



VC Series Video Conferencing System Administrator Guide

Copyright

Copyright © 2015 YEALINK NETWORK TECHNOLOGY

Copyright © 2015 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.

CE Mark Warning

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

Part 15 FCC Rules

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

1. This device may not cause harmful interference.
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 experienced 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.

Documents

This guide covers the VC400 and VC120 video conferencing systems. In addition to the administrator guide, the following related documents 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.

You can download the above documentations from Yealink website:

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

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

In This Guide

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 4, "[System Management](#)" describes how to manage system contacts and call history.
- Chapter 6, "[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.

Table of Contents

About This Guide	v
Documents	v
In This Guide	v
Table of Contents	vii
System Overview	1
VoIP Principles	1
Packaging Contents	2
Optional Accessory	4
System Component Instructions	5
VC400/VC120 Codec	5
VCC18 HD Camera	7
VCP40 Video Conferencing Phone	7
VCR10 Remote Control	10
Icon Instructions	12
Icons on Display Device	12
Icons on the VCP40 Video Conferencing Phone	13
LED Instructions	14
User Interfaces	15
Remote Control	16
Web User Interface	16
Getting Started	17
System Installation	17
Installing the VC400/VC120 Video Conferencing System	18
Installing the Camera	19
Installing Batteries in the Remote Control	21
Connecting the CPE80 Expansion Microphone	21
Powering the System On and Off	22
System Initialization	22
System Startup	23
Setup Wizard	23
Placing a Test Call from the Yealink VCS System	27
Configuring Network	29

Preparing the Network.....	29
Configuring LAN Properties	30
DHCP	30
Configuring Network Settings Manually	33
Configuring Network Speed and Duplex Mode.....	35
LLDP.....	37
VLAN.....	41
802.1X Authentication	44
H.323 Tunneling.....	49
Configuring the System for Use with a Firewall or NAT	52
Reserved Ports.....	53
NAT	56
H.460 Firewall Traversal.....	57
Intelligent Firewall Transversal	58
Quality of Service	59
VPN.....	62

Configuring Call Preferences 65

Configuring SIP Settings.....	65
Configuring H.323 Settings	68
Codecs	71
Call Type.....	72
Do Not Disturb.....	74
Auto Answer.....	75
Call Match.....	76
History Record.....	77
Bandwidth.....	78

Configuring System Settings 81

General Setting.....	81
Site Name.....	81
Backlight of the VCP40 Video Conferencing Phone	82
Language	83
Time and Date.....	84
Automatic Sleep Time	91
Hide IP Address.....	92
Reboot Offtime	93
Key Tone	94
Audio Setting	95
Audio Output Device	95
Audio Input Device.....	97
Volume.....	98
Adjusting MTU of Video Packets.....	99

Dual-Stream Protocol	101
Mix Sending.....	102
Configuring Camera Settings	103
Far Control of Near Camera.....	107
Camera Control Protocol	109
Tones	110
System Management.....	115
Local Directory	115
LDAP	120
Call History.....	124
Search Source List in Dialing	126
Dual Screen.....	127
Configuring Security Features.....	129
User Mode	129
Administrator Password	130
Web Server Type.....	132
Transport Layer Security	134
Secure Real-Time Transport Protocol	141
H.235	143
System Maintenance	147
Upgrading Firmware	147
Importing/Exporting Configuration	148
Resetting to Factory	148
SNMP.....	150
Troubleshooting	153
Troubleshooting Methods	153
Viewing Log Files.....	153
Capturing Packets	155
Getting Information from Status Indicators	156
Analyzing Configuration Files	157
Viewing Call Statistics	157
Using Diagnostic Methods.....	157
Troubleshooting Solutions	159
General Issues	159
Camera Issues.....	161
Video & Audio Issues.....	162
System Maintenance	163

Appendix	165
Appendix A: Time Zones	165
Appendix B: Trusted Certificates	167
Index	169

System Overview

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

- [VoIP Principles](#)
- [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 endpoints. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

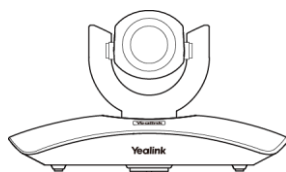
Packaging Contents

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

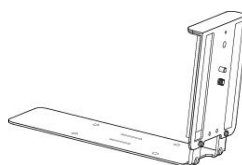
- **VC400/VC120 Codec**






- **VCC18 HD Camera**



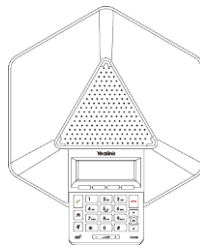
- **L-Bracket (for installing the camera)**



- **Camera Mounting Accessories**

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

- VCP40 Video Conferencing Phone



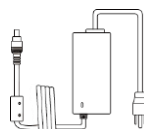
- VCR10 Remote Control



- 2 AAA Batteries



- Power Adapter



- Cables (for VC400)



DVI Cable



VGA Cable



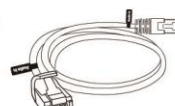
HDMI Cables × 2



3.5mm Audio Cable

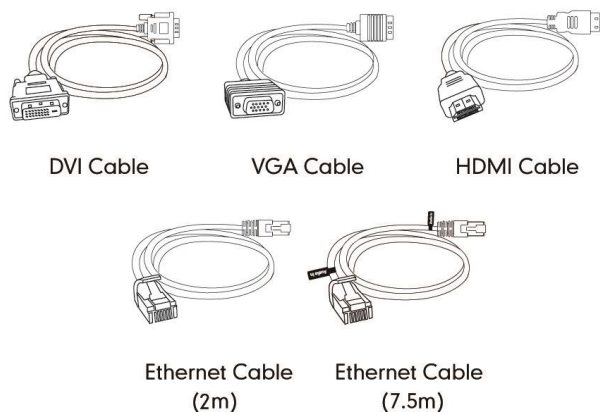


Ethernet Cable
(2m)



Ethernet Cable
(7.5m)

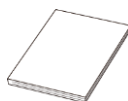
- **Cables (for VC120)**



- **7 Cable Ties**



- **Quick Start Guide**



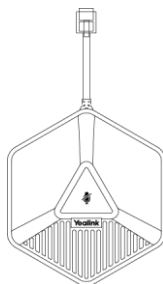
Check the list before installation. If you find anything missing, contact your system administrator.

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**



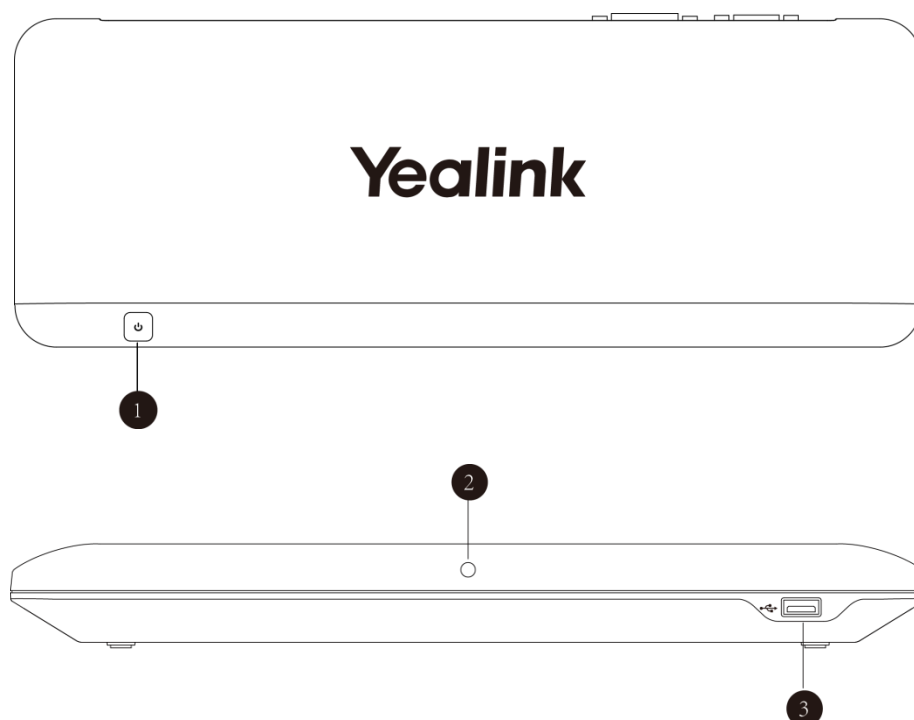
System Component Instructions

VC400/VC120 Codec

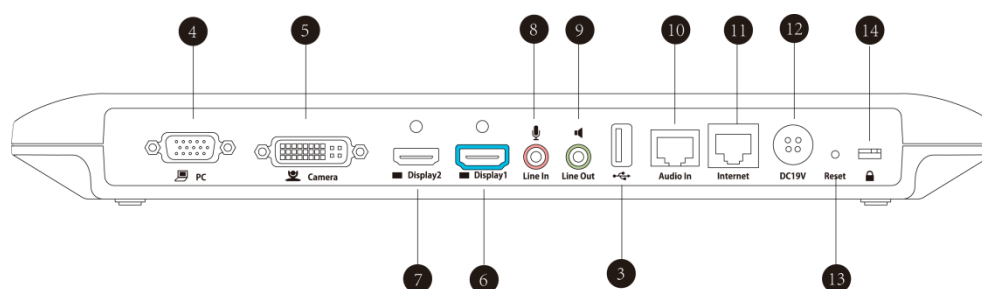
VC400/VC120 codec supports 1080P full HD video. It supports both H. 323 and SIP protocols and can connect to a mainstream video conferencing system.

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



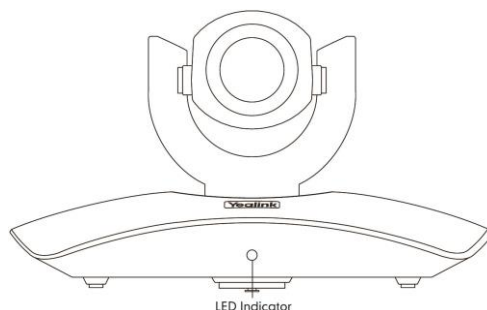
VC400/VC120 codec back panel



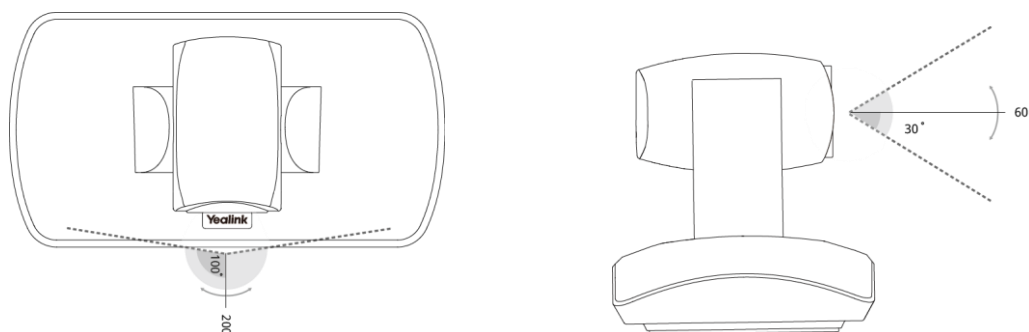
	Port Name	Description
①	Power Button	Powers the system on or off
②	LED Indicator	Indicates the system statuses
③	USB	Inserts a USB flash drive to the port for storing screenshots and recording videos
④	PC	Connects to a PC for sharing documents or videos during a conference call
⑤	Camera	Connects to a camera
⑥	Display1	Connects to a display device for displaying video images. When connecting only one display device to the VC400/VC120 codec, Display1 port is the only available port.
⑦	Display2	Connects to another display device for displaying video images
⑧	Line In	Connects to an audio input device using the supplied audio cable
⑨	Line Out	Connects to an audio output device using the supplied audio cable
⑩	Audio In	Connects to the VCP40 video conferencing phone
⑪	Internet	Connects to the network devices
⑫	DC19V	Connects to the 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.

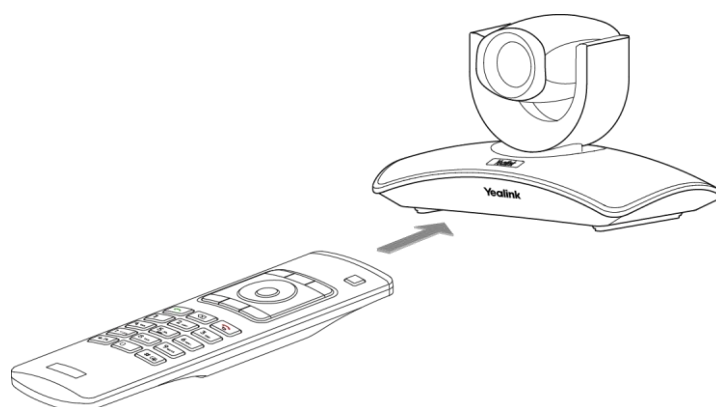


You can use the remote control to adjust the position or focus of the camera. The VCC18 camera can be panned (± 100 degrees range), tilted (± 30 degrees range).



Infrared Sensor

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

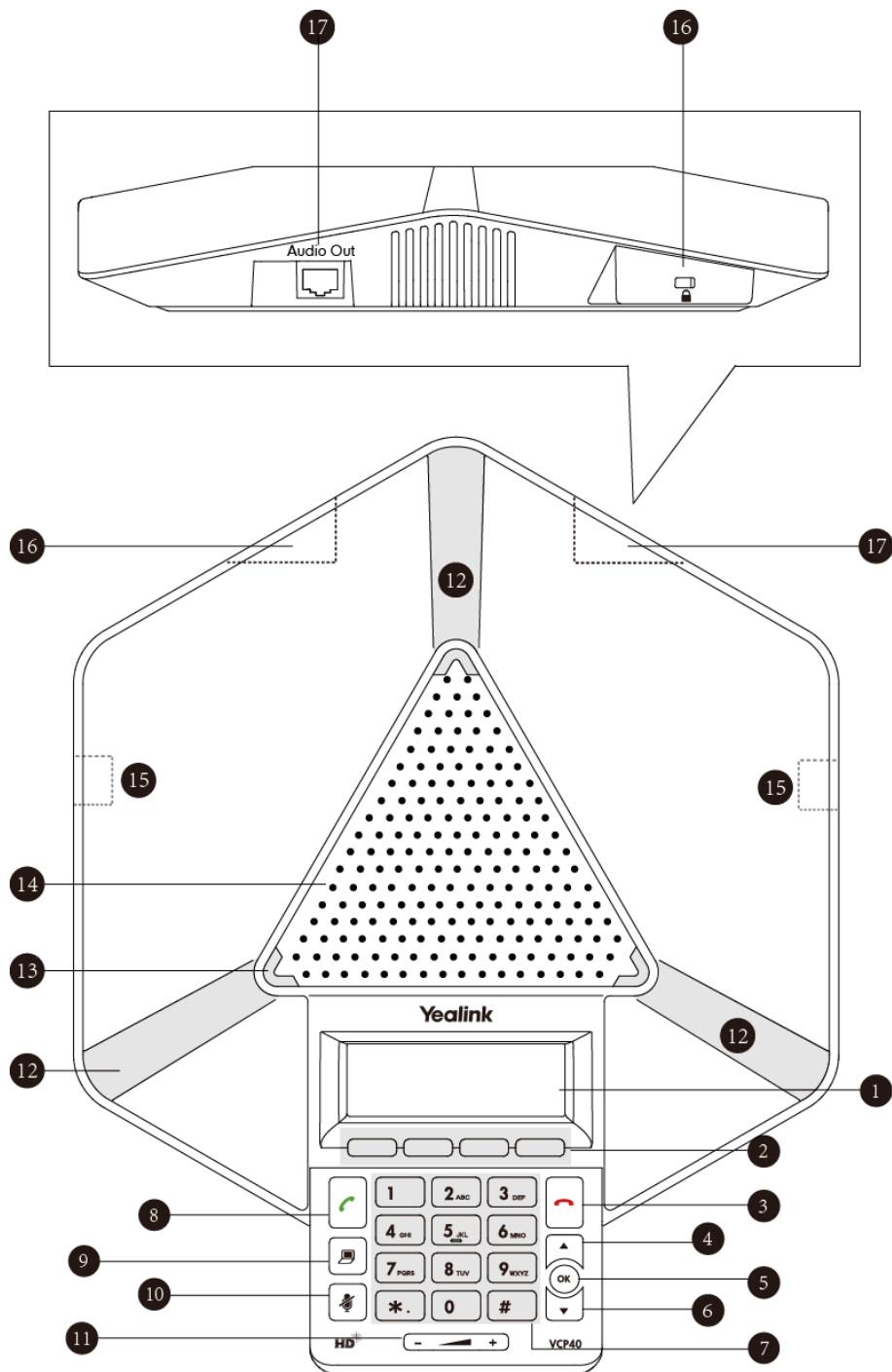


VCP40 Video Conferencing Phone





The VCP40 video conferencing phone can be used as the speakerphone and microphone for the system. It supports 360-degree audio pickup with a radius of 3

meters to achieve ultra-HD voice.

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

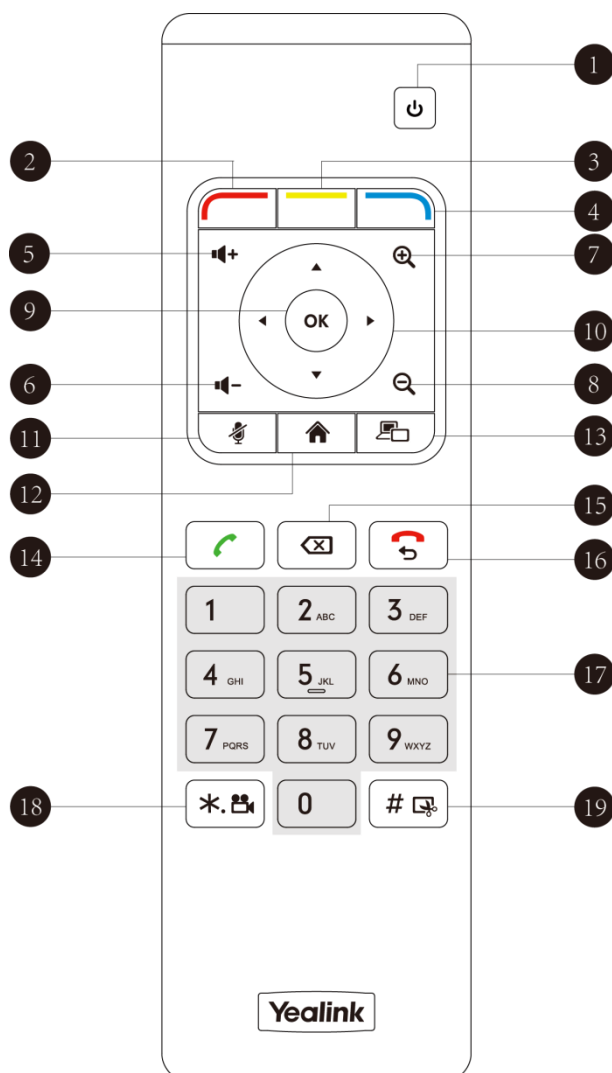


System component instructions for the VCP40 phone are:

	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 symbol 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.
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 Ethernet cable labeled Audio in. Provides the power supply for the VCP40 phone

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 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	Zooms the camera out.
⑧	Zoom in Key	Zooms the camera in.
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	Selects video input sources.
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 the entered characters.
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. Stores the preset position of the camera.
⑱	Video Recording Key	<ul style="list-style-type: none"> Provides the special characters "*" or ".". Starts/Stops recording video when the phone is idle.
⑲	Snapshot Key	<ul style="list-style-type: none"> Provides the pound key (#).
















	Item	Description
		<ul style="list-style-type: none"> Captures the on-screen image of the display device when the phone is idle.

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
	Symbol input mode of the on-screen keyboard
	Auto answer
	Missed calls
	Volume is 0
	Do not disturb
	Do not disturb during a call

Icon	Description
	Call mute
	Call encryption
	The content of the local camera
	Focus content
	Camera position
	Record a video
	Dialed calls
	Received calls
	Missed calls
	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)
	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)

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

Indicator LED on the camera:

LED Status	Description
Solid green	The camera is connected properly to the VC400/VC120 codec, and the VC400/VC120 codec is powered on.
Solid red	The VC400/VC120 codec is in the 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 call is muted.
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 conneted to the VC400/VC120codec 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 receving data

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 about the function of each key on the remote control, refer to [VCR10 Remote Control](#) on page 10. 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 the 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".

The system uses the HTTPS protocol to access the web user interface by default. For more information about the access protocol for web user interface access, refer to [Web Server Type](#) on page 132.

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.

You can monitor or place calls via the 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

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](#)
- [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/VC120 video conferencing system
- Mounting the camera on the TV
- Mounting the camera on a wall
- Installing batteries into 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 another display device to the Display2 port.

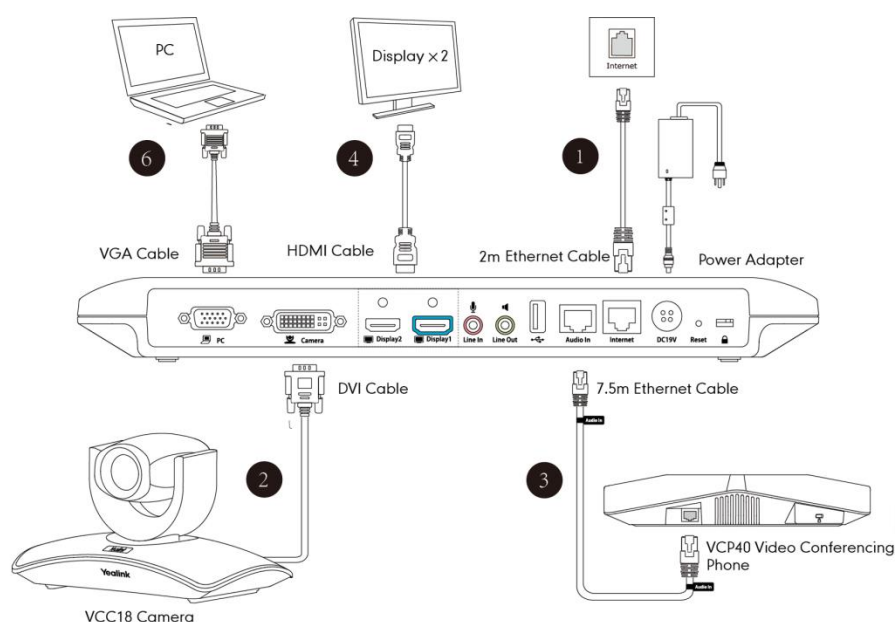
Because the DVI cable is tailor-made, please use the Yealink-supplied DVI cable.

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

Installing the VC400/VC120 Video Conferencing System

Do the following:

1. Connect the supplied 2m Ethernet cable to the Internet port on the VC400/VC120 codec and the switch/hub device port.
2. Connect the DVI cable to the Camera port on the VC400/VC120 codec and the camera.
3. Connect the supplied Ethernet cable with Audio In label to the Audio In port on the VC400/VC120 codec and Audio Out port on the VCP40 phone.
4. Connect the HDMI cable to the Display1 port on the VC400/VC120 codec and the HDMI port on the display device.
5. Connect the power line of the display device.
6. (Optional.) Connect the VGA cable to the PC port on the VC400/VC120 codec and a PC.
7. Connect the power adapter to the DC19V port on the VC400/VC120 codec and a power outlet.



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

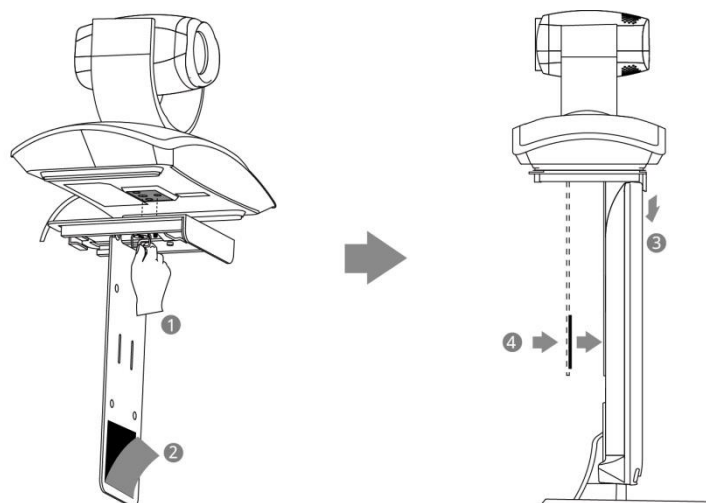


Installing the Camera

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 your TV is less than 120 mm thick, you can mount the camera on to your TV.



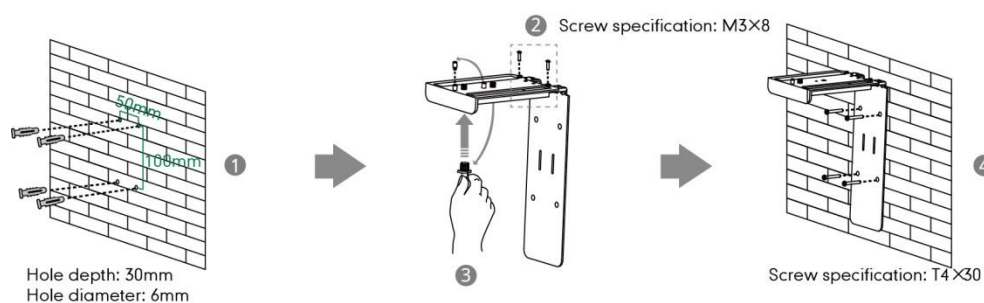
Do the following:

1. Lock the camera to the L-bracket.
2. Tear out the sticker on the L-bracket.
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.

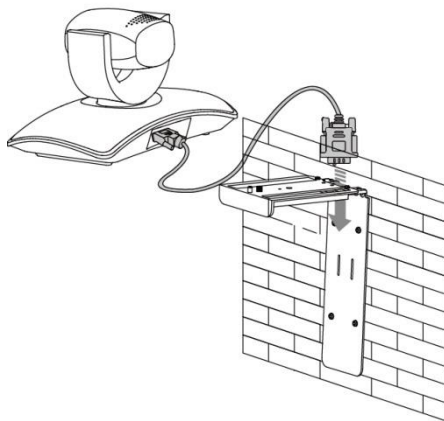
Do the following:



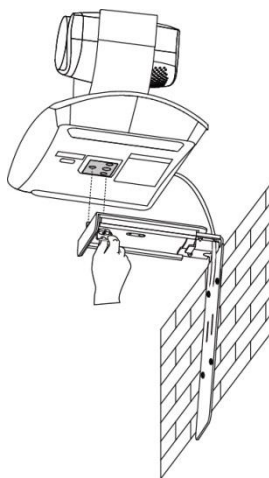
1. Punch holes into the wall and then insert the expansion bolts.

Installation location for the expansion bolts and punching requirement are shown above.

2. Lock the L-bracket with the M3×8 screws.
3. Move the setscrews on the L-bracket to the left holes.
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.



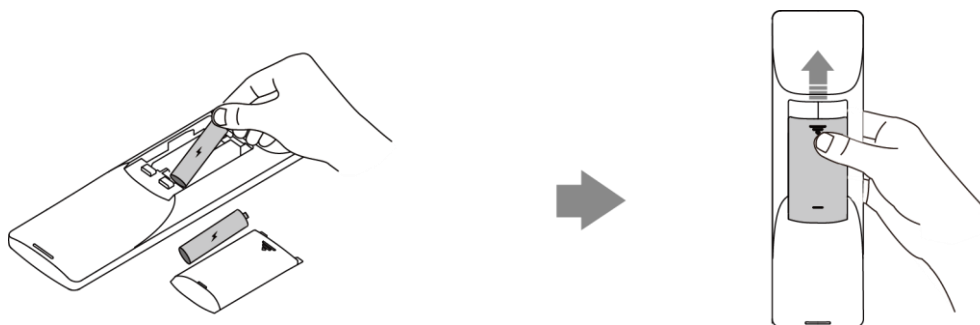
6. Lock the camera to the L-bracket, and then connect the other end of the DVI cable to the VC400/VC120 codec.



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.



Note

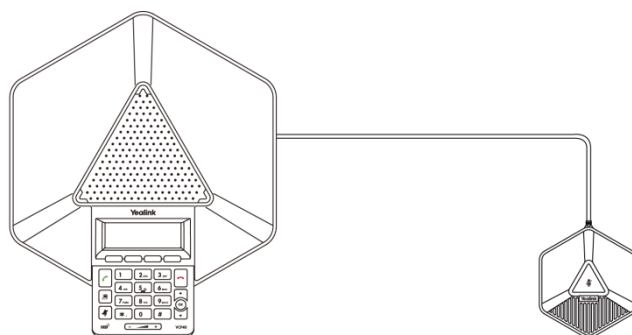
Dispose of waste batteries properly.

Remove the batteries if they are not in use for a long period of time.

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 to the location of the speaker.

CPE80 is a directional microphone. Its coverage range is a 60 degree. Always ensure that the speaker faces the expansion microphone.



VCP40 Video Conferencing Phone


CPE80 Expansion Microphone

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 about configuring network settings manually, refer to [Configuring Network Settings Manually](#) on page 33.

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 bootup screen.
4. The camera pans to the middle position automatically.
5. The display device displays the setup wizard (when you first start up, or upgrade or reset the system, the display device will display the setup wizard)

For more information about how to complete the setup wizard, refer to [Setup Wizard](#) on page 23.

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.

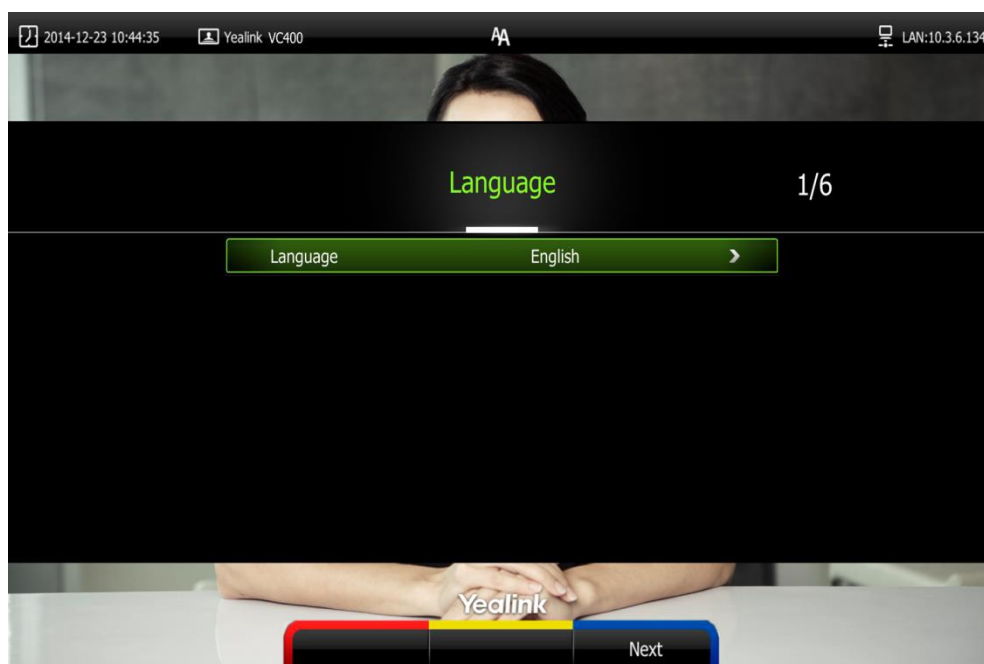
Setup Wizard


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

To complete the setup wizard via the remote control:

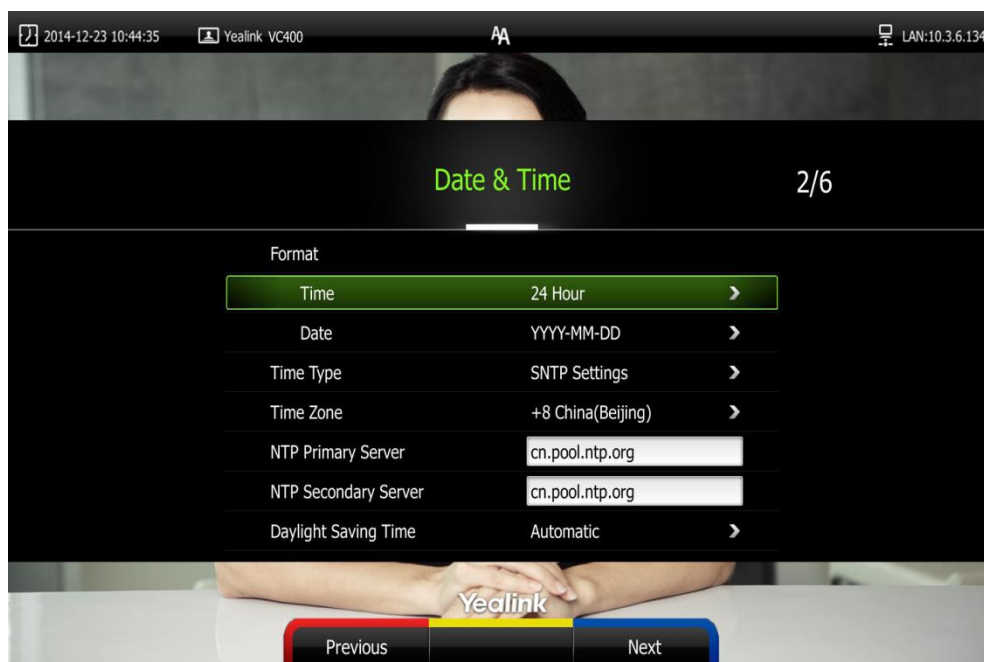
1. Set the language displayed on the display device.



The default language is English.

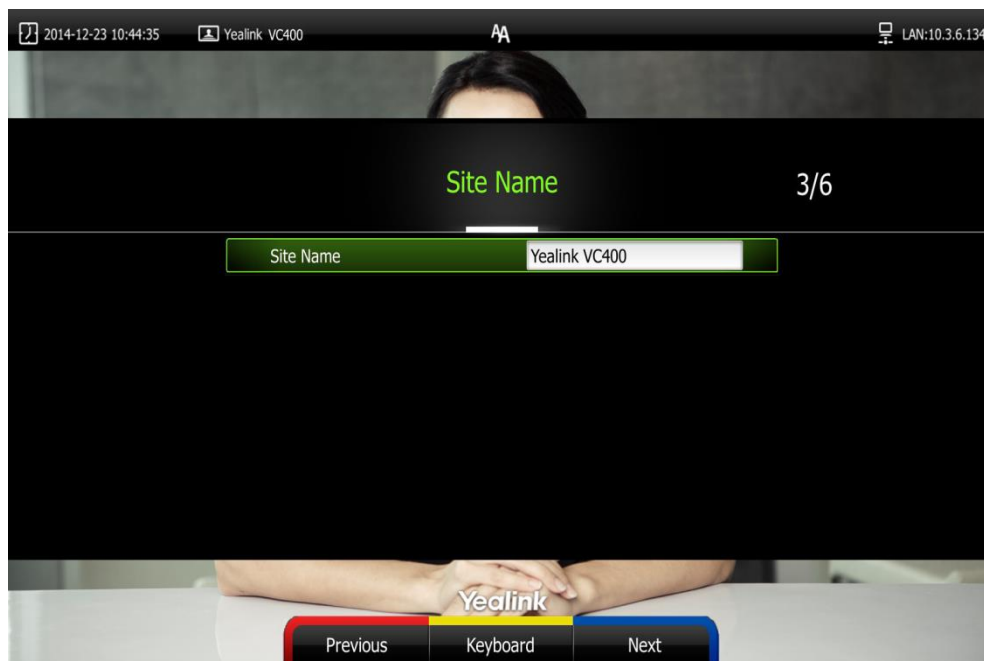




2. Press  (Next soft key) to continue.
3. Set the date and time (e.g., set the time zone, time format, date format and the type of the daylight saving time).

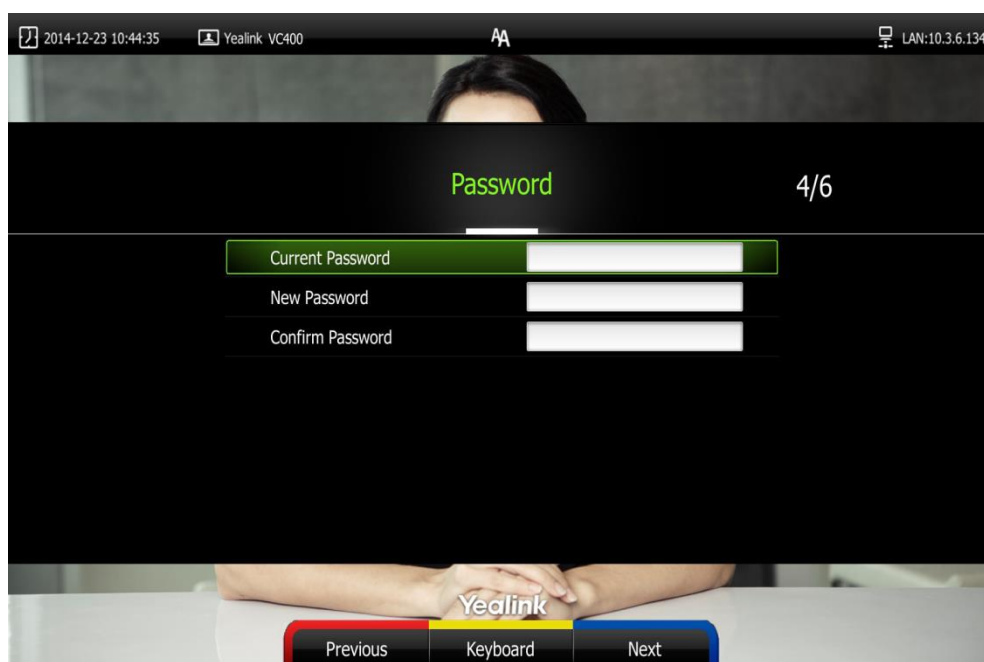
The system obtains the time and date from the NTP server automatically by default. You can also configure the time and date manually. For more information, refer to [Time and Date](#) on page 84.





4. Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.
5. Edit the site name.
The default site name is "Yealink VC400/VC120".

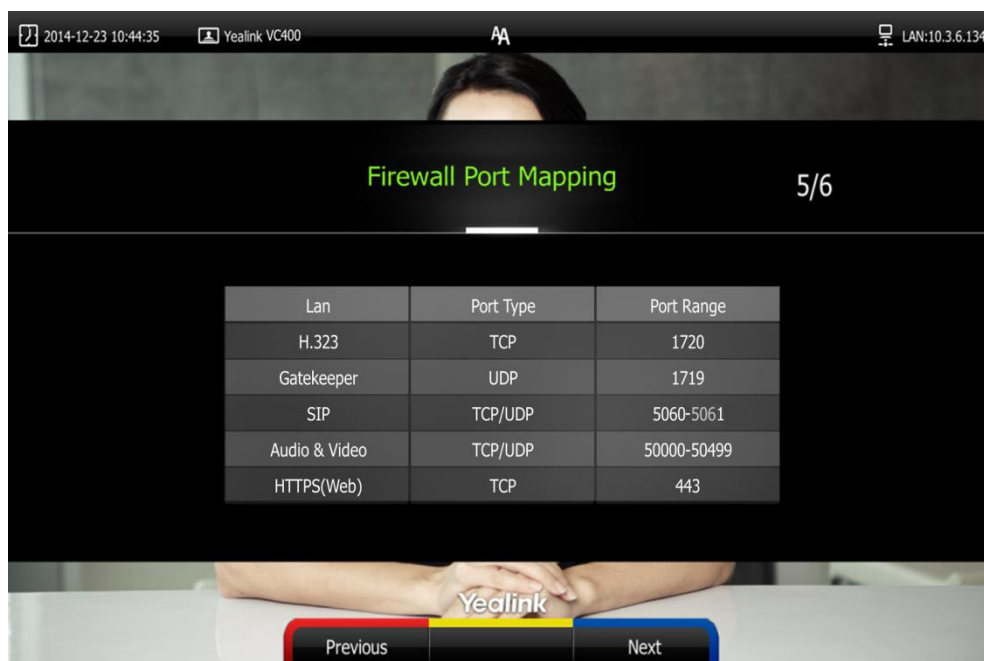




6. Press  (**Next** soft key) to continue or press  (**Previous** soft key) to return to the previous screen.
7. Change the administrator password.
The default administrator password is "0000". For security reasons, the administrator should change the default administrator password as soon as possible.



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

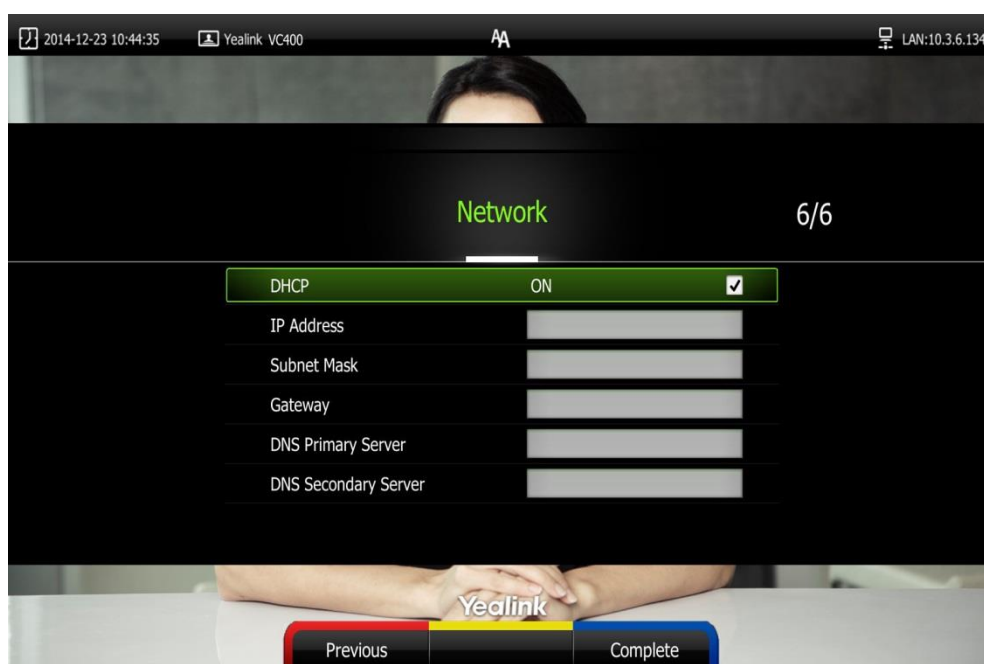
The display device displays firewall port mapping information.




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 30.



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

Note

Do to remember the new administrator password. 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 148.

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](#)
- [LLDP](#)
- [VLAN](#)
- [802.1X Authentication](#)
- [H.323 Tunneling](#)
- [Configuring the System for Use with a Firewall or NAT](#)
- [Intelligent Firewall Transversal](#)
- [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 Type	Register information of SIP account
	Register information of H.323 account

Type	Network Information
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.

Parameter	DHCP Option	Description
Domain Server	15	Specifies the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specifies the broadcast address in use on the 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 about 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 implement the changes.	Remote Control Web User Interface
Host Name	Configures the host name of the system. Default: Blank Note: When the system broadcasts DHCP DISCOVER	Web User Interface

Parameter	Description	Configuration Method
	<p>messages, it will report the configured host name to the DHCP server via DHCP option 12. Host name is optional, so it is not a mandatory configuration item. For more information, contact your network administrator.</p> <p>If you change this parameter, the system will reboot to implement the changes.</p>	

To configure DHCP via the web user interface:

1. Click on **Network->LAN Configuration**.
2. In the **IP Config** block, mark the **DHCP** radio box.
3. 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 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. On the left, the 'LAN Configuration' menu is expanded, showing 'NAT/Firewall', 'Advanced', and 'Diagnose'. The 'IP Config' section is active, with 'DHCP' selected via a radio button. Below it, there are input fields for 'IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS', and 'Secondary DNS'. The 'Host Name' field is set to 'VC400'. At the bottom, a table lists port configurations:

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Video, Audio & Data	TCP/UDP	50000-50499
HTTPS(Web)	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.

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 for the system to establish network connectivity.

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 implement the changes.	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 implement the changes.	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 implement the changes.	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 implement the changes.	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 implement the changes.	
Secondary DNS	Configures the secondary DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface

To configure network settings manually via the 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 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 (selected), NAT/Firewall, Advanced, and Diagnose. The main content area is titled 'IP Config' and shows two radio buttons: DHCP and Static IP (selected). Below the radio buttons, a red box highlights the input fields for Static IP configuration: IP Address (192.168.1.215), Subnet Mask (255.255.255.0), Gateway (192.168.1.254), Primary DNS (192.168.1.167), and Secondary DNS (192.168.1.166). The Host Name field is set to VC400. Below the form is a table showing port configurations:

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Video, Audio & Data	TCP/UDP	50000-50499
HTTPS(Web)	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 preferred 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.

Note

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

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 duplex modes supported by the system are: Auto, Half Duplex and Full Duplex. The network speeds supported by the system are: 10 Mbps, 100 Mbps and 1000 Mbps. Available that can be configured for the system are:

- Auto
- 10 Mbps Half Duplex
- 100 Mbps Half Duplex
- 10 Mbps Full Duplex
- 100 Mbps Full Duplex
- 1000 Mbps 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 implement the changes.</p>	Web User Interface

To configure the network speed via the 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.

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. 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 supported capabilities are Bridge, Telephone and Router. The enabled capabilities are Bridge and Telephone by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the system. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD.

TLV Type	TLV Name	Description
		Auto-Negotiation is: 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the 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	Software revision of the system.
	Inventory – Serial Number	Serial number of the system.
	Inventory – Manufacturer Name	Manufacturer name of the system. The default value is “IP Phone”.
	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	Remote Control Web User Interface

Parameter	Description	Configuration Method
	to implement the changes.	
Packet Interval(1-3600s)	<p>Configures the interval (in seconds) for the system to send LLDP requests.</p> <p>Default: 60</p> <p>Note: If you change this parameter, the system will reboot to implement the changes.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure LLDP via the web user interface:

1. Click on **Network->Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired time interval in the **Packet Interval (1-3600s)** field.

The screenshot shows the Yealink 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 LAN Configuration, NAT/Firewall, Advanced (selected), and Diagnose. The main content area displays the LLDP configuration page. The LLDP section is highlighted with a red box and contains two fields: 'Active' with a dropdown menu set to 'Enabled', and 'Packet Interval(1-3600s)' with a text input field containing '60'. Below the LLDP section is the VLAN configuration section, which includes fields for Internet Port (Disabled), VID(1-4094) (1), Priority (0), DHCP VLAN (Enabled), and Option (132).

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.

To configure LLDP via the remote control:

1. Select **Menu->Advanced** (default default password: 0000) -> **Advanced Network**.
2. In the **LLDP** block, check the **Active** checkbox.
3. Enter the desired value in the **Packet Interval (1-3600s)** field.
4. Press the **Save** soft key to accept the change.
The display device prompts "Reboot now?".
5. Select **OK** 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 can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

The purpose of VLAN configurations on the 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.

VLAN Discovery via DHCP

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 about VLAN, refer to *VLAN Feature on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

Parameters of VLAN feature on the system are described below.

Parameter	Description	Configuration Method
Internet Port->Active	Enables or disables VLAN feature on the system. Default: Disabled Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface
VID(1-4094)	Configures the VLAN ID. Default: 1 Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface
Priority	Configures the priority. Valid values: 0-7	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<p>7 is the highest priority, 0 is the lowest priority.</p> <p>Default: 0</p> <p>Note: If you change this parameter, the system will reboot to implement the changes.</p>	
DHCP VLAN->Active	<p>Enables or disables the DHCP VLAN discovery feature on the system.</p> <p>Default: Enabled</p> <p>Note: If you change this parameter, the system will reboot to implement the changes.</p>	Web User Interface
Option	<p>Configures the DHCP option from which the system obtains the VLAN settings.</p> <p>You can configure at most five DHCP options and separate them by commas.</p> <p>Valid Values: 128-254</p> <p>Default: 132</p> <p>Note: If you change this parameter, the system will reboot to implement the changes.</p>	Web User Interface

To configure the VLAN via the web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **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 lists 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is titled 'Network' and contains several configuration sections:

- LLDP**: Active (Enabled), Packet Interval(1-3600s) (60).
- VLAN** (highlighted with a red box): Internet Port settings including Active (Enabled), VID(1-4094) (10), and Priority (3).
- DHCP VLAN**: Active (Enabled), Option (132).
- QoS**: Audio Priority (63), Video Priority (34), Data Priority (63).
- MTU**: Video MTU (1500).

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 DHCP VLAN discovery via the 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 menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The 'Network' page displays several configuration sections: 'LLDP' (Active: Enabled, Packet Interval: 60), 'VLAN' (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 'DHCP VLAN' section is highlighted with a red box.

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.

To configure VLAN via the remote control:

1. Select **Menu->Advanced** (default 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.

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 about 802.1X authentication, refer to *Yealink 802.1X Authentication*, available online:

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

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 implement the changes.</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 implement the changes.</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 implement the changes.</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,</p>	Web User Interface

Parameter	Description	Configuration Method
	PEAP-MSCHAPV2 or EAP-TTLS/EAP-MSCHAPV2. Note: If you change this parameter, the system will reboot to implement the changes.	
Device Certificates	Configures the access URL of the device certificate when the 802.1x authentication mode is configured as EAP-TLS. Note: If you change this parameter, the system will reboot to implement the changes.	Web User Interface

To configure 802.1X via the web user interface:

- Click on **Network->Advanced**.
- In the **802.1x** block, select the desired protocol from the pull-down list of **Mode 802.1x**.
 - If you select **EAP-MD5**:
 - Enter the user name for authentication in the **Identity** field.
 - Enter the password for authentication in the **MD5 Password** field.

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 (selected), Setting, Directory, and Security. On the left, a sidebar shows configuration categories: 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 input field containing 'yealink'.
- MD5 Password:** A text input field with masked characters (dots).

Below the 802.1x section, there are two rows of certificate configuration:

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

- 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.

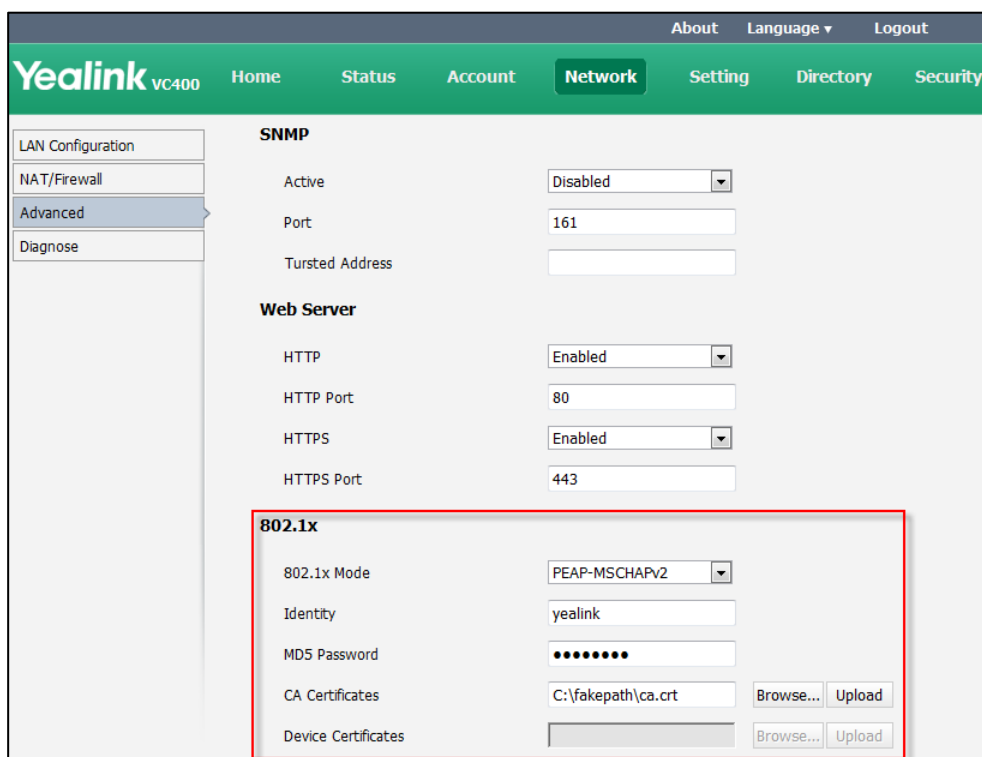
The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network' (selected), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area is divided into 'SNMP' and 'Web Server' sections. The '802.1x' section is highlighted with a red box and contains the following fields:

802.1x	
802.1x Mode	EAP-TLS
Identity	yealink
MD5 Password	••••••••
CA Certificates	C:\fakepath\ca.crt Browse... Upload
Device Certificates	C:\fakepath\client.pem Browse... Upload

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 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 'SNMP' section is expanded, showing 'Active' as 'Disabled', 'Port' as '161', and 'Trusted Address' as an empty field. The 'Web Server' section shows 'HTTP' as 'Enabled', 'HTTP Port' as '80', 'HTTPS' as 'Enabled', and 'HTTPS Port' as '443'. The '802.1x' section is highlighted with a red box and contains fields for '802.1x Mode' (set to 'PEAP-MSCHAPv2'), 'Identity' (set to 'yealink'), 'MD5 Password' (masked with dots), 'CA Certificates' (set to 'C:\fakepath\ca.crt' with 'Browse...' and 'Upload' buttons), and 'Device Certificates' (empty with '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 'SNMP', 'Web Server', and '802.1x'. The '802.1x' section is highlighted with a red box and contains the following fields:

- 802.1x Mode:** A dropdown menu set to 'EAP-TTLS/EAP-MSCHA'.
- 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.
- Device Certificates:** A text input field, with '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.

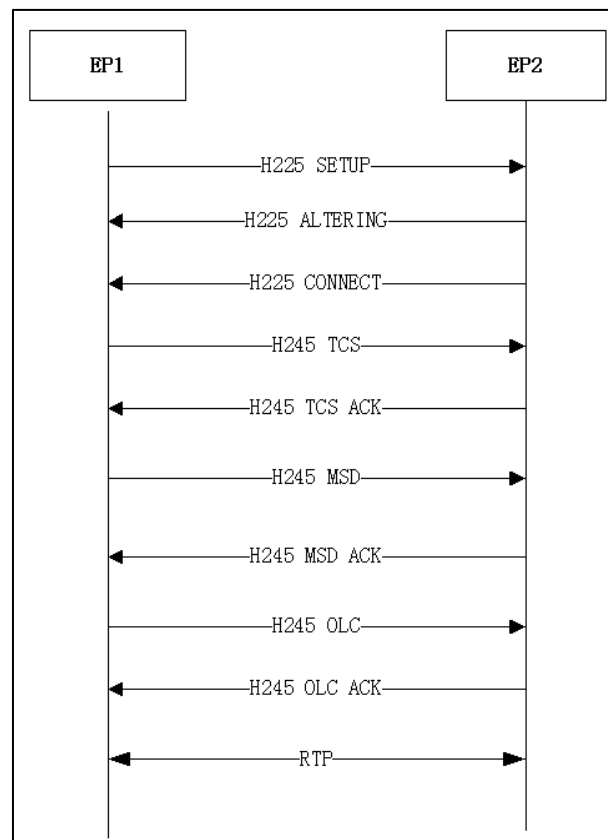
To configure the 802.1X via the remote control:

1. Select **Menu->Advanced** (default 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.

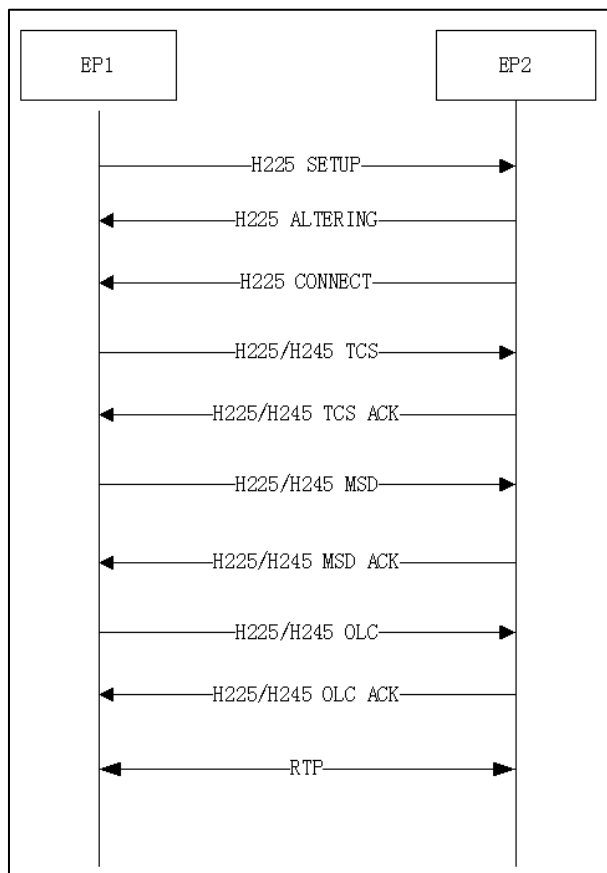
H.323 Tunneling

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 endpoints. The H.245 messages can be encapsulated and carried between H.225 controlled endpoints 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 endpoint-to-endpoint 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 a H.323 call are shown below:



If H.323 tunneling feature is enabled, the setup processes of a 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 the 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'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The 'Account' tab is selected. On the left, a sidebar shows 'H323', 'SIP', and 'Codec'. The main content area displays the H.323 configuration. The 'Register Status' is 'Registered'. The 'H.323 Active' dropdown is set to 'Enabled'. The 'H.323 Name' and 'H.323 Extension' are both '90000'. The 'Gatekeeper ID' is empty. The 'Gatekeeper Mode' is 'Manual'. The 'Gatekeeper IP Address 1' is 'h323.iot.yealink.com' with 'Port 1719'. The 'Gatekeeper IP Address 2' is empty with 'Port 1719'. The 'Gatekeeper Authentication' is 'Disabled'. The 'Gatekeeper Username' and 'Gatekeeper Password' fields are empty. The 'H.460 Active' dropdown is set to 'Disabled'. The 'H.323 Tunneling' dropdown is highlighted with a red box and set to 'Enabled'. The 'H.235' dropdown is set to 'Disabled'.

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 H.323 video conferencing equipment, you must configure the system and the firewall to allow video conferencing traffic to pass in and out of the network.

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

Description	Port Range	Port Type
H.323	1720	TCP
SIP (default transmission mode)	5060	UDP
SIP (when selecting the TCP transmission mode)	5060	TCP
SIP (when selecting the TLS transmission mode)	5061	TCP

Description	Port Range	Port Type
mode)		
Reserved ports on the system. For more information, refer to Reserved Ports on page 53.	50000-50499 (default range)	TCP/UDP
HTTPS (Optional)	443	TCP
H.323	1719	UDP

If the system and firewall are not properly configured, users placing calls through a firewall to systems may experience one-way audio or video.

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 an SIP Call	
VC400	Four-way video call and a presentation and an audio call	34 UDP 10 TCP	50000-50033 50000-50009	34 UDP	50000-50033
VC120	One-way video call and a presentation and an audio 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. A SIP call uses the higher half number of ports, and a H.323 call uses the lower half number of ports. For example, the port range is 50000-50200, SIP call uses the port range 50100-50200, and a H.323 call uses the port range 50000-50100. A H.323 call needs at least 100 ports.</p> <p>If you change this parameter, the system will reboot to implement the changes.</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
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. A SIP call uses the higher half number of ports, and a H.323 call uses the lower half number of ports. For example, the port range is 50000-50200, a SIP call uses the port range 50100-50200, and a H.323 call uses the port range 50000-50100. A H.323 call needs at least 100 ports.</p> <p>If you change this parameter, the system will reboot to implement the changes.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure reserved ports via the 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'. On the left sidebar, 'LAN Configuration' is expanded, showing 'NAT/Firewall' (selected), 'Advanced', and 'Diagnose'. The main content area is titled 'NAT Configuration'. It includes a 'Static NAT' dropdown set to 'Disabled' and a 'NAT Public IP Address' field. Below this is the 'Reserve Port' section, which is highlighted with a red box. It contains two rows: 'UDP Port Scope' and 'TCP Port Scope', each with input fields for '50000' and '50499' separated by a tilde '~'. At the bottom is the 'Intelligent Firewall Transversal' section with a dropdown set to 'On'.

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.

NAT

Network Address Translation (NAT) network environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices on the LAN to communicate with other devices outside the LAN. If your system is connected to a LAN that uses a NAT, you need to configure NAT Public (WAN) Address so that your system can communicate outside the LAN.

Note

If H.460 Firewall Traversal is enabled on the system, H.323 calls will automatically ignore the static NAT settings. For more information on H.460 Firewall Traversal, refer to [H.460 Firewall Traversal](#) on page 57.

NAT feature parameters on the system are described below:

Parameter	Description	Configuration Method
Static NAT	<p>Specifies whether the system should determine the NAT public address automatically.</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 specified Yealink server. <p>Default: Disabled</p>	<p>Remote Control</p> <p>Web User Interface</p>
NAT Public IP Address	<p>Displays the NAT public address obtained from the Yealink server if the NAT is configured to Auto, or configures the NAT public address for the system if you select to configure NAT manually.</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure NAT via the 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**.

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'. It features a 'Static NAT' dropdown menu set to 'Manual' and a text field for 'NAT Public IP Address' containing '117.28.234.34'. Below this is the 'Reserve Port' section with input fields for 'UDP Port Scope' (50000 ~ 50499) and 'TCP Port Scope' (50500 ~ 50900). At the bottom is the 'Intelligent Firewall Transversal' section with a dropdown menu set to 'On'.

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

To configure 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.

H.460 Firewall Traversal

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 can be configured to accept. Therefore using H.460, video conferencing endpoints 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 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 the 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 '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 'SIP' and 'Codec' options below it. The main content area displays configuration settings for H323. The 'Register Status' is 'Registered'. The 'H.323 Active' dropdown is set to 'Enabled'. The 'H.323 Name' is '90000' and the 'H.323 Extension' is '90000'. The 'Gatekeeper ID' is empty. The 'Gatekeeper Mode' is 'Manual'. The 'Gatekeeper IP Address 1' is 'h323.iot.yealink.com' with 'Port 1719'. The 'Gatekeeper IP Address 2' is empty with 'Port 1719'. The 'Gatekeeper Authentication' is 'Disabled'. The 'Gatekeeper Username' and 'Gatekeeper Password' fields are empty. The 'H.460 Active' dropdown is highlighted with a red box and set to 'Enabled'. The 'H.323 Tunneling' is 'Disabled' and 'H.235' is 'Disabled'.

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

Intelligent Firewall Transversal

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

In some cases, the head office is outside the LAN and lacks a VPN network, while the branch office is inside the LAN, and no port mapping is configured on its firewall, you can enable the intelligent firewall transversal feature on the system.

The intelligent firewall transversal feature makes the system easy to deploy and seamless to use.

The intelligent firewall transversal parameter is described below:

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

To configure intelligent firewall transversal via the web user interface:

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

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 sidebar, 'LAN Configuration' is expanded, showing 'NAT/Firewall' (selected), 'Advanced', and 'Diagnose'. The main content area is titled 'NAT Configuration'. It includes fields for 'Static NAT' (set to 'Disabled'), 'NAT Public IP Address', 'Reserve Port' (with UDP and TCP Port Scope fields set to 50000 ~ 50499), and 'Intelligent Firewall Transversal' (set to 'On'). The 'Intelligent Firewall Transversal' dropdown 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	Specifies the DSCP value for voice packets. Valid Values: 0-63 Default: 63 Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface
Video Priority	Specifies the DSCP value for video packets. Valid Values: 0-63 Default: 34 Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface
Data Priority	Specifies the DSCP value for data packets. Valid Values: 0-63 Default: 63 Note: If you change this parameter, the system will reboot to implement the changes.	Remote Control Web User Interface

To configure QoS via the 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 shows 'LAN Configuration', 'NAT/Firewall', 'Advanced' (selected), and 'Diagnose'. The main content area displays configuration options for LLDP, VLAN, and QoS. The QoS section is highlighted with a red box and contains the following fields:

Section	Field	Value
LLDP	Active	Disabled
	Packet Interval(1-3600s)	60
VLAN	Internet Port	
	Active	Disabled
	VID(1-4094)	1
	Priority	0
DHCP VLAN	Active	Enabled
	Option	132
QoS	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 endpoints 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 about how to package a TAR file, refer to *OpenVPN Feature on Yealink IP Phones*, available online: <http://www.yealink.com/DocumentDownload.aspx?CatId=142&flag=142>.

VPN feature parameters on the system are described below.

Parameter	Description	Configuration Method
VPN->Active	Enables or disables VPN feature on the system. 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 implement the changes.	Remote Control Web User Interface
Upload VPN Config	Upload the compressed package of VPN-related files (*.tar) to the system.	Web User Interface

To configure VPN via the 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' (highlighted), 'Setting', 'Directory', and 'Security'. The left sidebar shows 'LAN Configuration', '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), '802.1x' (802.1x Mode: Disabled, Identity: empty, MD5 Password: masked, CA Certificates: empty, Device Certificates: empty), and 'VPN' (Active: Enabled, Upload VPN Config: C:\fakepath\openvpn.tar, Browse... Upload buttons). The 'VPN' section is highlighted with a red box.

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 type and network bandwidth).

This chapter provides the following sections:

- [Configuring SIP Settings](#)
- [Configuring H.323 Settings](#)
- [Codecs](#)
- [Call Type](#)
- [Do Not Disturb](#)
- [Auto Answer](#)
- [History Record](#)
- [Call Match](#)
- [Bandwidth](#)

Configuring SIP Settings

Yealink VC400/VC120 video conferencing systems support Session Initiation Protocol (SIP). If your network supports SIP, you can use SIP to connect IP calls. To connect IP calls using SIP, you need to configure a SIP account for the system.

SIP settings parameters on the system are described below:

Parameter	Description	Configuration Method
SIP Active	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	Configures the register user name of the SIP account for register authentication. Default: blank	Remote Control Web User Interface
Password	Configures the register password	Remote Control

Parameter	Description	Configuration Method
	of SIP account for register authentication. Default: blank	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 can be configured 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 signaling. TCP—provides reliable transport via TCP for SIP signaling. TLS—provides secure communication of SIP signaling. Note: TLS is available only when the system is registered with a SIP server that supports TLS.	Remote Control Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the SIP server for SIP account. Default: 3600s	Remote Control Web User Interface

Parameter	Description	Configuration Method
DTMF	<p>Configures the DTMF type for the SIP account.</p> <ul style="list-style-type: none"> INBAND—DTMF digits are transmitted in the voice band. OUTBAND—DTMF digits are transmitted by the SIP messages. RFC2833—DTMF digits are transmitted by RTP Events compliant to RFC 2833. <p>Default: INBAND</p>	Web User Interface

To configure SIP account via the web user interface:

1. Click on **Account->SIP**.
2. Configure the SIP account settings.

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', 'SIP' (selected), and 'Codec'. The main content area displays the 'SIP' configuration settings. The 'Register Status' is 'Disabled'. The 'SIP Active' dropdown is set to 'Enabled'. The 'Register Name' and 'User Name' fields both contain '6001'. The 'Password' field is masked with dots. The 'Server Host' is '10.2.1.98' and the 'Port' is '5060'. The 'Enable Outbound Proxy Server' dropdown is set to 'Disabled'. The 'Outbound Proxy Server' field is empty, and its 'Port' is also '5060'. The 'Transport' dropdown is set to 'UDP'. The 'Server Expires' field contains '3600'. The 'SRTP' dropdown is set to 'Disabled'. The 'DTMF Type' dropdown is set to 'INBAND'.

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**.
2. Configure the SIP account settings.

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

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

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 Active	Enables or disables the H.323 account. Default: Enabled	Remote Control Web User Interface
H.323 Name	Specifies the name that the gatekeeper uses to identify the system. Default: blank	Remote Control Web User Interface
H.323 Extension	Specifies the extension that the gatekeeper uses to identify the system. Default: blank Note: Users can place calls using the extension.	Remote Control Web User Interface
Gatekeeper ID	Configures the gatekeeper ID. Note: This is set only when required by the gatekeeper. For example, for configurations with multiple gatekeepers. The gatekeeper ID must match the gatekeeper ID configured for the gatekeeper to which the system is registering. Do not configure this parameter if the gatekeeper does not require it, as this may result in failure to register with the gatekeeper.	Remote Control Web User Interface
Gatekeeper Mode	Configures the gatekeeper	Remote Control

Parameter	Description	Configuration Method
	<p>mode.</p> <ul style="list-style-type: none"> • Disabled—the system does not use a gatekeeper. • Auto—the system automatically discovers a gatekeeper. • Manual—specify the IP address and port for the gatekeeper manually. <p>Default: Disabled</p>	Web User Interface
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 H.235 Annex D authentication.</p> <p>Default: Disabled</p> <p>Note: When H.235 Annex D authentication is enabled, the gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper.</p>	Remote Control Web User Interface
Gatekeeper Username	<p>Specifies the user name for authentication with H.235 Annex D.</p> <p>Default: blank</p>	Remote Control Web User Interface
Gatekeeper Password	<p>Specifies the password for authentication with H.235 Annex D.</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</p>	Remote Control Web User Interface

Parameter	Description	Configuration Method
	H.460 Firewall Traversal on page 57.	
H.323 Tunneling	Enables or disables the H.323 tunneling on the system. Default: Disabled For more information, refer to H.323 Tunneling on page 49.	Remote Control Web User Interface
H.235	Specifies the H.235 type for the H.323 account. <ul style="list-style-type: none"> • Disabled—do not use H.235 in H.323 calls. • Enabled—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 143.	Web User Interface

To configure H.323 account via the web user interface:

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

2. Configure the H.323 account settings.

Setting	Value
Register Status	Registered
H.323 Active	Enabled
H.323 Name	90000
H.323 Extension	90000
Gatekeeper ID	
Gatekeeper Mode	Manual
Gatekeeper IP Address 1	h323.iot.yealink.com
Port	1719
Gatekeeper IP Address 2	
Port	1719
Gatekeeper Authentication	Disabled
Gatekeeper Username	
Gatekeeper Password	
H.460 Active	Disabled
H.323 Tunneling	Disabled
H.235	Disabled

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** .

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 signal with a minimum number of bits while retaining quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The following table summarizes the supported codecs on the system:





Codec	Algorithm	Bit Rate	Sample Rate	Reference
G722	G.722	64 Kbps	16 Ksps	RFC 3551

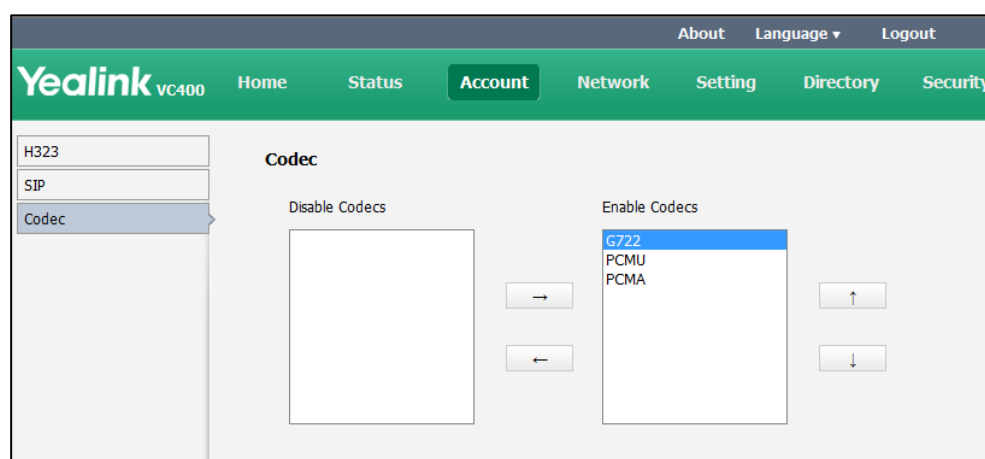
Codec	Algorithm	Bit Rate	Sample Rate	Reference
PCMU	G.711	64 Kbps	8 Ksps	RFC 3551
PCMA	G.711	64 Kbps	8 Ksps	RFC 3551

Codecs parameters on the system are described below:

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

To configure codecs via the 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 codec from the Enable Codecs column, and click  or  to adjust the priority of the selected codecs.



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

Call Type

The system supports SIP and H.323 protocols for incoming and outgoing calls. The default call type 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

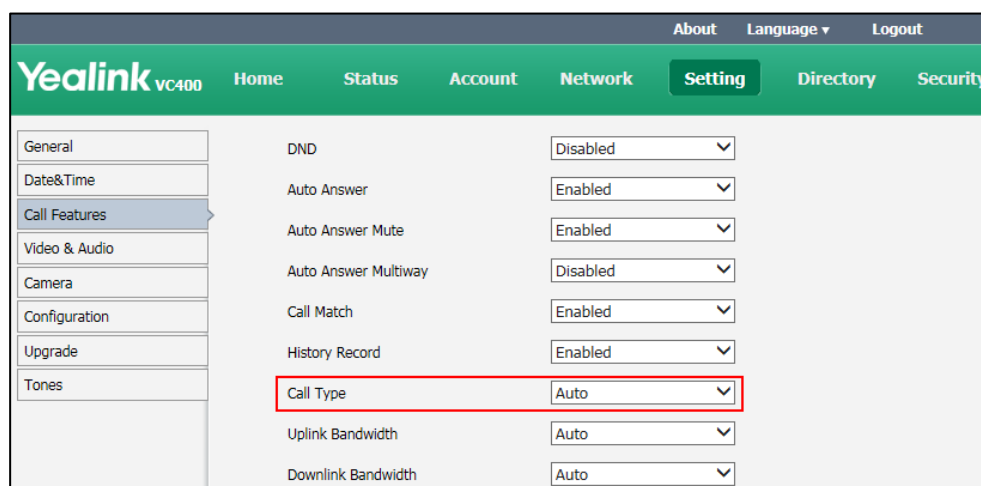
to place calls. Ensure the remote system supports the same protocol.

The call type parameter on the system is described below:

Parameter	Description	Configuration Method
Call Type	<p>Specifies the preferred call type for placing calls.</p> <ul style="list-style-type: none"> Auto—the system automatically uses the available call type. 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 Web User Interface</p>

To configure call type via the web user interface:

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



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

To configure call type via the remote control:

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

Do Not Disturb

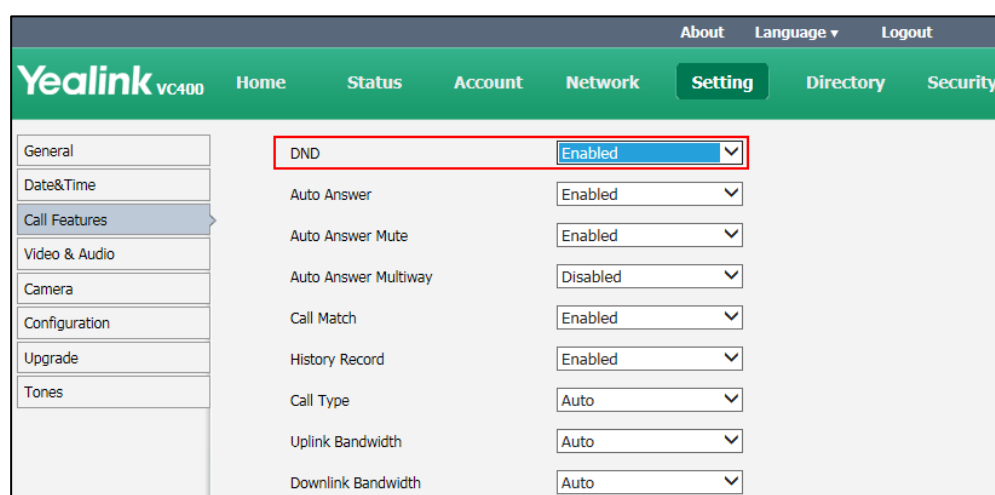
Do not Disturb allows the system to reject all incoming calls automatically. You can activate the DND mode for the system when it is idle, and the DND mode will be deactivated after the system places a call. You can also activate the DND mode for the system during a call, and the DND mode will be deactivated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

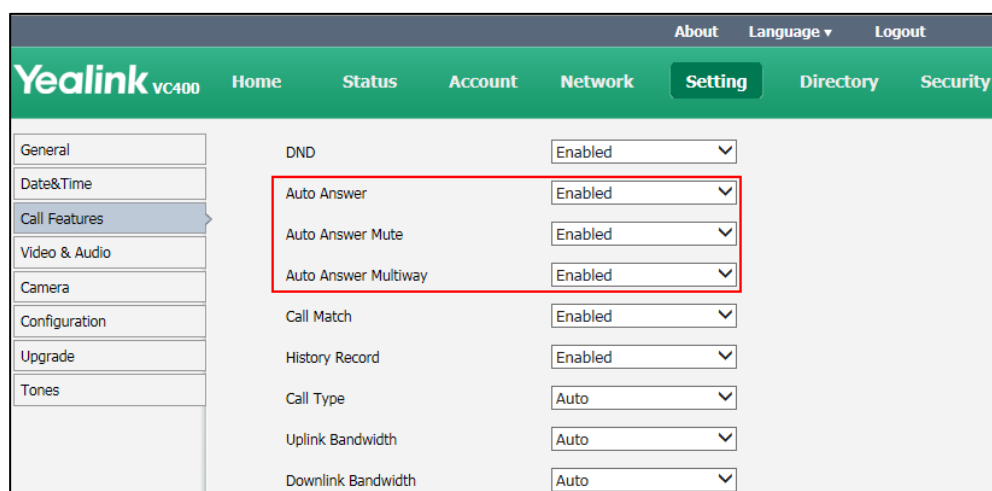
Auto answer parameters on the system are described below:

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	Remote Control Web User Interface

To configure auto answer via the 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**.
4. Select the desired value from the pull-down list of **Auto Answer Multiway**.



5. 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:

1. Select **Menu->Call Features**.
2. Check the **Auto Answer** checkbox.
3. Check the **Auto Answer Mute** checkbox.
4. Check the **Auto Answer Multiway** checkbox.
5. 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, and display results on the pre-dialing 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 about how to configure source list, refer to [Search Source List in Dialing](#) on page 126.

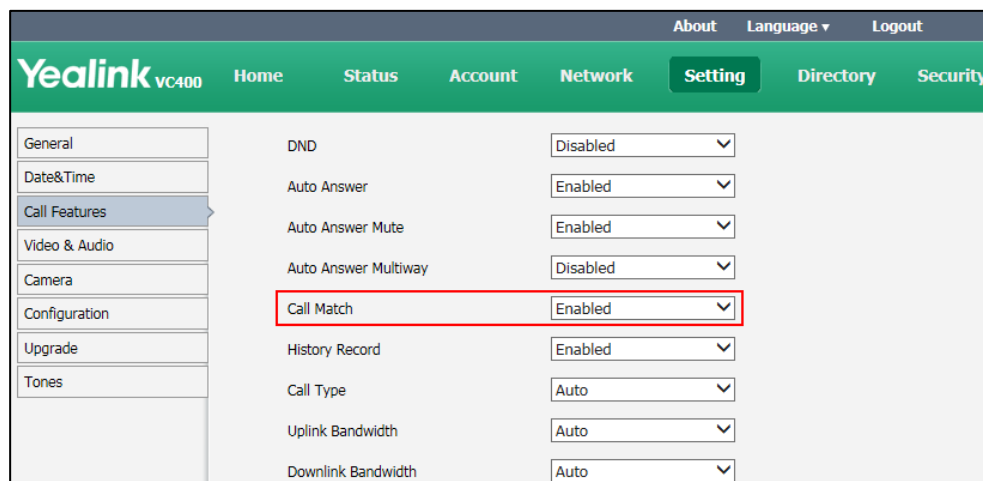
Parameter of call match on the system is described below:

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

Parameter	Description	Configuration Method
	Default: Enabled	

To configure call match via the 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

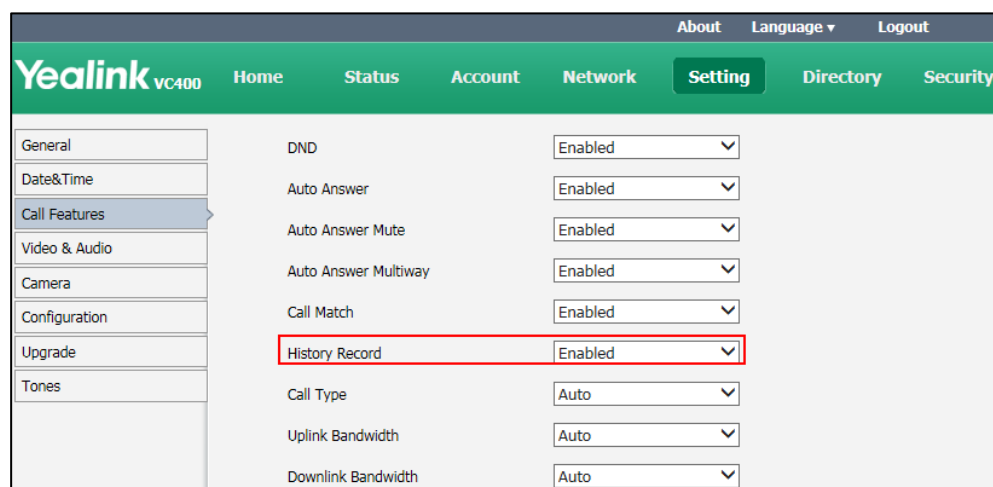
The system maintains a local call history, which contains call information such as remote party identification, time and date, and call duration. Users can manage call history list via the remote control, web user interface and VCP40 phone. To save call history, you must enable the history record feature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

The save call history parameter on the system is described below:

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

To configure save call history via the 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 save call history 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. You can specify the uplink and downlink bandwidths for the system to achieve the best result. Uplink bandwidth is the maximum transmitting bandwidth, and downlink bandwidth is the maximum receiving bandwidth. 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 dialing screen.

Note

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

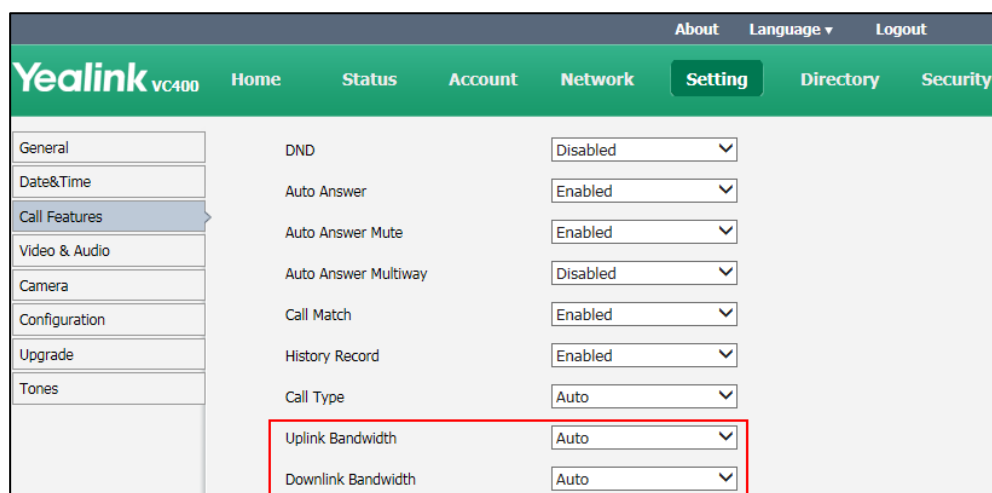
Bandwidth settings parameters on the system are described below:

Parameter	Description	Configuration Method
Uplink Bandwidth	Specifies the maximum transmitting bandwidth for the	Remote Control Web User Interface

Parameter	Description	Configuration Method
	system. Default: Auto If Auto is selected, the system will select the appropriate uplink bandwidth automatically.	
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 the 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**.



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.

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 Control of Near Camera](#)
- [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 the user makes 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 the 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 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, and Tones. The main content area is titled 'General Information' and contains several configuration fields. The 'Site Name' field is highlighted with a red rectangle and shows 'Yealink VC400'. Other fields include 'Automatic Sleep Time' (10 Min), 'Backlight Time' (Always On), 'Hide IP address' (Disabled), 'ReLogOffTime' (5), and 'Key Tone' (On).

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 backlight time for the VCP40 phone according to your actual needs.

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

- **Always On:** Backlight is turned on permanently.
- **15 s, 30 s, 10 min, 20 min, 30 min, 1 Hour, 2 Hour, 3 Hour, 4Hour:** 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.

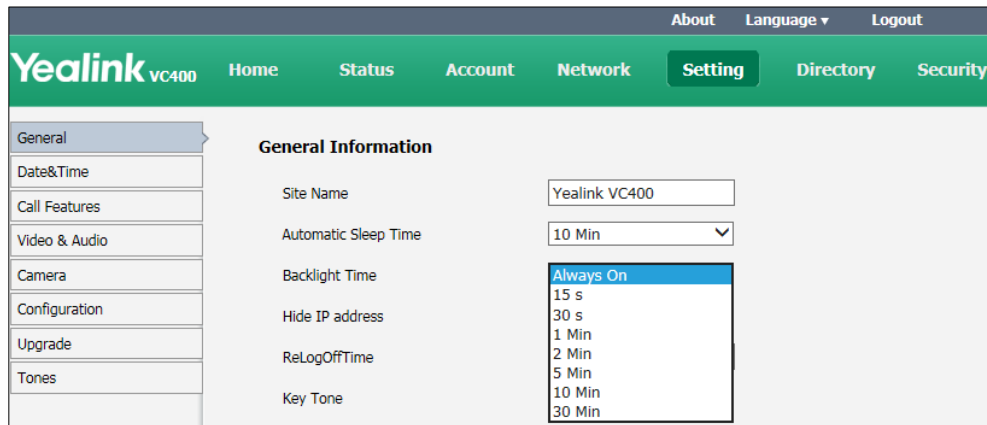
The backlight parameter on VCP40 phone is described below:

Parameter	Description	Configuration Method
Backlight Time	Configure the backlight time of	Web User Interface

Parameter	Description	Configuration Method
	the VCP40 phone. Default: Always On	

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

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



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.

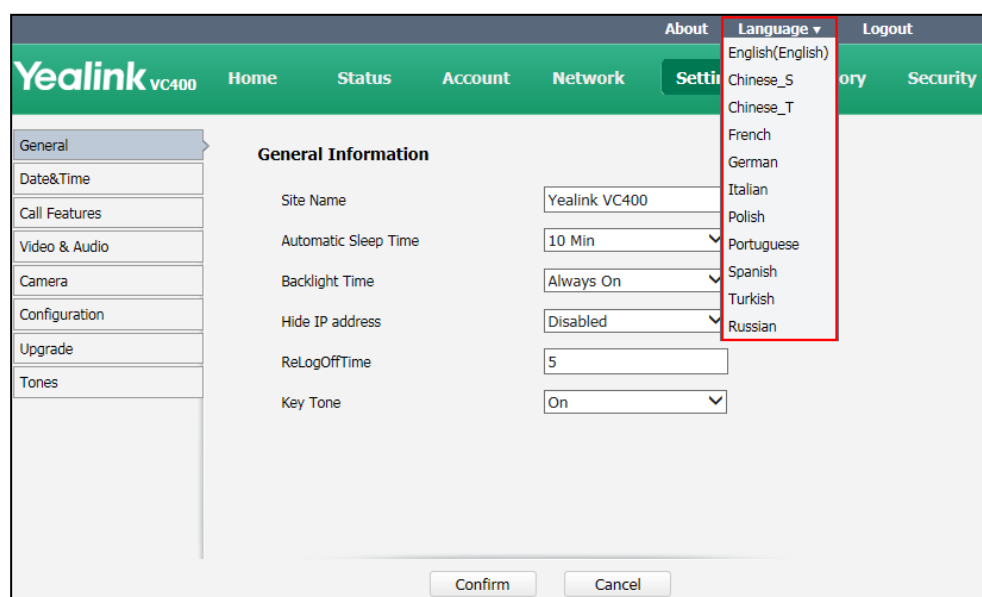
The default language of the web user interface is English. You can change the language of the web user interface via the web user interface. The available languages for system are English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish and Russian.

The language parameter on the system is described below:

Parameter	Description	Configuration Method
Language	Specifies the language for the web user interface	Web User Interface
Language	Specifies the language for the LCD screen of the display device and the VCP40 phone. Default: English	Remote Control

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

Time and Date

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 can be configured manually or obtained by DHCP via DHCP Option 42. 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	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 the primary NTP server. Default: cn.pool.ntp.org	Remote Control Web User Interface
Secondary Server/NTP Secondary Server	Configures the 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. • Enabled-use DST. You can manually configure the start time, end time and offset according to your needs.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<ul style="list-style-type: none"> 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 of the Daylight Saving Time is set to Enabled.</p>	Web User Interface
DST Start Month	When the DST calculation method is set to By Week .	Web User Interface
DST Start Day of Week		

Parameter	Description	Configuration Method
DST Start Day of Week Last in Month	Configures the time to start DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	
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. <ul style="list-style-type: none"> WWW MMM DD DD-MMM-YY YYYY-MM-DD DD/MM/YYYY MM/DD/YY 	Remote Control Web User Interface

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

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

1. Click on **Setting-> Date& Time**.
2. Select the desired value from the pull-down list of **DHCP 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 **Enabled** from the pull-down list of **Daylight Saving Time**.
 - 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.
7. Click **Confirm** to accept the change.

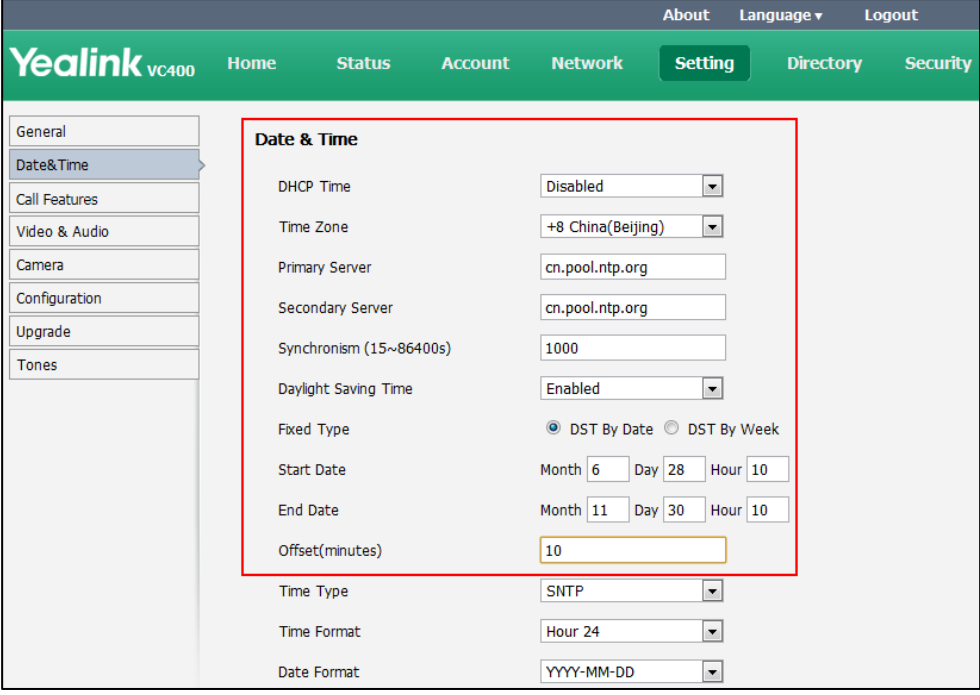
To configure the NTP server, time zone and DST via the web user interface:

1. Click on **Setting->Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Select the desired value from the pull-down list of **Daylight Saving Time**.

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

- Mark the **DST By Date** radio box in the **Fixed Type** field.
Enter the start time in the **Start Date** field.

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



Date & Time

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

Fixed Type: ☒ DST By Date ☐ DST By Week

Start Date: Month 6 Day 28 Hour 10

End Date: Month 11 Day 30 Hour 10

Offset(minutes): 10

Time Type: SNTP

Time Format: Hour 24

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 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', 'Date&Time' (highlighted), 'Call Features', 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', and 'Tones'. The 'Date & Time' settings are displayed, with a red box highlighting the 'Fixed Type' section. The settings are as follows:

Field	Value
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
Fixed Type	<input type="radio"/> DST By Date <input checked="" type="radio"/> DST By Week
DST Start Month	June
DST Start Day of Week	Sunday
DST Start Day of Week Last in Month	Second In Month
Start Hour of Day	10
DST Stop Month	November
DST Stop Day of Week	Sunday
DST Stop Day of Week Last in Month	Second In Month
End Hour of Day	10
Offset(minutes)	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 the 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 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', 'Date&Time' (highlighted), 'Call Features', 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', and 'Tones'. The 'Date & Time' settings are displayed, with a red box highlighting the 'Manual Time' section. The settings are as follows:

Field	Value
DHCP Time	Disabled
Time Type	Manual Time
Date	Year 2014 Month 8 Day 22
Time	Hour 14 Minute 2 Second 22
Time Format	Hour 24
Date Format	YYYY-MM-DD

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

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

1. Select **Menu->Basic->Date & Time**.
2. Configure the desired values according to the need.
3. 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 the web user interface:

1. 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'. Below this is a green header with 'Yealink VC400' and tabs for 'Home', 'Status', 'Account', 'Network', 'Setting' (selected), 'Directory', and 'Security'. On the left, a sidebar lists menu items: 'General' (selected), 'Date&Time', 'Call Features', 'Video & Audio', 'Camera', 'Configuration', 'Upgrade', and 'Tones'. The main content area is titled 'General Information' and contains several settings: 'Site Name' (Yealink VC400), 'Automatic Sleep Time' (20 Min, highlighted with a red box), 'Backlight Time' (Always On), 'Hide IP address' (Disabled), 'ReLogOffTime' (5), and 'Key Tone' (On).

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

To configure the automaticsleep 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 the 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 parameter to hide IP address 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 the 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'. Below this is a green header with 'Yealink VC400' and tabs for 'Home', 'Status', 'Account', 'Network', 'Setting' (selected), 'Directory', and 'Security'. On the left, a sidebar lists various settings categories: General, Date&Time, Call Features, Video & Audio, Camera, Configuration, Upgrade, and Tones. The main content area is titled 'General Information' and contains several settings: Site Name (Yealink VC400), Automatic Sleep Time (20 Min), Backlight Time (Always On), Hide IP address (Enabled, highlighted with a red box), ReLogOffTime (5), and Key Tone (On).

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 the web user interface.

The relog offtime parameter is described below:

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

To configure the relog offtime via the web user interface:

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

2. Enter the desired time in the **ReLogOffTime** 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', and 'Tones'. The 'General Information' section contains the following fields:

- Site Name: Yealink VC400
- Automatic Sleep Time: 20 Min
- Backlight Time: Always On
- Hide IP address: Enabled
- ReLogOffTime: 5** (highlighted with a red box)
- Key Tone: On

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

Key Tone

You can enable the key tone feature for the system to play a key tone when you press the key on the remote control. If you disable this feature, the system will not play a key tone when you press the 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 the 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, similar to the previous one. The 'General Information' section now includes the 'ReLogOffTime' field (set to 5) and the 'Key Tone' field, which is highlighted with a red box and set to 'On'.

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.

Audio Setting

Audio Output Device

The system supports the following audio output devices:

- **HDMI** (built-in speakerphone of the display device)
- **Line Output** (speakerphone connected to the Line Out port on the VC400/VC120 codec)
- **VCS Phone** (VCP40 phone)
- **Line out + HDMI** (speakerphone connected to the Line Out port on the VC400/VC120 codec and built-in speakerphone of the display device)

By default, the system automatically selects the available audio output devices. During a call, the system will select the audio output device with higher priority, and the priority is: VCS Phone>Line Output>HDMI. You can specify which audio output device to be used according to the current environment.

If Line Output is selected, ensure the speakerphone is connected to the Line Out port on the VC400/VC120 codec. If HDMI is selected, ensure your display device has a built-in speakerphone. If Line out + HDMI is selected, ensure speakerphone is connected to the Line Out port on the VC400/VC120 codec and your display device has a built-in speakerphone.

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 higher priority. • HDMI - selects the built-in speakerphone of the display device. • Line Output - selects the 	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>speakerphone connected to the Line Out port on the VC400/VC120 codec.</p> <ul style="list-style-type: none"> VCS Phone - selects the VCP40 phone. Line out + HDMI -selects the speakerphone connected to the Line Out port on the VC400/VC120 codec and built-in speakerphone of the display device. <p>Default: Auto</p>	

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

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

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:

- **Line Input** (microphone connected to the Line In port on the VC400/VC120 codec)
- **VCS Phone** (VCP40 phone)

By default, the system automatically selects the available audio input device. You can specify which audio input device to be used according to the current environment.

If the VCS Phone is selected and the Audio In port on the VC400/VC120 codec is connected to the VCP40 phone, the system will use the VCP40 phone as audio input device. If Line Input is selected, ensure a speakerphone is connected to the Line In port on the VC400/VC120 codec.

The audio output device parameter is described below:

Parameter	Description	Configuration Method
Audio Input	<p>Specifies the audio input device for the system.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • Auto- selects all available audio Input devices. • Line Input- selects the microphone connected to the Line In port on the VC400/VC120 codec. • VCS Phone- selects the VCP40 phone. <p>Default: Auto</p>	<p>Remote Control</p> <p>Web User Interface</p>

To configure the audio input device via the web user interface:

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

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

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, and Tones. The main content area is titled 'Audio Settings' and contains several configuration sections:

- Audio Settings:** Includes 'Audio Input' (a dropdown menu highlighted with a red box, currently set to 'VCS Phone'), 'Audio Output' (dropdown set to 'Auto'), 'Ringer Volume' (input field with value '2'), and 'Output volume' (input field with value '8').
- Presentation:** Includes 'H.239' (dropdown set to 'Enabled'), 'BFCP' (dropdown set to 'Disabled'), and 'Mix' (dropdown set to 'On').
- Far-end Camera Control:** Includes 'FECC(H.323)' (dropdown set to 'Enabled').

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.

Volume

You can adjust the ringer volume and output volume of the system. Ringer volume refers to the ringer volume when the system receives an incoming call. Output volume refers to the volume of the audio output device currently in use. If you select the VCP40 phone as audio output device, you can press the volume key on the VCP40 phone to adjust the ringer volume of the phone when the phone is idle, and adjust the speakerphone volume during an active call.

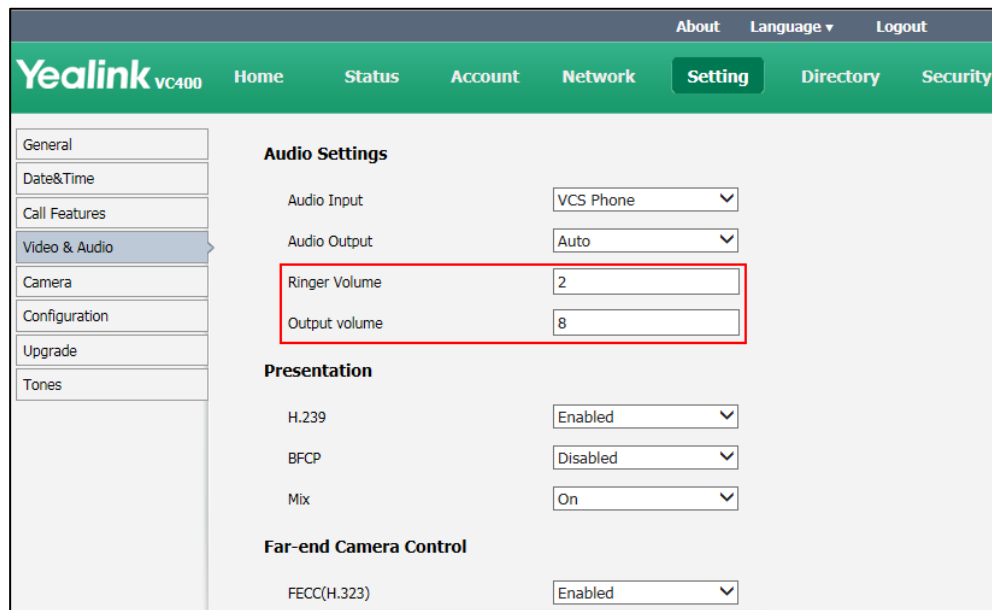
Volume configuration parameters are described below:

Parameter	Description	Configuration Method
Ringer Volume	Specifies the ringer volume for the system. Valid values: Integer from 1 to 10 Default: 8	Web User Interface
Output volume	Specifies the output volume for the system.	Web User Interface

Parameter	Description	Configuration Method
	Valid values: Integer from 1 to 10 Default: 8	

To configure the volume via the web user interface:

1. Click on **Setting->Video & Audio**.
2. Enter the desired value in the **Ringer Volume** field.
3. Enter the desired value in the **Output Volume** field.



4. Click **Confirm** 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	Specifies the maximum MTU size (in bytes) of video packets sent by the system.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	<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 implement the changes.</p>	

To configure MTU via the 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' (highlighted), 'Setting', 'Directory', and 'Security'. On the left, a sidebar lists 'LAN Configuration', 'NAT/Firewall', 'Advanced' (highlighted), and 'Diagnose'. The main content area shows various network settings: LLDP (Active: Disabled, Packet Interval: 60), VLAN (Internet Port: Disabled, VID: 1, Priority: 0, DHCP VLAN: Enabled, Option: 132), QoS (Audio Priority: 60, Video Priority: 34, Data Priority: 63), and MTU (Video MTU: 1400). The MTU section is enclosed in a red rectangular box.

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(0-1500)** 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, such as video or document. Both the video and the content 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 to send content in H.323 calls. BFCP protocol is used to send content in SIP calls. You can specify the protocol the system to use. Before enabling the desired protocol, ensure that the protocol is supported and enabled by the far site you wish to will call. If the far site does not support the protocol for sharing content, MCU will automatically mix the content and video, and send them in one channel. For more information about mix sending, refer to [Mix Sending](#) on page 102.

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. Default: Disabled	Web User Interface

To configure dual-stream protocol via the web user interface:

1. Click on **Setting->Video & Audio**.
2. In the **Presentation** block, select the desired value from the pull-down list of **H.239**.

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

The screenshot shows the Yealink VC400 web interface. The left sidebar contains a menu with options: General, Date, Call Features, Video & Audio (selected), Camera, Configuration, Upgrade, and Tones. The main content area is titled 'Audio Settings' and includes a 'Presentation' section highlighted with a red box. In this section, 'H.239' is set to 'Enabled' and 'BFCP' is set to 'Enabled'. Below this, the 'Mix' setting is set to 'On'. The 'Far-end Camera Control' section includes several other settings: 'FECC(H.323)' (Enabled), 'FECC(SIP)' (Disabled), 'Far Control Near Camera' (Enabled), 'Far Set of Camera Presets' (Disabled), and 'Far Move to Camera Presets' (Disabled).

4. 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 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 the web user interface:

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

- In the **Presentation** block, select the desired value from the pull-down list of **Mix**.

- 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>

Parameter	Description	Configuration Method
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 reproduction. ATW—Automatically adjust the white balance based on the video image shoot by the camera. Manual—Manual set red and blue gain. <p>Default: Auto</p>	<p>Remote Control</p> <p>Web User Interface</p>
Red Gain	<p>Configures the red gain of the camera.</p> <p>Valid Values: 0-100</p> <p>Default: 82</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>

Parameter	Description	Configuration Method
Blue Gain	Configures the blue gain of the camera. Valid Values: 0-100 Default: 69 Note: You can set this parameter only when the white balance mode is configured to Manual.	Remote Control Web User Interface
Saturation	Configures the saturation of the camera. Valid Values: 0-14 Default: 3	Remote Control Web User Interface
Sharpness	Configures the sharpness of the camera. Valid Values: 0-14 Default: 1 Note: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.	Remote Control Web User Interface
Brightness	Configures the brightness of the camera. Valid Values: 0-100 Default: 8	Remote Control Web User Interface
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	Specifies the noise reduction (3D)	Remote Control

Parameter	Description	Configuration Method
(3D)	<p>mode.</p> <ul style="list-style-type: none"> • Off • Low • Middle • High <p>Default: Off</p>	Web User Interface
Hangup Mode	<p>Enables or disables the reversed mode of the camera.</p> <p>If the reversed mode is enabled, the shooting picture will be displayed reversibly.</p> <p>Default: Off</p>	<p>Remote Control</p> <p>Web User Interface</p>
Camera Pan Direction	<p>Configures the pan direction of the camera.</p> <ul style="list-style-type: none"> • Normal • Reversed <p>Default: Normal</p> <p>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 control. In this case, you can set the camera pan direction to Reversed.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Camera Map	<p>Enables or disables the preview of camera presets.</p> <p>Default: On</p> <p>Note: If it is set to on, you can view the pre-saved camera presets.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Clear Preset	Clears all camera presets.	<p>Remote Control</p> <p>Web User Interface</p>
Reset Camera	<p>Reset the camera settings to factory defaults.</p> <p>Note: The camera presets will</p>	<p>Remote Control</p> <p>Web User Interface</p>

Parameter	Description	Configuration Method
	also be cleared.	

To configure camera settings via the 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 Control of Near Camera

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 of the 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 camera presets.

Far control of the near camera 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 control of near camera via the 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 'General', 'Date', 'Call Features', 'Video & Audio' (selected), 'Camera', 'Configuration', 'Upgrade', and 'Tones'. The main content area is titled 'Audio Settings' and includes sections for 'Audio Settings' (Audio Input: Auto, Audio Output: Auto, Ringer Volume: 1, Output volume: 8), 'Presentation' (H.239: Enabled, BFCP: Disabled, Mix: On), and 'Far-end Camera Control' (FECC(H.323): Enabled, FECC(SIP): Disabled, Far Control Near Camera: Enabled, Far Set of Camera Presets: Enabled, Far Move to Camera Presets: Enabled). The 'Far-end Camera Control' section is enclosed in a red rectangular box.

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

To configure far control of near camera 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 two camera control protocols: SIP and H.323. You can specify the camera control protocol for performing far control of the near camera. The camera control protocol should be the same as the protocol the call uses. To achieve far control of the near camera, both the far site and near site should enable the camera control protocol simultaneously. If the protocol is not enabled on one site, far control of near camera cannot be performed. For example, a SIP call is established between two sites, the two sites must enable the SIP protocol simultaneously to perform far control of the near camera. If two camera control protocols are both enabled, the system will select the appropriate camera control protocol according to protocol the call uses.

Camera control protocol parameters are described below:

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

To configure camera control protocol via the web user interface:

1. Click on **Setting->Video & Audio**.
2. Select the desired value from the pull-down list of **FECC(H.323)**.

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

The screenshot shows the Yealink VC400 web interface. The left sidebar contains a menu with options: General, Date, Call Features, Video & Audio (selected), Camera, Configuration, Upgrade, and Tones. The main content area is titled 'Audio Settings' and includes sections for 'Audio Settings', 'Presentation', and 'Far-end Camera Control'. The 'Far-end Camera Control' section is highlighted with a red box and contains the following settings:

Setting	Value
FECC(H.323)	Enabled
FECC(SIP)	Enabled
Far Control Near Camera	Enabled
Far Set of Camera Presets	Disabled
Far Move to Camera Presets	Disabled

4. 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	Customizes the ring-back tone for the system. tone = element1[,element2] [,element3]...[,element8]	Web User Interface

Parameter	Description	Configuration Method
	<p>Where</p> <p>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, 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 about 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>	Web User Interface

Parameter	Description	Configuration Method
	<p>For more information about 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>	
Auto Answer	<p>Customizes the auto answer tone for the system.</p> <p>For more information about 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 the 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'. Below this is a green header with 'Yealink VC400' and a menu with 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left, a sidebar lists various settings: General, Date, Call Features, Video & Audio, Camera, Configuration, Upgrade, and Tones (highlighted). The main content area shows the 'Tones' configuration. A red box highlights the 'Select Country' dropdown (set to 'Custom') and the 'Auto Answer' tone field, which contains the value '!800+500+1000+900/6000'. Other visible tone fields include 'Ring Back' (2000+800+600/500,3000+), 'Busy' (700+1200+400+6000/5000), and 'Call Waiting' (400+1200/500,1000+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 4 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 the web user interface, remote control and the VCP40 phone. But you can only edit or delete the local directory via the web user interface.

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

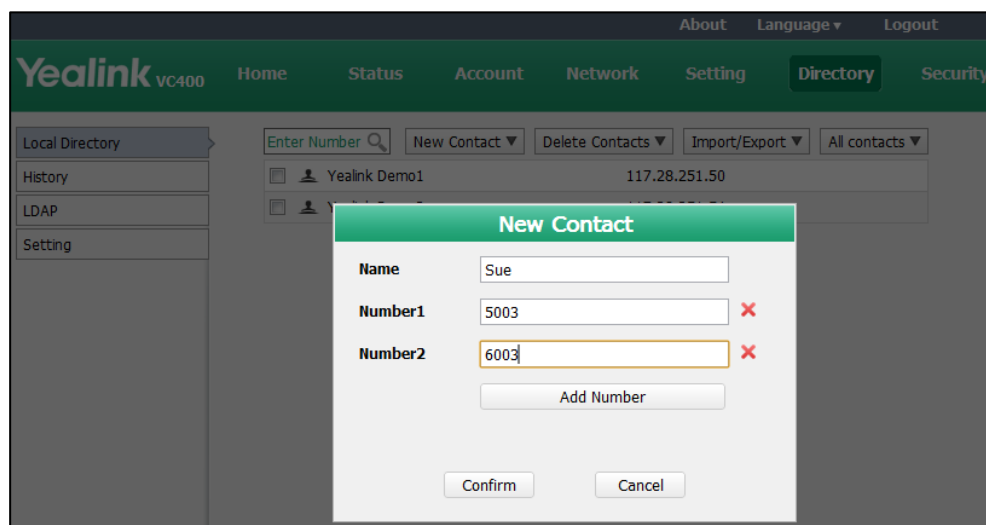
Note

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

To add local contacts via the 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.

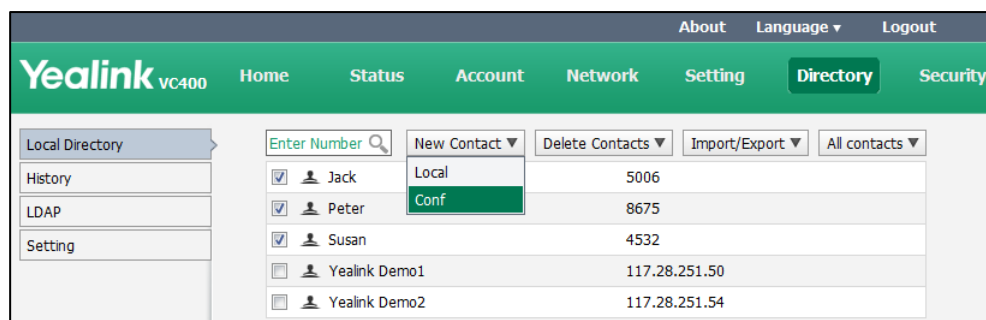
- Click **Add Number**, enter other number of the contact.



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

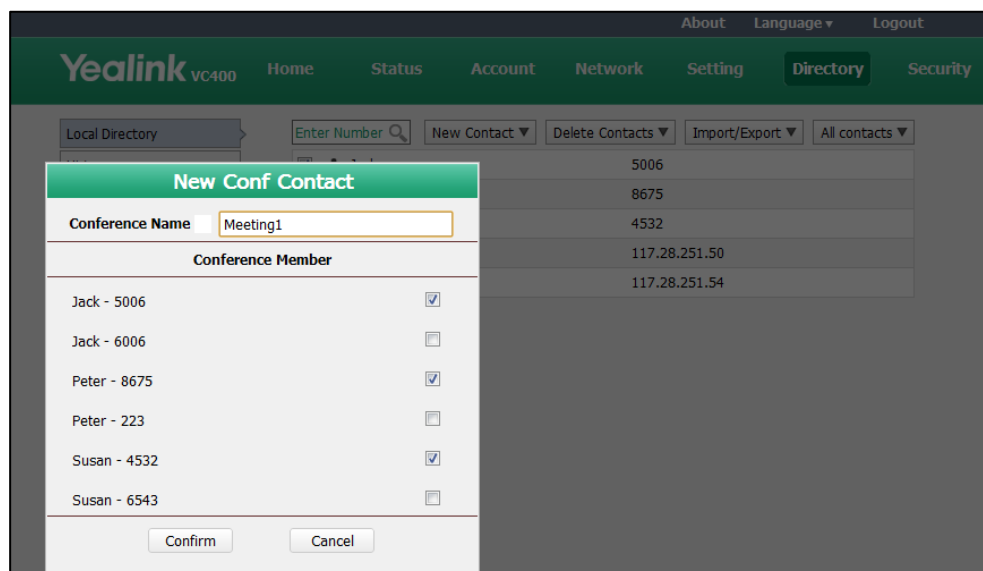
To add conference contacts via the web user interface:

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




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

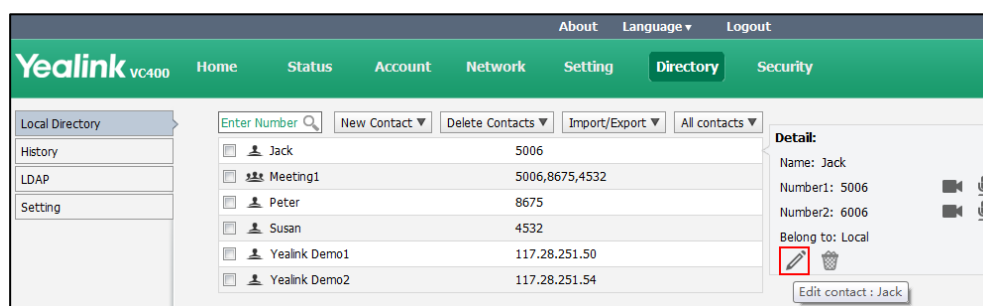
If multiple numbers are stored for the selected contacts, the system will select number 1 by default.



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



To edit contacts via the web user interface:

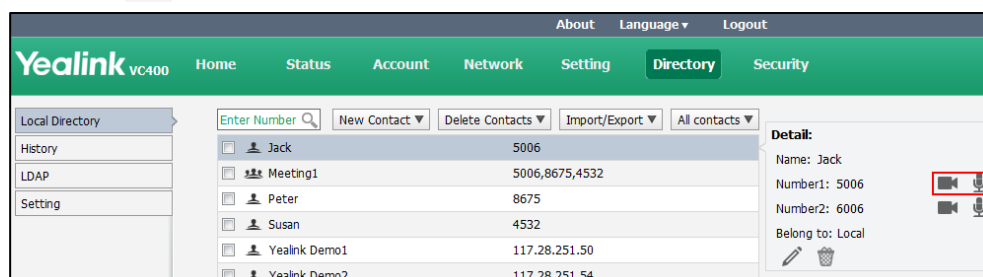
1. Click on **Directory->Local Directory**.
2. Hover your cursor over the contact you want to edit.
3. Click  in the pop-up detail box.



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

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

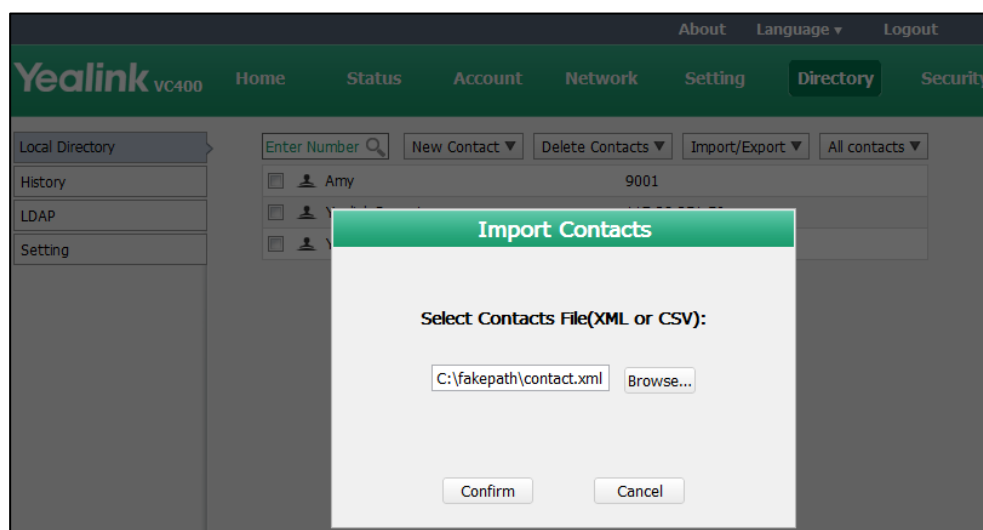
1. Click on **Directory->Local Directory**.
2. Hover your cursor over the desired contact.
3. Click  or  in the pop-up detail box to place a video or audio call.



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 the web user interface:

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



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

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

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

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

The web user interface is shown below:

Import CSV File Preview

☐ The first line as the title ☐ Delete Old Contacts

	display_name	office_number	mobile_number	other_number	line	ring
1	6002	6002			-1	
2	Aimee	2529			-1	Auto
3	Amy	2050			-1	Auto
4	Sam	2010			-1	Auto

Confirm Cancel

6. (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.
7. (Optional.) Check the **Delete Old Contacts** checkbox.
It will delete all existing contacts while importing the contact list.
8. 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: number3:

	display_name	group	number1	number2	number3
1	6002	Conference	6002		
2	Aimee	Conference	2529		
3	Amy	Conference	2050		
4	Sam	Conference	2010		
5	Stella	Conference	6009		
6	Susie	Conference	6002		
7	Yealink	Conference	9002		
8	display_name	Conference	office_number		

9. 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 the web user interface:

1. Click on **Directory->Local Directory**.
2. Click **Import/Export**.
3. Click **Export XML** or **Export CSV**.
4. 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 can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using 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 devicescreen 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 LADP is in the enabled search source lists)
- In the **Directory** screen, select **Company** to enter the LDAP search screen, and then enter the content 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	Web User Interface

Parameter	Description	Configuration Method
	LDAP searching. 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	Web User Interface

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

For more information about string representations of LDAP query filters, refer to RFC 2254 document: <http://www.ietf.org/rfc/rfc2254>.

To configure LDAP via the 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.

Setting	Value
LDAP Enable	Enabled
LDAP Name Filter	((!(cn=%)(sn=%)))
LDAP Number Filter	((!(telephoneNumber=%)(c))
LDAP Server Address	openladp.iot.yealink.com
Port	389
LDAP User Name	cn=manager, dc=yealink,
LDAP Password	*****
LDAP Base	dc=yealink, dc=cn
Max Hit(1~32000)	50
LDAP Name Attributes	cn sn
LDAP Number Attributes	telephoneNumber mobile
LDAP Display Name	%cn
Protocol	Version3
Match Incoming Call	Enabled
LDAP Sorting Results	Enabled

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 the web user interface or the remote control, but you can delete call history only via the 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 77.

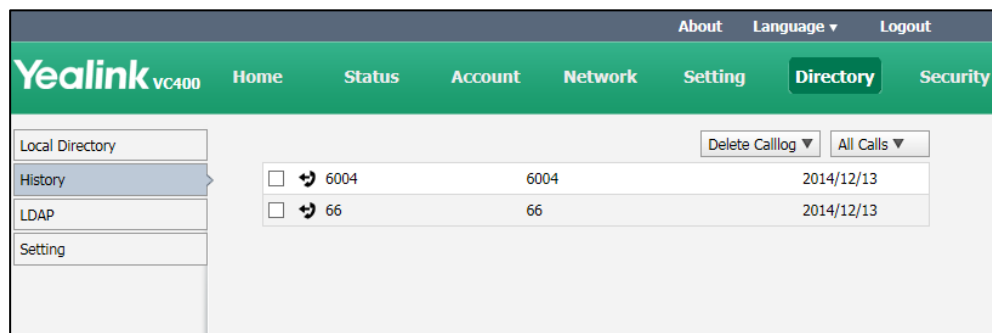
Note

VC120 video conferencing system only supports local call history. It does not support conference call history.

To view call history via the web user interface:

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

The web user interface displays all call history.





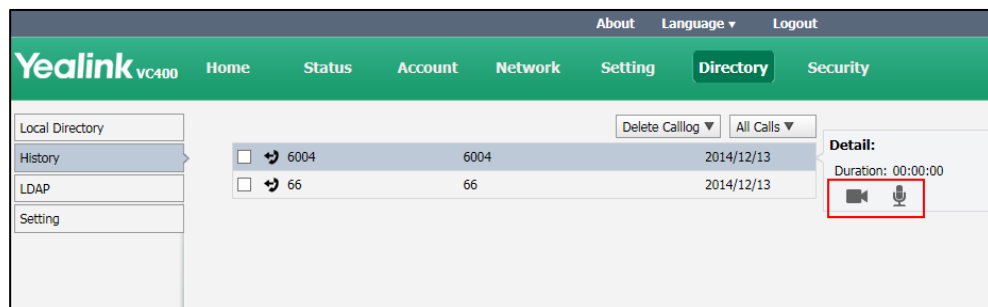
2. Click **All Calls**, select the desired call history list.

To place a call from the call history list via the 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 audio call.



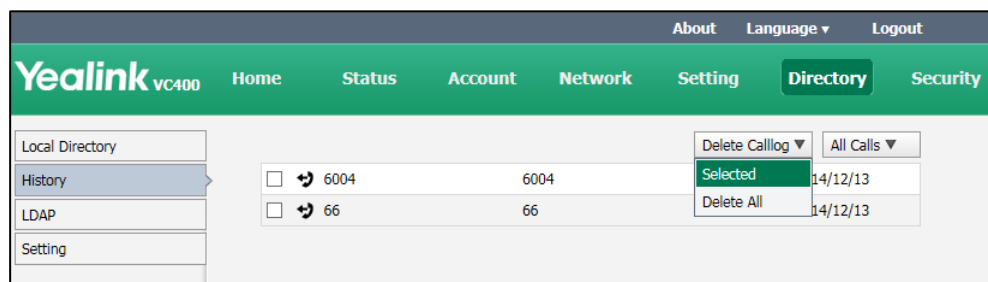
The web user interface prompts "Connecting, please wait!" and jumps automatically to the **Home** screen.

To delete an entry from the call history list via the web user interface:

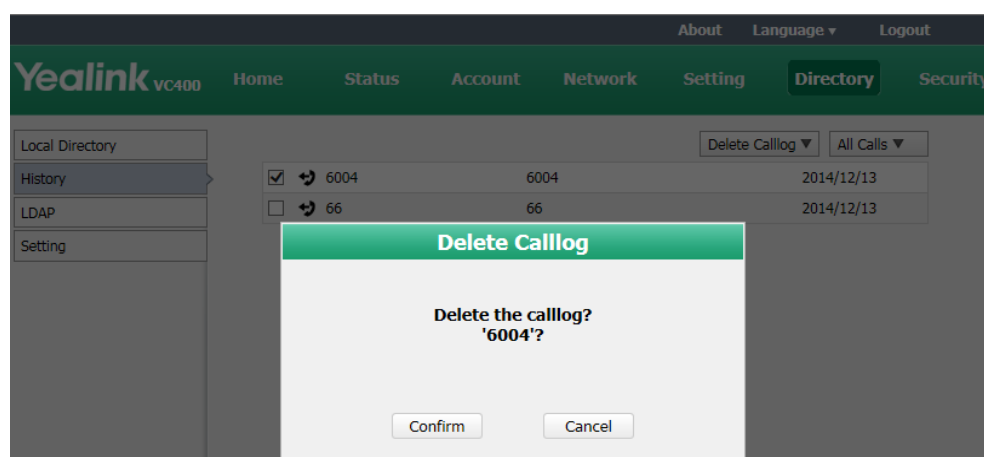
1. Click on **Directory->History**.

The web user interface displays all call history.

2. Mark the checkbox for the entry you want to delete.
3. Click **Delete Calllog**, and select **Selected**.



The web user interface prompts "Delete the callog?"



5. Click **Confirm** to delete the callog.


You can also select **Delete All** from the pull-down list of **Delete Callog** to delete all callog.

Search Source List in Dialing


When you enter a few characters in the dialing screen, the system will search **for** matching 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 about how to configure LDAP, refer to [LDAP](#) on page 120.

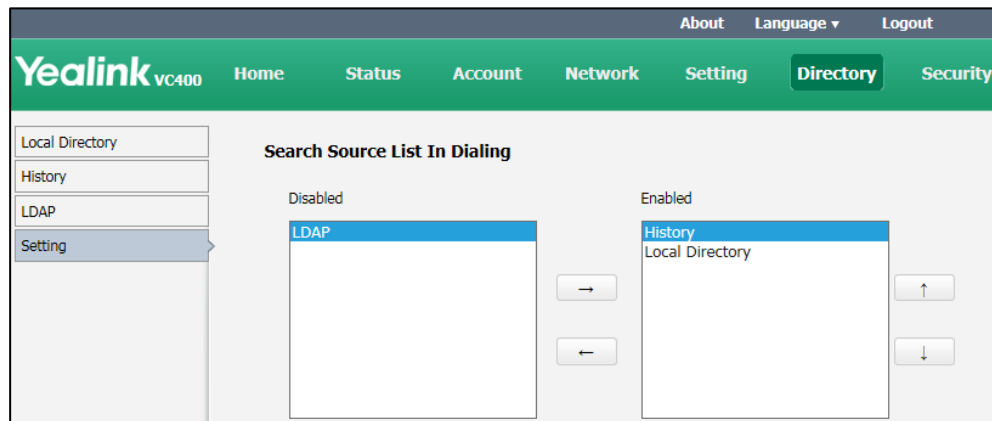
To configure search source list in dialing via the web user interface:

1. Click on **Directory->Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and click .

The selected list appears in the **Enabled** column.


3. Repeat step 2 to add more lists to the **Enabled** column.
4. (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. When two display devices are connected to the VC400/VC120 codec, the status bar on the main display device displays  icon. When the system is idle, the second display device displays a local video image by default. Menu and status bar are not displayed.

If a PC is connected to the PC port on the VC400/VC120 codec, the second display device displays the presentation of the PC by default. During a video call, the second display device displays a local video image by default. During a video call when the local system is sharing a presentation, the second display device also displays the presentation by default.

You can specify the display content on the second display device via the remote control.

To specify the displayed content on the second 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 second display device displays the selected content. The  icon is displayed on the focus content.

4. If the second display device displays the presentation initially, after reassigning the display content on the second display device, the presentation will automatically be displayed on the main display device.

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](#)

User Mode

Users can access the system menu options directly (except the “Advanced” menu option) on the display device. The “Advanced” menu option is protected by administrator privilege. You can enable the user mode to provide two levels of access for the menu options. 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 menu options (except the “Status” menu option). After the user mode is enabled, the user can login to the web user interface of the system with user privilege. The default user name is “user”.

User mode parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user mode. 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 login to 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 the 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 login to 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 mode.</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 the 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.

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 implement the changes.	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 implement the changes.	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 implement the changes.	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 implement the changes.	

To configure web server type via the 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: rmssserver (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 30 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 30 trusted

certificates, refer to [Appendix B: Trusted Certificates](#) on page 167.

- **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. <p>TLS is available only when the system is registered with a SIP server that supports TLS.</p>	<p>Remote Control</p> <p>Web User Interface</p>
Only Accept Trusted Certificates	<p>Enables or disables the system to only trust the server certificates in the Trusted Certificates list.</p>	<p>Web User Interface</p>

Parameter	Description	Configuration Method
	<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 implement the changes.</p>	
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 implement the changes.</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 implement the changes.</p>	Web User Interface
Upload Trusted Certificate File	<p>Upload the custom CA certificate to the system.</p> <p>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.</p>	Web User Interface
Device	Upload the customized CA	Web User Interface

Parameter	Description	Configuration Method
Certificates	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 implement the changes.	
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 the 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 links for About, Language, and Logout. The main menu has options for Home, Status, Account, Network, Setting, Directory, and Security. The left sidebar shows a tree view with License, Security (selected), Trusted Certs, and Server Certs. The main content area displays the 'Trusted Certs' configuration page. It features a table with 10 rows, each representing a certificate with an Index ID, Issued To, Issued By, Expiration, and a Delete checkbox. Below the table, there are three configuration options, each with a dropdown menu: 'Only Accept Trusted Certificates' (set to Enabled), 'Common Name Validation' (set to Disabled), and 'CA Certificates' (set to Default Certificates). A red box highlights these three settings. At the bottom, there is a section for 'Import Trusted Certificates' with a text input field for 'Upload Trusted Certificate File', a 'Browse...' button, and an 'Upload' button.

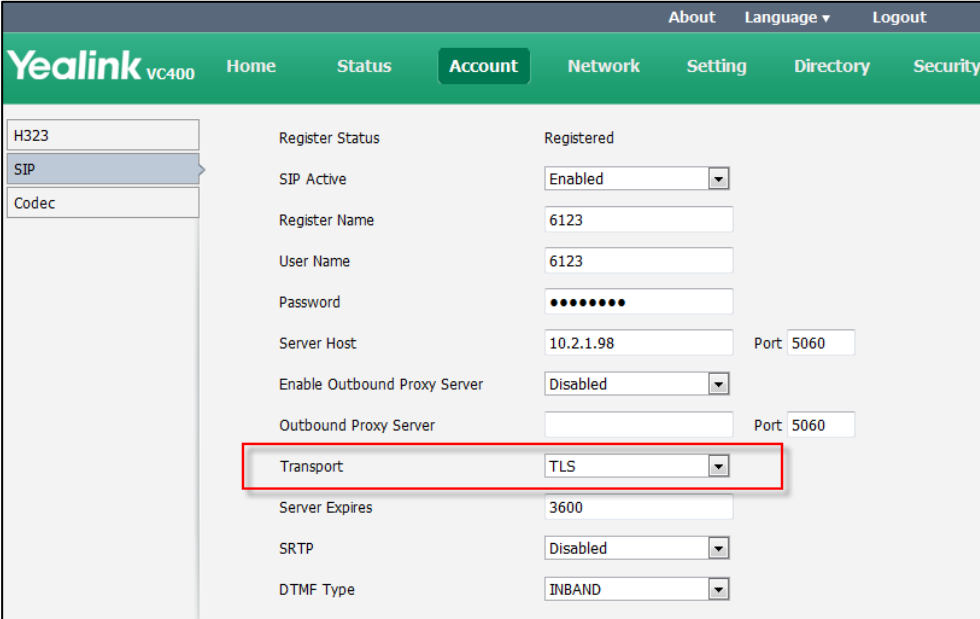
5. Click **Confirm** to accept the change.

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 the web user interface:

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



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 (selected), Network, Setting, Directory, and Security. On the left, a sidebar menu shows options for H323, SIP (selected), and Codec. The main content area is titled 'Register Status' and shows 'Registered'. The 'SIP Active' status is 'Enabled'. The 'Register Name' and 'User Name' are both '6123'. The 'Password' is masked with dots. The 'Server Host' is '10.2.1.98' 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 and shows 'TLS' selected. Other settings include 'Server Expires' at '3600', 'SRTP' as 'Disabled', and 'DTMF Type' as 'INBAND'.

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

To upload a CA certificate via the 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' (set to Disabled), 'Common Name Validation' (set to Disabled), and 'CA Certificates' (set to Default Certificates). A red box highlights the 'Import Trusted Certificates' section, which contains a text input for 'Upload Trusted Certificate File' with the value 'C:\fakepath\ca.crt', a 'Browse...' button, and an 'Upload' button.

- Click **Upload** to upload the certificate.

To configure the device certificate via the web user interface:

- Click on **Security->Server Certs**.
- Select the desired value from the pull-down list of **Device Certificates**.

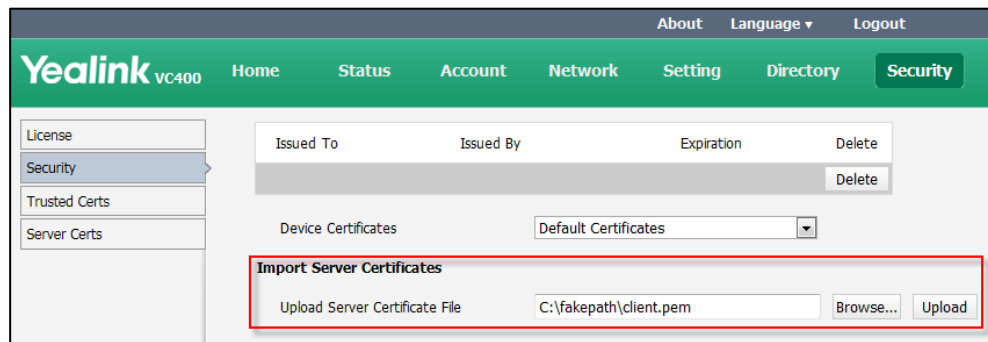
The screenshot shows the Yealink VC400 web interface. The top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting', 'Directory', and 'Security'. The left sidebar shows 'License', 'Security' (selected), 'Trusted Certs', and 'Server Certs'. The main content area displays a table of certificates with columns: Issued To, Issued By, Expiration, and Delete. A red box highlights the 'Device Certificates' dropdown menu, which is currently set to 'Default Certificates'. Below the dropdown is the 'Import Server Certificates' section, which contains a text input for 'Upload Server Certificate File', a 'Browse...' button, and an 'Upload' 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 the 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

Secure Real-Time Transport Protocol (SRTP) encrypts RTP streams during calls to avoid interception and eavesdropping. 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:NzFINTUwZDk2OGVIOTc3YzNkYTkwZWVhMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFM
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

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 for the SIP account.</p> <ul style="list-style-type: none"> Disabled—do not use SRTP in SIP calls. Enabled—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	Enabled	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Enabled	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

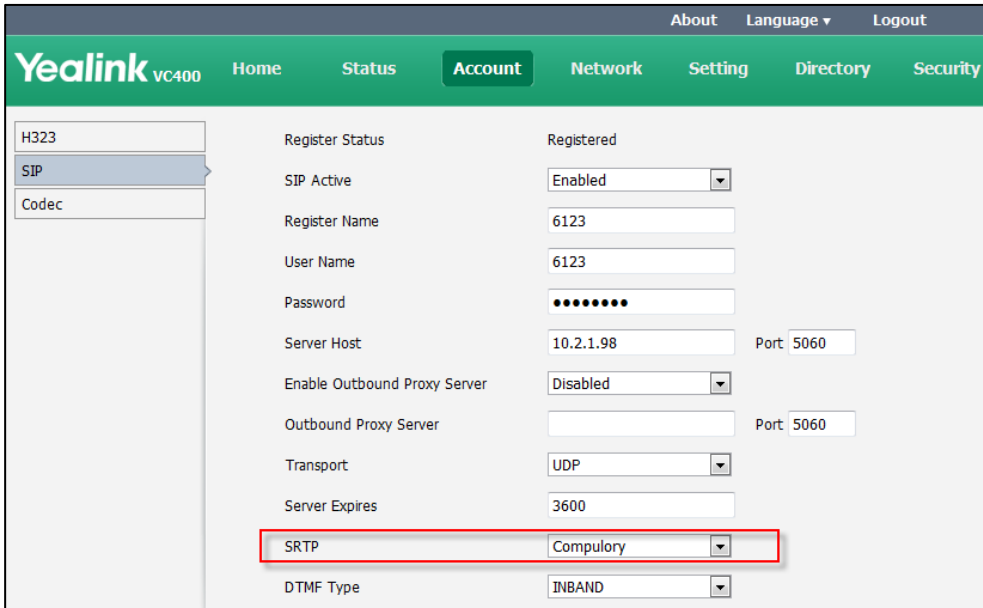
When SRTP is enabled on both systems, RTP streams will be encrypted, and the lock icon  appears on the display device of each system after successful negotiation.

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 134.

To configure SRTP via the web user interface:

1. Click on **Account->SIP**.
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, and the 'SIP' sub-tab is active. The 'SRTP' dropdown menu is highlighted with a red box, showing the 'Compulory' option selected. Other visible settings include: Register Status (Registered), SIP Active (Enabled), Register Name (6123), User Name (6123), Password (masked), Server Host (10.2.1.98), Port (5060), Enable Outbound Proxy Server (Disabled), Outbound Proxy Server (empty), Port (5060), Transport (UDP), Server Expires (3600), and DTMF Type (INBAND).

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

H.235

H.235 is the security recommendation for the H.3xx series systems. In particular, H.235 provides security procedures for H.323-, H.225.0-, H.245- and H.460-based systems. Yealink systems support H.235 for H.323 video conference 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	Specifies the H.235 type for the H.323 account.	Web User Interface

Parameter	Description	Configuration Method
	<ul style="list-style-type: none"> Disabled—do not use H.235 in H.323 calls. Enabled—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. <p>Default: Disabled</p>	

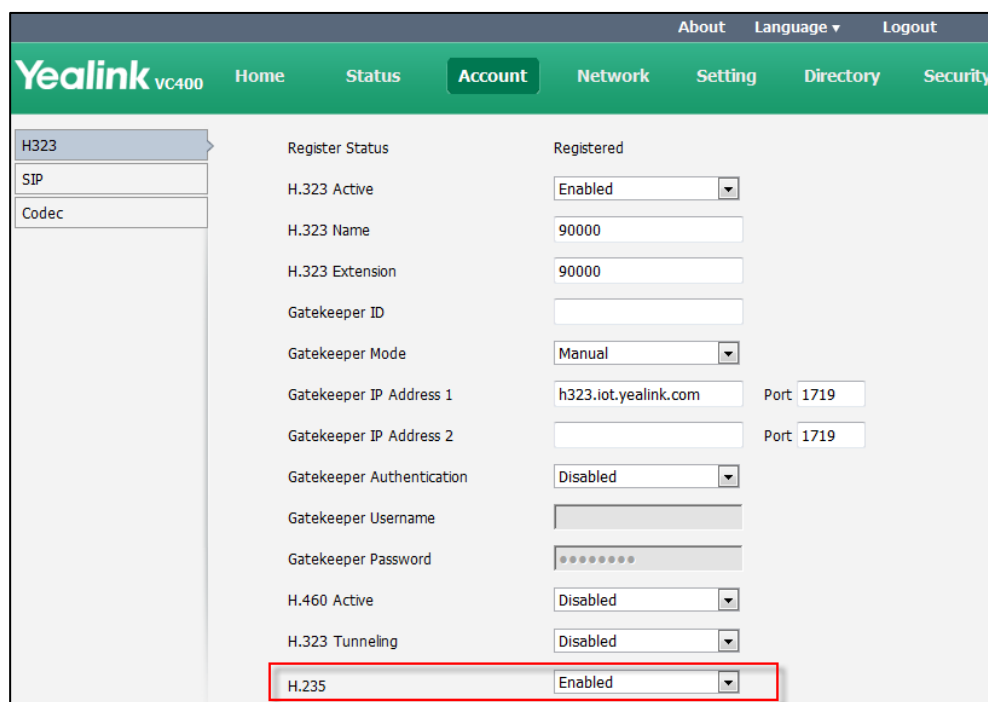
Rules of H.235 for media encryption in H.323 calls:

Far \ Near	Compulsory	Enabled	Disabled
Compulsory	H.235 Call	H.235 Call	Fail to establish call
Enabled	H.235 Call	H.235 Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

When H.235 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.

To configure H.235 via the web user interface:

1. Click on **Account->H323**.
2. Select the desired value from the pull-down list of **H.235**.



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 sidebar, 'H323' is selected. The main content area displays various configuration fields for H323, including 'Register Status' (Registered), 'H.323 Active' (Enabled), 'H.323 Name' (90000), 'H.323 Extension' (90000), 'Gatekeeper ID', 'Gatekeeper Mode' (Manual), 'Gatekeeper IP Address 1' (h323.iot.yealink.com), 'Gatekeeper IP Address 2', 'Gatekeeper Authentication' (Disabled), 'Gatekeeper Username', 'Gatekeeper Password', 'H.460 Active' (Disabled), 'H.323 Tunneling' (Disabled), and 'H.235' (Enabled). The 'H.235' dropdown menu is highlighted with a red box.

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

System Maintenance

This chapter provides basic operating instructions on how to upgrade firmware, import/export configurations and how to .Topics include:

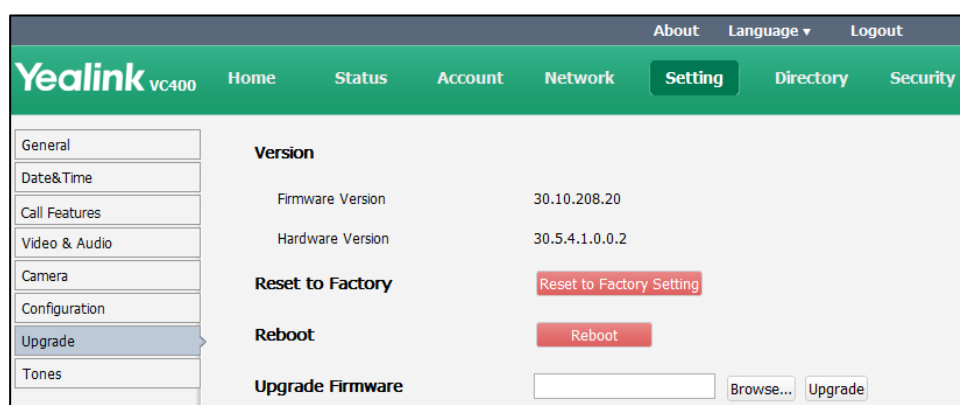
- [Upgrading Firmware](#)
- [Importing/Exporting Configuration](#)
- [Resetting to Factory](#)
- [SNMP](#)

Upgrading Firmware

The newly released firmware version may add new features. Because of this, Yealink recommends you to update the firmware regularly. You can upgrade the system firmware via the 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 system 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 the 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!".

4. 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 the web user interface.

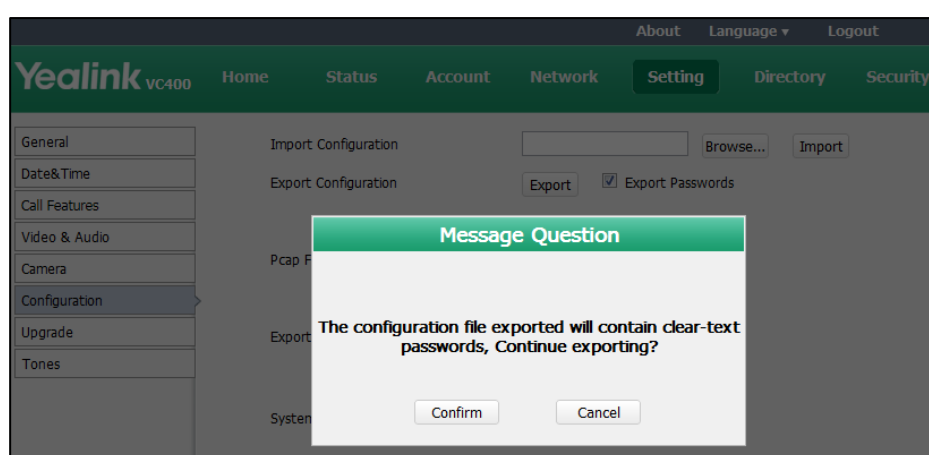
Importing/Exporting Configuration

We may need you to provide the system configurations to the engineer 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 the web user interface:

1. Click on **Setting->Configuration**.
2. Check or uncheck the **Export Passwords** checkbox according to actual demand.
3. Click **Export**.

If you check the **Export Passwords** checkbox, the web user interface is shown below:



4. Click **Confirm** to export the configurations.

To import the phone configurations via the web user interface:

1. Click on **Setting->Configuration**.
2. Click **Browse** to locate a configuration file from your local system.
3. 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. You need to note that all customized settings will be overwritten after reset, such as the registered account, contacts, and call history information. You can export the configuration first, so 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

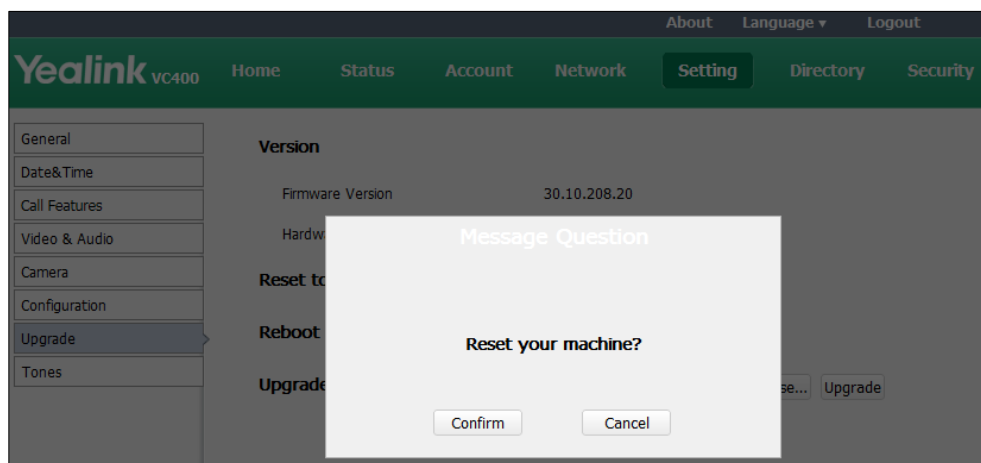
Reset of the system may take a few minutes. Do not power off until the phone starts up successfully.

To reset the system via the web user interface:

To reset your phone via the 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**.

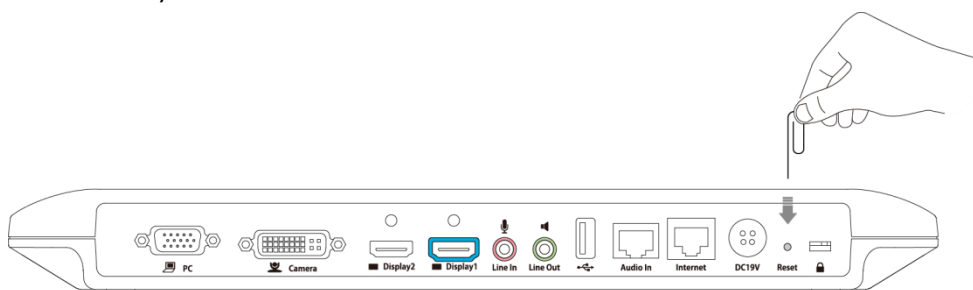
The display device prompts "Reset to Factory?"

3. Select **OK**, and then press **OK**.

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 hold the reset button for 15 seconds to reset the system.



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.

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. 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.
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.	The IP address of the system.

MIB	OID	Description
	9.0	
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 feature on the system. Default: Disabled Note: If you change this parameter, the system will reboot to implement the changes.	Web User Interface
Port	Specifies the SNMP port. Valid Values: 1-65535 Default: 161 Note: If you change this parameter, the system will reboot to implement the changes.	Web User Interface
Tursted 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.	Web User Interface

Parameter	Description	Configuration Method
	If you change this parameter, the system will reboot to implement the changes.	

To configure web server type via the 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 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 (selected), Setting, Directory, and Security. On the left, a sidebar shows configuration categories: LAN Configuration, NAT/Firewall, Advanced (selected), and Diagnose. The main content area is titled 'Network' and contains several configuration blocks: QoS (Audio Priority: 60, Video Priority: 34, Data Priority: 63), MTU (Video MTU: 1500), SNMP (Active: Enabled, Port: 161, Trusted Address: 192.168.10.50 192.168.1.3), Web Server (HTTP: Enabled, HTTP Port: 80, HTTPS: Enabled, HTTPS Port: 443), and 802.1x (802.1x Mode: Disabled, Identity, MD5 Password, and CA Certificates fields). The SNMP section is highlighted with a red rectangular box.

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

If your system encounters certain problems, log files are often needed. 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 9.

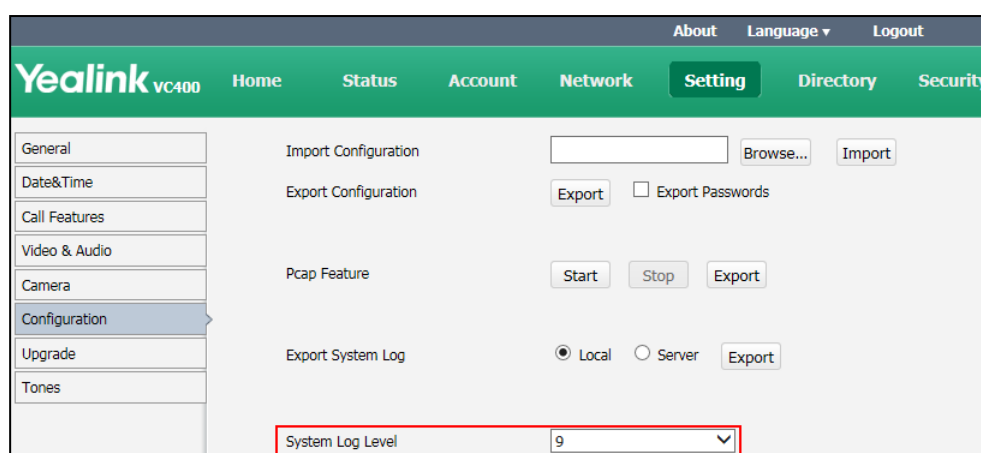
System log level parameters are described below:

Parameter	Description	Configuration Method
Export System Log	<p>Specify where the system log will be exported.</p> <p>Valid values:</p> <ul style="list-style-type: none">• Local-export the system log to the local computer.• Server-export the system log to the specified server.	Web User Interface

Parameter	Description	Configuration Method
	Default: Local	
Server Name	Specify the server address where the log will be exported. Note: It only works if the parameter "Export System Log" is set to Server.	Web User Interface
System Log Level	Specify the system log level. Note: The supported level is 0-9. Higher value indicates more detailed content. Default: 9	Web User Interface

To configure the system log level via the web user interface:

1. Click on **Setting->Configuration**.
2. Select the desired level from the pull-down list of **System Log Level**.



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

To export a log file to the local system via the web user interface:

1. Click on **Setting->Configuration**.
2. Mark the **Local** radio box in the **Export System Log** field.

- 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.exx
509 root      10344 SW  /yealink/bin/sipServer.exx
515 root      16424 SW  /yealink/bin/Screen.exe
517 root      16424 SW  /yealink/bin/Screen.exe
519 root      10344 SW  /yealink/bin/sipServer.exx
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.exx
525 root      SW< [IRQ 45]
526 root      10344 SW  /yealink/bin/sipServer.exx
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 RWN 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 the web user interface:

- Click on **Setting->Configuration**.
- 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 top navigation bar includes 'About', 'Language', and 'Logout'. The main menu has 'Home', 'Status', 'Account', 'Network', 'Setting' (highlighted), 'Directory', and 'Security'. On the left sidebar, 'Configuration' is selected. The main content area shows various configuration options. The 'Export System Log' section is highlighted with a red box, showing the 'Server' radio button selected and the 'Server Name' field containing '10.3.6.103'. Other options include 'Import Configuration', 'Export Configuration', 'Pcap Feature', and 'System Log Level'.

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

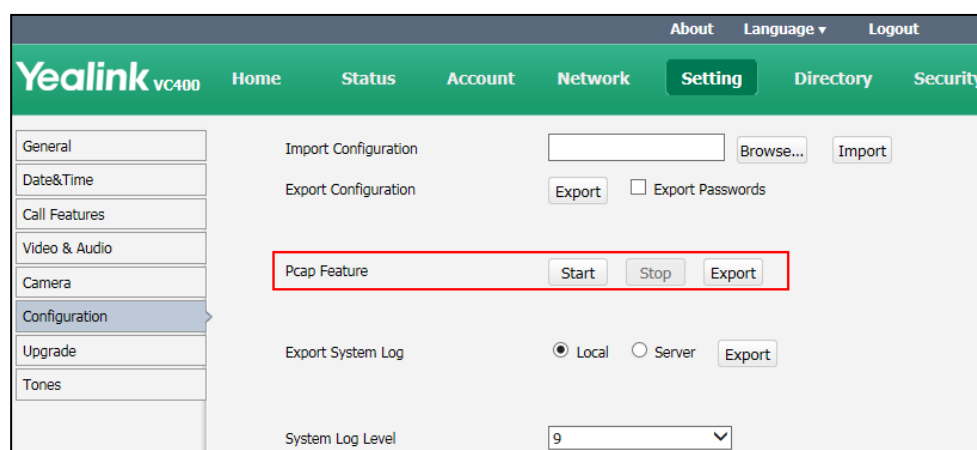
Capturing Packets

The administrator can capture packets in two ways: capturing the packets via the web

user interface or using the Ethernet software. By analyzing the packets captured for troubleshooting purpose.

To capture packets via the web user interface:

1. Click on **Setting->Configuration**.
2. Click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.




To capture packets using the Ethernet software:

Connect the Internet 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 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 about the icons, refer to [Icon Instructions](#) on page 12.

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 about how to export system configuration, refer to [Importing/Exporting Configuration](#) on page 148.

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 network between the near and far sites is connected.
- **Trace Route:** Check every network node between the near and far sites, and the time cost for each node.




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.

Trace Route:

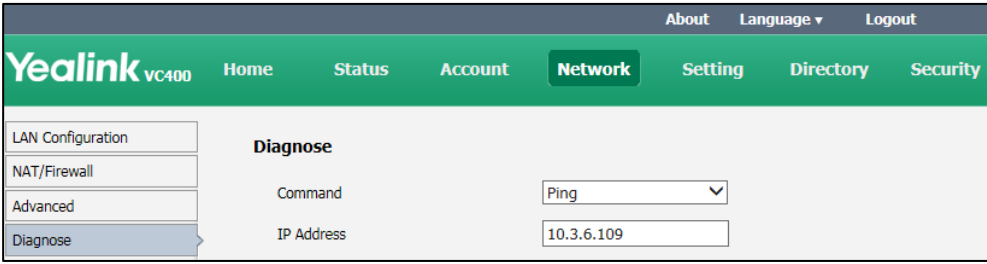
1. Select **Menu->Diagnose** menu.
2. Select **Trace Route**, and then press .
3. Enter IP address (for example, the IP address of the far site).
4. Press **Start**, and then press .

The display device displays the network diagnose information.

5. Press the **Back** soft key to return to the Diagnose menu.

To diagnose network via the web user interface:

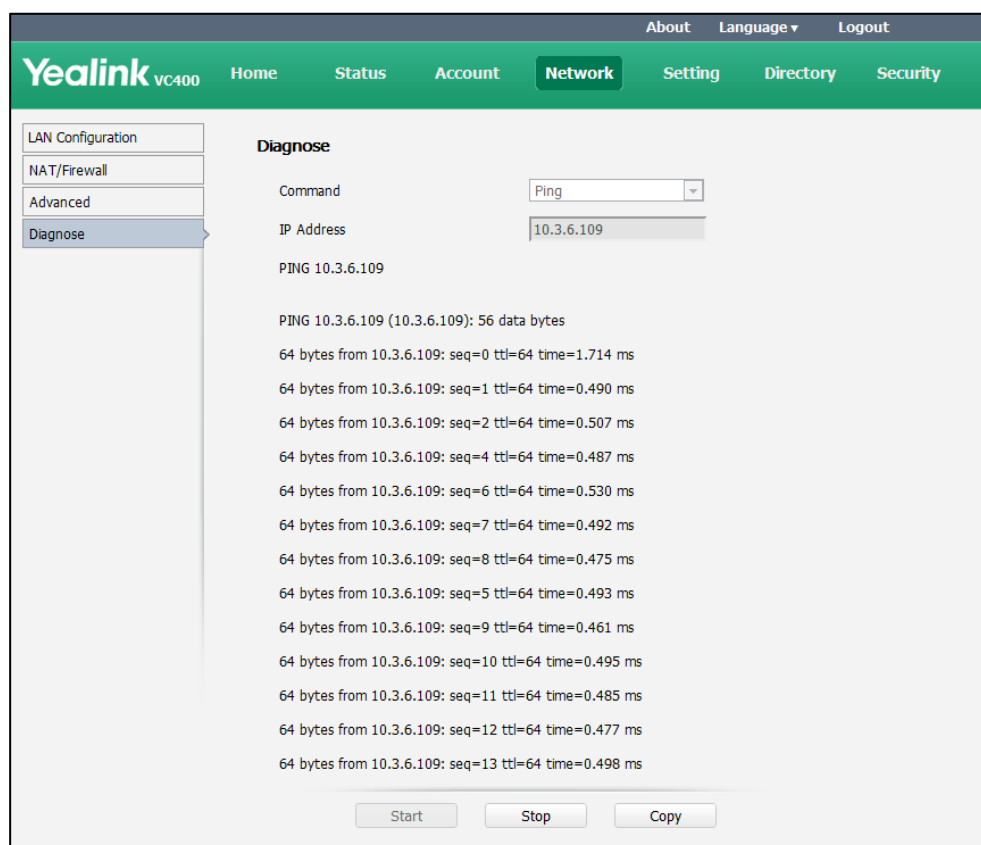
1. Click on **Network ->Diagnose**.
2. Select the desired diagnostic method from the pull-down list of **Command**.
3. Enter IP address in the **IP Address** field.



Yealink VC400		About	Language ▼	Logout
Home	Status	Account	Network	Setting Directory Security
LAN Configuration	Diagnose <div> <div>Command</div> <div>Ping ▼</div> </div> <div> <div>IP Address</div> <div>10.3.6.109</div> </div>			

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.

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 timezone 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 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.
- If the near site is forced to use encryption, ensure that the far site enables encryption too. For more information about call encryption, refer to [Secure Real-Time Transport Protocol](#) on page 141 and [H.235](#) on page 143.
- Ensure the far site supports the same call protocol as the near site.

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 about LAN property configuration, refer to [Configuring LAN Properties](#) on page 30.
- Check whether the system has enabled the hide IP address feature. For more information about disabling the hide IP address feature, refer to [Hide IP Address](#) on page 92.
- Check whether the system has configured firewall and NAT correctly. For more information about, refer to [Configuring the System for Use with a Firewall or NAT](#) on page 52.

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 red 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 I 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 of Near Camera feature. For more information, refer to [Far Control of Near Camera](#) on page 107.
- 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 109.

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information about packet loss, refer to [Viewing Call Statistics](#) on page 157.
- 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 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 start 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 101.


System Maintenance

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 the web user interface, ensure that the web user interface is not refreshed or closed during the upgrade process.

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 diagnosis 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.

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(Windhoek)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+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

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 134.

Index

Numeric

802.1x Authentication [44](#)

A

About This Guide [v](#)

Auto Answer [75](#)

Automatic Sleep Time [91](#)

Audio Input Device [97](#)

Audio Output Device [95](#)

Adjusting MTU of Video Packets [99](#)

Analyzing Configuration Files [157](#)

Administrator Password [130](#)

Appendix A: Time Zones [165](#)

Appendix B: Trusted Certificates [167](#)

B

Backlight of VCP40 Conference Phone [82](#)

Bandwidth [78](#)

C

Configuring H.323 Setting [68](#)

Configuring LAN Properties [30](#)

Configuring Networ [29](#)

Configuring Network Settings Manually [33](#)

Configuring Network Speed and Duplex Mode [35](#)

Configuring the System for Use with a Firewall or NAT [52](#)

Configuring Call Preferences [65](#)

Configuring SIP Settings [65](#)

Codecs [71](#)

Call Type [72](#)

Call Match [76](#)

Configuring System Settings [81](#)

Configuring Camera Settings [103](#)

Camera Control Protocol [109](#)

Call History [124](#)

Configuring Security Features [129](#)

Configuring Packets [155](#)

Camera Issues [161](#)

D

DHCP [30](#)

Do Not Disturb [74](#)

Dual-Stream Protocol [101](#)

Dual Screen [127](#)

F

Far Control of Near Camera [107](#)

G

Getting Information from Status Indicators [156](#)

Getting Started [17](#)

General Issues [159](#)

H

H.323 Tunneling [49](#)

H.460 Firewall Traversal [57](#)

History Record [77](#)

H.235 [143](#)

Hide IP Address [92](#)

I

In This Guide [v](#)

Index [169](#)

Incon on Display Device [12](#)

Incon on VCP40 Video Conferencing Phone [13](#)

Intelligent Firewall Transversal [58](#)

Importing/Exporting Configuration [148](#)

K

Key Tone [94](#)

L

- Language [83](#)
- LED Instructions [14](#)
- LLDP [37](#)
- Local Directory [115](#)
- LDAP [120](#)

M

- Mix Sending [102](#)

N

- NAT [56](#)

P

- Packaging Contents [1](#)
- Powering the System On and Off [22](#)
- Placing a Test Call from the Yealink Video Conferencing System [27](#)
- Preparing the Network [29](#)

Q

- Quality of Service [59](#)

R

- Remote Control [116](#)
- Reserved Ports [53](#)
- Reboot Offtime [93](#)
- Resetting to Factory [148](#)

S

- Search Source List in Dialing [126](#)
- System Component Instructions [5](#)
- System Installation [22](#)
- System Startup [23](#)
- Setup Wizard [23](#)
- Site Name [81](#)
- SNMP [150](#)
- Secure Real-Time Transport Protocol [141](#)
- System Maintenance Issues [163](#)

T

- Table of Contents [vii](#)
- Time and Date [83](#)
- Tones [110](#)
- Transport Layer Security [134](#)
- Troubleshooting [153](#)
- Troubleshooting Methods [153](#)
- Troubleshooting Solutions [157](#)

U

- User Mode [129](#)
- User Interfaces [15](#)
- Upgrading Firmware [147](#)
- Using Diagnostic Methods [157](#)

V

- Video Conferencing System Overview [1](#)
- VC400/VC120 Codec [5](#)
- VCC18HD Camera [7](#)
- VCP40 Video Conferencing Phone [7](#)
- VCR10 Remote Control [10](#)
- VoIP Principles [1](#)
- VLAN [41](#)
- VPN [62](#)
- Volume [98](#)
- Viewing Log Files [153](#)
- Viewing Call Statistics [157](#)
- Video & Audio Issues [162](#)

W

- Web Server Type [132](#)
- Web User Interface [16](#)