dual-stream protocol provides the ability to share content from a computer, such as video clips or documentation. Both the video and the documentation can be transmitted to the far site simultaneously, thus meeting the requirements of different conference scenarios, such as training or medical consultation.

The Yealink video conferencing system supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol). H.239 protocol is used when sharing content with the far site in H.323 calls. BFCP protocol is used when sharing content with the far site in SIP calls. Before enabling the desired protocol, ensure that the protocol is supported and enabled by the far site you wish to call. If the far site does not support the protocol for

sharing content, MCU will automatically mix the content and camera video, and send them in one channel. For more information on mix sending, refer to [Mix Sending](#) on page 154.

Dual-stream protocol parameters on the system are described below.

Parameter	Description	Configuration Method
H.239	Enables or disables the H.239 protocol for sharing content in H.323 calls. Default: Enabled	Web User Interface
BFCP	Enables or disables the BFCP protocol for sharing content in SIP calls or SIP IP call. Default: Disabled	Web User Interface

To configure dual-stream protocol for H.323 call via web user interface:

1. Click on **Account->H323**.
2. Select the desired value from the pull-down list of **H.239**.

The screenshot displays the Yealink VC400 web interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network, Setting, Directory, and Security. The 'Account' tab is active, and the 'H323' sub-tab is selected. On the left sidebar, there are links for H323, SIP Account, SIP IP Call, and Codec. The main content area shows the 'H.323 Account' configuration page. Various settings are listed, including H.323 Name, Extension, Gatekeeper Mode, IP addresses, Authentication, Username, Password, H.460 Active, H.323 Tunneling, H.235 Encryption, Protocol Monitor Port, DTMF Type, and H.239. The 'H.239' dropdown menu is highlighted with a red box, showing 'Enabled' as the selected option. Other settings like Gatekeeper IP Address 1 (10.2.1.43) and Gatekeeper IP Address 2 are also visible.

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

To configure dual-stream protocol for SIP call via web user interface:

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

2. Select the desired value from the pull-down list of **BFCP**.

The screenshot shows the Yealink VC400 web interface with the 'Account' tab selected. The 'SIP Account' sub-tab is active. The 'BFCP' dropdown menu is highlighted with a red box, showing 'Disabled' as the selected value. Other settings include User Name (9000), Password (masked), Server Host (10.2.1.48), Port (5060), Enable Outbound Proxy Server (Disabled), Outbound Proxy Server (empty), Transport (UDP), Server Expires (3600), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (96~127) (101), NAT_Traversal (STUN), Keep Alive Interval (30), RPort (Enabled), and FECC(SIP) (Disabled).

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

To configure dual-stream protocol for SIP IP call via web user interface:

1. Click on **Account-> SIP IP Call**.
2. Select the desired value from the pull-down list of **BFCP**.

The screenshot shows the Yealink VC400 web interface with the 'Account' tab selected. The 'SIP IP Call' sub-tab is active. The 'BFCP' dropdown menu is highlighted with a red box, showing 'Enabled' as the selected value. Other settings include Transport (TCP), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (96~127) (101), NAT_Traversal (Disabled), RPort (Enabled), and FECC(SIP) (Enabled).

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

Mix Sending

Content sharing allows users to share content with other conference participants during a call. When a PC is connected to the PC port on the VC400/VC120 codec, the display device can display both the camera video and the shared content. The content sharing feature is very useful in the conference scenario in which content sharing is needed (e.g., a slide or a flash).

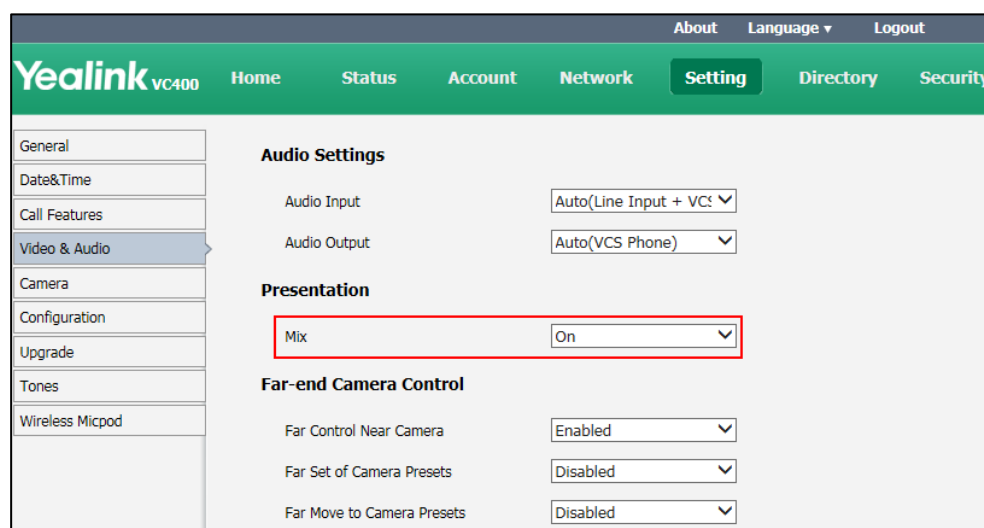
During a conference call, the far site may not support receiving shared content. In this case, you can enable mix sending feature on the system. Mix sending feature allows the sender to compound multiple video streams (local image+shared content) to one video stream, and then send it to the far site.

The mix sending parameter on the system is described below.

Parameter	Description	Configuration Method
Mix	Enables or disables the mix sending feature on the system. Default: Enabled	Web User Interface

To configure mix sending via web user interface:

1. Click on **Setting->Video & Audio**.
2. In the **Presentation** block, select the desired value from the pull-down list of **Mix**.



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

Configuring Camera Settings

To display high quality video image, you can configure camera settings as required, such as white balance, exposure and sharpness.

Camera settings parameters are described below.

Parameter	Description	Configuration Method
Exposure Compensation	<p>Disables or configures the value of camera exposure compensation.</p> <ul style="list-style-type: none"> Off 1 2 3 <p>Default: 1</p> <p>Exposure compensation is used to compensate the camera effectively when shooting in a backlight environment. If the environment light is dark, increase the compensation value.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Flicker	<p>Disables or configures the value of camera flicker frequency.</p> <ul style="list-style-type: none"> 50Hz 60Hz <p>Default: 50Hz</p> <p>Note: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by.</p>	<p>Remote Control</p> <p>Web User Interface</p>
White Balance Mode	<p>Configures the white balance mode of the camera.</p> <ul style="list-style-type: none"> Auto—Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. One push—Use the predefined color temperature settings to provide acceptable color 	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>reproduction.</p> <ul style="list-style-type: none"> ATW—Automatically adjust the white balance based on the video image shoot by the camera. Manual—Manually set red and blue gain. <p>Default: Auto</p>	
Red Gain	<p>Configures the red gain of the camera.</p> <p>Valid Values: 0-100</p> <p>Default: 83</p> <p>Note: You can set this parameter only when the white balance mode is configured to Manual.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Blue Gain	<p>Configures the blue gain of the camera.</p> <p>Valid Values: 0-100</p> <p>Default: 62</p> <p>Note: You can set this parameter only when the white balance mode is configured to Manual.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Saturation	<p>Configures the saturation of the camera.</p> <p>Valid Values: 0-14</p> <p>Default: 3</p>	<p>Remote Control</p> <p>Web User Interface</p>
Sharpness	<p>Configures the sharpness of the camera.</p> <p>Valid Values: 0-14</p> <p>Default: 1</p> <p>Note: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Brightness	<p>Configures the brightness of the camera.</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	Valid Values: 0-100 Default: 8	
Contrast	Configures the contrast of the camera. Valid Values: 0-100 Default: 45	Remote Control Web User Interface
Noise Reduction (2D)	Specifies the noise reduction (2D) mode. <ul style="list-style-type: none"> • Off • Low • Middle • High Default: Middle	Remote Control Web User Interface
Noise Reduction (3D)	Specifies the noise reduction (3D) mode. <ul style="list-style-type: none"> • Off • Low • Middle • High Default: Off	Remote Control Web User Interface
Hangup Mode	Enables or disables the camera to flip the image view when camera is handed at up-side-down position Default: Off	Remote Control Web User Interface
Camera Pan Direction	Configures the pan direction of the camera. <ul style="list-style-type: none"> • Normal • Reversed Default: Normal If the camera reversed mode is enabled, the camera pan direction will be reversed when pressing the left and right navigation keys on the remote	Remote Control Web User Interface

Parameter	Description	Configuration Method
	control. In this case, you can set the camera pan direction to Reversed.	
Camera Map	Enables or disables the preview of camera presets. Default: On Note: If it is set to on, you can view the pre-saved camera presets.	Remote Control Web User Interface
Clear Preset	Clears all camera presets.	Remote Control Web User Interface
Reset Camera	Resets the camera settings to factory defaults. Note: The camera presets will also be cleared.	Remote Control Web User Interface

To configure camera settings via web user interface:

1. Click on **Setting->Camera**.
2. Configure the camera settings.

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

To configure camera settings via the remote control:

1. Select **Menu->Video & Audio->Camera General Settings**.
2. Configure the camera settings.
3. Press the **Save** soft key to accept the change.

Far-end Camera Control

Local video is displayed on the display device of the far site during a call. For the best view, you can enable the Far Control Near Camera feature to allow the far site to control the focus and angle of the local camera. You can also specify whether the far site is allowed to store and use the local camera presets.

Far-end camera control parameters are described below.

Parameter	Description	Configuration Method
Far Control Near Camera	Enables or disables the far site to control the near site camera. Default: Enabled	Remote Control Web User Interface
Far Set of Camera Presets	Enables or disables the far site to store the camera presets. Default: Disabled	Remote Control Web User Interface
Far Move to Camera Presets	Enables or disables the far site to use the camera presets. Default: Disabled	Remote Control Web User Interface

To configure far-end camera control via web user interface:

1. Click on **Setting->Video & Audio**.
2. Select the desired values from the pull-down lists.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists settings categories: General, Date&Time, Call Features, Video & Audio (selected), Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area is titled 'Audio Settings' and includes sections for 'Audio Settings' (with 'Audio Input' and 'Audio Output' dropdowns), 'Presentation' (with a 'Mix' dropdown), and 'Far-end Camera Control'. The 'Far-end Camera Control' section contains three settings, each with a dropdown menu: 'Far Control Near Camera' (set to 'Enabled'), 'Far Set of Camera Presets' (set to 'Disabled'), and 'Far Move to Camera Presets' (set to 'Disabled'). This entire section is enclosed in a red rectangular box.

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

To configure far-end camera control via the remote control:

1. Select **Menu->Video & Audio->Far-end Camera Control**.
2. Make the desired changes.
3. Press the **Save** soft key to accept the change.

Camera Control Protocol

VC400/VC120 video conferencing systems support camera control protocols: FECC (Far End Camera Control). You can enable the FECC protocol for SIP call or H.323 call.

If far site wants to control the local camera, both the far site and near site should enable the camera control protocol simultaneously. If the FECC protocol is not enabled on either site, far-end camera control cannot be performed. For example, a SIP call is established between two sites, the two sites must enable FECC (SIP) protocol simultaneously to perform far-end camera control. If FECC (SIP) protocol and FECC (H.323) protocol are both enabled, the system will select the appropriate camera control protocol according to the protocol (SIP or H.323) the call uses.

Camera control protocol parameters are described below:

Parameter	Description	Configuration Method
FECC(H.323)	Enables or disables the FECC (H.323) protocol for far site to control near camera in H.323 calls. Default: Enabled	Web User Interface
FECC(SIP)	Enables or disables the FECC (SIP) protocol for far site to control near camera in SIP calls or SIP IP call. Default: Disabled	Web User Interface

To configure camera control protocol for H.323 calls via web user interface:

1. Click on **Account->H323**.

2. Select the desired value from the pull-down list of **FECC(H.323)**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is selected, and the 'H323' sub-tab is active. On the left, there is a sidebar with 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The main content area displays various settings for the H.323 account. The 'FECC(H.323)' option is highlighted with a red box, showing it is set to 'Enabled'.

Setting	Value
H.323 Account	Enabled
H.323 Name	9000
H.323 Extension	9000
Gatekeeper Mode	Manual
Gatekeeper IP Address 1	10.2.1.43
Gatekeeper IP Address 2	
Gatekeeper Authentication	Disabled
Gatekeeper Username	
Gatekeeper Password	*****
H.460 Active	Disabled
H.323 Tunneling	Disabled
H.235 Encryption	Disabled
Protocol Monitor Port	1720
DTMF Type	INBAND
H.239	Enabled
FECC(H.323)	Enabled

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

To configure camera control protocol for SIP calls via web user interface:

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

2. Select the desired value from the pull-down list of **FECC(SIP)**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is active. On the left, there's a sidebar with 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The 'SIP Account' section is expanded. The main area shows various settings for the SIP account, including User Name (9000), Password (masked), Server Host (10.2.1.48), Port (5060), Enable Outbound Proxy Server (Disabled), Outbound Proxy Server (empty), Port (5060), Transport (UDP), Server Expires (3600), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (96~127) (101), NAT_Traversal (STUN), Keep Alive Interval (30), RPort (Enabled), BFCP (Disabled), and FECC(SIP) (Disabled). The FECC(SIP) dropdown is highlighted with a red box.

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

To configure camera control protocol for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select the desired value from the pull-down list of **FECC(SIP)**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is active. On the left, there's a sidebar with 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The 'SIP IP Call' section is expanded. The main area shows various settings for the SIP IP call, including Transport (TCP), SRTP (Disabled), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (96~127) (101), NAT_Traversal (Disabled), RPort (Enabled), BFCP (Enabled), and FECC(SIP) (Enabled). The FECC(SIP) dropdown is highlighted with a red box.

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

Tones

When automatically answering an incoming call, the system 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 system. The default tones used on the system are the US tone sets. Available tone sets for the system:

- Australia
- Austria
- Brazil
- Belgium
- China
- Chile
- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States

Configured tones can be heard on the system for the following conditions:

Condition	Description
Ring Back	Ring-back tone
Busy	When the callee is busy
Call Waiting	Call waiting tone
Auto Answer	When answering a call automatically

Tones parameters on the system are described below:

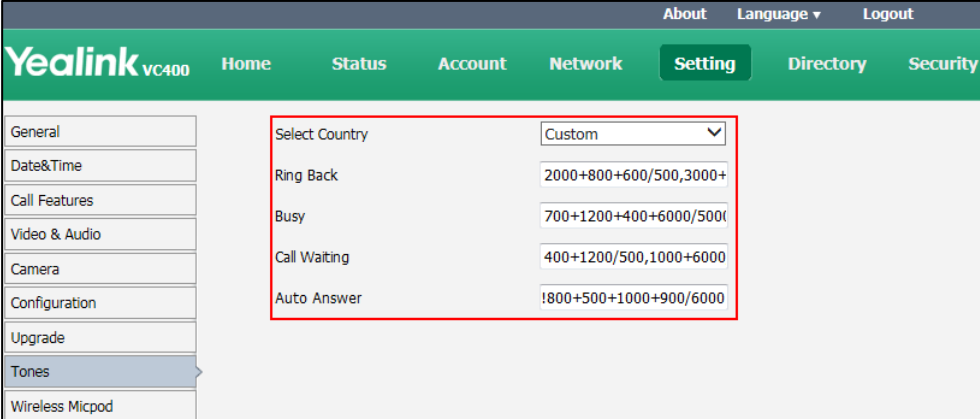
Parameter	Description	Configuration Method
Select Country	Customizes tones or selects the desired country tone set. Default: Custom	Web User Interface
Ring Back	<p>Customizes the ring-back tone for the system.</p> <p>tone = element1[,element2] [,element3]...[,element8]</p> <p>Where element = [!]Freq1[+Freq2][+Freq3][+Freq4]]/Duration</p> <p>Freq: the frequency of the tone (ranges from 200Hz to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone consists of at most four different frequencies.</p> <p>Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.</p> <p>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).</p> <p>If you want the system to play tones once, add an exclamation mark "!" before tones (e.g., !250/200, 0/1000,</p>	Web User Interface

Parameter	Description	Configuration Method
	<p>200+300/500, 600+700+800+1000/2000).</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Select Country" is set to Custom.</p>	
Busy	<p>Customizes the busy tone for the system.</p> <p>For more information on how to customize the tone, refer to the parameter "Ring Back".</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Select Country" is set to Custom.</p>	Web User Interface
Call Waiting	<p>Customizes the call waiting tone for the system.</p> <p>For more information on how to customize the tone, refer to the parameter "Ring Back".</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Select Country" is set to Custom.</p>	Web User Interface
Auto Answer	<p>Customizes the auto answer tone for the system.</p> <p>For more information on how to customize the tone, refer to the parameter "Ring Back".</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Select Country" is set to Custom.</p>	Web User Interface

To configure tones via web user interface:

1. Click on **Setting->Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

If you select **Custom**, you can customize the tone for indicating each condition of the system.



The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main navigation bar has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists configuration categories: General, Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, Tones (highlighted), and Wireless Micpod. The main content area displays the 'Tones' configuration page. A red box highlights the 'Select Country' dropdown menu, which is set to 'Custom'. Below it, the 'Ring Back' field is highlighted with a red box. The 'Busy', 'Call Waiting', and 'Auto Answer' fields are also visible.

Field	Value
Select Country	Custom
Ring Back	2000+800+600/500,3000+
Busy	700+1200+400+6000/500(
Call Waiting	400+1200/500,1000+6000
Auto Answer	!800+500+1000+900/6000

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

System Management

This chapter provides operating instructions, such as managing directory, call history and dual screen. Topics include:

- [Local Directory](#)
- [LDAP](#)
- [Call History](#)
- [Search Source List in Dialing](#)
- [Dual Screen](#)

Local Directory

The VC400 system can store up to 500 local contacts and 100 conference contacts. You can add multiple numbers for a contact (at most 3). A conference contact consists of one or more local contacts (at least 1, at most 3).

If multiple numbers are stored for a contact, when adding a conference contact, you can select the desired number of the contact. You can then place a conference call quickly via conference contacts (up to 5 parties, including yourself).

You can import or export the contact list to share the local directory. The system only supports the XML and CSV format contact lists. You can view local directory via web user interface, remote control and the VCP40 phone. But you can edit or delete the local directory via web user interface and remote control.

The following sections give you detailed steps on how to manage the local directory.

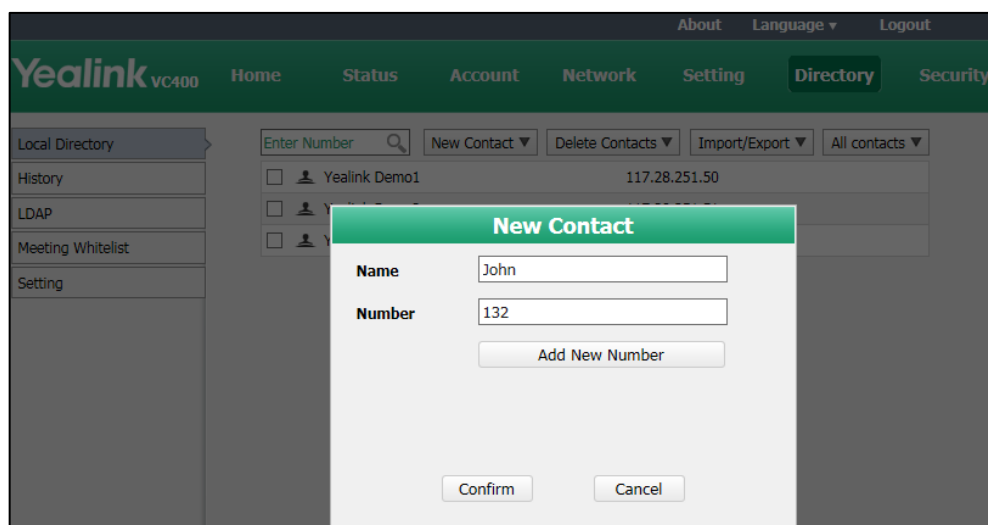
Note

The VC120 video conferencing endpoint only supports local contacts. It does not support conference contacts.

To add local contacts via web user interface:

1. Click on **Directory->Local Directory**.
2. Click **New Contact**, and select **Local**.
3. Enter the desired name in the **Name** field.
4. Enter the desired number in the **Number** field.

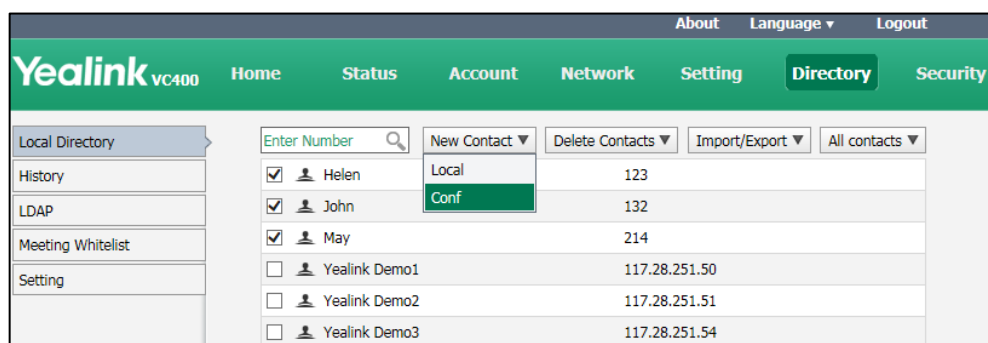
- Click **Add New Number**, enter other number of the contact.



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

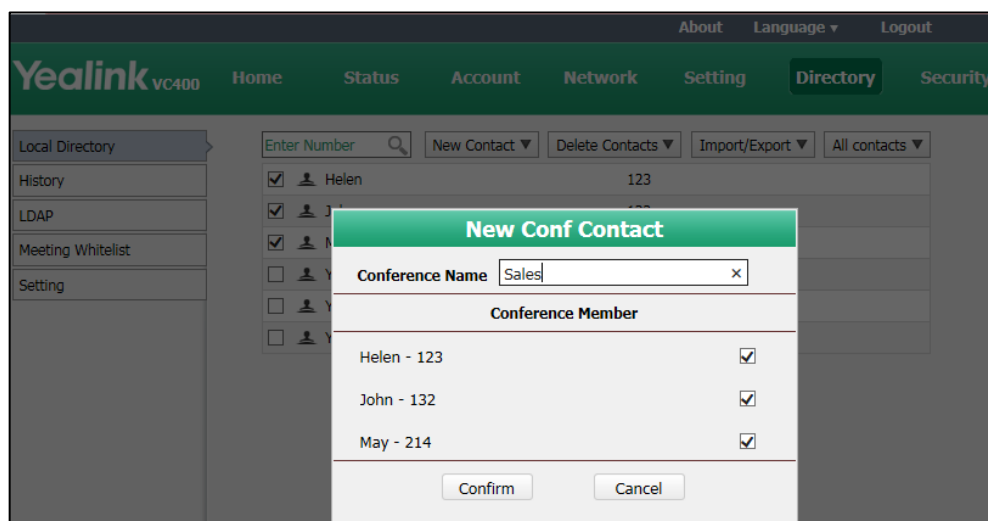
To add conference contacts via web user interface:

- Click on **Directory->Local Directory**.
- Check the checkboxes of the desired contacts.
- Click **New Contact**, and select **Conf**.




- Enter the desired name in the **Conference Name** field.

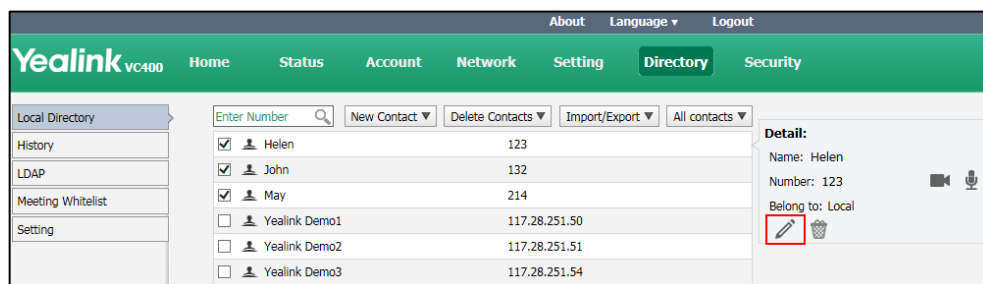
If multiple numbers are stored for the selected contacts, the system will select number 1 by default.



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

To edit contacts via web user interface:

1. Click on **Directory->Local Directory**.
2. Hover your cursor over the contact you want to edit.
3. Click  in the pop-up detail box.

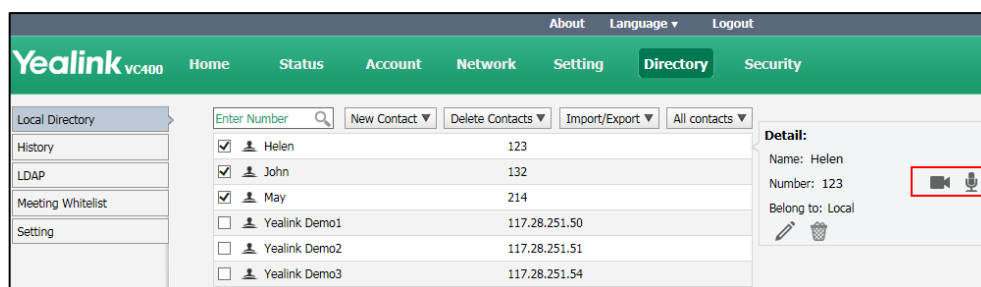


4. Edit the contact information.
5. Click **Confirm** to accept the change.

To place calls to contacts from the local directory via web user interface:

1. Click on **Directory->Local Directory**.
2. Hover your cursor over the desired contact.

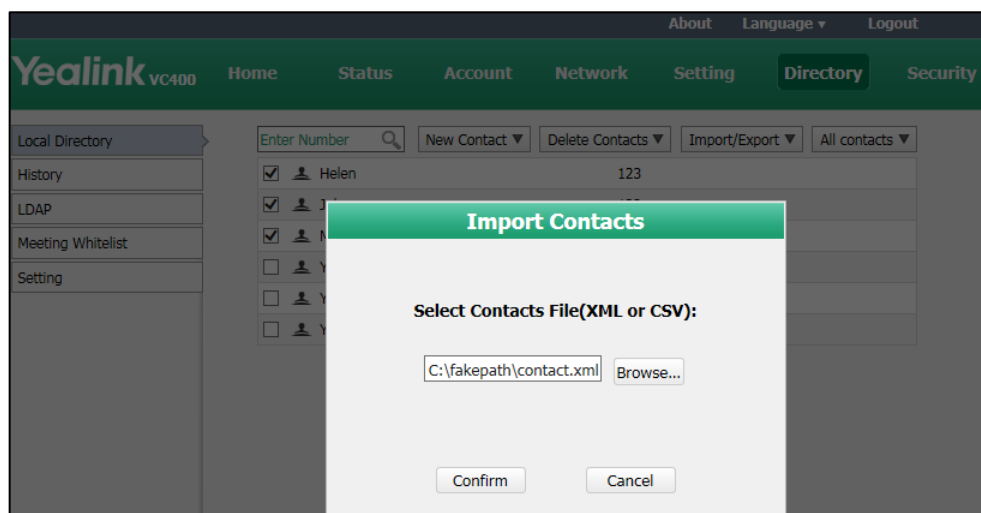
3. Click  or  in the pop-up detail box to place a video or voice call.



The web user interface prompts "Connecting, please wait!" and jumps automatically to the **Home** screen.

To import an XML file of the contact list via web user interface:

1. Click on **Directory->Local Directory**.
2. Click **Import/Export**, and select **Import**.
3. Click **Browse** to locate a contact list file (file format must be *.xml) from your local system.



4. Click **Confirm** to import the contact list.

The web user interface prompts "Contacts imported successfully!".

To import a CSV file of contact list via web user interface:

1. Click on **Directory->Local Directory**.
2. Click **Import/Export**, and select **Import**.
3. Click **Browse** to locate a contact list file (file format must be *.csv) from your local system.
4. Click **Confirm**.

The web user interface is shown below:

Import CSV File Preview

☐ The first line as the title ☐ Delete Old Contacts

	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore
1	display_name	group	number1	number2	number3	
2	Helen	Local	123			
3	John	Local	132			
4	May	Local	214			
5	Yealink Demo1	Local	117.28.251.50	xmdemo1.vcs.yealink.com		
6	Yealink Demo2	Local	117.28.251.51			
7	Yealink Demo3	Local	117.28.251.54			

Confirm Cancel

5. (Optional.) Check the **The first line as the title** checkbox.
It will prevent importing the title of the contact information which is located in the first line of the CSV file.
6. (Optional.) Check the **Delete Old Contacts** checkbox.
It will delete all existing contacts while importing the contact list.
7. Select the desired value from the pull-down list.
 - If **Ignore** is selected, this column will not be imported to the system.
 - If **Display Name** is selected, this column will be imported to the system as the contacts' name.

- If **number1/2/3** is selected, this column will be imported to the system as the contacts' number.

Import CSV File Preview

☒ The first line as the title ☒ Delete Old Contacts

Display Name ▼ Group ▼ number1 ▼ number2 ▼ Ignore ▼ Ignore ▼

	display_name	group	number1	number2	number3
1	Helen	Local	123		
2	John	Local	132		
3	May	Local	214		
4	Yealink Demo1	Local	117.28.251.50	xmdemo1.vcs.yealink.com	
5	Yealink Demo2	Local	117.28.251.51		
6	Yealink Demo3	Local	117.28.251.54		

Confirm Cancel

8. Click **Confirm** to complete importing the contact list.

The web user interface prompts "Contacts imported successfully!".

To export a XML/CSV file of the contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Click **Import/Export**, and select **Export XML** or **Export CSV**.
3. The contact list is saved to your local system.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. Yealink VCS systems are configurable 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 the system. 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 display device screen are read only. They

cannot be added to, edited or deleted by users. When an LDAP server is configured properly, the system 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 retrieve the desired information.

Configurations on the system limit the amount of displayed entries when querying from the LDAP server, and decide how the attributes are displayed and sorted.

Performing a LDAP search on the system:

- Enter search content in the dialing screen. (Ensure that the LDAP is in the enabled search source lists)
- In the **Directory** screen, select **Company** to enter the LDAP search screen, and then enter a few characters which you want to search.

The system will send the search request to the LDAP server, the LDAP server then performs a search based on the entered content and configured filter condition, and returns results to the system.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on the system:

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

LADP parameters are described below:

Parameter	Description	Configuration Method
LDAP Enable	Enables or disables the LDAP feature on the system. Default: Disabled	Web User Interface
LDAP Name Filter	Configures the name attribute for LDAP searching.	Web User Interface

Parameter	Description	Configuration Method
	Example: ((cn=*)(sn=*))	
LDAP Number Filter	Configures the number attribute for LDAP searching. Example: ((telephoneNumber=*)(mobile=*))	Web User Interface
LDAP Server Address	Configures the domain name or IP address of the LDAP server.	Web User Interface
Port	Configures the LDAP server port. Default: 389	Web User Interface
LDAP User Name	Configures the user name used to login the LDAP server. Note: The user name is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user name to access the LDAP server.	Web User Interface
LDAP Password	Configures the password to login the LDAP server. Note: The password is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user password to access the LDAP server.	Web User Interface
LDAP Base	Configures the root path of the LDAP search base. Example: cn=manager,dc=yealink,dc=cn	Web User Interface
Max Hit(1~32000)	Configures the maximum number of search results to be returned by the LDAP server.	Web User Interface
LDAP Name Attributes	Configures the name attributes of each record to be returned by the LDAP server.	Web User Interface

Parameter	Description	Configuration Method
	Note: multiple name attributes should be separated by spaces. Example: cn sn	
LDAP Number Attributes	Configures the number attributes of each record to be returned by the LDAP server. Note: multiple numbers attributes should be separated by spaces. Example: telephoneNumber mobile	Web User Interface
LDAP Display Name	Configures the display name of the contact record displayed on the LCD screen. Note: multiple numbers attributes should be separated by spaces. Example: %cn	Web User Interface
Protocol	Configures the protocol for the LDAP server. Note: Make sure the protocol value corresponds with the version assigned on the LDAP server.	Web User Interface
Match Incoming Call	Enables or disables the system to match caller numbers with LDAP contacts. Default: Disabled	Web User Interface
LDAP Sorting Results	Enables or disables the system to sort the search results in alphabetical order or numerical order. Default: Disabled	Web User Interface

For more information on string representations of LDAP query filters, refer to [RFC2254](#).

To configure LDAP via web user interface:

1. Click on **Directory->LDAP**.
2. Enter the values in the corresponding fields.

3. Select the desired values from the corresponding pull-down lists.

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

Call History

The VC400 video conferencing system maintains call history lists of All Calls, Missed Calls, Placed Calls and Received Calls. Call history lists supports up to 400 entries. You can view the call history, place a call or delete an entry from the call history list. You can view the call history and place a call from the call history list via web user interface or the remote control, but you can delete call history only via web user interface.

History record feature is enabled by default. If it is disabled, the call history won't be saved. For more information, refer to [History Record](#) on page 121.

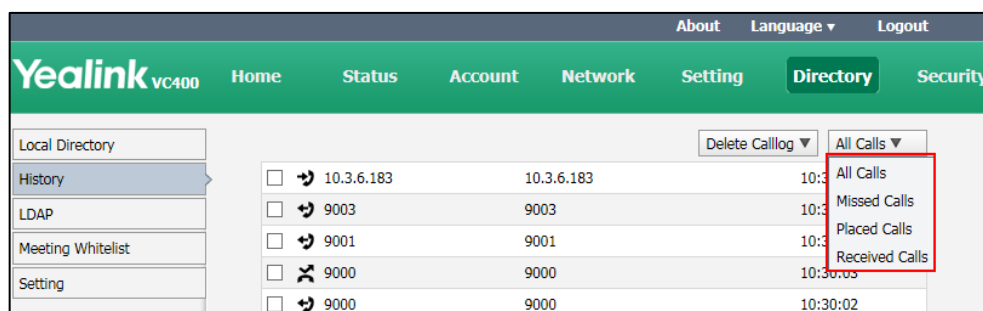
Note

VC120 video conferencing endpoint only supports local call history. It does not support conference call history.

To view call history via web user interface:

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

The web user interface displays all call history.





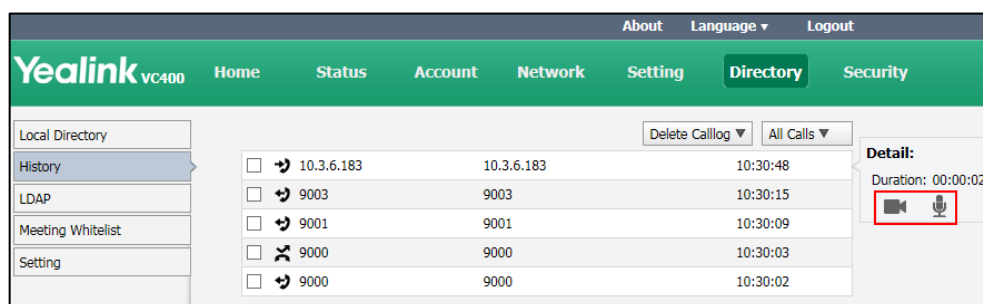
2. Click **All Calls**, select the desired call history list.

To place a call from the call history list via web user interface:

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

The web user interface displays all call history.

2. Hover your cursor over the entry you want to call.
3. Click  or  in the pop-up detail box to place a video or voice call.



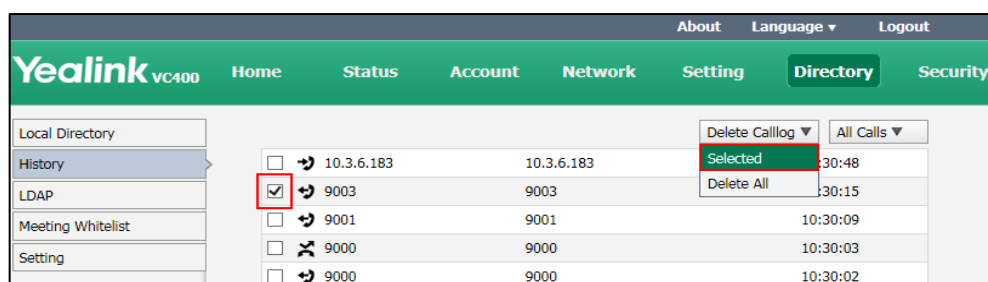
The web user interface prompts "Connecting, please wait!" and jumps automatically to the **Home** screen.

To delete an entry from the call history list via web user interface:

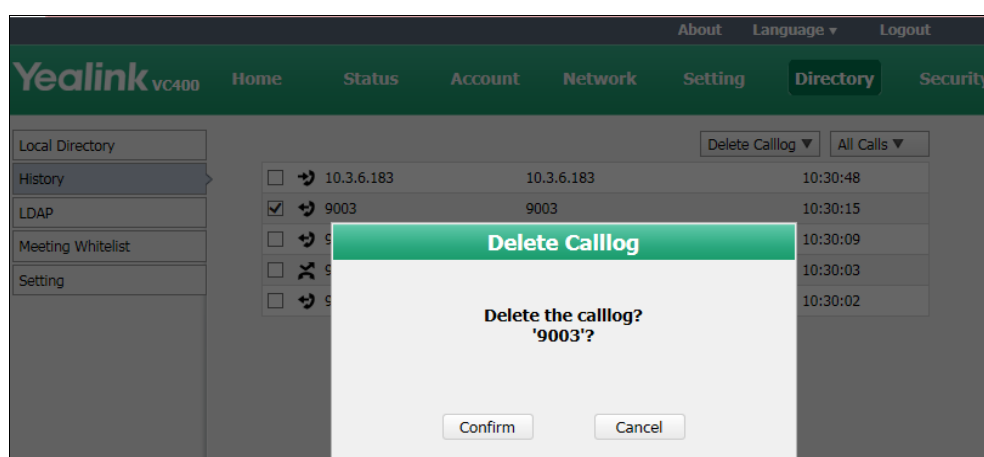
1. Click on **Directory->History**.

The web user interface displays all call history.

2. Mark the checkbox for the entry you want to delete.
3. Click **Delete Callog**, and select **Selected**.



The web user interface prompts "Delete the callog?"



- Click **Confirm** to delete the callog.

You can also select **Delete All** from the pull-down list of **Delete Callog** to delete all call log.

Search Source List in Dialing


When you enter a few characters in the dialing screen, the system will search for contacts from the enabled search source lists, and display the result in the dialing screen. The lists can be Local Directory, History and LDAP.



To match the desired list, you need to enable the search source list first. If you want to match the LDAP list, make sure LDAP is already configured. For more information on how to configure LDAP, refer to [LDAP](#) on page 172.

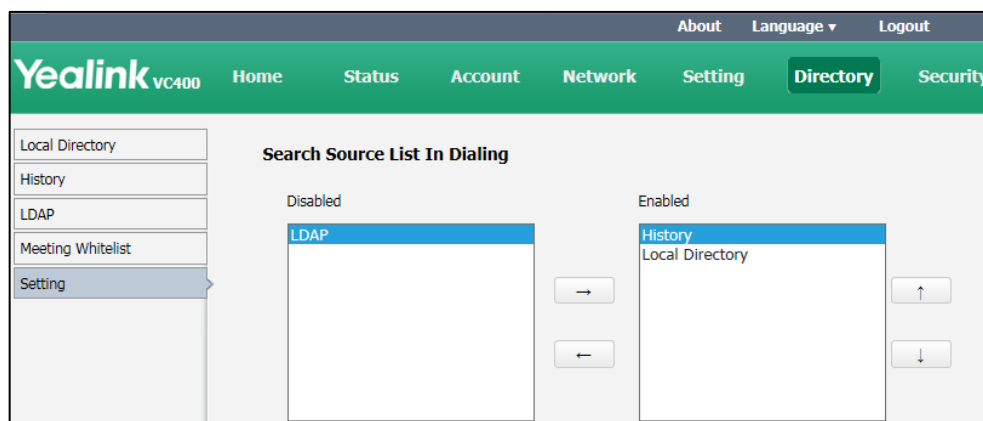
To configure search source list in dialing via web user interface:

- Click on **Directory->Setting**.
- 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.


- Repeat step 2 to add more lists to the **Enabled** column.
- (Optional.) 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.

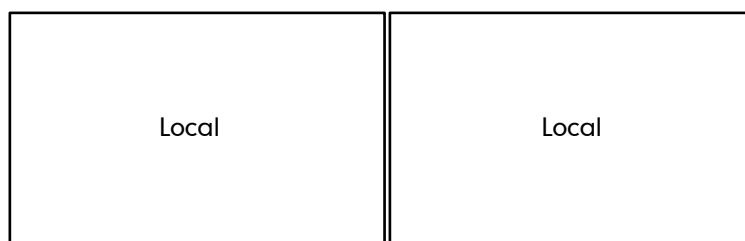
Dual Screen

The VC400/VC120 has two display ports. When connecting only one display device to the VC400/VC120 codec, Display1 port is the only available port. To make it easier for users to view video images, users can connect two display devices to Display1 and Display2 ports respectively. When two display devices are connected to the VC400/VC120 codec, the status bar of the primary display device will display  icon.

VC400 Screen Layout

Two display devices (dual screen) are connected to the VC400 codec:

- When the VC400 is idle and does not start a presentation:
 - In the primary display device, the local video image is shown in full size.
 - In the secondary display device, the local video image is shown in full size (no menu and status bar).

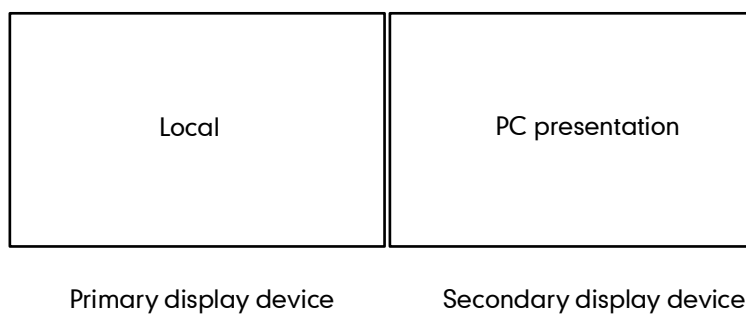


Primary display device

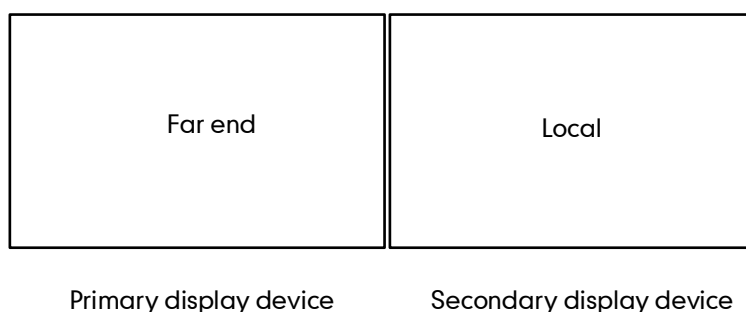
Secondary display device

- When the VC400 is idle and starts a presentation:
 - In the primary display device, the local video image is shown in full size.
 - In the secondary display device, the presentation is shown in full size (no menu and

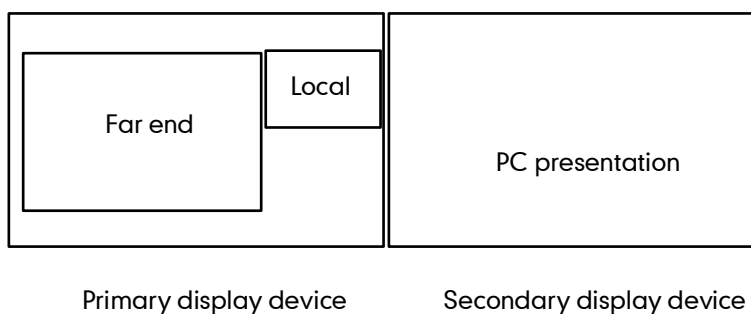
status bar).



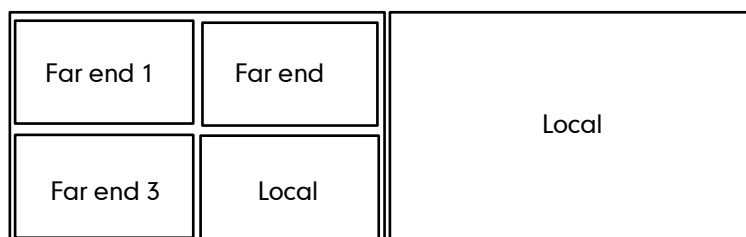
- When the VC400 is during a call and does not start a presentation:
 In the primary display device, the remote video image is shown in full size.
 In the secondary display device, the local video image is shown in full size.



- When the VC400 is during a call and starts a presentation:
 In the primary display device, the remote video image is shown in big size, and the local video image along the right side of the screen is shown in small size.
 In the secondary display device, the presentation is shown in full size.



- When the VC400 is during multiple active calls and does not start a presentation.
 In the primary display device, the video images are shown in the same size.
 In the secondary display device, the local video image is shown in full size.



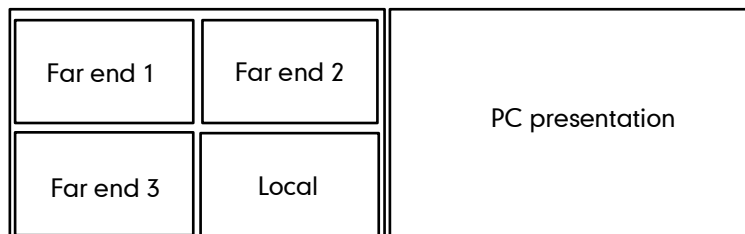
Primary display device

Secondary display device

- When the VC400 is during multiple active calls and starts a presentation.

In the primary display device, the video images are shown in the same size.

In the secondary display device, the presentation is shown in full size.



Primary display device

Secondary display device

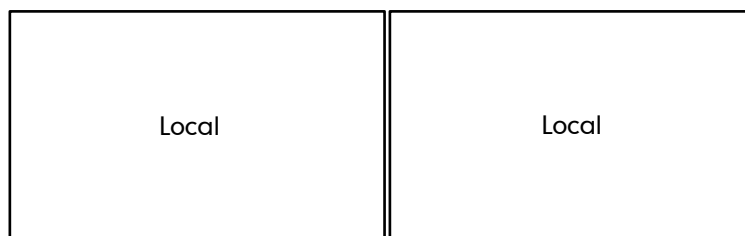
VC120 Screen Layout

Two display devices (dual screen) are connected to the VC120 codec:

- When the VC120 is idle and does not start a presentation.

In the primary display device, the local video image is shown in full size.

In the secondary display device, the local video image is shown in full size (no menu and status bar).



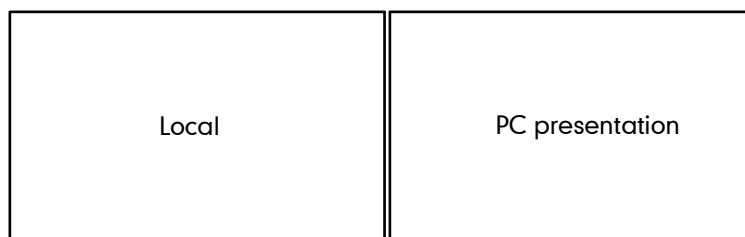
Primary display device

Secondary display device

- When the VC120 is idle and starts a presentation.

In the primary display device, the local video image is shown in full size.

In the secondary display device, the presentation is shown in full size (no menu and status bar).



Primary display device

Secondary display device

- When the VC120 is during a call and does not start a presentation.

In the primary display device, the remote video image is shown in full size.

In the secondary display device, the local video image is shown in full size.



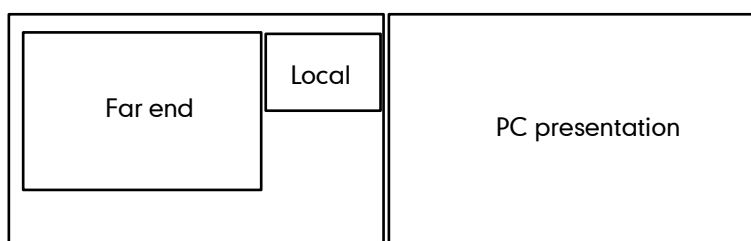
Primary display device

Secondary display device

- When the VC120 is during a call and starts a presentation.

In the primary display device, the remote video image is shown in big size, local video image along the right side of the screen is shown in small size.

In the secondary display device, the presentation is shown in full size.








Primary display device

Secondary display device

You can specify the display content on the secondary display device via the remote control.

To specify the display content on the secondary display device via the remote control:

1. Press the **More** soft key during an active call.
2. Select **Focus (Display2)**, and then press .
3. Press  or  to select the desired content, and then press .

The secondary display device displays the selected content. The  icon is displayed on the focus content.

After reassigning the display content on the secondary display device, the presentation will automatically be displayed on the primary display device.

License

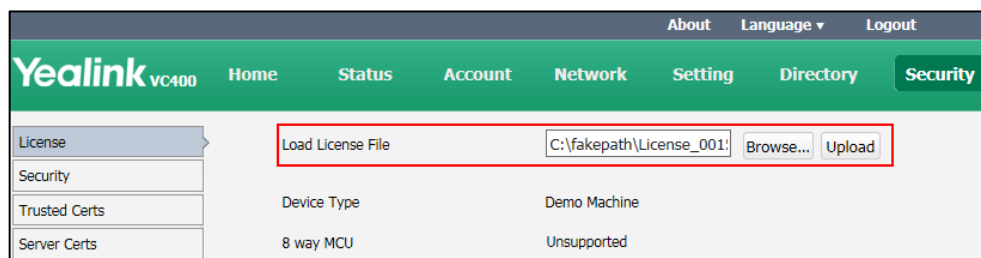
Device Type License

If the VC400/VC120 is a demo machine, namely it is used by agents to demonstrate system functions to the customers. The LCD screen of the system will prompt "DEMO ONLY, NOT FOR RESELL". You can change the VC400/VC120 from a demo machine to be a normal machine by importing a device type license. The device type license is

configurable via web user interface only.

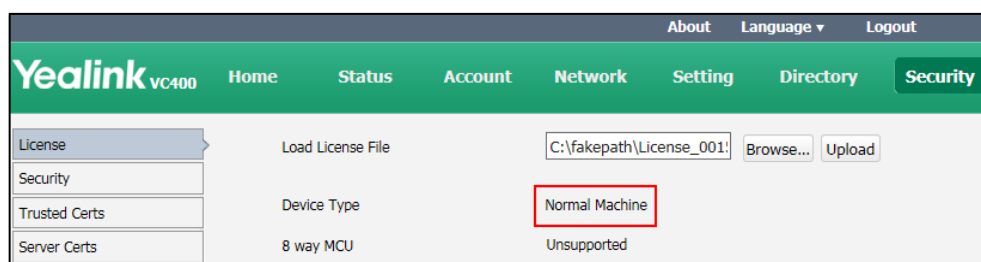
To import the device type license via web user interface:

1. Click on **Security** -> **License**.
2. Click **Browse** to locate the device type license (the file format must be *.dat) from your local system.



3. Click **Upload** to complete importing the device type license.

The device type will change from "Demo Machine" to "Normal Machine".



8-Way Conference License

The basic version of VC400 video conferencing system supports up to 4-way video calls and an additional voice call (an original caller and four other sites). You can import an 8-way conference license to extend the VC400 to support 8-way video calls and an additional voice call (an original caller and eight other sites). 8-way conference license is configurable via web user interface only.

Note

VC120 supports up to 2-way video calls and an additional voice call (an original caller and two other sites). 8-way conference feature is not applicable to VC120.

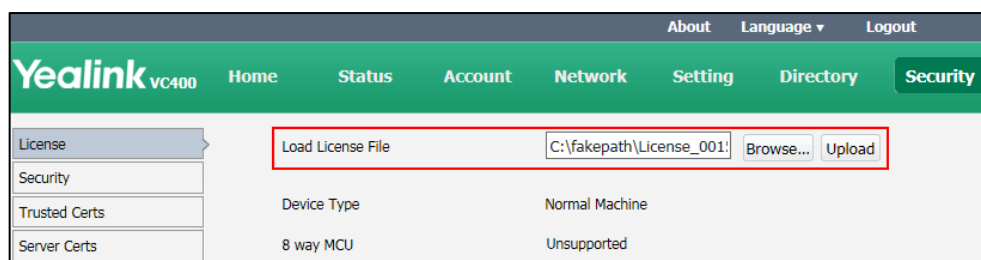
VC400 video conferencing system supports a permanent version of the 8-way conference license and a trial version of the 8-way conference license. They have the same feature.

- **Permanent version of the 8-way conference license:** each VC400 has a unique license. The license cannot be used for other systems. You need to contact Yealink resellers to purchase it, please provide the MAC address of your VC400 when purchasing.

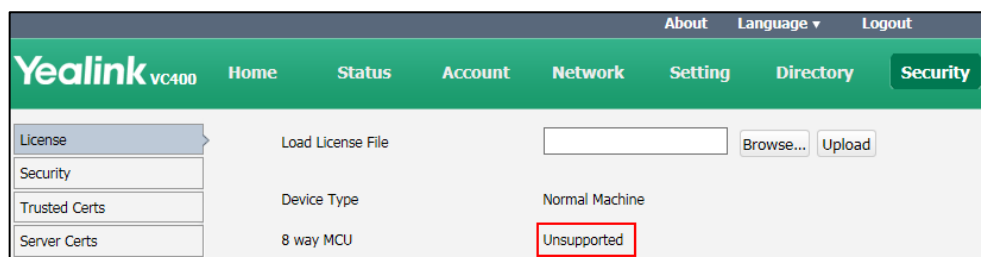
- **Trial version of the 8-way conference license:** VC400 models can share this license. You can download a 30 day trial from Yealink website.

To import the 8-way conference license via web user interface:

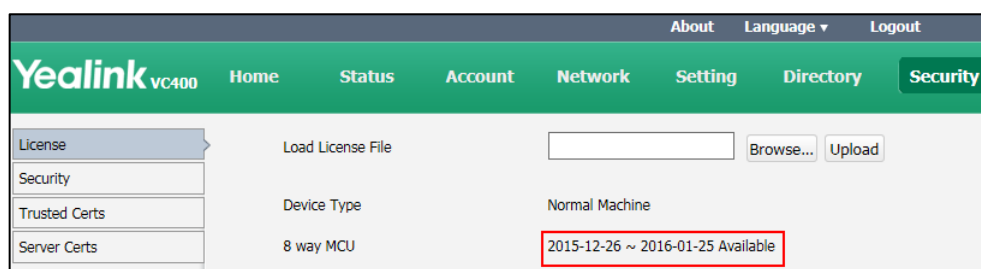
1. Click on **Security** -> **License**.
2. Click **Browse** to locate the 8-way conference license (the file format must be *.dat) from your local system.



3. Click **Upload** to complete importing the 8-way conference license.
 - If the 8 way MCU displays **Unsupported**, it means you have not imported an 8-way conference license. So the system supports 4-way video calls and an additional voice call (an original caller and three other sites).



- If the 8 way MCU displays **X~Y Available**, it means you have imported a trial version of 8-way conference license. So the system supports up to 8-way video calls and an additional voice call (an original caller and eight other sites) in X~Y period. When the trial license expires, your system supports 4-way video calls and an additional voice call (an original caller and three other sites).



- If the 8 way MCU displays **Eternal**, it means you have imported a permanent version of the 8-way conference license. So the system supports up to 8-way video calls and an additional voice call (an original caller and eight other sites) permanently.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. Below this is a green header with 'Yealink VC400' and a menu with 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Security' tab is active. On the left, a sidebar shows 'License', 'Security', 'Trusted Certs', and 'Server Certs'. The main content area has three sections: 'Load License File' with a text input and 'Browse...' and 'Upload' buttons; 'Device Type' set to 'Normal Machine'; and '8 way MCU' with a dropdown menu showing 'Eternal' (highlighted with a red box).

Note

Upgrading the system or performing a factory reset will not affect the imported 8-way license.

If the system has been imported a trial version of the 8-way license and the license has not expired, and you import a permanent version to the system, the permanent version will overwrite the trial version.

If the system has been imported a permanent version of the 8-way license, and you import a trial version to the system, the permanent version will not be overwritten.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- [User Mode](#)
- [Administrator Password](#)
- [Web Server Type](#)
- [Transport Layer Security](#)
- [Secure Real-Time Transport Protocol](#)
- [H.235](#)
- [Attack Defense in Public Network](#)

User Mode

Users can access the system menus directly (except the “Advanced” menu) on the display device. The “Advanced” menu requires administrator credentials. You can enable the user mode to provide two levels of access for the menus. You need to configure a password for the user when the user mode is enabled. Users are prompted to enter the password when accessing the menus (except the “Status” menu). After the user mode is enabled, the user can log into the web user interface of the system with user credentials. The default user name is “user”.

User mode parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. Default: Administrator Note: To enable the user mode, you need to select User for this parameter.	Web User Interface
User Mode	Enables or disables the user mode. Default: Disabled Note: It is only applicable to the user mode. The administrator mode is enabled by default.	Web User Interface
User Password	Configures a password for the user to access the menu options	Web User Interface

Parameter	Description	Configuration Method
	<p>or log into the web user interface.</p> <p>Note: It can only be configured when the user mode is enabled. The system supports ASCII characters 32-126(0x20-0x7E) in passwords. You can leave the password blank.</p>	

To configure user mode via web user interface:

1. Click on **Security->Security**.
2. Select **User** from the pull-down list of **User Type**.
3. Select **Enabled** from the pull-down list of **User Mode**.
4. Configure a password or leave it blank in the **User Password** field.

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

Administrator Password

The default enabled user type is administrator. Users can log into the web user interface and access the "Advanced" menu option with administrator privilege by default. The default administrator password is "0000" and can be only changed by an administrator. For security reasons, the administrator should change the default administrator password as soon as possible. The system supports ASCII characters 32-126(0x20-0x7E) in passwords.

Administrator password parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	<p>Specifies the user type.</p> <p>Default: Administrator</p> <p>Note: To configure a new administrator password, you need to select Administrator for this parameter.</p>	Web User Interface

Parameter	Description	Configuration Method
Old Password	Enters the old administrator password. Note: The default administrator password is "0000".	Remote Control Web User Interface
New Password	Configures a new administrator password. Note: You can leave the password blank.	Remote Control Web User Interface
Confirm Password	Enters the new configured administrator password. Note: The entered password must be the same as the one configured by the parameter "New Password".	Remote Control Web User Interface

To configure administrator password via web user interface:

1. Click on **Security->Security**.
2. Select **Administrator** from the pull-down list of **User Type**.
3. Enter the old administrator password in the **Old Password** field.
4. Enter a new password in the **New Password** field.
5. Enter the new password or leave it blank in the **User Password** field.

The screenshot shows the Yealink VC400 web interface. At the top, there's a navigation bar with 'About', 'Language', and 'Logout'. Below it, a green header contains 'Yealink VC400' and several menu items: 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security' (which is highlighted). On the left, a sidebar lists 'License', 'Security' (highlighted), 'Trusted Certs', and 'Server Certs'. The main content area shows the 'Security' configuration for 'Administrator'. It includes a 'User Type' dropdown set to 'Administrator', and three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a masked password (four dots).

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

To configure administrator password via the remote control:

1. Select **Menu->Advanced** (default password: 0000) -> **Password Reset**.
2. Enter the old password in the **Current Password** field.
3. Configure a new password in the **New Password** and **Confirm Password** fields.
4. Press the **Save** soft key to accept the change.

Web Server Type

Web server type determines the access protocol of the system's web user interface. The system supports 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.

Web server type parameters on the system are described below:

Parameter	Description	Configuration Method
HTTP	Enables or disables the user to access the web user interface of the system using the HTTP protocol. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
HTTP Port	Specifies the HTTP port for the user to access the web user interface of the system. Valid Values: 1-65535 Default: 80 Note: Ensure that the configured port is not used. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
HTTPS	Enables or disables the user to access the web user interface of the system using the HTTPS protocol. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
HTTPS Port	Specifies the HTTPS port for the user to access the web user interface of the system. Valid Values: 1-65535	Web User Interface

Parameter	Description	Configuration Method
	Default: 443 Note: Ensure that the configured port is not used. If you change this parameter, the system will reboot to make the change take effect.	

To configure web server type via web user interface:

1. Click on **Network->Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port in the **HTTP Port** field.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the desired HTTPS port in the **HTTPS Port** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, a sidebar shows 'LAN Configuration' with sub-items: 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is titled 'Network' and contains several configuration sections: 'QoS' (Audio Priority: 60, Video Priority: 34, Data Priority: 63), 'MTU' (Video MTU: 1500), 'SNMP' (Active: Disabled, Port: 161, Trusted Address: empty), 'Web Server' (highlighted with a red box, showing HTTP: Enabled, Port: 80, and HTTPS: Enabled, Port: 443), and '802.1x' (802.1x Mode: Disabled, Identity: empty, MD5 Password: masked).

6. Click **Confirm** to accept the change.
A dialog box pops up to prompt that the settings will take effect after a reboot.
7. Click **Confirm** to reboot the system immediately.

To configure web server type via the remote control:

1. Select **Menu->Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired value from the pull-down list of **Web Server Type**.
3. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing the system 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 system supports 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. The system supports 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 system and TLS server to establish an encrypted communication channel:

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

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: rmsserver (2244), Seq: 1482, Ack: 437, Len: 586

Secure Socket Layer

Step1: The system 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 system sends key session 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.

The system can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for the SIP account, the message of the SIP account will be encrypted after the successful TLS negotiation.

Certificates

The system 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 system requests a TLS connection with a server, the system should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The system has 31 built-in trusted certificates. You can upload up to 10 custom certificates to the system. The format of the

certificates must be *.pem, *.cer, *.crt and *.der. For more information on 31 trusted certificates, refer to [Appendix B: Trusted Certificates](#) on page 235.

- **Server Certificate:** When clients request a TLS connection with the system, the system sends the server certificate to the clients for authentication. The system 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 system. 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 a system (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 system may send a generic certificate for authentication.

The system 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 system accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the system to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

TLS parameters on the system are described below:

Parameter	Description	Configuration Method
Transport	<p>Configures the type of transport protocol for the SIP account.</p> <ul style="list-style-type: none"> • UDP—provides best-effort transport via UDP for the SIP signaling. • TCP—provides reliable transport via TCP for SIP signaling. • TLS—provides secure communication for SIP signaling. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. <p>Default: UDP</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>Note: TLS is available only when the system is registered with a SIP server that supports TLS.</p>	
Only Accept Trusted Certificates	<p>Enables or disables the system to only trust the server certificates in the Trusted Certificates list.</p> <p>Default: Enabled</p> <p>Note: If it is enabled, the system will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the system trust the server.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
Common Name Validation	<p>Enables or disables the system to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.</p> <p>Default: Disabled</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
CA Certificates	<p>Configures the type of certificates in the Trusted Certificates list for the system to authenticate for the TLS connection.</p> <ul style="list-style-type: none"> • Default Certificates • Custom Certificates • All Certificates <p>Default: Default Certificates</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
Upload Trusted Certificate File	Upload the custom CA certificate to the system.	Web User Interface

Parameter	Description	Configuration Method
	Note: A maximum of 10 CA certificates can be uploaded to the system. The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	
Device Certificates	Upload the customized CA certificate to the system. <ul style="list-style-type: none"> • Default Certificates • Custom Certificates Default: Default Certificates Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Upload Server Certificate File	Upload the custom device certificate to the system. Note: Only one device certificate can be uploaded to the system. The device certificate you want to upload must be in *.pem or *.cer format.	Web User Interface

To configure the trusted certificate feature via web user interface:

1. Click on **Security->Trusted Certs**.
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 Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main navigation bar has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The left sidebar shows 'License', 'Security' (selected), 'Trusted Certs', and 'Server Certs'. The main content area displays a table of certificates with columns: Index ID, Issued To, Issued By, Expiration, and Delete. Below the table is a 'Delete' button. A red box highlights the 'Only Accept Trusted Certificates' (Enabled), 'Common Name Validation' (Disabled), and 'CA Certificates' (Default Certificates) settings. Below these settings is the 'Import Trusted Certificates' section with an 'Upload Trusted Certificate File' input, a 'Browse...' button, and an 'Upload' button.

Index ID	Issued To	Issued By	Expiration	Delete
1				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

Only Accept Trusted Certificates: Enabled
Common Name Validation: Disabled
CA Certificates: Default Certificates

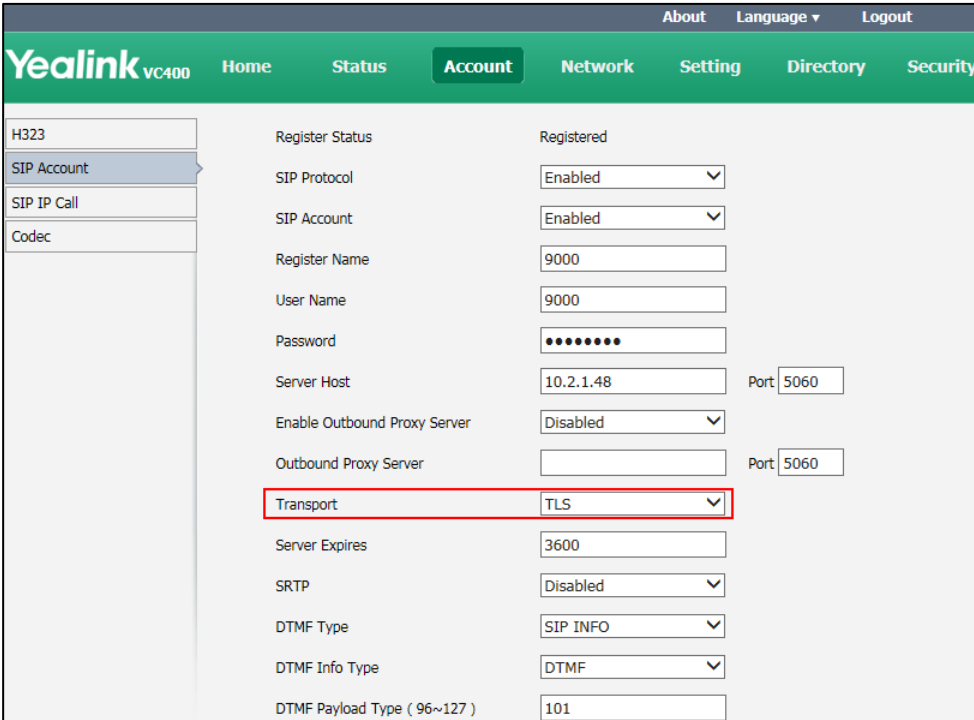
Import Trusted Certificates
Upload Trusted Certificate File:

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

To configure TLS for the SIP account via web user interface:

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

2. Select **TLS** from the pull-down list of the **Transport**.



The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. Below this is a green header with 'Yealink VC400' and a menu with 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'H323', 'SIP Account' (selected), 'SIP IP Call', and 'Codec'. The main content area displays the 'SIP Account' configuration. The 'Register Status' is 'Registered'. The 'SIP Protocol' is 'Enabled'. The 'SIP Account' is 'Enabled'. The 'Register Name' is '9000'. The 'User Name' is '9000'. The 'Password' is masked with dots. The 'Server Host' is '10.2.1.48' and the 'Port' is '5060'. The 'Enable Outbound Proxy Server' is 'Disabled'. The 'Outbound Proxy Server' is empty and the 'Port' is '5060'. The 'Transport' dropdown menu is highlighted with a red box, showing 'TLS' selected. Other settings include 'Server Expires' (3600), 'SRTP' (Disabled), 'DTMF Type' (SIP INFO), 'DTMF Info Type' (DTMF), and 'DTMF Payload Type (96~127)' (101).

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

To upload a CA certificate via web user interface:

1. Click on **Security->Trusted Certs**.

- Click **Browse** to locate the certificate (*.pem, *.cert, *.cer or *.der) from your local system.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The left sidebar shows 'License', 'Security' (selected), 'Trusted Certs', and 'Server Certs'. The main content area displays a table of certificates with columns: Index ID, Issued To, Issued By, Expiration, and Delete. Below the table are three dropdown menus: 'Only Accept Trusted Certificates' (Disabled), 'Common Name Validation' (Disabled), and 'CA Certificates' (Default Certificates). The 'Import Trusted Certificates' section is highlighted with a red box, showing the 'Upload Trusted Certificate File' field with the path 'C:\fakepath\ca.crt' and the 'Browse...' button.

- Click **Upload** to upload the certificate.

To configure the device certificate via web user interface:

- Click on **Security->Server Certs**.
- Select the desired value from the pull-down list of **Device Certificates**.

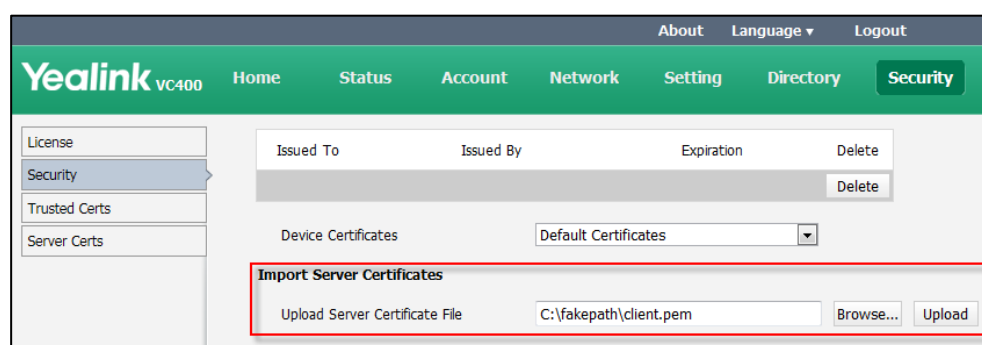
The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The left sidebar shows 'License', 'Security' (selected), 'Trusted Certs', and 'Server Certs'. The main content area displays a table of certificates with columns: Issued To, Issued By, Expiration, and Delete. Below the table is a dropdown menu labeled 'Device Certificates' with the option 'Default Certificates' selected. The 'Import Server Certificates' section is highlighted with a red box, showing the 'Upload Server Certificate File' field and the 'Browse...' button.

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

To upload a device certificate via web user interface:

- Click on **Security->Server Certs**.

- Click **Browse** to locate the certificate (*.pem or *.cer) from your local system.



- Click **Upload** to upload the certificate.

Secure Real-Time Transport Protocol

During a confidential call, you can configure Secure Real-Time Transport Protocol (SRTP) to encrypt RTP streams to avoid interception and eavesdropping. Both RTP and RTCP signaling may be encrypted using an AES algorithm as described in RFC3711.

Encryption modifies the data in the RTP streams so that, if the data is captured or intercepted, it cannot be understood—it sounds like noise. Only the receiver knows the key to restore the data. To use SRTP encryption for SIP calls, the participants in the call must enable SRTP simultaneously. When this feature is enabled on both systems, the encryption algorithm utilized for the session is negotiated between the systems. This negotiation process is compliant with RFC 4568.

When a site places a call on the SRTP enabled system, the system sends an INVITE message with the RTP encryption algorithm to the destination system.

The following is an 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:NzFINTUwZDK2OGVlOTc3YzNkYTkwZWVhMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWVm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWlZGZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
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.

The following is an 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
```

The SRTP parameter on the system is described below:

Parameter	Description	Configuration Method
SRTP	<p>Specifies the SRTP type. You can specify it to the SIP account or SIP direct account separately.</p> <ul style="list-style-type: none"> Disabled—do not use SRTP in SIP calls. Optional—negotiate with the far site whether to use SRTP for media encryption in SIP calls. Compulsory—compulsory use SRTP for media encryption in SIP calls. <p>Default: Disabled</p>	Web User Interface

Rules of SRTP for media encryption in SIP calls:

Far \ Near	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

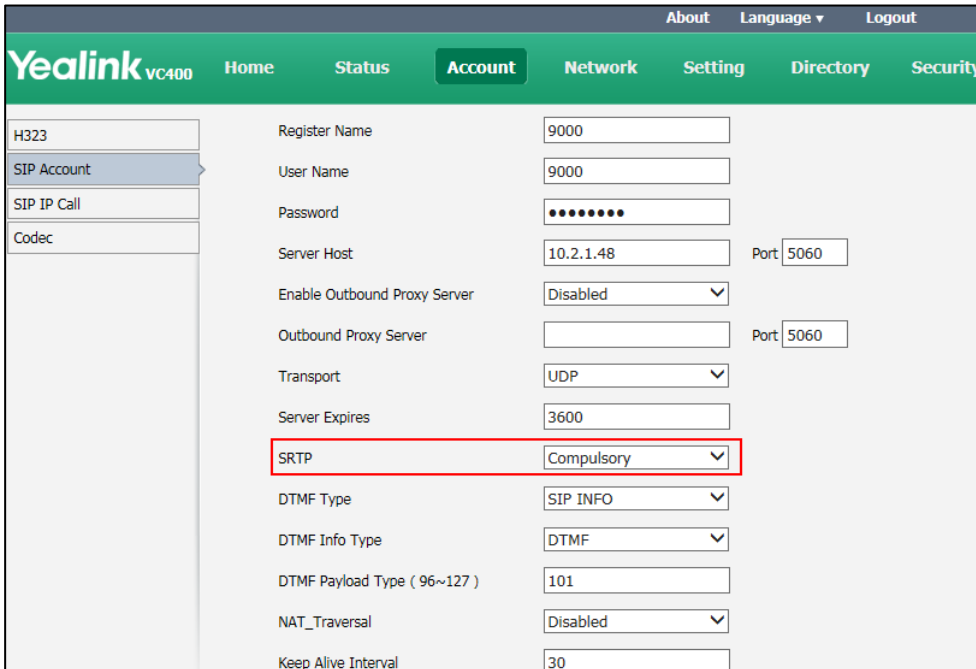
When SRTP is enabled on both systems, RTP streams will be encrypted, and the lock icon  appears on the display device of each system after successful negotiation.

Note

If SRTP is enabled for the SIP account, you should also configure the transport type to TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to [Transport Layer Security](#) on page 192.

To configure SRTP for SIP account via web user interface:

1. Click on **Account->SIP Account**.
2. Select the desired value from the pull-down list of **SRTP**.



The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' section is expanded, showing 'H323', 'SIP Account', 'SIP IP Call', and 'Codec'. The 'SIP Account' configuration page is displayed with the following fields:

Register Name	9000	
User Name	9000	
Password	••••••••	
Server Host	10.2.1.48	Port 5060
Enable Outbound Proxy Server	Disabled	
Outbound Proxy Server		Port 5060
Transport	UDP	
Server Expires	3600	
SRTP	Compulsory	
DTMF Type	SIP INFO	
DTMF Info Type	DTMF	
DTMF Payload Type (96~127)	101	
NAT_Traversal	Disabled	
Keep Alive Interval	30	

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

To configure SRTP for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.

2. Select the desired value from the pull-down list of **SRTP**.

The screenshot shows the Yealink VC400 web interface. The 'Account' tab is selected in the top navigation bar. On the left sidebar, 'SIP IP Call' is highlighted. The main content area displays various SIP settings. The 'SRTP' dropdown menu is highlighted with a red rectangle, and it shows 'Compulsory' as the selected value. Other settings include Transport (TCP), DTMF Type (SIP INFO), DTMF Info Type (DTMF), DTMF Payload Type (101), NAT Traversal (Disabled), RPort (Enabled), BFCP (Enabled), and FECC(SIP) (Enabled).

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

H.235

Yealink video conferencing systems support H.235 128-bit AES algorithm using the Diffie-Hellman key exchange protocol in H.323 calls. To use H.235 feature for H.323 calls, the participants in the call must enable the H.235 feature simultaneously. When a site places a call on the H.235 feature enabled system, the system negotiates the encryption algorithm with the destination system.


The H.235 parameter on the system is described below:

Parameter	Description	Configuration Method
H.235 Encryption	<p>Specifies the H.235 type for the H.323 calls.</p> <ul style="list-style-type: none"> Disabled—do not use H.235 in H.323 calls. Optional—negotiate with the far site whether to use H.235 in H.323 calls. Compulsory—compulsively use H.235 in H.323 calls. <p>Default: Disabled</p>	Web User Interface

Rules of H.235 security in H.323 calls:

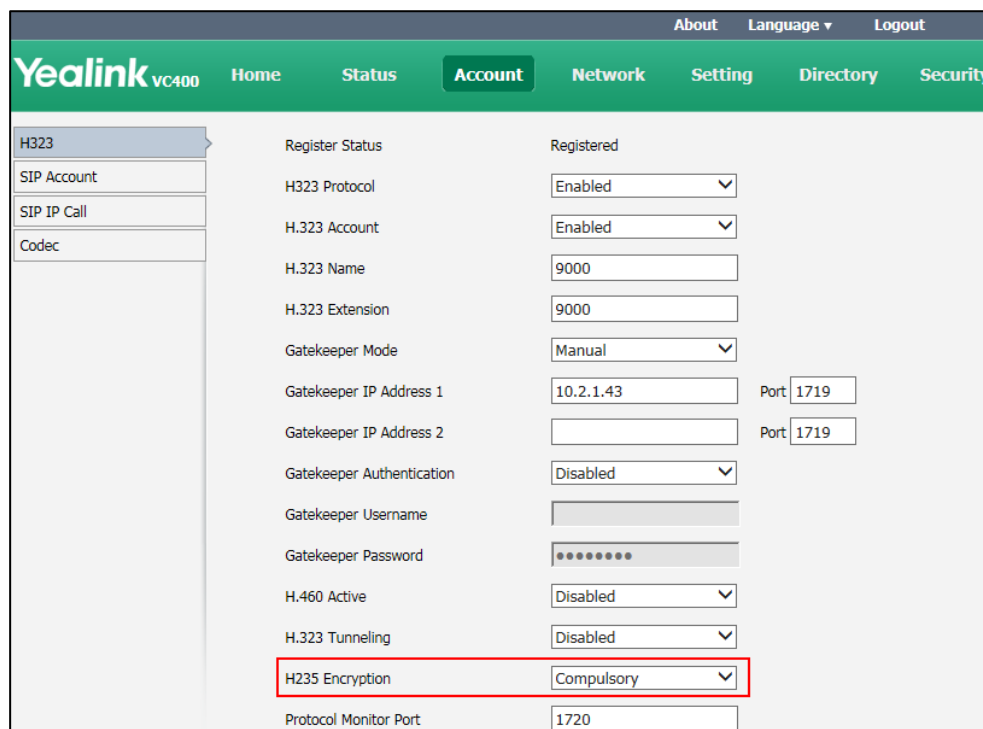
Far \ Near	Compulsory	Optional	Disabled
Compulsory	Encrypted Call	H.235 Call	Fail to establish call
Optional	H.235 Call	H.235 Call	Unencrypted Call

Far \ Near	Compulsory	Optional	Disabled
Disabled	Fail to establish a call	RTP Call	RTP Call

When H.235 is enabled on both systems, calls will be encrypted, and the lock icon  appears on the display device of each system during a call.

To configure H.235 via web user interface:

1. Click on **Account->H323**.
2. Select the desired value from the pull-down list of **H.235 Encryption**.



The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main navigation bar has 'Home', 'Status', 'Account' (selected), 'Network', 'Setting', 'Directory', and 'Security'. The left sidebar shows 'H323' selected, with sub-items 'SIP Account', 'SIP IP Call', and 'Codec'. The main content area displays the H323 configuration page. The 'H.235 Encryption' dropdown menu is highlighted with a red box and set to 'Compulsory'. Other settings include 'Register Status' (Registered), 'H323 Protocol' (Enabled), 'H.323 Account' (Enabled), 'H.323 Name' (9000), 'H.323 Extension' (9000), 'Gatekeeper Mode' (Manual), 'Gatekeeper IP Address 1' (10.2.1.43), 'Gatekeeper IP Address 2' (empty), 'Gatekeeper Authentication' (Disabled), 'Gatekeeper Username' (empty), 'Gatekeeper Password' (masked), 'H.460 Active' (Disabled), 'H.323 Tunneling' (Disabled), and 'Protocol Monitor Port' (1720).

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

Attack Defense in Public Network

VoIP phones often suffer from network attacks in public network, which results in communication failure. To ensure the safety of the enterprise VoIP phone, you can configure abnormal call answering feature for handling abnormal calls using the SIP protocol. For abnormal calls using the H.323 protocol, you can configure safe mode call feature to handle them.

Abnormal Call Answering

The abnormal call answering parameters on the system are described below:

Parameter	Description	Configuration Method
Abnormal call answering	<p>Specifies the account type for answering SIP incoming call</p> <p>Specifies the account type for answering SIP incoming call from public network.</p> <ul style="list-style-type: none"> • Disabled—reject the SIP incoming call from public network. • Account Answer—use first SIP account to answer the SIP incoming call from public network. • IP Call Answer—use IP to answer the SIP incoming call from public network. <p>Default: IP Call Answer</p>	Web User Interface

To configure abnormal call answering via web user interface:

1. Click on **Setting->Call Features**.

2. Select the desired value from the pull-down list of **Abnormal call answering**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features (highlighted), Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area displays the 'Call Features' settings. A list of parameters is shown with their current values and dropdown menus. The 'Abnormal call answering' parameter is highlighted with a red rectangle, and its dropdown menu is open, showing 'IP Call Answer' as the selected option. Other parameters include DND (Disabled), Auto Answer (Enabled), Auto Answer Mute (Enabled), Auto Answer Multiway (Disabled), Call Match (Enabled), History Record (Enabled), Call Protocol (Auto), Uplink Bandwidth (Auto), Downlink Bandwidth (Auto), Safe mode call (Disabled), Ringback Timeout(30-240) (200), Auto Refuse Timeout(30-240) (120), and URI Call Mode (SIP IP Call).

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

Configuring Safe Mode Call

You can configure safe mode call feature to handle abnormal H.323 calls.

The safe mode call parameters on the system are described below:

Parameter	Description	Configuration Method
Safe mode call	<p>Enables or disables the safe mode call feature for H.323 incoming call from public network.</p> <ul style="list-style-type: none"> Disabled—do not use safe mode call. Enabled—use safe mode call. <p>Default: Enabled</p> <p>Note: If it is enabled, the system will reject H.323 incoming call from public network. If it is disabled, any H.323 incoming call from public network can be accepted.</p>	Web User Interface

To configure safe mode call via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **Safe mode call**.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main navigation bar has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists configuration categories: General, Date&Time, Call Features (highlighted), Video & Audio, Camera, Configuration, Upgrade, Tones, and Wireless Micpod. The main content area displays various settings with their current values in dropdown menus:

Setting	Value
DND	Disabled
Auto Answer	Enabled
Auto Answer Mute	Enabled
Auto Answer Multiway	Disabled
Call Match	Enabled
History Record	Enabled
Call Protocol	Auto
Uplink Bandwidth	Auto
Downlink Bandwidth	Auto
Abnormal call answering	IP Call Answer
Safe mode call	Enabled
Ringback Timeout(30-240)	200
Auto Refuse Timeout(30-240)	120
URI Call Mode	SIP IP Call

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

System Maintenance

This chapter provides basic system maintenance, including upgrading firmware, managing configurations, resetting systems and how to monitor network via SNMP. Topics include:

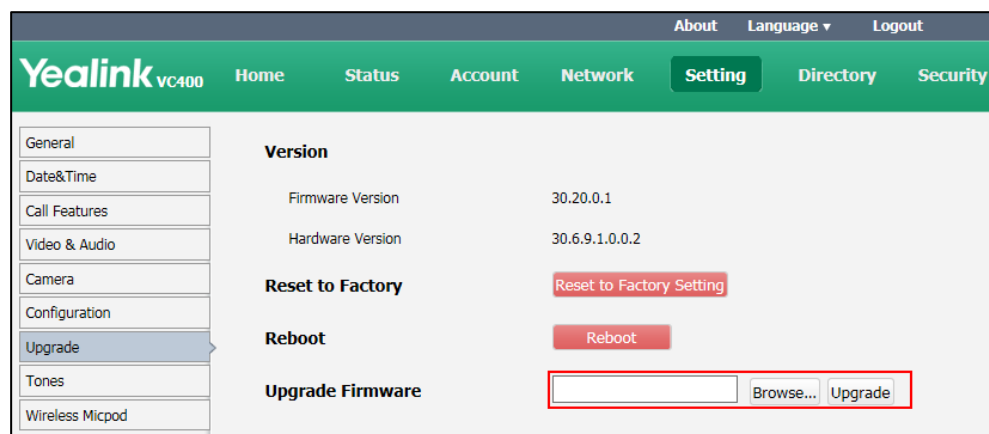
- [Upgrading Firmware](#)
- [Importing/Exporting Configuration](#)
- [Resetting to Factory](#)
- [SNMP](#)

Upgrading Firmware

The newly released firmware version may add new features. Because of this, Yealink recommends you to update the latest firmware. You can upgrade the system firmware via web user interface. The firmware name of the VC400 video conferencing system is: 30.x.x.x.rom (x is the actual firmware version), the firmware name of the VC120 video conferencing endpoint is: 40.x.x.x.rom (x is the actual firmware version). You can download the latest firmware version from the Yealink website.

To upgrade firmware via web user interface:

1. Click on **Setting->Upgrade**.
2. Click **Browse** to locate the firmware from your local system.



3. Click **Upgrade** to upgrade the firmware.

The browser pops up the dialog box "Firmware of the video conference system will be updated. It will take 5 minutes to complete. Please don't power off!".

- Click **Confirm** to confirm upgrading.

Note

Caution! Don't remove the Ethernet cable and power cord during the upgrade process. Don't close or refresh the web page when upgrading the firmware via web user interface.

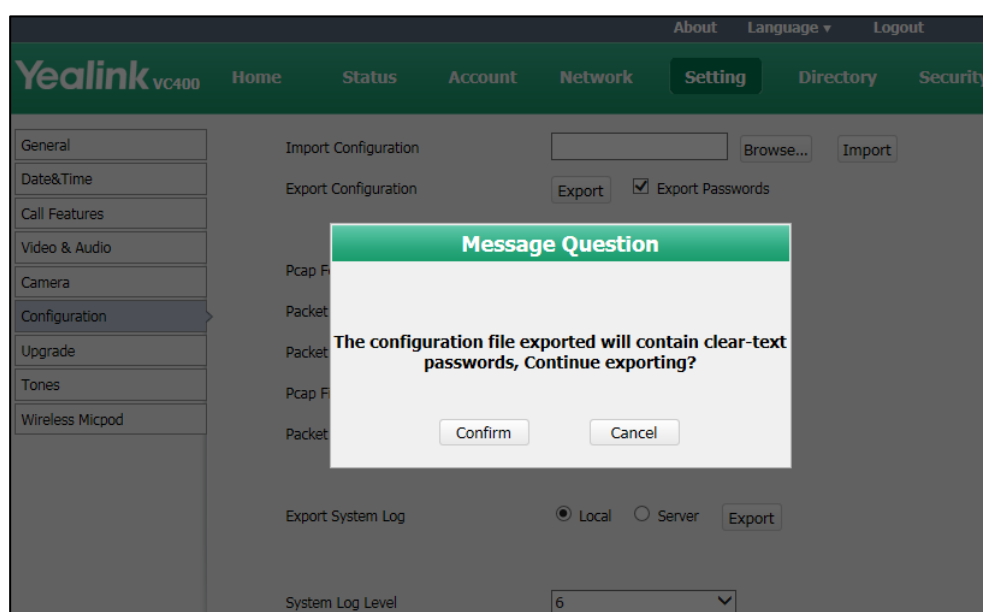
Importing/Exporting Configuration

We may need you to provide the system configurations for the Yealink field application engineers to help analyze problems. You can import configurations to your system to configure your system quickly. The file format of configuration file must be *.bin.

To export the system configurations via web user interface:

- Click on **Setting->Configuration**.
- Check or uncheck the **Export Passwords** checkbox according to actual demand.
- Click **Export**.

If you check the **Export Passwords** checkbox, the web user interface is shown below:



- Click **Confirm** to export the configurations.

To import the phone configurations via web user interface:

- Click on **Setting->Configuration**.
- Click **Browse** to locate a configuration file from your local system.
- Click **Import** to import the configuration file.

Resetting to Factory

Reset the system to factory configurations after you have tried all appropriate troubleshooting suggestions but still have not solved your problems.

When factory resetting the video system, the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.
- All system parameters will be reset to default values.
- All custom files will be deleted. Such as, certificates, local contacts and registered accounts.

It is not possible to undo a factory reset. But you can export the configuration first, and then you can re-import the configuration to recovery the system after the reset.

You can reset the system via the reset key on the VC400/VC120 codec, remote control or web user interface.

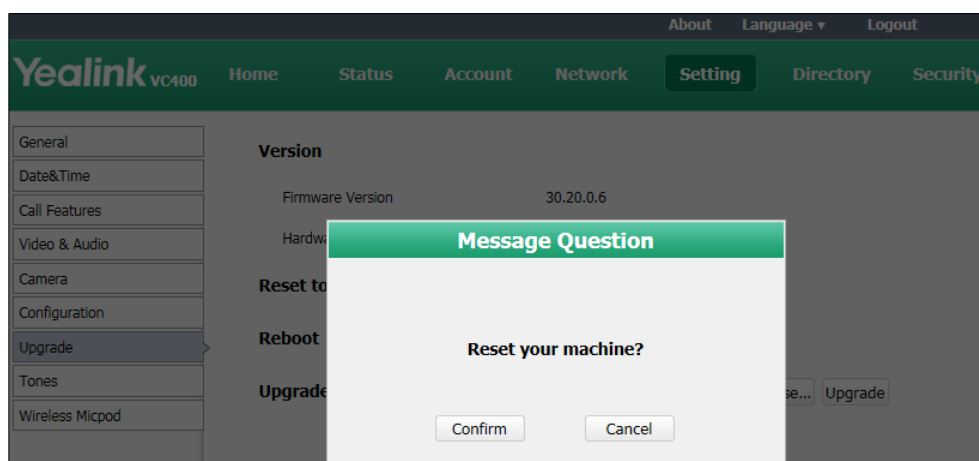
Note

Reset of the system may take a few minutes. Do not power off until the phone starts up successfully.

To reset the system via web user interface:

1. Click on **Setting->Upgrade**.
2. Click **Reset to Factory Setting** in the **Reset to Factory** field.

The web user interface prompts the message "Reset your machine?".



3. Click **Confirm** to confirm the resetting.

To reset the system via the remote control:

1. Select **Menu ->Advanced** (default password: 0000)->**Reboot & Reset**
2. Select **Reset**, and then press **OK**.

The display device prompts "Reset to Factory?".

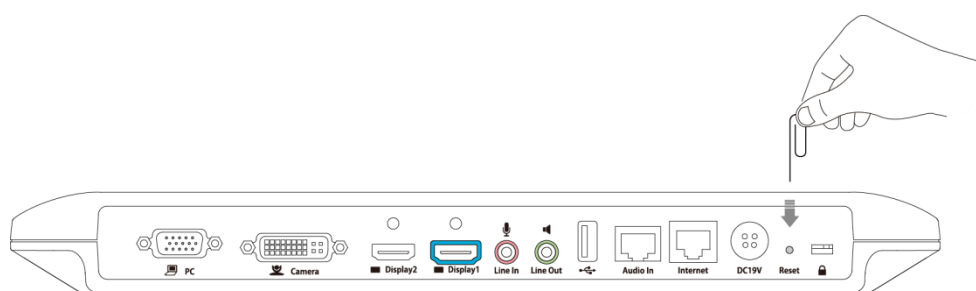
3. Select **OK**, and then press .

The system reboots automatically. The system will reset to factory successfully after startup.

To reset the system via the reset key on the VC400/VC120 codec:

Using tiny objects (for example, the paper clip) to press and hold the reset button for 15 seconds until the screen turns black.

Do not power off the system during the factory restore process. The system reverts to the default factory settings and restarts automatically. This will take a few minutes.



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. These variables can then be queried (and sometimes set) by managing applications. The variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs).

Yealink systems 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. Yealink systems only support the GET request from the SNMP server.

You can download SNMP application to monitor and manage information on a network entity.

The following table lists the basic object identifiers (OIDs) supported by the system.

MIB	OID	Description
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.1.0	The textual identification of the contact person for the system, together with the contact information.

MIB	OID	Description
		For example, Sysadmin (root@localhost)
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.2.0	An administratively-assigned name for the system. If the name is unknown, the value is a zero-length string. For example, Yealink VCS.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.3.0	The physical location of the system. For example, Server Room
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 system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.6.0	The hardware version of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.7.0	The system's model.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.8.0	The MAC address of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.9.0	The IP address of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.10.0	The target version to which the current version is updated automatically. 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 the system reboot. Format: snmpset -v 2c XXXX public 37459.2.1.11.0 s reboot XXXX refers to the IP address of the system.

SNMP parameters on the system are described below:

Parameter	Description	Configuration Method
SNMP->Active	Enables or disables SNMP	Web User Interface

Parameter	Description	Configuration Method
	feature on the system. Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	
Port	Specifies the SNMP port. Valid Values: 1-65535 Default: 161 Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Trusted Address	Configures IP address(es) or domain name of the trusted SNMP server. Multiple IP addresses or domain names should be separated by spaces. Note: If it is left blank, the system accepts and handles GET requests from any SNMP server. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

To configure SNMP via web user interface:

1. Click on **Network->Advanced**.
2. In the **SNMP** block, select **Enabled** from the pull-down list of **Active**.
3. Enter the SNMP port in the **Port** field.
4. Enter the IP address or domain name of the SNMP server in the **Trusted Address** field.

Multiple IP addresses or domain names should be separated by spaces.

The screenshot shows the Yealink VC400 Network Configuration interface. The 'Advanced' tab is selected in the left sidebar. The 'SNMP' section is highlighted with a red box, showing the following settings:

Section	Parameter	Value
SNMP	Active	Enabled
	Port	161
	Trusted Address	192.168.10.50 192.168.1.3
QoS	Audio Priority	60
	Video Priority	34
	Data Priority	63
MTU	Video MTU	1500
Web Server	HTTP	Enabled
	HTTP Port	80
	HTTPS	Enabled
	HTTPS Port	443
802.1x	802.1x Mode	Disabled
	Identity	
	MD5 Password	
	CA Certificates	

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

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using the VC400/VC120 video conferencing system.

Troubleshooting Methods

The system can provide feedback in a variety of forms, such as log files, packets, status indicators and so on, which can help an administrator to find the system problem more easily and resolve it.

The following sections will help you to better understand and resolve the working status of the system.

- [Viewing Log Files](#)
- [Capturing Packets](#)
- [Getting Information from Status Indicators](#)
- [Analyzing Configuration Files](#)
- [Viewing Call Statistics](#)
- [Using Diagnostic Methods](#)

Viewing Log Files

The log files are Yealink specific debug files which may be requested by the Yealink support organization if you need technical support. The current log files are time stamped event log files. You can export the log files to a syslog server or the local system. The administrator can specify the location where the log will be exported to and the severity level of the log.

System Log Level specifies the log level to be recorded. The default system log level is 6.

System log level parameters are described below:

Parameter	Description	Configuration Method
Export System Log	Specify where the system log will be exported. Valid values: <ul style="list-style-type: none">• Local-export the system log	Web User Interface

Parameter	Description	Configuration Method
	<p>to the local computer.</p> <ul style="list-style-type: none"> Server-export the system log to the specified server. <p>Default: Local</p>	
Server Name	<p>Specify the server address where the log will be exported.</p> <p>Note: It only works if the parameter "Export System Log" is set to Server.</p>	Web User Interface
System Log Level	<p>Specify the system log level.</p> <p>Note: The supported level is 0-9. Higher value indicates more detailed content.</p> <p>Default: 6</p>	Web User Interface

To configure the system log level via web user interface:

1. Click on **Setting->Configuration**.
2. Select the desired level from the pull-down list of **System Log Level**.

The screenshot shows the Yealink VC400 web user interface. The top navigation bar includes links for About, Language, and Logout. The main menu has tabs for Home, Status, Account, Network, Setting (selected), Directory, and Security. On the left, a sidebar lists various configuration categories: General, Date&Time, Call Features, Video & Audio, Camera, Configuration (selected), Upgrade, Tones, and Wireless Micpod. The main content area displays the Configuration page with various settings. At the bottom, the 'System Log Level' is highlighted with a red box, showing a dropdown menu with the value '6' selected.

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

To export a log file to the local system via web user interface:

1. Click on **Setting->Configuration**.

2. Mark the **Local** radio box in the **Export System Log** field.

The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (selected), 'Directory', and 'Security'. On the left, a sidebar lists various settings: General, Date&Time, Call Features, Video & Audio, Camera, Configuration (selected), Upgrade, Tones, and Wireless Micpod. The main content area is divided into sections: 'Import Configuration' with a 'Browse...' button and an 'Import' button; 'Export Configuration' with an 'Export' button and an 'Export Passwords' checkbox; 'Pcap Feature' with 'Start', 'Stop', and 'Export' buttons; 'Packet Capture Count' with a value of 5; 'Packet Capture Clip Bytes' with a value of 1024; 'Pcap Filter Type' with a dropdown set to 'Custom'; and 'Packet Filter String' with an empty text field. At the bottom, the 'Export System Log' section is highlighted with a red box, showing the 'Local' radio button selected and the 'Export' button. Below this, the 'System Log Level' is set to 6.

3. Click **Export** to open the file download window, and then save the file to your local system.

The following figure shows a portion of a log file:

```

496 root      8876 SW  /yealink/bin/ggsvca_ipp
497 root      8876 SW  /yealink/bin/ggsvca_ipp
498 root      8876 SW  /yealink/bin/ggsvca_ipp
499 root      8876 SW  /yealink/bin/ggsvca_ipp
500 root      8876 SW  /yealink/bin/ggsvca_ipp
501 root      8876 SW  /yealink/bin/ggsvca_ipp
507 root      16424 SW  /yealink/bin/Screen.exe
508 root      10344 SW  /yealink/bin/sipServer.exe
509 root      10344 SW  /yealink/bin/sipServer.exe
515 root      16424 SW  /yealink/bin/Screen.exe
517 root      16424 SW  /yealink/bin/Screen.exe
519 root      10344 SW  /yealink/bin/sipServer.exe
521 root      16424 SW  /yealink/bin/Screen.exe
522 root      16424 SW  /yealink/bin/Screen.exe
523 root      16424 SW  /yealink/bin/Screen.exe
524 root      10344 SW  /yealink/bin/sipServer.exe
525 root      SW< [IRQ 45]
526 root      10344 SW  /yealink/bin/sipServer.exe
527 root      16424 SW  /yealink/bin/Screen.exe
528 root      16424 SW  /yealink/bin/Screen.exe
529 root      16424 SW  /yealink/bin/Screen.exe
1147 root     1788 SWN  sleep 1000
1227 root     10120 SWN  ConfigManApp.com
1228 root     4624 SW  /yealink/bin/mini_httpd -p 80 -d /yealink/html -c cgi
1229 root     2812 SWN  sh -c cd /tmp;ifconfig >> Messages.ps >> Messages.tar
1230 root     2812 SWN  ps
Feb 29 06:01:09 mini_httpd[388]: mini_httpd.c(1510):child process 1227 exit!
Feb 29 06:01:12 mini_httpd[1232]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1232 exit!
Feb 29 06:01:12 mini_httpd[1233]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1233 exit!
Feb 29 06:01:12 mini_httpd[1234]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1234 exit!

```

To export a log file to a syslog server via web user interface:

1. Click on **Setting->Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.

- Enter the IP address or domain name of the syslog server in the **Server Name** field.

The screenshot shows the Yealink VC400 web interface. The 'Configuration' menu item is selected in the left sidebar. The 'Export System Log' section is highlighted with a red box. It contains the following fields and controls:

- Export System Log:** Two radio buttons, 'Local' and 'Server'. The 'Server' radio button is selected.
- Server Name:** A text input field containing the value '10.3.6.103'.
- Export:** A button next to the radio buttons.
- System Log Level:** A dropdown menu set to '6'.

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

- Click **Confirm** to reboot the system immediately.

Capturing Packets

The administrator can capture packets in two ways: capturing the packets via web user interface or using the Ethernet software. Engineers can analyze the packets to troubleshoot problems.

Packets parameters are described below:

Parameter	Description	Configuration Method
Pcap Feature	Start and stop capturing packets or export the captured packets.	Web User Interface
Packet Capture Count	Configures the count of the number of packets to capture. Default: 5	Web User Interface
Packet Capture Clip Bytes	Configures the maximum size (in KB) of every packet to capture. Default: 1024	Web User Interface
Pcap Filter Type	Configures the filter type of the packet to capture. Valid Values: <ul style="list-style-type: none"> Custom—Customize the 	Web User Interface

Parameter	Description	Configuration Method
	<p>packet filter string.</p> <ul style="list-style-type: none"> • SIP or H245 or H225—Capture SIP, H245 and H225 packets. It depends on the supportive protocol of the system. • RTP—Capture RTP packets. <p>Default: SIP or H245 or H225</p>	
Packet Filter String	<p>Customizes the packet filter string.</p> <p>Syntax: Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression</p> <p>Protocol: Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used.</p> <p>Direction: Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2".</p> <p>Host(s): Values: net, port, host, portrange. If no host(s) is specified, the "host" keyword is used. For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1".</p> <p>Logical Operations: Values: not, and, or. Negation ("not") has highest</p>	Web User Interface

Parameter	Description	Configuration Method
	<p>precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right.</p> <p>For example:</p> <p>"not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23".</p> <p>"not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)".</p> <p>Example: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8</p> <p>Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8.</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Pcap Filter Type" is set to Custom.</p>	

To capture packets via web user interface:

1. Click on **Setting->Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.
If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Click **Start** to start capturing signal traffic.
6. Reproduce the issue to get stack traces.
7. Click **Stop** to stop capturing.

8. Click **Export** to open the file download window, and then save the file to your local system.

The screenshot shows the Yealink VC400 web interface. The left sidebar contains a menu with options: General, Date&Time, Call Features, Video & Audio, Camera, Configuration (highlighted), Upgrade, Tones, and Wireless Micpod. The main content area is titled 'Setting' and includes sections for Import/Export Configuration, Pcap Feature, Export System Log, and System Log Level. The 'Pcap Feature' section is highlighted with a red box and contains the following fields:

- Pcap Feature: Start, Stop, Export buttons
- Packet Capture Count: 5
- Packet Capture Clip Bytes: 1024
- Pcap Filter Type: Custom (dropdown)
- Packet Filter String: (text input)

Below the red box, the 'Export System Log' section has radio buttons for 'Local' (selected) and 'Server', and an 'Export' button. The 'System Log Level' is set to 6.


To capture packets using the Ethernet software:

Connect the Internet ports of the system and the PC to the same hub, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic. You can also set mirror port on a switch to monitor the port connected to the system.

Getting Information from Status Indicators

In some instances, status indicators are helpful for finding system troubles. Status indicators may consist of the power LED, icons on the status bar of the display device or prompt messages.

The following shows two examples of obtaining the system information from status indicators:

- If a LINK failure of the system is detected, the icon  will appear on the status bar of the display device, indicating the current network is not available.
- If the power LED does not light, it indicates the system is not powered on.

For more information on the icons, refer to [Icon Instructions](#) on page 27.

Analyzing Configuration Files

Wrong configurations may have an impact on your system use. You can export configuration file to check the current configuration of the system and troubleshoot if necessary. For more information on how to export system configuration, refer to [Importing/Exporting Configuration](#) on page 210.

Viewing Call Statistics

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Uplink Bandwidth and Downlink Bandwidth.
- **Video:** Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost(%)
- Protocol used during a call.
- Device information of the far site.
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost(%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.



Use the remote control to select **More->Call Statistics** during an active call to view call statistics.

Using Diagnostic Methods


The system supports the following diagnostic methods:



- **Audio Diagnose:** Check whether the audio input device and audio output device are working properly.
- **Camera Diagnose:** Check whether the camera can pan and change focus normally.
- **Ping:** Check whether the system can establish contact with the IP address that you specify.
- **Trace Route:** Display the route (path) and measure transit delays of packets across an Internet Protocol (IP) network.

To diagnose audio via the remote control:



1. Select **Menu->Diagnose** menu.
2. Select **Audio Diagnose**, and then press .
3. Speak into the microphone.
4. Check whether the microphone can pick up audio and play back the audio properly.
If the system plays back the audio normally, it means that audio works well.
5. Press  to stop audio diagnostics.

To diagnose the camera via the remote control:



1. Select **Menu->Diagnose** menu.
2. Select **Camera Diagnose**, and then press .
3. Press navigation keys to adjust the camera position.

4. Press  or  to adjust the focus.
If the camera can move and zoom normally, it means that the camera works properly.
5. Press the **Back** soft key to stop camera diagnose.

To diagnose network via the remote control:

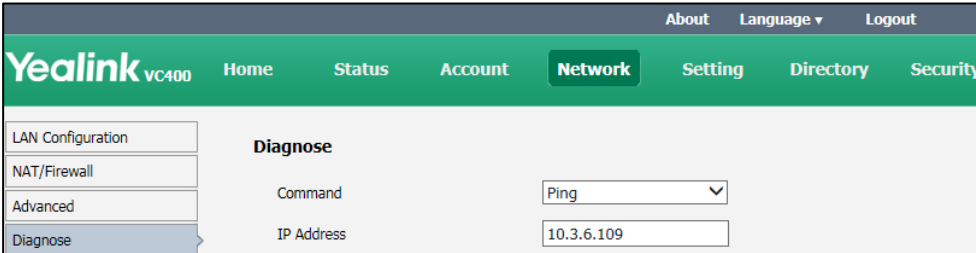
1. Select **Menu->Diagnose** menu.
 2. Select **Ping**, and then press .
 3. Enter IP address (for example, the IP address of the far site).
 4. Press **Start**, and then press .
- The display device displays the network diagnose information.
5. Press the **Back** soft key to return to the Diagnose menu.
- It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.

Trace Route:

1. Select **Menu->Diagnose** menu.
 2. Select **Trace Route**, and then press .
 3. Enter IP address (for example, the IP address of the far site).
 4. Press **Start**, and then press .
- The display device displays the network diagnose information.
5. Press the **Back** soft key to return to the Diagnose menu.
- If the test is successful, the VC400/VC120 system lists the hops between the system and the IP address you entered. You can check whether congestion happens via the time cost between hops.

To diagnose network via web user interface:

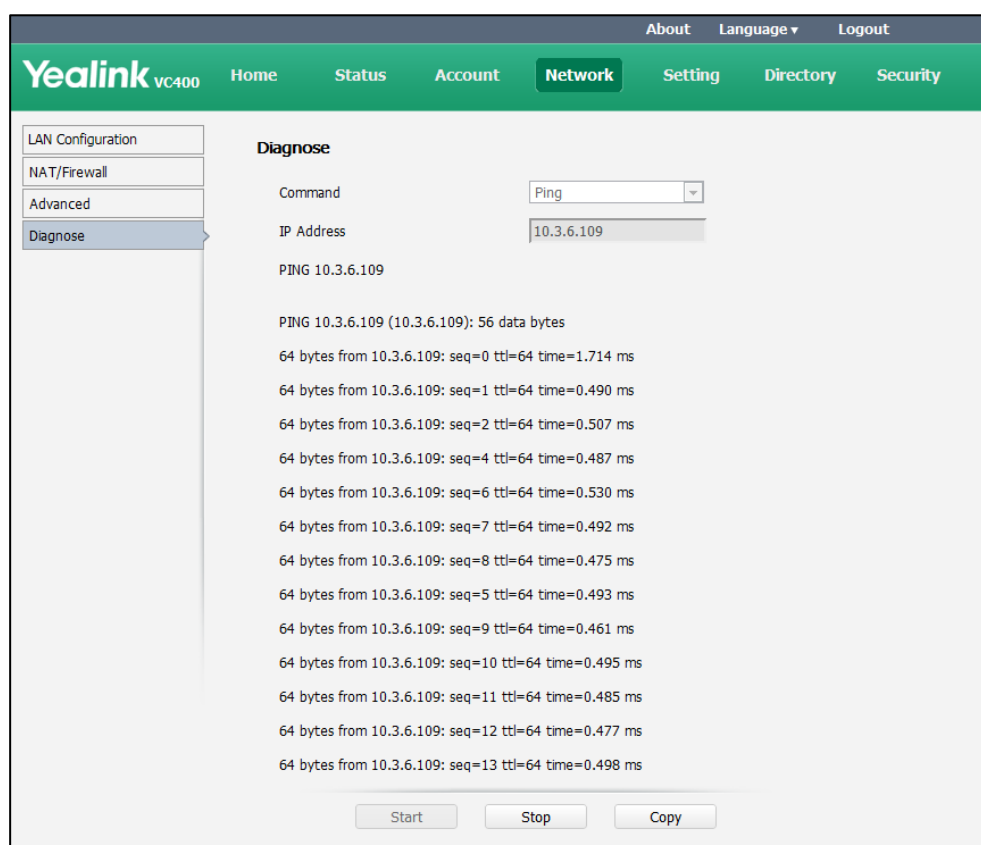
1. Click on **Network ->Diagnose**.
2. Select the desired diagnostic method from the pull-down list of **Command**.
3. Enter IP address in the **IP Address** field.



Yealink VC400		
About Language Logout		
Home Status Account Network Setting Directory Security		
LAN Configuration		
NAT/Firewall		
Advanced		
Diagnose		
Diagnose		
Command	Ping	
IP Address	10.3.6.109	

4. Click **Start** to start diagnosing.

The web page displays the diagnosis:



5. Click **Stop** to complete diagnosing.

You can click **Copy** to copy the content to the clipboard.

Troubleshooting Solutions

This chapter provides general troubleshooting solutions to help you solve the problems you might encounter when using your system.

Ensure the system has not been physically damaged when experiencing a problem. Check whether the cables are loose and the connections are correct and secure. These are common causes of problems.

If problems you encounter are not mentioned in this chapter, you can contact your distributor or Yealink FAE.

General Issues

Why is the display device black?

- Check whether the display device is connected properly to the VC400/VC120 codec.

- Check whether the system is in sleep mode. Press any key on the VCP40 phone or remote control to resume system operation.
- Check whether the display device is in sleep mode or is turned off. Press the power button on the remote control or on the display device.
- Check whether you have selected the correct video input source. You can try to switch video input source.

Why doesn't the display device display time and date correctly?

- If you have configured the system to obtain the time and date from the NTP server automatically, ensure that SNTP server and time zone are configured correctly in the system and whether the connection between the system and NTP server is working properly.
- If you have configured the system to obtain the time and date manually, ensure that you have configured the time and date correctly.

Why doesn't the remote control work?

- Check whether the system is powered on.
- Check whether the positive and negative charges of the battery are connected correctly.
- Check whether the battery has sufficient power left.
- Check whether no special fluorescent or neon signs nearby.

Why does the system fail to call the far site?

- Check whether the network of the near site is available.
- Check whether the network of the far site is available.
- Check whether the far site enables the DND feature.
- Check whether the accounts have been registered correctly, and the system uses the appropriate account to call the far site.
- Ensure that the number you are calling is correct.
- Check whether the far site rejects your call.
- Check whether the firewall blocks the inbound traffics from the other site.
- Check whether the far site has already up to maximum call-in limitation.
- If the near site is forced to use encryption, ensure that the far site enables encryption too. For more information on call encryption, refer to [Secure Real-Time Transport Protocol](#) on page 200 and [H.235](#) on page 203.

- Ensure the far site supports the same call protocol as the near site.

Why does the system fail to call the far site via IP address?

- Ensure that at least one call protocol is enabled on both sites. For more information, refer to [Configuring SIP Settings](#) on page 99 and [Configuring H.323 Settings](#) on page 104.
- Ensure that the network is connected correctly.
- Ensure that the network is configured correctly. For more information, refer to [Configuring LAN Properties](#) on page 50.
- Ping the IP address of the far site. Contact your system administrator if it fails. For more information, refer to [Using Diagnostic Methods](#) on page 224.

Why doesn't the status bar of the display device display IP address?

- Check whether the network is available.
- Check whether the LAN property is configured correctly. For more information on LAN property configuration, refer to [Configuring LAN Properties](#) on page 50.
- Check whether the system has enabled the hide IP address feature. For more information on disabling the hide IP address feature, refer to [Hide IP Address](#) on page 140.
- Check whether the system has configured firewall and NAT correctly. For more information on, refer to [Configuring the System for Use with a Firewall or NAT](#) on page 75.

Why does the network keep losing packets?

- Check whether the network is available and the LED indicator on the left of the Internet port illuminates green.
- Try to use the low speed connection to check whether packets are lost. Deficient bandwidth is an important reason for packet loss.
- Check the configuration of the network speed and duplex mode on the system, switch and router.

Camera Issues

Why can't I adjust the camera angle and focus?

- You can adjust the camera when the system is idle or during a call. The camera

cannot be adjusted when the system is in the menu screen.

- Ensure that the batteries in the remote control are in good working condition, and installed correctly.
- Aim the remote control at the sensor when operating the unit.
- Ensure that no objects are obstructing the sensor on the front of the camera.
- Ensure that the LED on the front of the camera flashes green when you use the remote control to operate the unit.
- Ensure that what you are controlling is the local camera.
- Reboot the system.
- If the above suggestions cannot solve your problem, perhaps the remote control is broken. You can contact your system administrator for help.

Why can't adjust the remote camera during an active call?

- Use the remote control to control the local camera to check whether the remote control can be used normally.
- Ensure that the far site has enabled the Far Control Near Camera feature. For more information, refer to [Far-end Camera Control](#) on page 159.
- Ensure that what you are controlling is the remote camera. Select **More->Near/Far Camera** during an active call and then select the remote video image.
- Ensure the far site supports the same call protocol as the near site. For more information, refer to [Camera Control Protocol](#) on page 160.

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information on packet loss, refer to [Viewing Call Statistics](#) on page 224.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

Video & Audio Issues

Why can't I hear the audio during a call?

- Ensure that the local audio output device is connected correctly.
- Use audio diagnose to check whether the audio device is working normally.

- Ensure that the ringer volume is not set to the minimum.
- Check whether the far site is muted.

Why can't the far site hear the local audio?

- Ensure that the local audio input device is connected correctly.
- Check whether the near site is muted.
- Check whether the system has enabled the auto answer mute feature.

Why can't I hear the other site clearly during a call?

- Ensure that the speaker volume of the far site is not set too low.
- Muffled audio reception from the far side may be caused by highly reverberant rooms. Speak in close proximity to the phone.
- Adjust the priority order for your audio codec if you have chosen a low-bandwidth audio codec to be first. For more information, refer to [Audio Codecs](#) on page 113.
- For best results, ensure that the caller is using a Yealink video conferencing system. Audio quality from your video conferencing system will vary when calling a non-Yealink system.
- Dust and debris may cause audio quality. Do not use any kind of liquid or aerosol cleaner on the phone. A soft, slightly damp cloth should be sufficient to clean the top surface of the phone if necessary.

Why is the voice quality poor?

Users may receive poor voice quality during a call, such as intermittent voice, low volume, echo or other noise. It is difficult to diagnose the root causes of the voice anomalies. The possible reasons are:

- Users sit too far from or near to the microphone.
- The audio pickup device is moved frequently.
- Intermittent voice is probably caused by voice packet loss or jitter. Voice packet loss may occur due to network congestion. Jitter may occur due to information reorganization of the transmission or receiving equipment, such as, delay processing, retransmission mechanism or buffer overflow.
- Noise devices, such as computers or fans, may make it difficult to hear each other's voices clearly.
- Wires may also cause this problem. Replace the old with the new cables, and then reconnect to check whether the new cables provide better connectivity.

Why can't I view the local video image?

- Check whether the near site camera is connected to the VC400/VC120 codec correctly.
- Check whether camera is powered on, and the LED indicator illuminates green.
- Check whether the camera is selected for the current video input source.
- Check the screen layout to see whether the remote video image is shown in full size.

Why can't I view the menu?

- Check whether the Display1 port of VC400/VC120 codec is connected to the HDMI port on the display device.

Why can't I start a presentation?

- Check whether a PC is connected to the VC400/VC120 codec.
- Check whether the PC is sending a signal.
- Check the call statistics to see whether the system is sharing content.
- Ensure that dual-stream is configured correctly. For more information, refer to [Dual-Stream Protocol](#) on page 151.

System Maintenance

How to prevent monitor burn-in?

Refer to your monitor's documentation for specific recommendations and instructions. The following guidelines help prevent image burn-in:


- Ensure that static images are not displayed for long periods.
- Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.
- Configure the automatic sleep time to be 1 hours or less.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

How to reboot the system?

When you do one of the following, the system will reboot:

- Reboot system
- Reset system
- Upgrade firmware
- Configure some features need to take effect after a reboot

You can reboot the system in the following ways:

- Long press the power button on the VC400/VC120 codec.
- Select **Menu->Advanced (default password: 0000) ->Reboot & Reset->Reboot**, and then press  .
- Login web user interface and click on **Setting->Upgrade->Reboot**, and then click **Confirm**.

To avoid corrupting the system, you should not unplug the power adapter from the system to power off the system.

Why does the system fail to upgrade?

- Ensure that the firmware is different from the firmware currently in use.
- Ensure that the downloaded firmware applies to the system.
- Ensure that the system is powered on normally, and the network is available during the upgrade process.
- When upgrading firmware via web user interface, ensure that the web user interface is not refreshed or closed during the upgrade process.

Appendix

Appendix A: 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

Time Zone	Time Zone Name
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)
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	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(Windhoeck)
+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)
+02:00	Syria(Damascus)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)

Time Zone	Time Zone Name
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)
+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 B: Trusted Certificates

Yealink IP phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2

- GeoTrust Primary CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA - G1 (EV)
- Thawte Primary Root CA - G2 (ECC)
- Thawte Primary Root CA - G3 (SHA256)
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ROOT CA

Note

Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to [Transport Layer Security](#) on page 192.

Index

Numeric

802.1x Authentication [66](#)

A

About This Guide [v](#)

Auto Answer [119](#)

Auto Refuse Timeout [125](#)

Automatic Sleep Time [139](#)

Audio Output Device [145](#)

Audio Input Device [147](#)

Adjusting MTU of Video Packets [150](#)

Auto Refuse Timeout [125](#)

Analyzing Configuration Files [223](#)

Administrator Password [188](#)

Attack Defense in Public Network [204](#)

Abnormal Call Answering [205](#)

Appendix A: Time Zones [233](#)

Appendix B: Trusted Certificates [235](#)

B

Bandwidth [122](#)

Backlight of VCP40 Conference Phone [130](#)

C

Configuring Network [49](#)

Configuring LAN Properties [50](#)

Configuring Network Settings Manually [54](#)

Configuring Network Speed and Duplex Mode [57](#)

Configuring the System for Use with a Firewall or NAT [75](#)

Configuring Call Preferences [99](#)

Configuring SIP Settings [99](#)

Configuring H.323 Setting [104](#)

Codecs [110](#)

Call Protocol [114](#)

Call Match [120](#)

Configuring System Settings [129](#)

Configuring Camera Settings [154](#)

Camera Control Protocol [160](#)

Call History [176](#)

Configuring Safe Mode Call [206](#)

Configuring Packets [220](#)

Camera Issues [228](#)

D

Documentations [v](#)

DHCP [50](#)

DHCP VLAN [65](#)

DTMF [108](#)

Do Not Disturb [117](#)

Date and Time [132](#)

Dual-Stream Protocol [151](#)

Dual Screen [179](#)

E

Enabling Communication with Other Systems [47](#)

F

Firmware [v](#)

Far-end Camera Control [159](#)

G

Getting Started [35](#)

Getting Information from Status Indicators [220](#)

General Issues [226](#)

H

H.323 Tunneling [71](#)

H.460 Firewall Traversal [89](#)

History Record [121](#)

Hide IP Address [140](#)

H.235 [202](#)

I

In This Guide [v](#)

Icons on Display Device [27](#)

Icons on VCP40 Video Conferencing Phone [29](#)

Intelligent Firewall Traversal [91](#)

Importing/Exporting Configuration [210](#)

Index [237](#)

K

Keep Alive [87](#)

Key Tone [142](#)

L

LED Instructions [30](#)

LLDP [60](#)

Language [131](#)

Local Directory [167](#)

LDAP [172](#)

License [182](#)

M

Manual Configuration for VLAN [63](#)

Methods of Transmitting DTMF Digit [109](#)

Meeting Password [143](#)

Meeting Whitelist [144](#)

Mix Sending [154](#)

N

Static NAT [79](#)

O

Optional Accessory [6](#)

P

Packaging Contents [1](#)

Physical Features of Yealink VCS System [2](#)

Powering the System On and Off [41](#)

Placing a Test Call from the Yealink Video

Conferencing System [47](#)

Preparing the Network [49](#)

Q

Quality of Service [92](#)

R

Remote Control [32](#)

Remote Control Battery Safety Information [40](#)

Reserved Ports [75](#)

Rport [88](#)

Ringback Timeout [124](#)

Ringback Timeout [124](#)

Reboot Offtime [141](#)

Resetting to Factory [211](#)

S

Summary of Changes [vi](#)

System Component Instructions [6](#)

System Installation [42](#)

System Startup [42](#)

Setup Wizard [43](#)

Static DNS [53](#)

STUN on page [83](#)

Site Name [129](#)

Search Source List in Dialing [178](#)

Secure Real-Time Transport Protocol [200](#)

SNMP [212](#)

System Maintenance Issues [231](#)

T

Table of Contents [ix](#)

Tones [163](#)

Transport Layer Security [192](#)

Troubleshooting [217](#)

Troubleshooting Methods [217](#)

Troubleshooting Solutions [226](#)

U

User Interfaces [31](#)

URI Call Mode [126](#)
User Mode [187](#)
Upgrading Firmware [209](#)
Using Diagnostic Methods [224](#)

V

VoIP Principles [1](#)
VC400/VC120 Codec [6](#)
VCC18HD Camera [8](#)
VCP40 Video Conferencing Phone [10](#)
VCM60 Video Conferencing Wireless
Microphone on page [12](#)
VCM30 Video Conferencing Microphone Array
[22](#)
VCR10 Remote Control [22](#)
VLAN [59](#)
VPN [95](#)
Video Codecs [114](#)
Viewing Log Files [217](#)
Viewing Call Statistics [224](#)
Video & Audio Issues [229](#)

W

Web User Interface [32](#)
Web Server Type [190](#)